NUCLEAR ENGINEERING

MASSACHUSETTS INSTITUTE
OF TECHNOLOGY



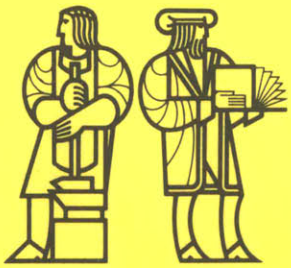
# DYNAMIC EVENT TREES IN ACCIDENT SEQUENCE ANALYSIS

by

N. Siu, C. Acosta, and N. Rasmussen

March, 1990

MITNE–289



Nuclear Engineering Department
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139



# DYNAMIC EVENT TREES IN ACCIDENT SEQUENCE ANALYSIS

by

N. Siu, C. Acosta, and N. Rasmussen
March, 1990

MITNE–289

Prepared for:

Office of Nuclear Regulatory Research
United States Nuclear Regulatory Commission
Washington, D. C. 20555

Project Monitor:

Thomas G. Ryan

Grant Number NRC–04–88–143

## 1. Abstract

This supplementary progress report briefly describes the dynamic event tree approach adopted in this project for analyzing nuclear power plant accident scenarios, and an early application of this approach to a PWR steam generator tube rupture (SGTR) scenario. The report is intended to provide technical information on dynamic event trees not included in the accompanying letter report to NRC [1]; this information is needed to determine the both the promise and the practical limitations of the approach, and to identify methods for overcoming the limitations.

The report defines dynamic event trees, describes the general approach used to apply these to the accident sequence portion of a nuclear power plant probabilistic risk assessment (PRA), and presents some of the details of an initial application to the SGTR scenario. It should be noted that the details described are characteristic of the model as of the end of the current reporting period (2/28/90); work on improving the application to better reflect possible SGTR accident sequences is ongoing.

## 2. Background

A dynamic event tree is an event tree in which branchings (which, in the case of a nuclear plant front–end model, reflect stochastic variability in the process) are allowed to occur at different points in time. Figure 1 shows a simple dynamic event tree for a plant model containing two binary systems (A and B). Three characteristics of interest shown in this figure are: a) all possible combinations of system states must be considered at each branching point, b) branchings are performed at arbitrary, but discrete, points in time, and c) the number of event sequences can quickly grow to an unmanageable size if various approximations designed to limit the problem are not applied. It should be noted that the last point means that the practical application of the approach is a simulation–oriented one. Event sequences are generated by user–supplied rules as the analysis progresses, rather than specified in their entirety as an initial step in the analysis.

The reason for adopting the dynamic event tree approach for use in PRA accident sequence analysis is that this allows explicit treatment of time dependence and process variables, as well as of the plant hardware. This, in turn, allows the modeling of the dynamic interaction between the plant and operators. Refs. 2–5 argue the importance of

such modeling in assessing the likelihood of multiple failures, and, therefore, the risk for a given plant.

The notion of dynamic event trees is not new to this work. The accident progression models used in NUREG–1150 to model plant response following core damage can be viewed as implicit dynamic event trees (although time–dependent branchings are only done for a very small number of accident phases) [6]. Ref. 7 develops a detailed model for the interaction between the operators and the plant in which the passage of time is considered implicitly. More directly, Ref. 8 (and many related papers by the same authors) develops the DYLAM methodology (reviewed in Ref. 4), which represents an application of dynamic event trees to detailed systems analyses. The intended purpose of this work is to develop a practical dynamic event tree methodology that can be used in PRA accident sequence analysis; the differences between this approach and DYLAM lie primarily with the details of implementation.

## 3. Overall Approach

Before discussing the basic modeling approach used in this project, the parameters distinguishing dynamic event tree analyses must be defined. Four characteristic sets define the dynamic event tree approach. These are:

- the set of variables included in the "branching set"[1]
- the set of variables defining the "plant state"[2]
- the set of rules used to determine if branching should occur
- the set of rules used to limit sequence expansion
- the quantification tools

The "branching set" is the set of variables that determine the space of possible branches (i.e., new event tree sequences) at any node in the tree. In the example of Figure 1, branchings are determined by the joint status of Systems A and B; the branching

---

[1]The term "branching set" is may not be conventionally used in the simulation community; we will search for an appropriate term.

[2]The term "plant state" is used instead of the more typical "system state" because of the PRA distinction between "plant" and "system" level analyses.

set can then be written as $\{X_A,X_B\}$, where $X_A$ is the binary indicator variable for the state of System A (e.g., $X_A = 1$ if System A is good and 0 if the system is failed) and $X_B$ is the indicator variable for System B.

The "plant state" defines the current state of the plant relevant to the event tree; it is defined by the values of the variables that influence the probability assignments for the various branchings. In Figure 1, the plant state at any node in the tree is defined by the value of the branching set $\{X_A,X_B\}$ (there are no other variables that may influence probability assignments). In general, the system state may be a function of more variables than those contained in the branching set since a number of characteristic variables may be deterministic functions of the current event sequence, yet may affect the likelihood of subsequent branchings.

The third bullet in the list refers to the set of rules used to determine when a branching should take place. In its simplest form, the branching rule set is a set of branching times (or a constant $\Delta t$) selected prior to the analysis (in Figure 1, it is the set $\{t_1,t_2\}$). The fourth bullet refers to the set of rules used to limit the sequence expansion (not applied in Figure 1). The last bullet refers to the needs of the quantitative portion of the analysis; deterministic state variables (e.g., process variables) as well as branching probabilities must be computed.

Choices regarding these characteristics must be made selectively in a practical analysis. For example, increases in the size of the branching set, the number of different values each $X_i$ can take, or the number of branching points will lead to geometric increases in the number of sequences to be analyzed. If the branching set is $\{X_1,X_2,...,X_k\}$, if each $X_i$ can take on m values, and if there are n branching points, the number of sequences to be analyzed is, without any expansion limiting rules, given by

$$\text{number of sequences} = k^{m^n}$$

To illustrate the size of the problem, if 8 binary systems are being analyzed over 30 time steps ($k = 8$, $m = 2$, $n = 30$), this leads to roughly $10^{54}$ sequences. Note that on current supercomputers, a single floating point operation (e.g., an addition of two real numbers) performed for all of these sequences will require on the order of $10^{45}$ seconds (much longer than the age of the universe)!

For the above reasons, it is expected that a dynamic event tree model will not be able to reach the level of detailed hardware analysis employed in conventional, static event tree analyses (where n = 1). Certain modeling trade–offs must be made in order to include time–dependent behavior. The following choices characterize the modeling approach used in this project, and reflect these modeling trade–offs.

1) Branching Set:
In this project, the branching set consists of variables characterizing the status of the plant hardware systems, i.e., the "hardware state," and variables characterizing the "operator crew state." The treatment of plant systems as single entities is intended to limit the value of k. The actual list of systems treated in the case study is provided in the next section. As of the end of the reporting period, the definition of "operator crew state" was somewhat preliminary. An initial attempt, focusing on the operating procedures, is briefly mentioned in Section 5[3].

2) Plant State:
The plant state is formed by combining the branching set with the set of process variables (including time derivatives) that define the current physical state of the plant. It is assumed that, with reasonable accuracy, the process variables can be computed deterministically for a given event sequence, and therefore need not be used to determine possible branchings. However, as argued in Refs. 2–5, they do affect the likelihood of the different branchings.

3) Branching Rules:
In principle, hardware systems can fail on demand or while running. In practice, the latter failure mode is quite unlikely during the course of an accident. A basic branching rule employed in this analysis is that system failures can only occur when: a) the system is demanded, or b) when the operators act to fail the system. This

---

[3]Currently, it is believed that the operator crew state is defined by three substates: the crew's cognitive state (i.e., their belief concerning the current condition of the plant), the crew's action state (i.e., the set of actions they are supposed to perform), and the crew's emotional state. More precise definitions of these substates are being developed. The hardware state is defined by three substates: the state of the frontline systems, the state of the support systems, and the state of the instrumentation.

assumption leads to significant reductions in the number of event sequences to be analyzed.

4) Expansion Limiting Rules:

Even with the above restrictions on the branching set and on the branching rules, a practical application of the dynamic event tree approach is likely to require rules for:
a) removing sequences that are unlikely to lead to the undesired state, and
b) grouping sequences that are judged to be similar. No work has been done in this area yet. However, it is anticipated that future efforts will be directed at defining and applying two quantitative functions.

The first proposed function, tentatively titled the "potential function," is used to represent the "potential" that a given sequence has for leading to the undesired state (e.g., core damage). The potential function will be developed dynamically for each sequence; it will include both the probability of being in the current sequence (as defined by the plant state and the current time) and the conditional probability (estimated in some fashion) that the sequence will lead to the undesired state. Sequences with high potential will continue to undergo expansion in the dynamic event tree; sequences with low potential will be truncated. The user will have control over the degree of approximation by adjusting the threshold for acceptance.

The second proposed function, tentatively titled the "similarity function," is used to measure the degree of similarity between sequences, and determine if different sequences should be grouped. Unlike the case of the potential function (which we believe to be a workable concept), it is not clear if a meaningful similarity function can be developed. This question will be considered later.

5) Quantitative Tools:

Special attention needs to be paid to the physical model used to update plant process variables. Two issues are of special importance. First, the model must be very simple, since computations are performed for each sequence developed. Second, the model must be able to function in a dynamic event tree setting, i.e., it must be able to input some summary representation of the plant state at a given point in time, and update the plant state over the next $\Delta t$. The physical model used in this project is briefly described in Section 4. Comparisons with a more sophisticated code indicate that the accuracy of the model should be adequate for our purposes.

## 4. Application to Steam Generator Tube Rupture

The preceding discussion provides the basic framework for our application of dynamic event trees to accident sequence analysis. The specific elements developed to implement this approach in an analysis of a steam generator tube rupture (SGTR) scenario are described in this section.

The SGTR scenario was chosen for the case study for a number of reasons. First, it can involve considerable interaction between the operators and the plant, and therefore is a natural situation for applying a dynamic analysis tool. Second, it has some degree of safety significance since it can lead to a direct release of radioactivity to the atmosphere. Finally, a reasonable amount of information on the scenario is available to the study team. The information includes reports of actual events (e.g., [9–11]), observations of simulator training exercises, a fast PC–based PWR simulation model that treats SGTR [12], relevant emergency operating procedures [13–16], and PRA analyses of SGTR (e.g., [17,18]).

### 4.1 Model Elements

The dynamic event tree analysis approach, being simulation oriented, is implemented quite naturally via computer code. Figure 2 is a flow chart indicating the elements of such a computer code. As can be seen in this figure, the code will eventually include the following elements.

1. A routine that defines possible branchings at any given node due to variations in hardware state (e.g., system successes or failures on demand).
2. A routine incorporating the physical model used to simulate the dynamic behavior of process variables during an accident.
3. A logical pruning routine that eliminates plant states that are impossible, according to the branching rules. This routine, for example, will remove branchings associated with the failure of a backup system if the physical model routine does not indicate a demand for the system and if the operators do not try to start the system.
4. A routine for modeling the operating crew. The operator model must be able to take, as input, the current plant status (defined in terms of hardware, process variables, and operator state), and provide, as output, possible operator actions, possible changes in operator state, and the likelihood of these different

actions and states.

5. A routine for calculating the likelihood of each event tree sequence.
6. A routine for computing the "potential function" (proposed in Section 3), and for using this function to remove unimportant sequences.
7. A routine for grouping event sequences whose projected future paths are similar (using the "similarity function" proposed in Section 3). Like the potential function routine, this aims to reduce the combinatorial explosion problem inherent with the dynamic event tree approach.

The solid borders in Figure 2 reflect essentially complete portions of the code (as of 2/28/90). Shaded borders are used for work in progress, and the dashed line borders represent work yet to be started.

## 4.2 SGTR – General Progression

This subsection briefly describes the general characteristics of a nominal SGTR accident (where all systems work as intended), and some of the options available to operators if some of the systems are failed. Additional details can be found in Ref. 12. Risk assessment analyses of SGTR (e.g., [17,18]) are also useful, since they provide additional information on scenarios that deviate from the nominal accident progression.

A steam generator tube rupture accident breaks the barrier between the reactor coolant and the secondary side of the steam generator. The difference in pressure between the primary system and the steam generators causes the reactor coolant to flow from the primary into the secondary side of the faulted steam generator. As a result of this loss of primary coolant, the pressurizer pressure and pressurizer level drop (the rate of decrease depends on the size and the number of ruptures). The decrease in primary pressure will eventually result in a reactor trip.

The leakage of the contaminated primary coolant increases the activity of the secondary side, causing radiation monitors to actuate. The leakage also increases the level and pressure of the faulted steam generator, depending on the size of the rupture. Moreover, the leakage leads to a reduction in feedwater flow, in order to compensate for the high steam generator level in the faulted steam generator.

The reactor trip causes the core power to rapidly decrease to decay heat levels, the steam flow to the turbine to terminate and the steam dump (i.e., the turbine bypass) system to actuate. Soon afterwards, the continued decrease in primary pressure leads to actuation of the safety injection (SI) signal; this signal causes isolation of the main feedwater (MFW) system and initiates the high pressure injection (HPI) system and the auxiliary feedwater (AFW) system.

Following the reactor trip, the operator's concerns are to: a) establish a secondary heat sink, b) identify and isolate the faulted steam generator, c) cooldown and depressurize the primary system, and d) provide for long term cooling. Refs. 13–16 describe specific items that must be accomplished to address these concerns.

The auxiliary feedwater (AFW) system provides the cooling water supply to the steam generators for heat removal from the primary system under nominal conditions. If the AFW system fails, the operator can provide water to the steam generators through the condensate system; however, this requires depressurization of at least one steam generator. If water cannot be provided to the steam generators (so that the steam generators are not available), "bleed and feed" cooling can be performed. Bleed and feed cooling involves the letdown of primary coolant through the pressurizer power–operated relief valve (PORV), and the injection of water into the reactor coolant system using the high pressure injection (HPI) system. Failure to establish a heat sink by one of these mechanisms will result in core damage.

The identification and isolation of the faulted steam generator is essential to control the release of radioactive coolant outside of the containment building. The faulted steam generator can be identified by an unexpected rise in the steam generator level (specifically, a rise in the narrow range level), high radiation measurements for the steam line, or high radiation measurements from steam generator samples. Once identified, isolation of the faulted steam generator requires closing of the steam generator relief valves, blowdown isolation valves, upstream drain valves and main steamline isolation and bypass valves.

After isolating the faulted steam generator, the operators must initiate cooldown and depressurization of the primary system. The primary objective of this task is to equalize the primary system and faulted steam generator pressures and thus reduce the leakage from the primary side to the secondary side. The cooldown ensures that the primary coolant does not reach saturation during depressurization. The turbine bypass valves are used in

the cooldown. If these are not available, the steam generator atmospheric dump valves can be used. Depressurization involves the use of the primary pressurizer spray, auxiliary pressurizer spray, or pressurizer PORV. Once the pressures are equalized, high pressure injection must be terminated to prevent the primary pressure from increasing.

Once the previous tasks are accomplished, long term cooling to cold shutdown is necessary to allow repair of the broken tube(s). This can be accomplished using a wide variety of options. At the present, it is envisioned that, in order to limit the scope of the project, this portion of the SGTR accident will not be treated.

### 4.3 Thermal Hydraulic Model

As discussed earlier, the physical model used to compute current levels of process variables is an important part of a dynamic event tree model. This subsection summarizes a simple model developed to simulate plant behavior during a PWR transient. The model, which is partially based on similar models described in Refs. 19 and 20, is somewhat specialized towards the analysis of SGTR in a Westinghouse 4–loop PWR, but can be modified relatively simply to handle other relatively slowly progressing accidents in other PWRS.

In the model, the plant is divided into a set of nodes: the primary node, the pressurizer, the faulted steam generator, and the intact steam generators (see Figure 3). Within each node, the thermodynamic properties of the water (e.g., temperature and pressure) are assumed to be constant. The model is designed to determine the thermodynamic properties of each node.

The primary node includes the reactor vessel and the reactor coolant system piping. It is assumed to always contain subcooled liquid; saturation is considered to be an absorbing state for the purposes of sequence development. The pressure in the primary node is assumed to equal the pressure in the pressurizer node; the temperature in the primary node is determined using an energy balance equation, where energy gains are from an internal source (the core) and energy losses are to the steam generator node. The temperature calculation accounts for the heat capacity of fuel cladding and structural material. Once the pressure and temperature are known, other thermodynamic properties can be determined. For example, the fixed volume of the of the primary node and the specific volume of the water (which is a function of temperature and pressure) are used to

compute the total coolant mass in the primary node. Note that mass can leave the primary node by outsurge to the pressurizer, by leakage through the ruptured tube, or by leakage through the PORV (if open). Mass can enter by insurge from the pressurizer or by injection from HPI (if on).

The pressurizer node is treated in a manner similar to that of Ref. 20. It is assumed that the both the liquid and the vapor in the pressurizer are maintained at saturation conditions. Mass and energy balances are used to determine the pressurizer pressure and the vapor volume fraction. The mass balance includes the net surge flow rate from the primary node (e.g., when the coolant expands or contracts), the pressurizer spray rate, and the rate of mass loss through the PORV.

The steam generator nodes model the secondary side coolant; the primary side coolant in the steam generator tubes is included in the primary node. These nodes are assumed to be at saturation at all times. Any heat added to the nodes is used to convert liquid to steam which, in turn, goes to either the turbine or the condenser. Nominally, the rate of steam production equals the rate of feedwater flow into the steam generator plus the rate of inflow through the ruptured tube. After reactor trip, the steam generated is limited by the capacity of the steam dump. If the heat added can generate more steam than the steam dump capacity, the surplus heat raises the steam generator coolant temperature and the pressure adjusts accordingly (using the saturation curve). On the other hand, if the enthalpy of the feedwater is less than that of the steam generator liquid, the temperature (and pressure) of the coolant drops to compensate for cold water inflow.

Two steam generator nodes are included in the model. The intact steam generator node has three times as much capacity as the faulted steam generator node.

The predictions of this model have been compared (for a limited number of initial conditions) against those of PRISM, a more sophisticated PC–based simulation code which has many of the physical models and control algorithms built into the Seabrook plant simulator [12]. The comparisons indicate that, for the cases considered, the simple four node model's qualitative predictions match those of PRISM, and the quantitative error is reasonably small. For example, the predicted time to trip following tube rupture differs by only 15 seconds from the time predicted by PRISM. For the purposes of this project, it appears that the simple model is sufficiently accurate.

As discussed in Section 3, a second important requirement for the physical model used in this project, in addition to the requirement for a fast running code, is that the model be able to function in a dynamic event tree setting. This means that the model must be able to characterize the current plant physical state with a limited number of process variables, since a different set of values must be stored for each node in the event tree.

The process variables currently used to characterize the plant physical state are listed in Table 1. Note that, in addition to the process variables, the time derivatives of the process variables are included as well. Note also, that if the assumptions underlying the physical model are relaxed (e.g., the assumption that the steam generator always operates at saturation conditions), the list will grow in length.

### 4.4 Initial Application – Assumptions and Results

An initial dynamic event tree for the SGTR initiating event is shown in Figure 4. This tree identifies the systems failed at any given point in time. Table 2 provides the values of some key process variables at t = 450 seconds. Other plant process variables were computed in the simulation, but are not shown. Sequence likelihoods were not computed; all possible branchings were performed.

The assumptions underlying Figure 4 are as follows.

1. The hardware systems (or groups of systems) included in the analysis are: the condensate system (CS) which is assumed to include the 40% dump valves that bypass the turbine, the safety injection signal (SI), the high pressure injection system (HPI) which is assumed to include both centrifugal charging pumps and safety injection pumps, the main feedwater system (MFW), the auxiliary feedwater system (AFW), the startup feed pump (SUFP), the steam generator relief valves (SRV) which are assumed to include the 10% atmospheric dump valves and the the safety relief valves, the pressurizer spray system (SS), the pressurizer pilot operated relief valve (PORV), and the main steam isolation valves (MSIV). The reason for including these systems is that these systems significantly affect the behavior of the plant during the early part of the steam generator tube rupture event (starting from the initiation of the steam generator tube rupture and culminating when cooldown and depressurization of the primary system commences).

Table 3 lists the systems modeled explicitly, and their impacts on the sequence. Systems not on this list are assumed to function as designed. For example, it is assumed that reactor trip and turbine trip both occur on demand.

2. Branchings can occur only when a plant system is demanded. For example, at t = 60 seconds, the code determines if $P_p$, the primary node pressure, falls below the safety injection setpoint (1875 psi). If so, the HPI system is demanded (and can therefore fail) at that time. Branchings due to operator actions are not included in this tree. (In other words, the branching set consists of the indicator variables for the systems shown in the figure.)
3. Plant process variables are updated every second (for every event sequence). The parameters used in the physical model are representative of Seabrook Unit 1 (a 1150 MWe Westinghouse PWR). It is assumed that a single tube ruptures at t = 20 seconds (prior to that, plant status is nominal). The break area used is 1.584 $in^2$.
4. Repairs of failed systems are not recoverable.

Although operator actions are not included in the figure, a number of interesting points can be made. First, as expected, sequences with identical hardware states can be associated with different process variable values. Sequences 14 and 29 in Table 2 show a 35 psi difference in primary pressure, for example, although these sequences have only had some 215 seconds to deviate. As argued in Refs. 2–5, this is potentially important in determining the likelihood of operator error. Second, the tree illustrates the exact order of system failures for a given sequence. This too can have an impact on the likelihood of operator error. Third, the tree shows that a dynamic analysis does not necessarily imply an enormously large number of sequences requiring analysis; reasonable assumptions (such as ignoring the runtime failure of systems) can trim the problem without adding a significant degree of error. Fourth, such a model can be used to determine the distribution for the time to demand of various systems – this can be very useful input to conventional PRAs (which often rely upon nominal scenario analyses and judgment to determine time windows for operator actions). Fifth, the analysis, when carried out to an appropriate end state (e.g., primary node saturation) can even be directly useful in situations where it is assumed that the operators allow the accident to run its course. While not particularly realistic for current plants, this may actually be a reasonable approach for the more highly automated plants being proposed.

## 5. Operator Modeling – Early Steps

The application described in Section 4 does not include tree branchings due to operator actions. Such branchings can add much greater complexity to the analysis. First, system failures could then occur at arbitrary points in time, rather than when the systems are actuated by automatic signals (which respond to the current levels of process variables). Second, operators may repair failed systems (also at arbitrary points in time).

As discussed in Section 3, it is recognized that the dynamic event tree model needs to perform branching for the "operator state," as well as for the plant hardware state. An interesting initial exercise is to model the operators as procedure followers with highly limited error modes. Figure 5 presents an indication of the results of such an exercise. It should be emphasiszed that this figure is highly preliminary; its purpose is to show how the dynamic event tree can qualitatively change with inclusion of operators. The figure is generated using the following assumptions:

- Operators follow the emergency operating procedures as closely as possible (i.e., they do not skip or rush through steps, or slow down at any particular step).
- The length of time required to execute steps in the procedures can be deterministically specified before starting the analysis.
- The only time operators can make errors is when the procedure reaches a branching point (e.g., depending upon the value of a process variable, one procedure may direct the operator to start a new procedure).

Figure 5 shows the operator branchings following a demand and loss of AFW at $t = 240$ seconds. The labels above the branches are acronyms for the procedures being followed; the tree, therefore, shows a spectrum of possible activities, and when transitions to different procedures might be expected (given the above assumptions). In particular, it shows when feed and bleed cooling might be required, and under what circumstances it might be required. It should be pointed out that the number of branchings is still quite manageable.

Of course, some of the above assumptions need modification. For example, the long delays shown in Figure 5 often correspond to operator recovery actions; since repair is not allowed in the model, the operators continue to attempt recovery until a new branch point in the procedure is reached. Branches away from the procedure, when it is judged that

recovery is unlikely, needs to be treated. More generally, the branching does not account for the operators' understanding of the state of the plant (which can differ from their understanding of the actions to be performed), or for their emotional state. Work is being done to develop a more careful definition of "operator state" useful for the dynamic event tree analysis. This includes an investigation of currently available operator models (e.g., MAPPS [21]) and increased interaction with the companion M.I.T. project on operator crew modeling [5].

## 6. References


1. N. Siu, "Physical Dependencies in Accident Sequence Analysis," Second Progress Report, Grant NRC–04–88–143, Department of Nuclear Engineering, M.I.T., March 1990.

2. N. Siu and N. Rasmussen, "Physical Dependencies in Accident Sequence Analysis," Research Proposal for Grant NRC–04–88–143, Department of Nuclear Engineering, M.I.T., January 1988.

3. N. Siu, "Dynamic Accident Sequence Analysis in PRA: A Comment on 'Human Reliability Analysis – Where Shouldst Thou Turn?'," accepted for publication, *Reliability Engineering and System Safety*, 1990.

4. N. Siu, "Physical Dependencies in Accident Sequence Analysis," First Progress Report, Grant NRC–04–88–143, Department of Nuclear Engineering, M.I.T., October 1989.

5. N. Siu and D. Lanning, "A Systems Model for Dynamic Human Error During Accident Sequences," Research Proposal for Grant NRC–04–89–356, Department of Nuclear Engineering, M.I.T., July 1989.

6. United States Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," Second Draft, NUREG–1150, June 1989.

7. C.J. Hsu, R. Youngblood, R. Fitzpatrick, and P. Amico, "Technical Evaluation Report: Assessment of the Risk Significance of 'Category C' Events in B&W Plants," Draft Report, Brookhaven National Laboratory, August 1987.

8. A. Amendola, "Accident Sequence Dynamic Simulation Versus Event Trees," *Reliability Engineering and System Safety, 22*, 3–25(1988).

9. P. Hinsberg, "NRC Staffers Say Abandonment of Procedures Made Ginna Matters Worse," *Inside NRC, 4*, No. 3, 1–2(February 8, 1982).

10. "NRC Compares the Ginna Actions with Basic Westinghouse Guidance," *Inside NRC, 4*, No. 3, 2–4(February 8, 1982).

11. J.P. Adams and M.B. Sattison, "Frequency and Consequences Associated with an SGTR Event," *Transactions of the American Nuclear Society, 60*, 390–391(1989).

12. S. Kao, "PRISM User's Manual, Revision 2.0," January 1990.

13. Westinghouse Electric Corporation, "Westinghouse Owners Group Emergency Response Guidelines: Background Volume E–3, ECA–3 (High Pressure Version)", (September 1, 1983).

14. "E–0: Reactor Trip or Safety Injection," Seabrook Station Emergency Procedure, Revision 6, December 2, 1988.

15. "E–3: Steam Generator Tube Rupture," Seabrook Station Emergency Procedure, Revision 6, December 2, 1988.

16. "FR–H.1: Response to Loss of Secondary Heat Sink," Seabrook Station Emergency Procedure, Revision 8, November 11, 1989.

17. Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG–0300, December 1983.

18. Nuclear Safety Analysis Center, Electric Power Research Institute, Duke Power Company, "Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3," NSAC–60, June 1984.

19. T. L. Chu and G. Apostolakis, "Assessment of Uncertainties Associated with the Core Uncovery Time in TMI–Type Accidents," *Reliability Engineering, 8*, 23–56(1984).

20. S. Nguyen, "Incorporating Physical Dependencies into Accident Sequence Analysis," S.M. Thesis, Department of Nuclear Engineering, M.I.T., May 1989.

21. A.I. Siegel, W.D. Bartter, J.J. Wolf, H.E. Knee, and P.M. Haas, "Maintenance Personnel Performance Simulation (MAPPS) Model: Summary Description," NUREG/CR–3626, Vol. 2, ORNL/TM–904/V2, May 1984.

Table 1 – Process Variables Carried In Dynamic Event Tree Model for SGTR

| Variable | Definition |
|---|---|
| $P_p, \frac{dP_p}{dt}$ | Primary node pressure and derivative |
| $T_p, \frac{dT_p}{dt}$ | Primary node temperature and derivative |
| $M_p, \frac{dM_p}{dt}$ | Primary node mass and derivative |
| $M_{pzr}$ | Pressurizer mass |
| $\alpha, \frac{d\alpha}{dt}$ | Pressurizer vapor volume fraction and derivative |
| $M_{sg1}, \frac{dM_{sg1}}{dt}$ | Faulted steam generator mass and derivative |
| $P_{sg1}$ | Faulted steam generator pressure |
| $T_{sg1}, \frac{dT_{sg1}}{dt}$ | Faulted steam generator temperature and derivative |
| $M_{sg2}, \frac{dM_{sg2}}{dt}$ | Intact steam generators mass and derivative |
| $P_{sg2}$ | Intact steam generators pressure |
| $T_{sg2}, \frac{dT_{sg2}}{dt}$ | Intact steam generators temperature and derivative |

Table 2 – Process Variables Associated with Plant States
Dynamic Event Tree Example (t = 450 sec)

| Sequence | Primary Pressure[1] | Primary Temperature[2] | Faulted SG Temperature[2] | Intact SG Temperature[2] |
|---|---|---|---|---|
| 1 | 1819.7 | 555.8 | 563.4 | 571.1 |
| 2 | 1819.2 | 555.8 | 560.8 | 571.1 |
| 3 | 1817.9 | 555.8 | 547.8 | 571.1 |
| 4 | 1821.2 | 555.8 | 567.3 | 571.1 |
| 5 | 1817.4 | 555.8 | 557.3 | 563.3 |
| 6 | 1819.7 | 555.8 | 563.4 | 571.1 |
| 7 | 1810.3 | 555.7 | 563.4 | 571.1 |
| 8 | 1809.8 | 555.9 | 560.9 | 571.1 |
| 9 | 1808.5 | 555.9 | 547.9 | 571.1 |
| 10 | 1811.9 | 555.9 | 567.5 | 571.1 |
| 11 | 1808.0 | 555.9 | 557.3 | 563.2 |
| 12 | 1810.3 | 555.9 | 563.4 | 571.1 |
| 13 | 1844.8 | 555.8 | 562.8 | 653.5 |
| 14 | 1844.8 | 555.8 | 560.2 | 653.5 |
| 15 | 1844.8 | 555.8 | 562.9 | 653.5 |
| 16 | 1844.8 | 555.8 | 560.0 | 653.5 |
| 17 | 1845.1 | 555.8 | 562.0 | 653.5 |
| 18 | 1845.1 | 555.8 | 562.0 | 653.5 |
| 19 | 1845.1 | 555.8 | 562.0 | 653.5 |
| 20 | 1845.1 | 555.8 | 562.0 | 653.5 |
| 21 | 1840.2 | 555.9 | 562.9 | 653.7 |
| 22 | 1840.1 | 555.9 | 560.4 | 653.7 |
| 23 | 1840.1 | 555.9 | 563.0 | 653.7 |
| 24 | 1840.1 | 555.9 | 560.1 | 653.7 |
| 25 | 1840.5 | 555.9 | 562.2 | 653.7 |
| 26 | 1840.5 | 555.9 | 562.2 | 653.7 |
| 27 | 1840.5 | 555.9 | 562.3 | 653.7 |
| 28 | 1840.5 | 555.9 | 562.3 | 653.7 |
| 29 | 1880.4 | 555.8 | 612.7 | 653.3 |

[1]Pressure is given in psig
[2]Temperature is given in degrees Farenheit

Table 3 – Systems Included in Dynamic Event Tree Model for SGTR
(Page 1 of 2)

| System | Notes |
|---|---|
| High Pressure Injection (HPI) | Provides primary coolant from the Reactor Water Storage Tank (RWST) upon actuation of safety injection signal. If auxiliary feedwater system fails, HPI is needed for bleed and feed cooling. Includes centrifugal charging pumps, safety injection pumps, and RWST. |
| Pressurizer Power–Operated Relief Valve (PORV) | Used to relieve primary pressure; opens when setpoint value is reached. Used to depressurize system when pressurizer spray system fails or during bleed and feed cooling. |
| Safety Injection Signal (S–signal) | Actuation of this signal creates a demand for other systems (see below). Signal actuates when pressurizer pressure drops below 1875 psi. |
| Main Feedwater (MFW) | Provides water to the steam generators which remove heat from the primary side and produce steam during normal operation. Water comes from the condenser hot well. Automatically isolates when S–signal, high–high steam generator level signal, or low $T_{avg}$ signal occurs. |
| Auxiliary Feedwater (AFW) | Provides water to the steam generator when MFW is isolated or off. Automatically starts on S–signal. Includes the condensate storage tank (CST) from where water is obtained. |
| Start–Up Feed Pump (SUFP) | Serves as a back up to the MFW and the AFW pumps. Automatically starts when both MFW pumps trip with no S–signal or high–high steam generator level signal or loss of offsite power. In case of S–signal and the failure of AFW, SUFP can provide water to the steam generator. Takes suction from the CST. Ref. 16 treats SUFP as part of the AFW. It is treated separately here since it is a backup for AFW. |
| Pressurizer Spray (SPRY) | Includes both the pressurizer normal and the auxiliary sprays. Actuates when the pressurizer pressure reaches its set point or when the operator decides to reduce primary pressure. |
| Condenser and Condensate System (CONDSR) | Removes heat from secondary coolant. Assumed to include turbine bypass valves (40% dump). Turbine bypass actuates following reactor trip. |

Table 3 – Systems Included in Dynamic Event Tree Model for SGTR
(Page 2 of 2)

| System | Notes |
|---|---|
| Steam Generator Safety Relief Valves (SRV) | Includes steam generator PORVs (10% atmospheric steam dump) and safety relief valves. Serves to relieve the steam generator pressure. The PORVs dump steam when the turbine bypass (40% condenser dump) is not available. |
| Main Steam Isolation Valves (MSIV) | Includes main steam isolation valves and check valves. Controls the flow of steam from the steam generator to the turbine and the condenser. Isolation of the ruptured steam generator (to prevent any release of radioactive coolant outside of the containment) includes closing of the MSIV of that loop. |

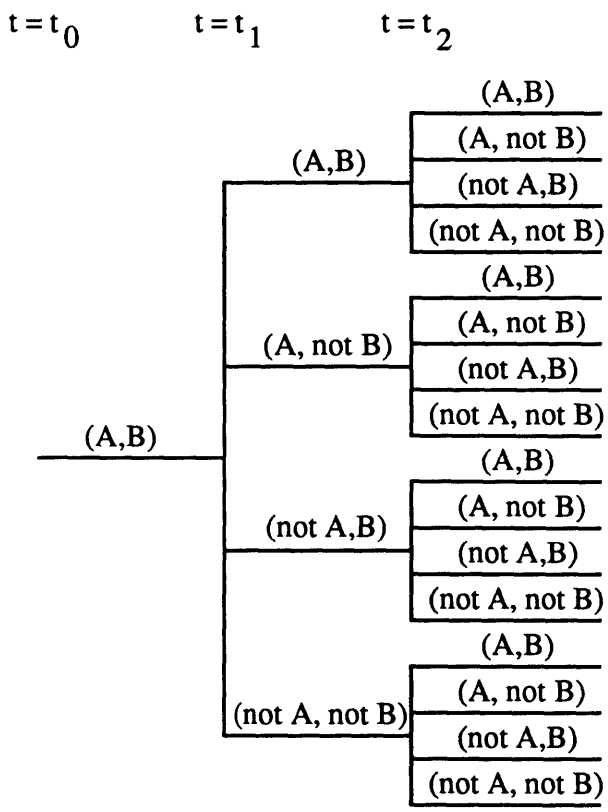



Figure 1 - Example Dynamic Event Tree for Two Binary Systems (Two Time Steps)

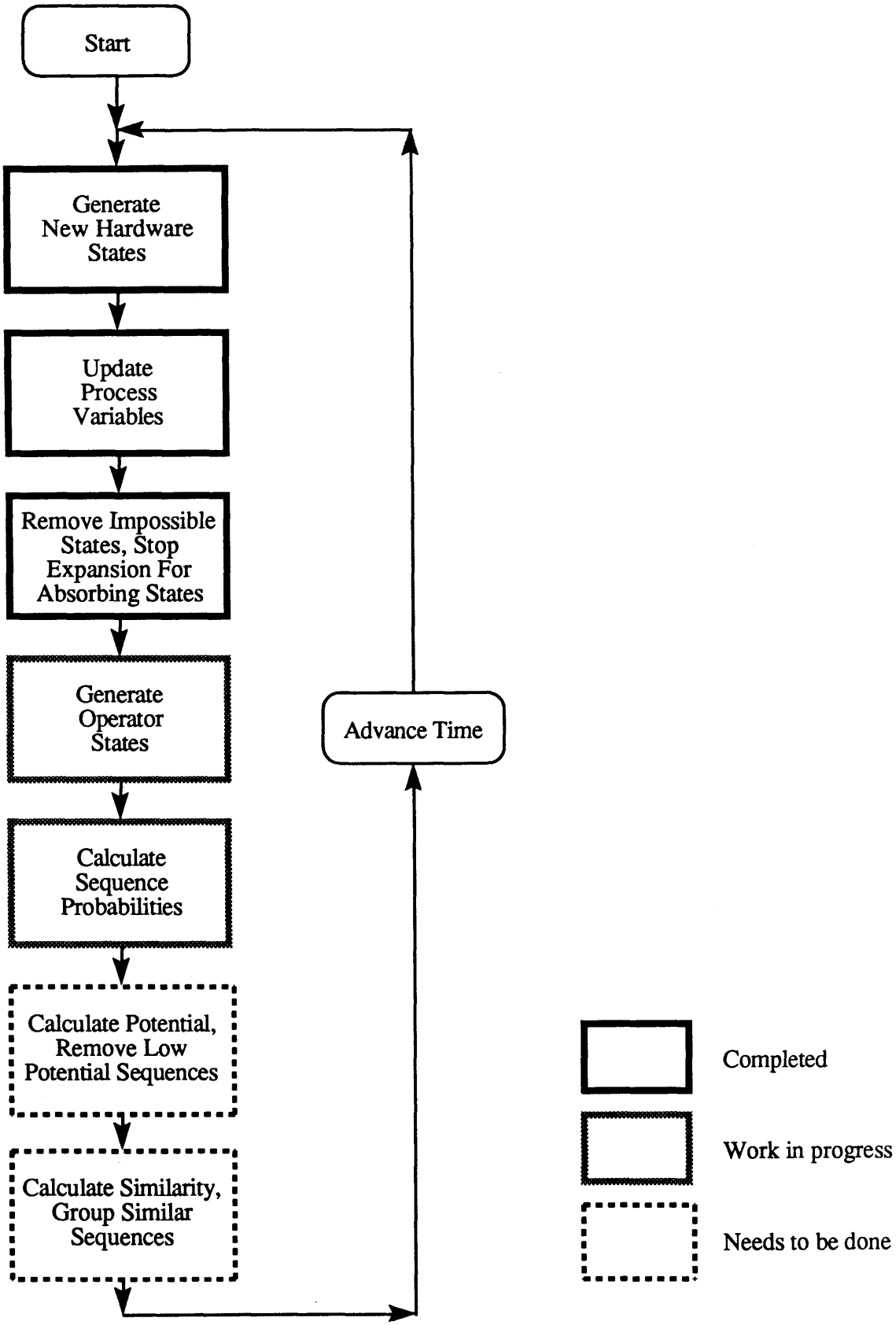



Figure 2 - Schematic for Dynamic Event Tree Model

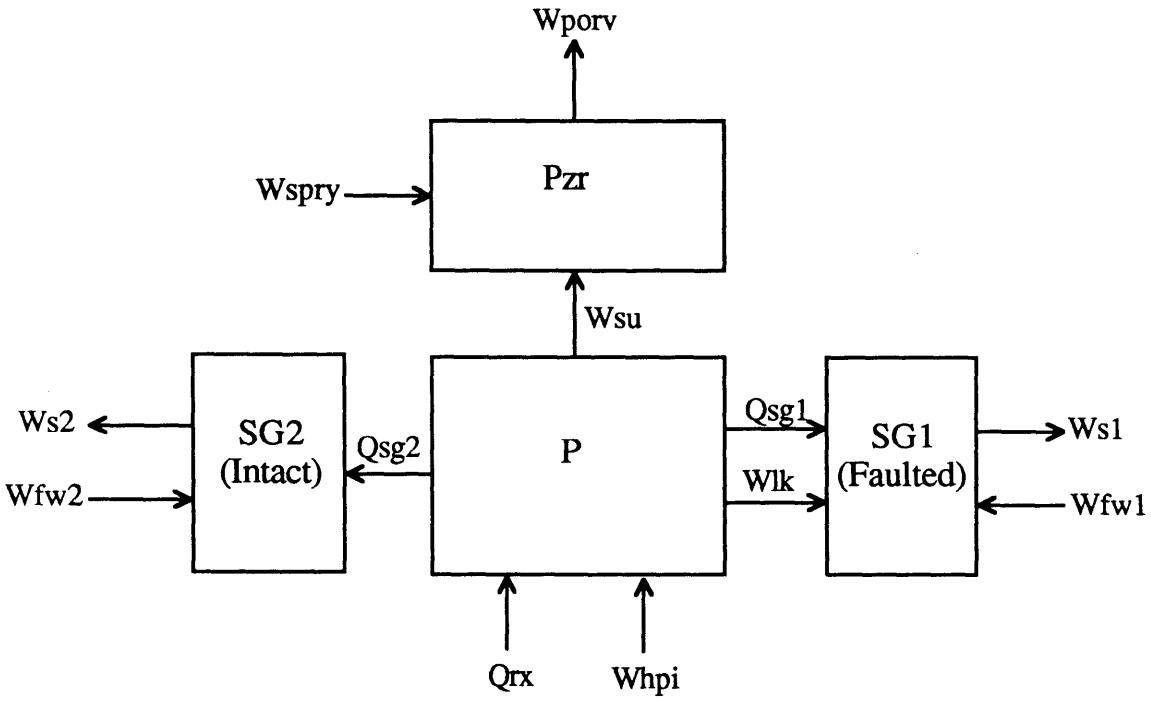
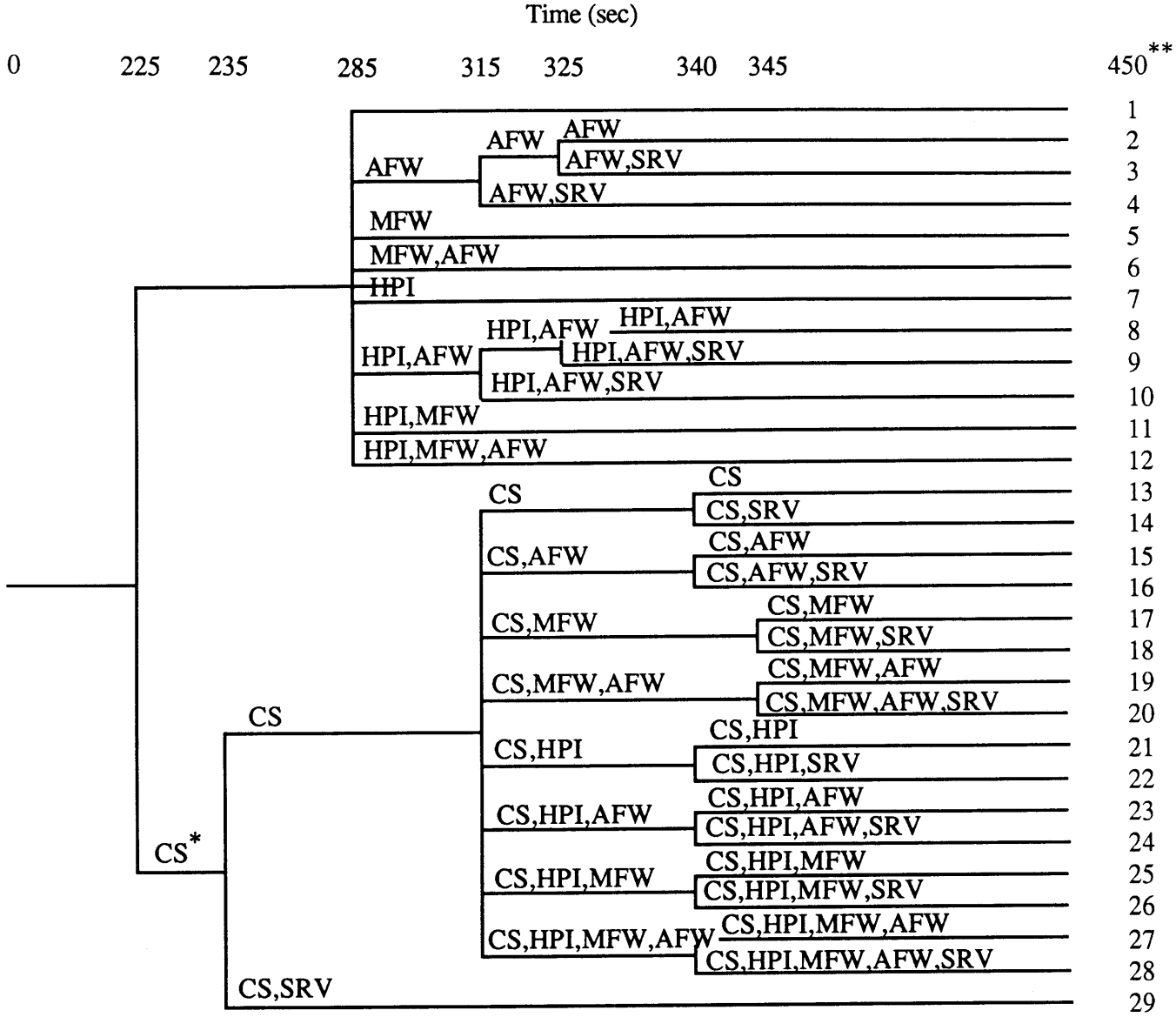



Figure 3 - Simple 4-Node Physical Model

P : Primary Node
Pzr: Pressurizer Node
SG1 : Steam Generator Node (Faulted SG)
SG2 : Steam Generator Node (Intact SG)
Whpi : High Pressure Injection Mass Flowrate (to P node)
Wlk : Leakage Mass Flowrate (to SG node)
Wfw : Feedwater Mass Flowrate (to SG node)

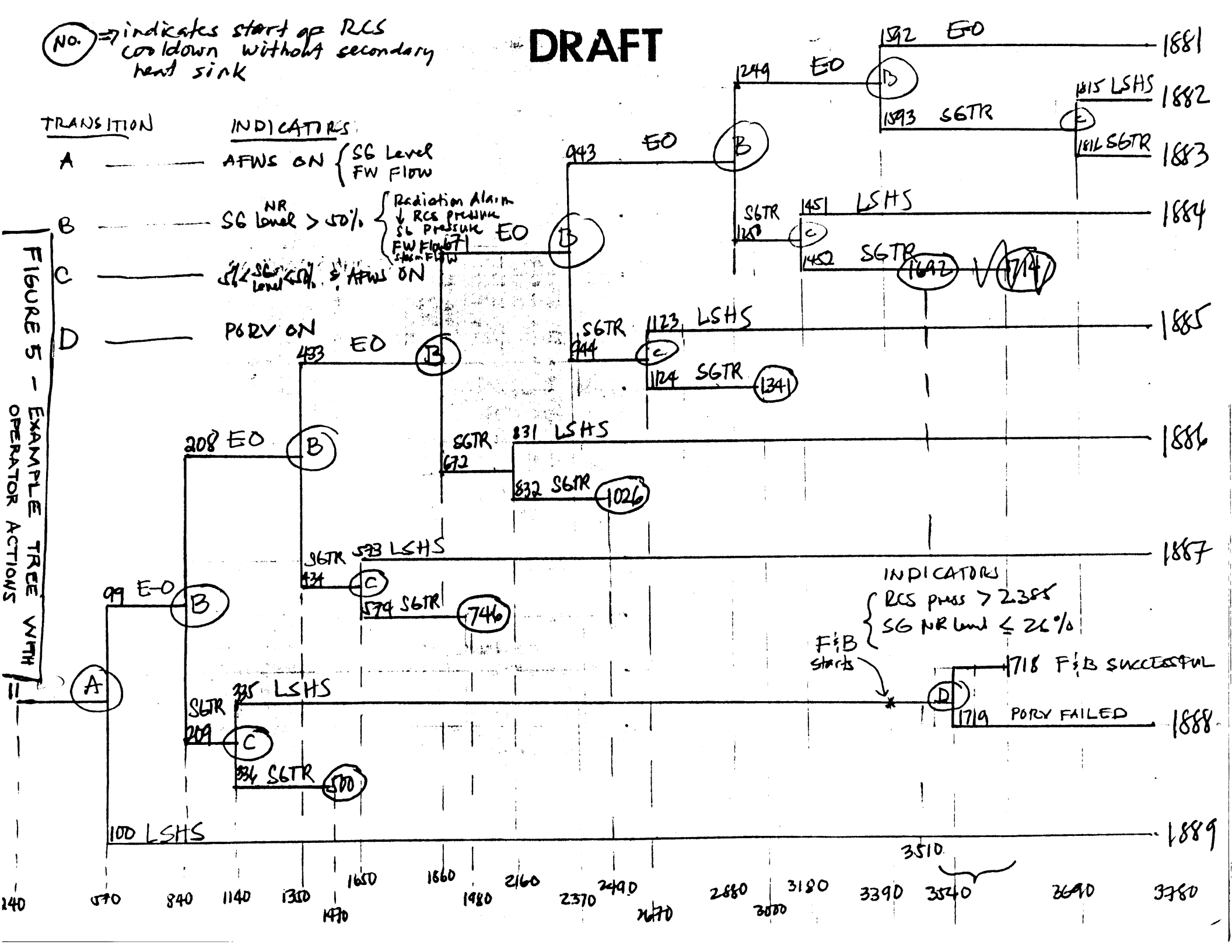
Wsu : Surge Mass Flowrate (to Pzr node)
Ws : Steam Mass Flowrate (from SG node)
Wspry : Spray Mass Flowrate (to Pzr node)
Wporv : PORV Mass flowrate (from Pzr node)
Qrx : Core Heat Generation Rate
Qsg : Heat Transfer Rate to SG node

Figure 4 - Sample Dynamic Event Tree (With No Operator Actions)




* INDICATES FAILED SYSTEM(S)
CS - CONDESATE SYSTEM AND THE 40% DUMP
HPI - HIGH PRESSURE INJECTION SYSTEM
MFW - MAIN FEED WATER SYSTEM
AFW - AUXILIARY FEED WATER SYSTEM
SRV - SAFETY RELIEF VALVE (10% ATM DUMP AND SG RELIEF VALVES)
SS - PRESSURIZER SPRAY SYSTEM
PORV - PRESSURIZER POWER-OPERATED VALVE
MSIV - MAIN STEAM ISOLATION VALVE

** PLANT STATE NUMBER
AT TIME = 450 SECONDS


(NO.) => indicates start up RCS cooldown without secondary heat sink
DRAFT
TRANSITION
INDICATORS
A — AFWS ON { SG Level, FW Flow
B — SG NR Level > 50% { Radiation Alarm, RCS pressure, SG pressure, FW Flow, Steam Flow
C — 5% < SG NR Level < 50% & AFWS ON
D — PORV ON
FIGURE 5 - EXAMPLE TREE WITH OPERATOR ACTIONS
1592 EO 1881
1249 EO
1815 LSHS 1882
1593 SGTR
1811 SGTR 1883
943 EO
S6TR 145 LSHS 1884
1452 SGTR 1642 1714
1123 LSHS 1885
SGTR 944
1124 SGTR 1341
433 EO
208 EO
SGTR 831 LSHS 1886
672
832 SGTR 1026
SGTR 523 LSHS 1887
99 E-O
574 SGTR 746
INDICATORS
RCS press > 2385
SG NR Level ≤ 26%
F&B starts
1718 F&B SUCCESSFUL
335 LSHS
SGTR
209
1719 PORV FAILED 1888
334 SGTR 570
100 LSHS 1889
3510
240 570 840 1140 1350 1650 1660 2160 2490 2680 3180 3390 3540 3690 3780
1470 1980 2370 2770 3080