Reliability Engineering and System Safety **41** (1993) 135–154

Dynamic event trees in accident sequence analysis: application to steam generator tube rupture

C. Acosta & N. Siu*‡

Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

(Received 28 April 1992; accepted 22 January 1993)

A dynamic event tree method for analyzing the risk associated with dynamic nuclear power plant accident sequences is presented. The method provides a framework for treating stochastic variations in operating crew states (defined by substates characterizing the accident diagnosis, the planned actions, and the crew quality) as well as stochastic variations in hardware states. Plant process variables are treated deterministically; they are used when determining the likelihood of stochastic branchings. The method is used in an analysis of a steam generator tube rupture (SGTR) accident; it is shown that a number of important operator behavior patterns can be reasonably represented, and that, comparing with conventional event trees, sources of dependencies between failure events can be better defined.

1 INTRODUCTION

1.1 Background

Probabilistic risk assessment (PRA) is a tool that is being increasingly used in risk management for nuclear power plants. Naturally, in such an application, it is important that the PRA study identify and quantify all significant accident scenarios. In this regard, the event tree/fault tree methodology, introduced in WASH-1400[1] and currently used in both industry and government-sponsored nuclear power plant PRAs, has enjoyed widespread success. The methodology has led to important generic lessons and is routinely used to identify scenarios that represent risk outliers and to suggest means to reduce the risk from these scenarios.

On the other hand, there has been a growing sentiment in recent years that the event tree/fault tree methodology has weaknesses in treating complex scenarios whose development is strongly affected by operator actions. For example, Ref. 2 provides a critique of current human reliability analysis (HRA) methods as well as some suggestions for future improvements; this critique is provided in the context of standard PRA analysis, in which detailed HRA is done for a limited number of scenarios (i.e., those that survive an initial screening process). Additional comments on the basic structure of the event tree/fault tree methodology are provided in Refs 3–5.

The basic issue is that event trees and fault trees do not, nor are they intended to, literally simulate the integrated, dynamic response of the plant/operating crew system during an accident. Instead, each accident scenario is represented as a set of hardware failures and operator errors. The latter are treated in much the same fashion as hardware failures, and often treated at a very broad level, e.g., failure to depressurize the reactor coolant system in τ minutes.

There are two major consequences to this approach. First, many of the conditions affecting the likelihood of operator errors (e.g., previous decisions by the operating crew, behavior of plant process variables) are not explicitly included in the model. The lack of contextual information can lead to incorrect assessments of dependence between events. For example, as a practical matter, PRA models

* Present address; EG & G Idaho Inc. PO Box 1625, MS 3855, Idaho Falls, ID 83415, USA.
‡ To whom correspondence should be addressed.

Reliability Engineering and System Safety 0951-8320/93/$06.00

rarely identify risk significant situations in which operators turn off needed safety systems, although this was a prime contributor to the TMI-2 accident. In the absence of a proper (dynamic) context, it is difficult for an analyst to justify the assignment of non-negligible probabilities to such events. Current PRA studies do not entirely neglect the dynamic aspects of accident progression. Offline thermal hydraulic analyses and detailed task analyses are often employed to indicate the time requried for operators to perform specific tasks, the time window available, and the operator burden during task performance (see, e.g., Ref. 6). However, these analyses are not fully integrated into the PRA; rather, they are used to shape judgments used to quantify the PRA parameters.

The second consequence of treating human errors in an analogous fashion to hardware failures is that the remainder of the accident sequence following an error is not modeled accurately. In the current approach, the likelihood that an operating crew fails to perform a required task correctly (within a given amount of time) is treated explicitly. However, the different ways in which the crew may perform the task incorrectly, and the resulting dynamic responses of the plant/crew system to these different errors, are not treated. Therefore, in PRA terms, the proper boundary conditions for establishing the conditional split fractions for top events downstream of the task performance failure are not provided (as discussed earlier).

A number of methodologies have been proposed and implemented to treat dynamic scenarios in which operators play key roles. Reference 3 describes a simple Markovian state-transition model for the TMI-2 accident in which the different system states correspond to different sequences in a static event tree. Operator actions are treated statically, but the approach can incorporate dynamic actions as well. Reference 7 presents an expanded event tree methodology useful for analyzing complex accident sequences; detailed top events for the hardware and operating crew states are used to better simulate the integrated behavior of the plant and operators. The accident progression event trees used in NUREG-1150 represent another expanded event tree approach for treating complex physical processes and hardware failures.[8]

References 9 and 10 describe more general methodologies for treating dynamic accident scenarios. Reference 9 describes the dynamic logical analytical methodology (DYLAM), designed to treat the integrated behavior of process variables and hardware in a system analysis. This simulation-based methodology involves the generation of a dynamic event tree (discussed in the next section) to model the different ways the system can evolve over time. The methodology is extended in Ref. 4 to treat accident scenarios and in Ref. 11 to treat three operator error types: slips, lapses, and mistakes. Slips (errors in execution but not in intention) are deterministically generated as a function of operator stress and the salience of important cues. Lapses (errors associated with forgetting) are generated stochastically as a function of stress. Mistakes (errors in intention) are generated deterministically as a function of the operator's knowledge base. Reference 10, on the other hand, presents a more analytically based extended Markovian framework in which the system state is defined as a function of the 'operator state' (as defined by the user), the system hardware state, and the current values of the process variables.

Discrete event simulation (a particular form of Monte Carlo simulation) is also a potentially powerful tool for dynamic accident scenario analysis. The primary advantage of this approach is its great flexibility in treating plant and operator behavior; its drawbacks are its potentially long running times in the absence of good variance reduction techniques (see, e.g., Ref. 12) and its weakness in producing structured, discrete scenario oriented output.

Of the above-mentioned methodologies, DYLAM appears to be the most promising for near-term application to nuclear plant accident scenario analysis. Compared with more analytical state-transition modeling approaches, it does not require the explicit definition of plant states prior to the analysis. It also allows a non-Markovian treatment of operator behavior. Compared with discrete event simulation, a DYLAM-based approach has a somewhat more obvious structure and preserves the notion of discrete accident scenarios (which is useful for decomposing risk for the purpose of risk management).

The drawbacks with the current DYLAM methodology in the context of dynamic, plant level scenario analysis are twofold. First, as discussed above, DYLAM is limited in its treatment of the stochastic behavior of operators (only lapses are modeled stochastically, and these are treated in a binary fashion analogous to hardware failures). Further, being originally designed to treat hardware-oriented scenarios, DYLAM appears to lack the flexibility needed to integrate a general stochastic model for operators. The second drawback is that, as indicated by its developers, DYLAM appears to be an impractical tool for a full plant-level accident scenario analysis due to the large number of scenarios to be quantified and the computational requirements of current cognitive models to be coupled with the analysis. These drawbacks do not invalidate the general DYLAM concept. Rather, they indicate (1) areas where the DYLAM structure needs to be extended, and (2) the need for significant approximations in practical applications.

1.2 Objective and outline

This paper describes a generalization of the DYLAM concept, called the dynamic event tree analysis method (DETAM), and its demonstration application in an analysis of steam generator tube rupture (SGTR) accidents. This method allows a more general treatment of the integrated response of a nuclear power plant and its operators to an initiating event. The approach treats the time-dependent evolution of plant hardware states, process variable values, and operator states over the course of a scenario. The effect of the plant operating procedures on scenario evolution is explicitly modeled. The approach provides the context needed to assess dependencies between multiple errors, and between hardware failures and human errors. In particular, it provides a formal framework for assessing the likelihoods of various errors of commission (especially when instrumentation failures are treated).

Section 2 of this paper discusses the general dynamic event tree approach, as applied to nuclear plant accident sequence analysis. Of primary interest are the choices of state variables that determine the possible space of scenarios. Section 3 discusses many of the details needed to apply the general approach to a specific accident: a steam generator tube rupture (SGTR) in a pressurized water reactor (PWR). These details include the various modeling assumptions regarding process variable prediction, hardware state definitions, and operating crew state definitions. Section 4 presents results from the dynamic event tree analysis, including a demonstration of DETAM's ability to treat various error forms, a comparison with the results of conventional PRA analyses of SGTR, and some qualitative insights following the application of the methodology that are somewhat independent of the PRA analysis. (Additional details on the SGTR analysis modeling assumptions and results are provided in Ref. 13.) Finally, Section 5 provides concluding remarks concerning the advantages and disadvantages of the dynamic event tree approach, potential areas of application, and further work required to improve the practicality of the methodology.

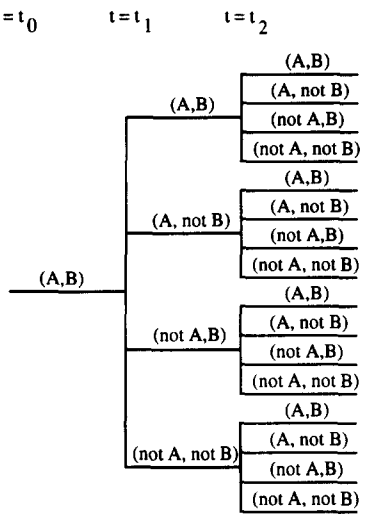

Fig. 1. Example dynamic event tree for two binary systems (two time steps).

2 DYNAMIC EVENT TREES

2.1 Concept

A dynamic event tree is an event tree in which branchings 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, System A and System B. Three characteristics of interest shown in this figure are as follows: (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. The last point means that a practical application of the approach is should be a simulation-oriented one. Event sequences are generated by rules as the analysis progresses, rather than specified in their entirety as an initial step in the analysis. The rules themselves are specified at the beginning of the analysis.

Noting that the user is free to define the 'systems' in Fig. 1 and that each system can have more than two states, it can be seen that a dynamic event tree can be a very general model. To formalize the concept, we identify five characteristic sets that define the dynamic event tree approach. These are (a) the 'branching set', (b) the set of variables defining the system state, (c) the 'branching rules', (d) the 'sequence expansion rules', and (e) 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 Fig. 1, branchings are determined by the joint status of Systems A and B; the branching 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 overall system state is defined by the variables that influence the frequency assignments for the various branchings. 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

Table 1. Dynamic event tree characterization of DYLAM

Branching set:	indicator variables for components and certain operator actions (indicating if a lapse does/does not occur)
Plant state:	defined by branching variables, process variables, operator stress, salience of cues, operator state of knowledge
Branching rules:	branching occurs at fixed points in time (the algorithm presented in Ref. 4 allows branching when the frequency of remaining in a system state is a user-specified fraction of the initial state frequency)
Expansion rules:	sequences associated with multiple simultaneous independent failures, sequences whose total number of failures exceeds a user-defined value, and sequences with frequencies lower than a user-defined value are truncated; sequences exhibiting similar physical behavior are grouped
Tools;	problem-specific models for physical plant behavior, stress, salience of cues, operator knowledge base

event sequence, yet may affect the likelihood of subsequent branchings. (Plant process variables and the operator stress variable modeled in Ref. 11 provide examples of variables affecting the system state but not necessarily included in the branching set.)

The 'branching rules' are the 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 Δt) selected prior to the analysis. Other branching rules can be associated with a specific application. For example, in an accident scenario analysis, it may be desired to allow hardware-associated branchings (e.g., system failures) only when a system is demanded.

The 'sequence expansion rules' are the rules used to limit the number of sequences and, hence, tree expansion. These rules should involve, as a minimum, sequence termination when a maximum simulation time or one of a set of user-defined absorbing states is reached. They will also usually include a rule for sequence termination when the sequence frequency falls below a user-specified lower limit.

The quantitative tools are those used to compute the deterministic state variables (e.g., process variables) as well as the branching frequencies.

Specific choices for each of these five sets define a particular application of the dynamic event tree concept. For example, including the operator model described in Ref. 11, DYLAM can be characterized as shown in Table 1.

2.2 Dynamic event trees for accident scenario analysis

In order to model the dynamic, integrated response of plant and operators to an initiating event, the dynamic event tree must carry information on the following:

- current hardware status
- current levels of process variables
- current 'operator state'
- scenario history
- time

It is also important, on the other hand, to ensure that the resulting tree is not too large for practical analysis. Table 2 presents a set of dynamic event tree characteristics useful for accident scenario analysis. With these choices of characteristics, the analysis explicitly treats the plant process variables, the operator's understanding of the current situation, the operators' internal conditions, and the actions planned by the operators.

The plant process variables (e.g., steam generator and pressurizer level, reactor coolant system pressure) are important because they determine the timing of events (e.g., demands for safety system actuations, occurrence of undesired physical plant states). Requirements for operator actions are often keyed to the process variables; these actions lead to changes in the process variables which, in turn, lead to different required actions.

The operators' understanding of the current

Table 2. Characteristics of dynamic event trees for accident scenario analysis

Branching set:	variables indicating status of plant systems, crew diagnosis state, crew quality state, and crew planning state
Plant state;	defined by branching variables and plant process variables (including first derivatives of key variables)
Branching rules:	branching occurs at fixed points in time
Expansion rules:	low frequency sequences are truncated; 'similar' sequences are grouped
Tools;	problem-specific models for physical plant behavior, stress, conditional frequency of operator state changes

accident situation, called the crew's 'diagnosis state', clearly can affect the likelihood of future actions. Representations of the diagnosis state are potentially quite complex, but need not be. For example, Ref. 14 demonstrate how experimental observations/inferences of an operator's mental model during simulation exercises might be mapped as a trajectory on a fairly simple two-dimensional matrix in which the rows and columns of the matrix represent different levels of abstraction along the 'whole–part' and 'means–ends' dimensions. The first dimension corresponds to the diagnosis state, as it defines where the operator thinks the current problem is (e.g., at plant level, at system level, at train level, etc.). The second dimension is more concerned with the actions the operator is thinking of taking to deal with the problem; this corresponds to the planning state, discussed shortly.

The internal condition of the operating crew, called the crew's 'quality state', characterizes the crew's ability to efficiently perform tasks. This condition is defined by such factors as time pressure, workload, and crew group structure, which can affect crew performance and can change over time. (Note that a variety of organizational factors, e.g. training, can affect crew performance, but need not be dynamically simulated since they will remain static through the course of the scenario.) The operator stress models discussed in Refs 11 and 15 illustrate potential approaches for quantifying one important aspect of the crew's quality state. Models for the dynamics of characteristics other than stress (e.g., communication effectiveness), need to be developed and integrated into the analysis. Reference 15 provides some initial steps in this direction.

The actions planned by the operators define the 'planning state' for the crew. In the highly proceduralized environment of current plants, the planning state is strongly affected by the procedural requirements on the operators. Of course, deviations in procedure following can occur, and have been observed in actual incidents. Note that the separate treatment of diagnosis and planning allows modeling of situations where the correct steps are taken, although an incorrect diagnosis has been made.

Figure 2 shows how the characteristics listed in Table 2 are implemented in an accident scenario analysis. This figure applies to a single scenario within a single time step; the same process is applied repeatedly during the simulation for all scenarios and all time steps. As shown in the figure, the first task is the deterministic computation of the plant process variables. The next task is to stop the branching process if an absorbing state is reached. Absorbing states can represent the successful completion of the scenario, or the achievement of a particular undesired physical state. In the next task, the new set of possible hardware states, and their associated likelihoods, are generated. Changes in hardware states can occur when process variables reach their associated setpoints and when operators start/stop equipment; errors in executing actions (as opposed to errors in planning actions) are reflected at this step. In the fourth

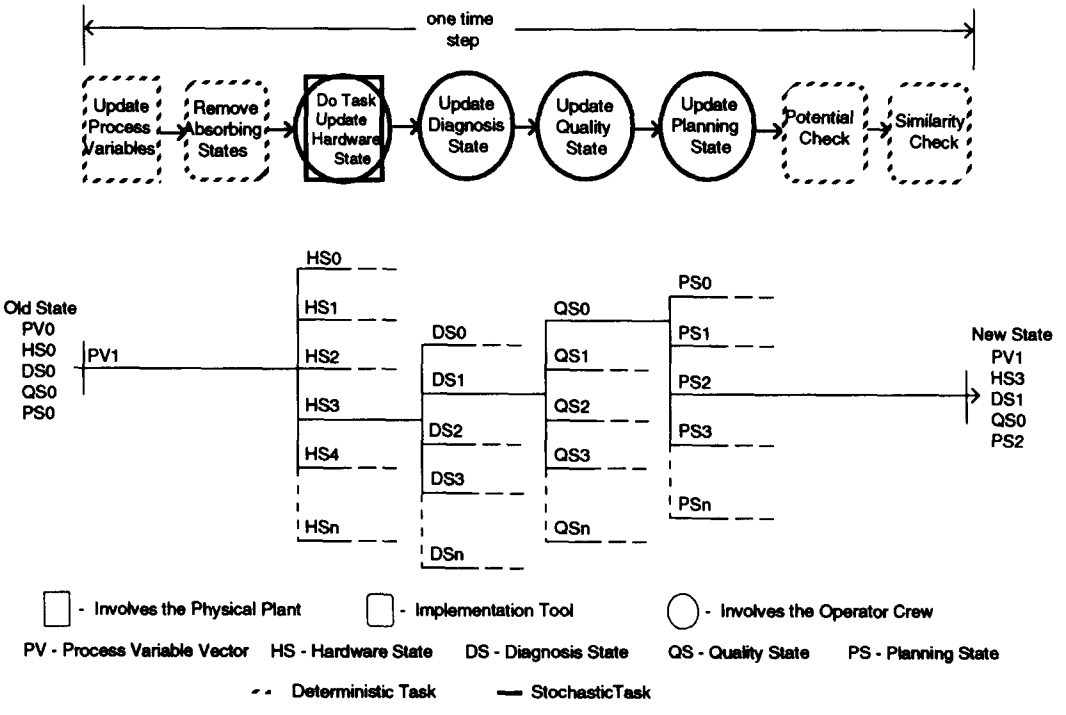

Fig. 2. DETAM tasks performed during a single time step.

through sixth tasks, branchings associated with the crew diagnosis, quality, and planning states are generated. In the seventh task, current scenario probabilities are calculated. Scenarios without significant potential to contribute to overall risk are screened out. (This screening is similar in concept to the approach for Monte Carlo sampling variance reduction described in Ref. 12, which also employs the notion of scenario importance to focus the analysis.) In the last task, similar scenarios are grouped together to reduce the degree of 'scenario explosion'[4] inherent in the dynamic event tree approach. It is interesting to note a limiting situation for the analysis; if the sole criterion for scenario similarity is based on hardware states, the dynamic event tree collapses into a structure quite similar to a conventional event tree.

2.3 Discussion

The general dynamic event tree concept is not a new one. Indeed, the event trees used in the formal field of decision analysis, from which the event tree concept used in WASH-1400 was originally borrowed,[1] often represent sequences of events (decisions and random occurrences) over time. The state-transition diagram presented in Ref. 3, the expanded event trees described in Ref. 7, the Markov methodology described in Ref. 10, and DYLAM[4,9] can all be viewed as specific implementations of the dynamic event tree approach. This paper discusses a particular choice of dynamic event tree characteristics that is both useful and practical for complex accident scenario analysis. As seen in Table 2, this choice is quite similar to that made by DYLAM (see Table 1); the primary difference is that DYLAM does not emphasize the stochastic nature of operator behavior as strongly.

The diagnosis state/quality state/planning state representation of the operating crew used in this analysis is intermediate between the empirical operator models widely used in PRA studies and a number of detailed cognitive models undergoing development (see, e.g., Refs 15 and 16). Unlike purely Markovian models, this representation captures some of the influence of scenario history needed for an evaluation of multiple failures linked by operator actions and better allows the incorporation of 'limited rationality' models for human error,[17] i.e., models in which operators are assumed to make reasonable decisions, given their state of knowledge, available resources, etc. The approach does not, however, necessarily require the use of complex, high fidelity operator simulations. An analysis can proceed if experts knowledgeable about operator behavior during accidents are available. In this manner, the approach is similar to that used in a conventional human reliability analysis for current PRAs (the difference being that, in the case of the dynamic event tree analysis, the time-dependent context for the operator actions is directly available to the expert). The remainder of this paper discusses an application of DETAM towards the analysis of steam generator tube rupture (SGTR) accidents.

3 MODELING STEAM GENERATOR TUBE RUPTURE (SGTR)

This section briefly summarizes a demonstration application of the DETAM approach towards the analysis of pressurized water reactor (PWR) scenarios initiated by a steam generator tube rupture. The discussion illustrates a number of important details that must be addressed when developing a dynamic event tree application for accident sequence analysis. Additional details on the application are provided in Ref. 13.

The SGTR scenario is 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 can be an important contributor to public health risk, since it can lead to both a core melt and a direct release of radioactivity to the atmosphere (bypassing containment).[31] Finally, various forms of information on the scenario are available, including reports of actual events, observations of simulator training exercises, a fast PC-based PWR simulation model that treats SGTR, relevant emergency operating procedures, and PRA analyses of SGTR.

3.1 Thermal hydraulic model

The simple physical model used to compute current levels of process variables during the accident employs four nodes: the primary node, the pressurizer, the faulted steam generator, and the intact steam generators. 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. This model is somewhat specialized towards the analysis of SGTR in a Westinghouse four-loop PWR. However, it can be modified relatively simply to handle other relatively slowly progressing accidents in other PWRs.

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. Within the pressurizer node, it is assumed that both the liquid and the vapor

are maintained at saturation conditions. The two steam generator nodes are treated as being homogeneous and at saturation. 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 a PWR plant simulator.[18] 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 early in the accident. Later in the accident, the model's predictions can diverge considerably, limiting the usefulness of the simulation.

3.2 Hardware state model

The explicit treatment of the time dimension in a dynamic event tree analysis can require the processing of much larger amounts of information than are treated in a static analysis of comparable detail. Given that conventional PRA models are already quite large and that computing resources are finite, a practical dynamic analysis must sacrifice some level of detail in the hardware, process physics, and operating crew models. In this analysis, the following hardware-related assumptions are made to limit the amount of information to be processed.

First, the hardware states in the model are defined by the status of a limited number of frontline systems. Support systems are not treated, nor are individual trains or components within the frontline systems. Event tree branches can be generated for only those hardware systems (or groups of systems) which can significantly affect the behavior of the plant during the early part of the SGTR scenario (starting from the initiation of the steam generator tube rupture and culminating when cooldown and depressurization of the primary system commences). These include the emergency feedwater system (EFWS), the high pressure injection system (HPIS), the safety injection signal (S-signal or SI), the start-up feed pump (SUFP), the pressurizer power-operated relief valves (PORV), the 40% steam dump valves that bypass the turbine and condensate system (SDV), and the atmospheric relief valves on the ruptured and intact steam generators (ARVI and ARV2). These latter include the 10% atmospheric dump valves and the safety relief valves. Note that the SUFP provides an additional backup source of feedwater for the steam generators.

Systems not included in this list are assumed to function as designed (i.e., their indicator variables are not included in the branching set). One such system is the Safety Parameter Display System (SPDS). As discussed in Ref. 19, the SPDS informs the operators through color-coded status trees the current status of the critical safety functions; a red color indicates that the critical safety function is in danger and that immediate operator action is necessary, whereas a green color requies no operator action.

A second hardware-related modeling assumption is that only failures on demand require treatment. The demand can be due to an operator action or to an automatic signal sent when a process variable reaches a setpoint. Failures during operation are generally of lower likelihood and are neglected; equipment unavailability due to testing or maintenance can be treated as an initial condition for the analysis, and need not be simulated dynamically. Operator errors in executing planned actions are included in the hardware state branching frequencies.

Two other hardware-related modeling assumptions used in the analysis are as follows: (a) hardware failures are not recoverable; and (b) instrumentation failures for most equipment are not treated. None of the above assumptions result from structural limitations in the dynamic event tree methodology; they are employed to limit the scope of the analysis.

3.3 Operating crew state model

The three-substate crew model described in Section 2 (which distinguishes between the diagnosis, quality, and planning states of the crew) builds on work performed by other investigators interested in human behavior during nuclear power plant accidents. Reference 17 points out that, in the course of a scenario, the operator crew performs four fundamental activities: monitoring, explanation building, action planning, and action implementation. Monitoring involves keeping track of the different indicators and instrumentation. Explanation building refers to crew efforts to understand the ongoing scenario. Planning refers to the crew's building of a strategy or set of actions in response to the situation. Implementation entails the actual execution of planned tasks or strategy. Note that the actual ordering of these tasks may vary (e.g., operators may start to plan actions before they have completely explained the situation). This representation of crew activities is quite similar to the operator action tree (OAT) notion, originally described in Ref. 20 and applied in a number of PRAs. The OAT used in Ref. 21 has three top events: diagnosis, action, and rediagnosis. The tasks of monitoring, explanation formulation, and planning are included in the diagnosis top event in the OAT. The action implementation activity, on the other hand, corresponds to the action top event in the OAT.

It can be seen that two of the three substates used

in the DETAM model for the operating crew cover these concepts. For example, the diagnosis state models the results of the monitoring and the explanation building activities; the planning state models the results of the planning activity. Of course, the repetitive application of these substates in a dynamic simulation renders the rediagnosis top event in the OAT unnecessary. (Note that the quantitative analysis of diagnosis state transitions can change over the course of the scenario, due to the interactions within the crew, between the crew and the technical support center, etc.) The third substate, the crew quality state, models the influence of such performance shaping factors (PSFs) as stress. These PSFs are treated in conventional human reliability analyses, as well. A DETAM analysis allows the treatment of the dynamic development of these PSFs in response to the operator/plant interaction, when appropriate models become available.

3.3.1 Crew diagnosis state

The crew diagnosis state indicates the crew's understanding of the plant's past and current conditions. As discussed in Ref. 14, this understanding can be represented at a variety of levels (e.g., plant level, system level). The DETAM analysis defines the diagnosis state in terms of the crew's understanding of the general scenario and the states of five safety functions.

At the general scenario level, it is assumed the operating crew may believe that the plant is at steady-state conditions, or undergoing an as yet undetermined transient, or undergoing an SGTR, or undergoing a small loss of coolant accident (SLOCA). The SLOCA diagnosis is included because the SLOCA signature shares some similarities with that of SGTR; both SGTR and SLOCA lead to decreases in RCS pressure and pressurizer level; the statuses of the radiation alarm and the steam generator (SG) level determine if the accident is an SGTR or an SLOCA. Simple rules are employed to assign the likelihood of incorrect diagnoses, given that an SGTR is underway. Some details are provided in Section 3.4; additional information is provided in Ref. 13.

The five safety functions are primary pressure: control, primary inventory control, secondary heat sink, secondary pressure control, and secondary heat removal. These functions are also monitored by the Safety Parameter Display System. In keeping with the general assumption of this analysis that nearly all instrumentation functions correctly, it is assumed that the operators correctly understand the status of these functions.

3.3.2 Crew quality state

The crew quality state is used to model the dynamic portion of the internal state of the crew that affects its ability to plan and perform required tasks. It includes such dynamic factors as the crew's group structure, emotional condition, and degree of coordination in executing members' respective assigned tasks. The general model shown in Fig. 2 allows for stochastic treatment of the quality state. However, in this demonstration analysis, variations in the quality state, and the associated effect on scenario branchings, are not treated.

3.3.3 Crew planning state

The crew planning state refers to the set of actions that the crew plans to perform. In keeping with crew training and plant operating policies, this analysis treats the planning state as being procedure-oriented, i.e., the crew tends to follow procedures as closely as possible. Changes in the planning state based on actions not included in the procedures are treated only on a limited basis.

In the case of procedure following, the crew planning state at any point in time can be described in terms of two substates: the procedure substate, which indicates which emergency procedure is to be followed, and the step substate, indicating the specific step in the selected procedure to be performed. (Recall that, as shown in Fig. 2, the actual execution of planned actions affecting equipment is simulated in the next time step when the likelihoods of the new hardware states are determined.) In this analysis, the procedure substate can be any of the four emergency operating procedures, namely: Reactor Trip or Safety Injection Response (E-0). Response to Loss of Secondary Heat Sink (FR-H.1), Loss of Reactor or Secondary Coolant (E-1), and Steam Generator Tube Rupture (E-3). These four emergency operating procedures are modeled because they are the likely procedures that the crew will use for the portion of the SGTR scenario being analyzed. Because information on the appropriate procedures for crew response to warnings from the critical safety function status trees was not obtained in this study, this demonstration of DETAM treats the occurrence of a red or orange SPDS signal as a boundary condition, terminating the development of the associated scenario.

The step substate refers to the specific steps of the emergency procedures. There are 37 E-0 steps, 16 FR-H.1 steps, 13 E-1 steps, and 18 E-3 steps modeled. The time allocated to complete each step is assessed using information obtained from an SGTR simulation exercise. Steps which involve systems not explicitly modeled in the analysis are assumed to be successful (time is allocated to perform the required actions).

A limited number of actions that are not included in the operating procedures are incorporated in the planning state analysis. As long as non-procedural actions can be incorporated as pseudo-procedures (or

pseudo-steps within actual procedures), they can be incorporated into the analysis.

Transitions between planning states can involve transitions from one procedure to another, or from one step to another within a given procedure. Regarding transitions between procedures, it is assumed that the operator is very unlikely to transfer to a new procedure unless it is prescribed by the current step in the procedure being followed. (Recall that the SPDS, which can be used in practice to change the chosen course of response, is being used in this analysis to provide boundary conditions, as discussed above.) Regarding transitions between steps, a degree of randomness is introduced by allowing operators to skip steps or to stay in a given step (with user-specified probabilities).

3.4 Branching likelihood assignments

Branching frequencies are required for branchings associated with transitions between hardware states, diagnosis states, and planning states. In the case of hardware-related branchings, the approach is conventional; system unavailabilities are conservatively used as demand failure frequencies (recall that runtime failures are not modeled explicitly, and that testing and maintenance contributions are treated as initial conditions). The potential effect of process variables on failure rates (see, e.g., Ref. 22) is not treated.

In the cases of diagnosis state and planning state transitions, judgment is employed more extensively. To ensure some degree of consistency in the estimation process, a two-step procedure is followed. First, possible transitions are assigned qualitative likelihoods. Second, the qualitative likelihoods are quantified. The range of qualitative likelihoods used in this study, along with the associated numerical values, appear in Table 3.

The diagnosis state branching frequencies developed for this analysis are presented in Ref. 13. They are based on a study of the relevant procedures (to determine the indicators monitored by the operator crew and the criteria used by the crew to identify which scenario is in progress), walk-throughs of some sequences to understand how the crew might treat the indicators during the event, consultations with a training instructor knowledgeable about the SGTR scenario and crew responses to that scenario, and discussions with an analyst experienced in human reliability analysis. These frequencies are affected by variations in the critical SGTR indicators (radiation alarm status and SG level), as well as by the initial diagnosis state. The frequency assignment procedure reflects, in a limited fashion, the phenomenon of 'confirmation bias', in which a person clings to an initial diagnosis in spite of evidence to the contrary.[23]

Table 3. Qualitative likelihoods

Qualitative likelihood	Probability
Certain no	0·00
Very very unlikely	0·01
Very unlikely	0·10
Unlikely	0·30
Even	0·50
Likely	0·70
Very likely	0·90
Very very likely	0·99
Certain yes	1·00

The planning state transition frequencies are also based on a study of relevant procedures and discussions with persons knowledgeable about operator behavior and human reliability analysis. To help ensure consistency in assigning transition likelihoods, meta-rules indicating how the transition likelihood is affected by the consistency between (a) the crew's diagnosis state and the procedure being considered, and (b) the available indicators and the procedure being considered, are developed.[13] The planning state transitions are also affected by the relative importance of the indicators monitored and the potential consequence of the operator action. By considering these factors, allowances are made for the possibility that the operators may intentionally or unintentionally choose a different procedure than that called for, skip steps in executing a procedure, delay in performing procedural steps, or even perform actions not in the procedures. Errors in executing planned actions, are treated using estimates obtained from Ref. 24.

Note that well-accepted estimates for the operator-related branching frequencies are not yet available, and may depend upon on the development of advanced cognitive models for operating crews (e.g., CES[16]). For the purposes of demonstrating the elements of the dynamic event tree analysis method, subjectively assessed branching frequencies are judged to be adequate. It should be pointed out that DETAM exercises expert judgment in situations more tightly defined than those for conventional PRA analyses; it is hoped that this will reduce the degree of subjectivity in estimates for human error rates for plant level actions.

3.5 Branching rules

As shown in Table 2, branchings are allowed to (but need not) occur at fixed points in time. In this analysis, uniform time steps of 30 seconds are used. This time step is chosen largely to represent the time scale for the operator actions considered. If an event (e.g., an automatic system demand) occurs during the time step, it is treated as occurring at the end of the time step. Branching is also limited by the restriction that only demand-related hardware failures are treated.

The regularly spaced branching intervals used in the

current analysis allow a simple treatment of the branching process, but may not be especially efficient. In future, improved analyses, dynamic time steps (accounting for the time required by process variables to reach key values, as well as the time required for operators to perform key actions) might be used. This can reduce the number of calls to the branching process, and will reduce the physical model computations performed for a given scenario.

3.6 Stopping rules

Figure 2 shows that the development of dynamic scenarios can be stopped at three points. First, scenario development can be stopped when an absorbing state (either desired or undesired) is reached. Second, it can be stopped if the potential contribution to risk from the scenario is judged to be insignificant. Third, it can be stopped if it is similar to another scenario; in this case, all similar scenarios are grouped and treated as a single scenario.

The thermal–hydraulic model used largely determines the absorbing states used in this application. This model cannot treat such issues as the behavior of the plant following steam generator dryout or the generation of a steam bubble in the main loop (as observed at Ginna). Thus, the model is restricted to the early phase of an SGTR.

The limited number of operating procedures explicitly included in the model spaces additional restrictions on the analysis. For example, procedures dealing with situations where the critical safety functions reach and pass warning levels are not incorporated. The following plant conditions are treated as absorbing states in the analysis:

- Successful completion of the reactor coolant system cooldown and depressurization
- Successful depressurization through bleed and feed cooling
- A critical safety function monitored by the SPDS reaches orange or red status
- The reactor coolant system node reaches saturation
- The intact steam generators dry out
- The ruptured steam generator overfills
- The pressurizer overfills
- Bleed and feed cooling cannot be initiated successfully on demand

By truncating scenarios when these absorbing states are reached, severe physical modeling inaccuracies, which will lead to incorrect modeling of hardware demands and operator actions, are avoided. On the other hand, the full set of accident sequences is not modeled; this complicates comparisons of the DETAM results with conventional results. Improved physical models must be incorporated into the DETAM analysis to avoid this problem.

Regarding the scenario truncation and grouping tasks indicated in Fig. 2, this analysis employs simple approaches. Scenarios are truncated when their frequencies fall below a user-specified threshold. Scenarios are grouped at any given time step only if (a) they have identical hardware and operator crew states, and (b) their primary pressures and temperatures are within 5 psia and 5°F, respectively. More powerful methods for truncating and grouping scenarios may need to be developed for more detailed applications of DETAM. From a mathematical perspective, the notion of distance from a minimal cutset, operationalized in a Monte Carlo sampling variance reduction technique presented in Ref. 12, could be quite useful. From a phenomenological perspective, work may need to be done on the difficult issue of grouping scenarios based on operator perceptions of similarity.

3.7 Application notes

The DETAM approach, being simulation oriented, is implemented using a computer. A computer code called DETCO-SGTR has been constructed to perform a DETAM analysis for the SGTR scenario, subject to the boundary conditions discussed above. DETCO-SGTR is application-specific; significant changes in the analysis assumptions (e.g., in the tables for transition rates between operator crew substates) will require some programming modifications. Note that the thermal–hydraulic plant model used by the code is incorporated in a single subroutine; an improved plant simulator can be used as long as code interface issues are properly dealt with.

DETCO-SGTR is written in C (it has approximately 6000 lines). On a 20 MHz 386-class PC, longer runs take on the order of 30 minutes to execute; other runs can finish much more quickly. Due to the large number of sequences generated, the computer currently used cannot accommodate the entire SGTR analysis (memory limits are reached during the simulation). Therefore the runs performed (see Table 4) involve conditional analyses in which a specific frontline system (or set of systems) is assumed to fail.

The input required by DETCO-SGTR includes the initial values of all variables describing the plant state, the thermal–hydraulic model parameters, the simulation time duration, setpoint values, the number of possible states of each branching variable, and hardware failure and human error rates. DETCO-SGTR produces as output all dynamic event tree nodes, along with their associated likelihoods and values of relevant plant state variables, created during the simulation. The user needs to post-process the output to construct a dynamic event tree. Run turnaround times can be substantially reduced by automating most of this post-processing.

Table 4. DETAM runs performed

Run no.	Unavailable system	Systems allowed to fail	Cut-off frequency[a]	Operator error treated?
1	None	EFWS, SDV, HPI	0·0	No
2	None	PORV, ARV1, ARV2, SUFP, EFWS, HPI, SDV	5·E-6	Yes
3	Rad alarm monitor	PORV, ARV1, ARV2, SUFP, EFWS, HPI, SDV	1·E-4	Yes
4	EFWS	PORV, ARV1, ARV2, SUFP, HPI, SDV	1·E-5	Yes
5	EFWS, Rad alarm monitor	PORV, ARV1, ARV2, SUFP, HPI, SDV	1·E-4	Yes
6	EFWS, SDV	PORV, ARV1, ARV2, SUFP, HPI	1·E-4	Yes
7	EFWS, HPI	PORV, ARV1, ARV2, SUFP, SDV	1·E-4	Yes
8	None (lower ARV1 setpoint)	PORV, ARV1, ARV2, SUFP, EFWS, HPI, SDV	1·E-6	Yes

[a]Cut-off frequencies are conditioned on the unavailability of systems indicated in column 2 and on the occurrence of SGTR.

4 DEMONSTRATION SGTR ANALYSIS RESULTS

This section discusses the qualitative and quantitative results obtained from the demonstration application of DETAM towards the analysis of SGTR accidents. In addition to a set of dominant scenarios and endstates, the qualitative results include insights concerning the capabilities and practicality of DETAM, potential improvements in SGTR emergency operating procedures, the relative importance of instrumentation, and dependencies between failure events not necessarily treated in conventional analyses.

4.1 Runs performed

A variety of DETCO-SGTR runs are performed to check the feasibility of the DETAM approach in a practical application. The runs and their associated assumptions are listed in Table 4. It should be noted that Runs 2, 4, 6 and 7 are separate parts of a single analysis. Runs 2, 4, 6 and 7 are performed separately because DETCO-SGTR cannot treat an entire SGTR analysis in a single pass (the tree becomes too large to manipulate in a personal computer). It is also simpler to perform the runs separately, since this reduces the difficulty of post-processing the large amount of output generated by a single DETCO-SGTR run. Each run is performed assuming that a certain subset of the systems that are demanded when the safety injection signal (SI) actuates† will fail on demand; the final results are obtained by combining the weighted results of all runs, where the weights are computed using the system failure frequencies.

The other runs listed in Table 4 are used to check the sensitivity of the analysis (both modeling and results) to various assumptions. Run 1 does not treat human error (and is very much like a simple DYLAM analysis); it shows how the plant can reach an undesired state even if there are no faults in procedure following. The remaining runs treat potential operator errors. Runs 3 and 5 are performed to demonstrate how instrumentation can be accommodated in the analysis, and to determine the importance of the radiation alarm monitor (RAM). In both cases, the unavailability of the RAM makes the diagnosis of SGTR more difficult. Consequently, the likelihood of premature termination of cooldown and depressurization increases, due to an increase in the likelihood of delayed initiation of the cooldown and depressurization process.

Comparing the results of Run 5 with those of Run 4 in Table 5 (both runs are conditioned on the failure of EFWS), a number of differences can be observed. One difference is expecting a decrease in the likelihood of successful cooldown and depressurization. The RAM unavailability in Run 5 also generates new important endstates. The termination of the cooldown and depressurization process with the RCS pressure still greater than the ruptured steam generator pressure happens because the E-3 procedure directs the termination of cooldown and depressurization if the pressurizer level reaches a specified level (75%). The pressurizer attains the specified level due to the cooldown and depressurization delay caused by the difficulty in diagnosing the event (due to unavailable RAM).

The pressurizer could overfill (or become 'solid') if

† The high pressure injection system (HPIS), emergency feedwater system (EFWS), and steam dump valves (SDV) are demanded when the SI actuates.

Table 5. Most frequent endstates (Runs 2–7)

Run no.	Plant endstate	Likelihood[a]
2	Successful cooldown and depressurization (total)	9·9E − 1
	Cooldown and depressurization terminated with RCS pressure > ruptured steam generator pressure	3·0E − 3
	Ruptured steam generator overfills	1·3E − 3
3	Successful cooldown and depressurization	9·1E − 1
	Cooldown and depressurization terminated with RCS pressure > ruptured steam generator pressure	3·3E − 2
4	Successful cooldown and depressurization	8·9E − 1
	Successful bleed and feed cooling	5·3E − 3
	Intact steam generator dries out	1·1E − 3
	Secondary heat sink indicator turns Red	1·0E − 1
5	Successful cooldown and depressurization	7·2E − 1
	Secondary heat sink indicator turns Red	9·0E − 2
	Cooldown and depressurization terminated with RCS pressure > ruptured steam generator pressure	8·2E − 2
	Cooldown and depressurization terminated with RCS pressure > ruptured steam generator pressure and HPI turned off	3·3E − 2
	Successful cooldown and depressurization with HPI turned off	6·4E − 2
	Pressurizer becomes solid	8·4E − 4
6	Ruptured steam generator overfills	9·0E − 1
	Secondary heat sink indicator turns Red	9·9E − 2
	Ruptured steam generator relief valve demanded	4·2E − 3
7	Primary coolant reaches saturation point	9·1E − 1
	Secondary heat sink indicator turns Red	9·4E − 2

[a]Likelihoods are conditioned on the occurrence of SGTR and the unavailability of relevant systems.

the crew ignores the rising pressurizer level. It is also possible that the crew will turn off the HPIS (to prevent the overfilling of the pressurizer as in the TMI-2 incident). Note that the slight decrease in the likelihood of a red secondary heat sink indication shown in Table 5 is due to an arguable assumption that the crew becomes more cautious in following the procedures when the RAM is unavailable, thus resulting in a lower likelihood of skipping the step that checks the status of the EFWS. (This assumption is arguable because the crew may not recognize that the RAM should be indicating increased radiation levels, at least until other indications of SGTR become available.)

Run 6 involves multiple frontline system failures, and results in no desirable endstates (the failure of SDV is predicted by the thermal–hydraulic model to significantly reduce the crew's ability to cool down and depressurize the RCS before the ruptured SG overfills). Run 7 also involves multiple frontline system failures (EWFS and HPIS). In this case, an undesirable endstate (either RCS saturation or a red indication for the secondary heat sink critical safety function) is reached in 750 seconds.

In Run 8, the pressure setpoint for the atmospheric relief valves on the faulted steam generator (ARV1) is lowered artificially from 1140 psia to 1100 psia. The purpose of this sensitivity analysis is to see if varying the relief valve setpoint can compensate for the simplistic steam generator model used. The setpoint of ARV1 becomes important when dealing with scenarios involving delayed cooldown and depressurization. Delayed cooldown and depressurization should lead to a slowly increasing ruptured steam generator pressure and to an eventual demand for the ARV1 to open. Since the simple model used in this analysis predicts pressures for the ruptured steam generator that are much lower than those predicted by PRISM,[18] lowering the relief valve setpoint (by an amount equal to the difference between the PRISM results and the simple model's results) should lead to a better representation of the timing of key events in the scenario. However, the results of this analysis indicate that the setpoint change does not lead to a relief valve challenge. The pressure predicted is too low and does not rise quickly enough over time.

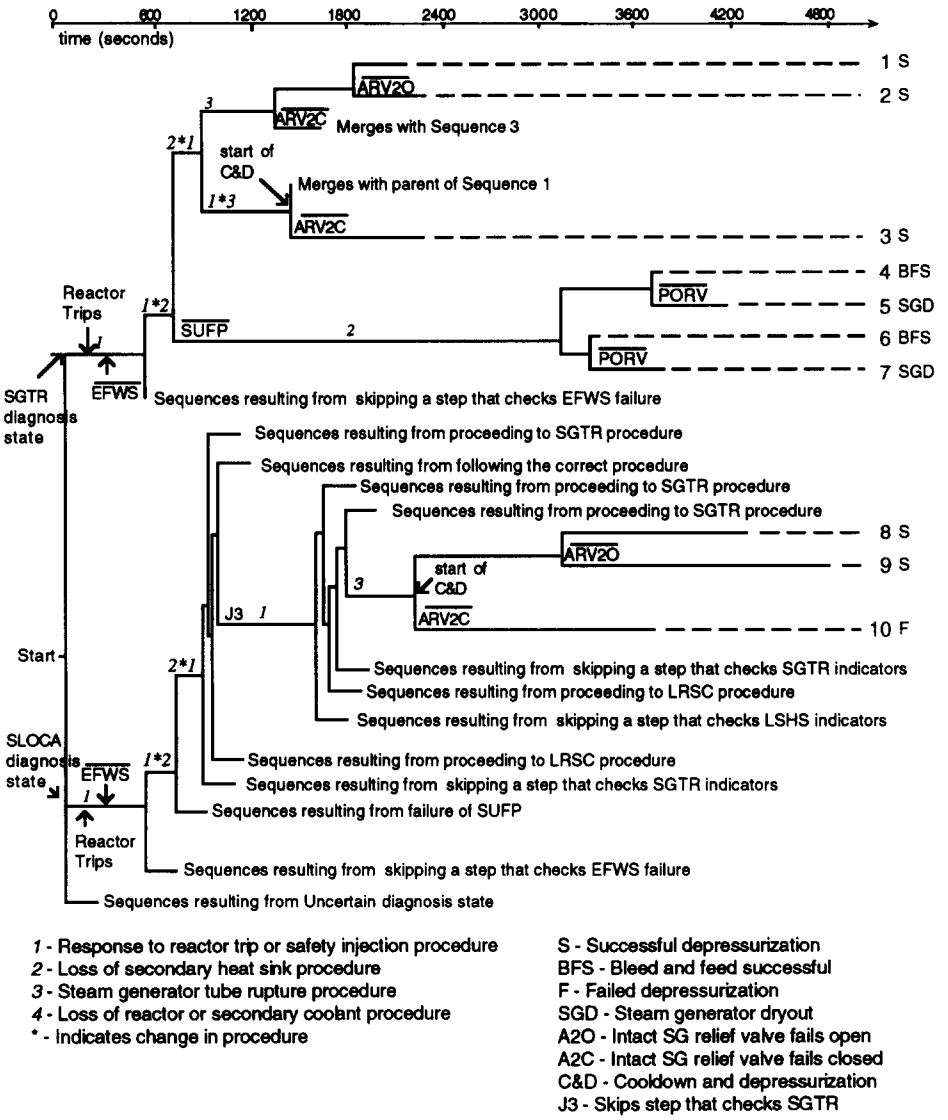

Fig. 3. Portion of SGTR dynamic event tree with failed EWFS.

4.2 Practicality of DETAM

One of the important requirements for a dynamic scenario analysis methodology is that its results be manageable (in terms of size) and understandable. Figure 3 shows the dynamic event tree for a scenario involving the failure of EWFS (Run 4). In principle, with 128 possible hardware states (seven binary systems plus the EWFS assumed failed), 324 possible crew planning states, and 2304 possible crew diagnosis states, there are approximately $9{\cdot}6 \times 10^7$ distinct possible plant states to which each plant state can transfer at each time step. Naturally, the total number of possible scenarios increases geometrically as the number of time steps increases. The relatively small size of the tree shown in Fig. 3 (52 scenarios are represented) is attributable to the modeling assumptions and cut-off frequencies used. Assumptions involving the neglect of the runtime failures of hardware systems, the treatment of crew behaviour as being heavily influenced by available procedures, the high level treatment of operator diagnosis states, and the neglect of instrumentation failures, lead to context-dependent branching rules that trim the analysis considerably (the entire problem is represented using roughly 200 scenarios). The cut-off frequencies are quite low (recall that the sequences quantified are all conditioned on the occurrence of SGTR; many are further conditioned on the failure of a hardware system as well), but also have a significant effect on reducing the tree size.

4.3 DETAM capabilities

The DETAM runs performed demonstrate a number of capabilities for dynamic scenario analysis not shared by the conventional event tree/fault tree methodology. One such capability, inherent in the

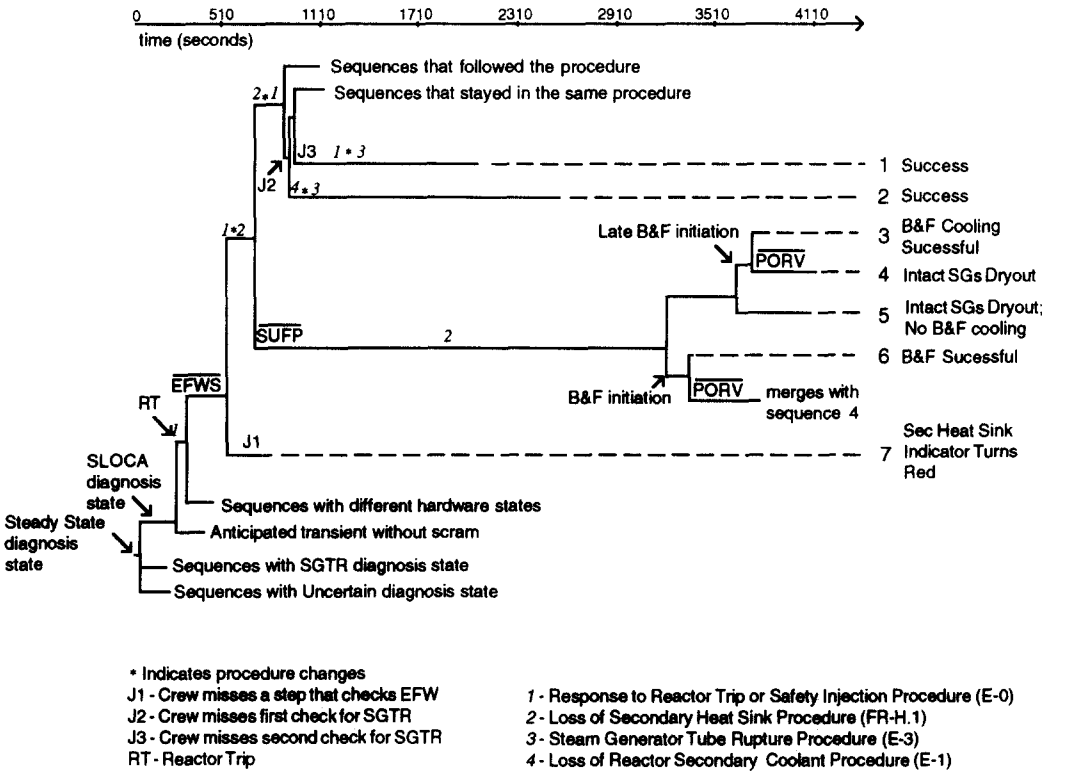

Fig. 4. Portion of dynamic event tree illustrating different errors and behaviors.

DETAM approach, is the explicit treatment of contextual information (e.g., process variables, current procedure step) needed to assess the likelihood of various operator actions. Two other important capabilities are the ability to represent a wide variety of operator behaviors and the ability to model the consequences of operator actions.

The dynamic event tree treatment of the following errors and behaviors is illustrated in Fig. 4:

- Improper diagnosis (e.g., SLOCA instead of SGTR)
- Overly quick procedure following (e.g., skipping of procedure steps)
- Overly slow procedure following (e.g., delay of bleed and feed initiation)
- Following of inappropriate procedure (e.g., E-1 instead of E-3)
- Looping

The 'looping' behavior pattern refers to situations where the cues needed to allow transfer to a new procedure are not available (or are not observed by the operator crew). In such cases, it is assumed in the analysis that the operator crew remains in the procedure with no chance of escape. Sequence 7 represents a situation where looping could occur if the secondary heat sink safety function indicator does not alarm; here, the procedures are written in such a way that a crew blindly following procedures will remain in the current procedure until steam generator dryout occurs. Of course, the assumption that the operators will not exit the loop (at least until an absorbing state is reached) is somewhat unrealistic. More detailed models (statistical or causal) are needed to determine if and when loop-exiting occurs.

DETAM also allows the analyst to treat the so-called 'error of commission'. This error is closely associated with misdiagnosis errors, although the occurrence of a misdiagnosis does not always result in an error of commission. Since DETAM allows branching based on misdiagnosis, it can account for any erroneous action, e.g. turning off the HPIS when it is actually needed, that occurs after the initial misdiagnosis. Put another way, DETAM provides a framework for the analyst to employ a causal model for errors of commission. This will aid the quantification of such errors, and will also aid the development of specific schemes to reduce the impact of the more significant errors.

More generally, DETAM treats a spectrum of detailed operator behaviors and actions (state changes), some of which may be classified as 'successes', and some of which may be classified as 'failures'. This treatment enables a causal (although not necessarily deterministic) analysis of the consequences of the remainder of the sequence following a decision or action. Consider, for example, the middle portion of Fig. 3. This structure represents the consequences of a misdiagnosis—the operators believe that the plant is undergonig an SLOCA accident,

rather than an SGTR accident. Not surprisingly, this portion of the tree differs significantly from that following a correct diagnosis (the upper part of Fig. 3). Further examination shows that situations can arise where the hardware states of two different scenarios can be identical, yet the two scenarios lead to different end states.

4.4 Comparison of DETAM and conventional PRA results

Because of the differences in scope and sequence modeling assumptions between the DETAM and conventional SGTR PRA analyses, and because there is considerable uncertainty in the detailed branching frequency assignments made in the DETAM analysis, a direct quantitative comparison of results is difficult. This section provides a limited comparison of the DETAM, Seabrook,[25] and Sequoyah[26] analysis results. Differences in selected endstate and partial sequence frequencies are discussed.

The Seabrook study employs a three-stage event tree model. The first stage models the support systems (e.g., electric power, service water) and the second state models the early frontline system and operating crew response to SGTR. Depending on the plant condition after early response, the third stage evaluates either the plant response (if recirculation is required) or the operability of the containment systems (if core melt occurs). The frontline early event tree has 16 top events, some of which are purely hardware-related while others involve both hardware and operating crew response. Top event OR (Operator Controls Break Flow) provides an example of the latter. If all systems respond as designed, OR entails the opening of the intact generators' atmospheric relief valves to cool down the primary coolant, the closing of relief valves when the primary temperature reaches the desired level, and pressurizer spray actuation to depressurize the primary system to the ruptured steam generator pressure. Otherwise, OR involves bleed and feed cooling.

The Sequoyah study uses the 'fault tree linking method'. In this approach, the top events are defined somewhat more broadly than those in the Seabrook tree; single top events in the Sequoyah model can represent a number of top events in the Seabrook model. Furthermore, the Sequoyah tree includes support system response (as modeled by the system fault trees for the top events), early frontline support system response, and long term frontline system response. Reference 26 employs an intentionally simple model, and models less of the plant dynamic response than does Ref. 25. For example, regardless of the status of the top events, one set of time windows is used to establish the frequency of failure of critical safety functions or operator actions. Furthermore, bleed and feed cooling is not treated.

Table 6 shows the likelihoods of two undesired endstates and the dominant sequences leading to those endstates predicted by the DETAM, Seabrook, and Sequoyah models. The two endstates are ruptured steam generator overfill and failure of bleed and feed cooling. The former state leads to the release of radioactive coolant to the environment. On the other hand, it does not guarantee the occurrence of core damage. The latter state does eventually lead to core damage (unless other sources of heat removal are found).

Comparing the dominant sequences leading to the

Table 6. Comparison of conventional and dynamic event tree endstate conditional frequencies

Endstate	Study	Conditional frequency[a]	Dominant scenario description
Faulted SG overfill and release	Seabrook[25]	5·0E − 2[b]	OR (Failure to control break flow), SL (Secondary leak to atmosphere)
	Sequoyah[26]	1·1E − 2/1·6E − 4[b]	O_d (Failure to cooldown and depressurize), Q_s (Loss of faulted steam generator integrity)
	DETAM	4·3E − 3	Correct diagnosis as SGTR, relief valves on intact SGs fail to open, operators prematurely end depressurization to avoid pressurizer overfill
Bleed and feed cooling failure	Seabrook[25]	2·2E − 5[b]	EF (Emergency feedwater unavailable), OR (Failure to control break flow)
	Sequoyah[26]	5·3E − 4/4·2E − 5[b]	L (Emergency feedwater unavailable)
	DETAM	4·8E − 7	Correct diagnosis as SGTR, EFWS fails, operators initiate bleed and feed cooling but PORV fails to open

[a]Endstate conditional frequencies are conditioned on the occurrence of SGTR.
[b]Value includes results of recovery analysis.

steam generator overfill endstate, the Seabrook analysis identifies the failure to control break flow (top event OR) and the occurrence of a secondary side leak (top event SL), whereas the Sequoyah analysis identifies the failure to cool down and depressurize (top event O_d) followed by the loss of steam generator integrity (top event Q_s). Both of these sequences are quite similar. Note, however, that, although the Seabrook analysis predicts a higher frequency of occurrence, it does not assume that core damage necessarily ensues. On the other hand, the Sequoyah analysis assumes (with substantially lower frequency when recovery actions are included) that core damage will occur in this situation. The DETAM analysis produces a dominant sequence that is similar in a broad sense to those treated in the Seabrook and Sequoyah analyses, but somewhat different in detail. This sequence involves correct diagnosis of SGTR, successful identification and early isolation of the ruptured steam generator (SG), failure of the intact SG atmospheric relief valves to open on demand, and procedure-directed throttling of high pressure injection to prevent the pressurizer from filling up. In this scenario, the ruptured steam generator overfills because the primary coolant system has not been sufficiently depressurized.

In the case of the unsuccessful bleed and feed cooling end state, the Seabrook analysis predicts a dominant sequence involving the failures of emergency feedwater (EF) and bleed and feed cooling (OR), while the dominant Sequoyah sequence only includes the failure of emergency feedwater (L). Reference 26 states that bleed and feed cooling results in primary pressure increase and thus counteracts efforts to control the break flow; therefore, that study does not consider the possible success of bleed and feed cooling. The dominant DETAM sequence for this endstate involves failure of emergency feedwater and operator failure to initiate bleed and feed cooling in time; this scenario represents one subscenario of the Seabrook scenario.

Table 6 indicates that although the qualitative scenario descriptions are at least roughly comparable, the quantitative DETAM risk predictions appear to be generally lower than those from the conventional analyses. In the case of the more severe endstate, unsuccessful bleed and feed cooling, the DETAM frequency predictions are lower by two orders of magnitude. In the case of the steam generator overfill endstate, the endstate frequency is higher than that resulting from the Sequoyah analysis including recovery actions. However, as argued in Ref. 25, even after this endstate is reached, a considerable amount of time is available to attempt recovery; additional failures in the long term response of the plant to the accident are required before core damage can result.

The reduced conservatism in the DETAM results is not surprising, given that the DETAM analysis explicitly treats procedure-directed 'recovery actions' that may not be included in conventional analyses. However, it cannot be expected that a DETAM analysis will always yield lower results than those provided by conventional event trees. In fact, Ref. 13 provides some examples where the frequencies of partial sequences, as predicted by DETAM, are higher than those obtained in the conventional analyses. Indeed, as pointed out in Section 1, the concern motivating the development of DETAM is that conventional analyses may, in some situations, not correctly (or even conservatively) treat dependencies between multiple failure events.

4.5 Other results

Although the SGTR analysis documented in this paper is constructed primarily to demonstrate the DETAM approach, and although the demonstration model has a number of weaknesses that affect the accuracy of its predictions, a number of useful results are obtained from this analysis. These results cover (a) the current operating procedures pertaining to SGTR, (b) the importance of instrumentation in this accident, and (c) dependencies between conventional SGTR event tree top events.

4.5.1 SGTR procedures

In a DETAM application to accident analysis, it is necessary for the analyst to explicitly model the written procedures. This modeling provides the primary basis for the detailed definitions of the possible crew planning states and the transitions between states. As a byproduct of the modeling process, weaknesses in current procedures can be identified.

In the case of the procedures reviewed in the analysis, it appears that the provision of redundancy in a few spots in the procedures, through the addition of backup checks for key symptoms and of additional procedure transfer steps, could improve procedure effectiveness. A DETAM analysis can identify if changes are needed, where the changes should be made, and if the added redundancy provided by these changes outweighs the associated negative effects (e.g., possible increases in crew response times). Compared to a detailed procedure review, a DETAM analysis can (in principle) provide quantitative measures of effectiveness; compared to a conventional human reliability analysis, DETAM can provide a fuller, more explicit context for evaluating procedures.

4.5.2 Instrumentation

Instrumentation, being the primary link between the operators and the plant, intuitively is an important

factor in the development of an accident scenario. Faulty or failed instrumentation could lead to an incorrect diagnosis of the plant condition and hence erroneous crew actions. For example, instrumentation readings serve as primary bases not only in selecting the procedure to follow but also in making decisions within a procedure (e.g., whether to initiate bleed and feed cooling or not). Despite this importance, instrumentation failures generally are not treated explicitly in conventional PRA studies.

Table 5 provides a comparison of the results obtained from Runs 2 and 3 and from Runs 4 and 5 (defined in Table 4) and indicates the quantitative impact of instrumentation failures. In both cases, the conditional frequency of successful cooldown and depressurization (given SGTR) drops and the conditional frequency of ruptured steam generator overfill increases when the RAM is failed. Note that in Run 5, the unavailable RAM also leads to the generation of new sequences.

Clearly, the analysis can be extended to treat more general sets of instrumentation failures. Thus, the dynamic event tree approach provides a useful framework for evaluating the risk significance of instrumentation.

4.5.3 Dependent failures

As discussed in Section 1, the identification of dependent system failures is key to quantitative risk assessment. The DETAM approach explicitly treats human and process variable related causal links between failure events. Thus, it can identify groups of dependent failures that are not necessarily treated by conventional event tree analyses.

For example, there is a two-way dependence between the actions associated with depressurizing the reactor coolant system (top events OR and O_d in the Seabrook and Sequoyah studies, respectively) and the integrity of the faulted steam generator (Seabrook and Sequoyah top events SL and Q_s). If the operators fail to depressurize the reactor coolant system, flow into the secondary side of the faulted steam generator will continue, increasing the likelihood that a steam generator relief valve will be challenged and will open. On the other hand, the relevant operating procedures require the operator crew to perform actions to isolate the ruptured steam generator prior to the actions for controlling the break flow. Moreover, failure to isolate the ruptured steam generator can affect the likelihood of a successful cooldown and depressurization. It is believed that in the Ginna event, faulty steam generator isolation actions led to complications and delays during depressurization.[27] The conventional event tree analyses treat the dependence of SL/Q_s (the following top events) on OR/O_d (the preceding top events), but not the dependence of OR/O_d on SL/Q_s. DETAM, by virtue of its simulation-based approach, treats the two-way dependence directly.

A more interesting example of a dependent failure group is provided by the earlier discussion on instrumentation failures. As stated earlier, the failure of the radiation alarm monitor (RAM) increases the difficulty of correctly diagnosing the SGTR, and increases the likelihood of faulted steam generator overfill. In other words, there is a link between the failures of the RAM and of the faulted steam generator atmospheric relief valves (considered as part of the top event SL in the Seabrook SGTR model, and as part of the top event Q_s in the Sequoyah SGTR model). Furthermore, when the emergency feedwater system is failed (Runs 4 and 5), the DETAM analysis predicts that the loss of the RAM increases the likelihood that the high pressure injection system (HPIS) will be turned off by the operators. This affects the Seabrook top event HP and the Sequoyah top event D_1 (these top events model the availability of the high pressure injection system).

This latter example indicates that the failures of RAM, SL/Q_s, and HP/D_1 are dependent. Because neither the Seabrook study nor the Sequoyah model the RAM, the direct links between the RAM and SL/Q_s and between the RAM and HP/D_1 are not treated. More significantly, the link between SL/Q_s and HP/D_1, which are now correlated through the RAM failure, is not treated. Thus, the DETAM analysis indeed can identify sources of dependency between event tree top events that are not modeled in current analyses.

5 CONCLUDING REMARKS

The key issue in nuclear power plant probabilistic accident scenario analysis is the treatment of dependencies between top event (e.g., system) failures. Improper treatment can lead to the incorrect screening of accident scenarios and inaccurate estimates of risk. The conventional event tree/fault tree methodology currently used in PRA studies is naturally suited for modeling common-cause initiating events, functionally coupled top events, and shared-equipment dependencies, but does not directly provide all of the information needed to handle other types of dependencies. In particular, the event tree/fault tree methodology, which does not simulate the dynamic response of the plant/operating crew system to an accident, does not explicitly treat process variables, operator states, detailed scenario history, or time. The DETAM approach, described in this paper, provides a potentially practical framework for treating these factors.

5.1 Advantages and disadvantages of DETAM

Three positive characteristics of the DETAM approach deserve emphasis. First, as discussed earlier, DETAM provides a more comprehensive definition of plant state than that provided by conventional event treets. Second, DETAM integrates an operator crew model with a plant physical model. As a result of these two characteristics, the environment in which operator decisions are made is modeled explicitly. DETAM accounts for the processes leading to crew actions, the actions themselves, and the consequences of these actions. Third, DETAM has a flexible, modular structure. This means that a DETAM model can be constructed (and improved) incrementally. It also means that the analyst can divide complex modeling tasks into more manageable parts.

The primary drawback with DETAM is a practical one: a considerable amount of effort is required to construct a dynamic event tree. Physical models must be developed (or adapted), operating procedures must be explicitly modeled, and branching frequencies must be estimated. Since the analysis results are sensitive to the accuracy of the physical model employed (modeling inaccuracies can lead to situations where the qualitative, as well as the quantitative, predictions of scenario development are wrong), the analyst needs to ensure that the models used are quite accurate.

It should be pointed out that the tasks required in a DETAM analysis are not very different from the tasks performed in the human reliability analysis portion of a conventional PRA. Plant physical models are often used to determine time windows and top event success criteria, and analysts must study the written procedures and training practices to develop an understanding of the crew behavior during the accident. The additional work in a DETAM analysis arises because DETAM requires that these issues (including such subjective ones as the operators' understanding of a scenario) be treated explicitly and formally within the framework of a dynamic event tree.

It should also be pointed out that DETAM, as a methodology, has a significant limitation in that it does not provide a causal model for operator behavior. Lacking such a model, it relies on the analyst to supply the likelihood of operator state transitions. The context supplied by DETAM is intended to aid the assessment, and to prompt the analyst to ask appropriate questions. However, it cannot guarantee that failures not previously experienced or explicitly identified beforehand will be treated in an analysis. Advanced operator/crew models such as those described in Refs 15 and 16, with further development, could be useful in addressing this weakness.

5.2 Potential applications

In principle, dynamic event trees can be used in place of conventional event trees to analyze all possible accident scenarios in nuclear power plant risk assessments. In practice, the implementation tools required (e.g., the operator state transition models for all scenarios) are not ready for immediate application. Moreover, it is not clear that future developments of DETAM should be aimed at replacing event tree analysis. Dynamics do not play an important role (and need not be explicitly analyzed) in all accident scenarios. Conventional event trees handle a wide variety of modeling issues, such as the impact of support system losses on frontline system performance, that would be computationally inefficient to include in a DETAM analysis. (Note that there are some scenarios involving support system failures which may require dynamic treatment, e.g. station blackout. Improved computational methods are probably needed to employ DETAM in these situations.)

Thus, DETAM should be viewed as a tool to supplement the current, hardware-based event tree models for accident scenarios, rather than as a replacement. As a supplementary tool, DETAM can be used to support current human reliability analyses (e.g., by providing scenario-sensitive distributions for the time available to perform actions and for the time actually required to perform these actions, by providing a 'what-if' capability for human reliability analysis), to identify situations where qualitatively different scenarios can result despite the same hardware failures, to identify less than obvious sources of dependencies between top events, and even to provide scenario-dependent failure probabilities (conditional split fractions) for selected top events. DETAM also appears to be well suited for assessing the risk associated with the use of completely automatic control systems, since the definition of operator crew states would not be an issue. (In this situation, the approach would be virtually identical with DYLAM and the Markov model described in Ref. 10.)

Aside from PRA applications, DETAM can be used to evaluate operating procedures. It can be used to determine if there is sufficient time to follow the as-written procedures, and if the procedures handle all risk-significant scenarios. The difference between a DETAM evaluation and a conventional evaluation, of course, is that the DETAM evaluation delineates all possible scenarios (with significant likelihood), rather than a few nominal ones.

DETAM might also be useful for analysis of severe accidents progressing beyond the core damage stage and for devising strategies to deal with these

accidents. Many of the issues addressed in the currently used Accident Progression Event Trees[8] belong to the general categories of methodological issues raised in this report. An application of DETAM could provide the framework needed to better integrate operator actions into the analysis, and to identify improved, scenario-dependent courses of action.

5.3 Areas for improvement

The DETAM application discussed in this paper is aimed at demonstrating the potential practicality of DETAM. The demonstration model, however, employs simplifications that prevent the treatment of a full core damage scenario, sometimes lead to predicted scenario evolutions that differ qualitatively from those of the actual scenarios, and prevent treatment of some potentially significant factors (e.g,, the dynamic development of the crew quality state). To address these simplifications, additional work is needed in the following areas:

- the plant physical model
- The operator model
- the plant instrumentation model
- the treatment of uncertainties
- methods to limit the tree size

The plant physical model currently used is adequate for predicting the primary side response to SGTR in the early stages of the accident. Once saturation is reached, the model is no longer satisfactory. The model is also not very good at predicting the secondary side response. As a result, the steam generator pressure rise and resulting challenges to the atmospheric relief valves (which could stick open, leading to a potential containment bypass scenario) are underestimated. Better physical models are available; work is needed to integrate these models into the dynamic event tree analysis.

The finite-state crew model employed by DETAM is intermediate between the current human reliability models used in current PRAs and advanced crew and cognitive models currently being developed. To make the model more practical for routine analysis, work on operationalizing the different crew states (and their transitions) needs to be done. Further, work is needed to operationalize the crew quality state. It is important that a multidisciplinary team be involved in order to assure that the state definitions adequately reflect current knowledge.[28]

Regarding plant instrumentation, the current model only treats the effect of a failed secondary side radiation alarm monitor. Because the dynamic event tree method explicitly treats the dynamic response of the operators to available indications, the area of instrumentation should be one where DETAM is visibly superior to conventional methods. Additional examination of scenarios involving failed instrumentation is needed to determine if this expectation is indeed correct.

The model for SGTR described in this report does not treat uncertainties in the predictions of its simplistic four-node physical model. Given that a DETAM analysis requires a fast-running thermal–hydraulic simulation, it is likely that any physical model that can be practically used will yield predictions that have significant uncertainties. Reference 29 discusses uncertainties in thermal–hydraulic models for accident progression; Ref. 30 discusses a Bayesian approach to quantify modeling uncertainties. These ideas and methods need to be incorporated in the dynamic scenario analysis. Of course, state-of-knowledge uncertainties in other parts of the model (e.g., in the operator state transition rates) need to be addressed as well. (The dynamic event tree branchings treat stochastic uncertainties).

Finally, when the more detailed models described above are implemented, it is likely that more powerful methods for grouping and truncating scenarios will be required. An extension of the cutset-based variance reduction methodology proposed in Ref. 12 for Monte Carlo simulation could be quite useful.

ACKNOWLEDGMENTS

The authors would like to thank N. Rasmussen, Y. Huang, T. Ryan, V. Dang, and the paper reviewers for their useful comments. Special thanks are given to S. Kao, M. Boyle and New Hampshire Yankee for their generous technical support. This paper was prepared with the support of the US Nuclear Regulatory Commission (NRC) under grant NRC-04-88-143. The opinions, findings, conclusions and recommendations expressed herein are those of the authors and do not necessarily reflect the view of the NRC.

REFERENCES

1. US Nuclear Regulatory Commission, *Reactor Safety Study*, WASH-1400, NUREG-75/014, 1975.
2. Dougherty, E. M., Human reliability analysis—where shouldst thou turn, Guest Editorial, *Reliability Engineering and System Safety*, **29** (1990) 283–99.
3. Apostolakis, G. & Chu, T. L., Time-dependent accident sequences including human actions, *Nuclear Technology*, **64** (1984) 115–26.
4. Amendola, A., Accident sequence dynamic simulation versus event trees, in *Accident Sequence Modeling: Human Actions, System Response, Intelligent Decision*

Support, ed. G. Apostolakis, G. Mancini & P. Kafka, Elsevier Applied Science, London, 1988.
5. Siu, N., Dynamic accident sequence analysis in PRA: a comment on 'Human reliability analysis—where shouldst thou turn', *Reliability Engineering and System Safety*, **29** (1990) 359–64.
6. Bley, D. C., Buttemer, D. R. & Stetkar, J. W., Light Water Reactor sequence timing: its significance to probabilistic safety assessment modeling, *Reliability Engineering and System Safety*, **22** (1988) 3–22.
7. Hsu, C. J. *et al.*, *A Probabilistic Evaluation of the Safety of Babcock & Wilcox Nuclear Reactor Power Plants with Emphasis on Historically Observed Operational Events*, NUREG/CR-5206, 1988.
8. US Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, January 1991.
9. Cacciabue, P. C., Amendola, A. & Cojazzi, G., Dynamic logical analytical methodology versus fault tree: the case study of the auxiliary feedwater system of a nuclear power plant, *Nuclear Technology*, **74** (1986) 195–208.
10. Devooght, J. & Smidts, C., A framework for time dependent interaction between operator and reactor during a transient involving human error, *Proceedings of PSA'89: International Topical Meeting on Probability, Reliability, and Safety Assessment*, Pittsburgh, PA, 2–7 April, 1989, pp. 936–42.
11. Cacciabue, P. C., Mancini, G. & Bersini, U. A model of operator behaviour for man–machine system simulation, *Automatica*, **26** (1990) 1025–34.
12. Marseguerra, M. & Zio, E., Non-linear Monte Carlo reliability analysis with biasing towards top event, *Reliability Engineering and System Safety*, **40** (1993) 31–42.
13. Acosta, C. G. & Siu, N., *Dynamic Event Tree Analysis Method (DETAM) for Accident Sequence Analysis*, MITNE-295, Massachusetts Institute of Technology, October 1991.
14. Itoh, J. *et al.*, Cognitive task analysis of nuclear power plant operators for man–machine interface design, *Proceedings of the ANS Topical Meeting on Advances in Human Factors Research on Man/Computer Interactions: Nuclear and Beyond*, Nashville, TN, 10–14 June, 1990, pp. 96–102.
15. Huang, Y. *et al.*, *Modeling Control Room Crews in Accident Sequence Analysis*, MITNE-296, Massachusetts Institute of Technology, December 1991.
16. Woods, D. D., Pople, H. E., Jr, & Roth, E. M., *The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability*, NUREG/CR-5213, June 1990.
17. Woods, D. D., Roth, E. M. & Pople, H., Jr, Modeling human intention formation for human reliability assessment, *Reliability Engineering and System Safety*, **22** (1988) 169–200.
18. Kao, S., PRISM: An integrated RCS and steam generator simulation model, *Proceedings of the ANS International Topical Meeting on Advances in Mathematics, Computations, and Reactor Physics*, Pittsburgh, PA, 28 April–1 May, 1991.
19. *Seabrook Nuclear Plant Station Final Safety Analysis Report, Amendment 55*, New Hampshire Yankee, July 1985.
20. Hall, R. E., Fragola, J. R. & Wreathall, J., *Post-Event Human Decision Errors: Operator Action Trees/Time Reliability Correlation*, NUREG/CR-3010, 1982.
21. Wakefield, D. J., Application of the human cognitive reliability model and confusion matrix approach in a probabilistic risk assessment, *Reliability Engineering and System Safety*, **22** (1988) 295–312.
22. Nakada, K., *et al.*, A method of state transition analysis under system interactions: an analysis of a shutdown heat removal system, *Nuclear Technology*, **82** (1988) 132–46.
23. Kahneman, D., Slovic, P. & Tversky, A. (eds), *Judgment under Uncertainty: Heuristics and Biases*, Cambridge University Press, Cambridge, 1982.
24. Swain, A., *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, 1987.
25. Pickard, Lowe & Garrick, Inc., *Seabrook Station Probabilistic Safety Assessment*, prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, December 1983.
26. Bertucio, R. C. & Brown, S. R., *Analysis of Core Damage Frequency: Sequoyah, Unit 1 Internal Events*, NUREG.CR-4550, SAND86-2084, Vol. 5, Rev. 1, Parts 1 and 2, April 1990.
27. NRC compares the Ginna actions with basic Westinghouse guidance, *Inside NRC*, **4**(3) (8 February 1982) 2–4.
28. Ryan, T., A task analysis-linked approach for integrating the human factor in reliability assessments of nuclear power plants, *Reliability Engineering and System Safety*, **22** (1988) 219–34.
29. Boyack, B. E., *et al.*, Quantifying reactor safety margins, part I: an overview of the code scaling, applicability, and uncertainty evaluation methodology, *Nuclear Engineering and Design*, **119** (1990) 1–15.
30. Siu, N., Karydas, D. & Temple, J., Bayesian assessment of modeling uncertainty: application to fire risk assessment, *Analysis and Management of Uncertainty: Theory and Application*, ed. B. M. Ayyub, M. M. Gupta & L. N. Kanal, Elsevier, North-Holland, 1992.
31. Gregory, J. J. *et al.*, *Evaluation of Severe Accident Risks: Sequoyah, Unit 1*, NUREG/CR-4551, SAND86-1309, Vol. 5, Rev. 1, Part 1, December 1990.