Control Room Fire Analysis : A Multidisciplinary Problem

Dennis C. BLEY
PLG, Newport Beach, CA USA
Nathan O. SIU
Massachusetts Institute of Technology, Cambridge, MA USA

ABSTRACT

A class of problems that has received little attention in the nuclear plant PSA and operations communities involves dynamic human actions that cannot be neatly broken down into a few discrete possibilities. Control room fires present an excellent example. Several past attempts at modeling such events are reviewed and found wanting. An integrated approach to writing new procedures and analyzing control room fires is proposed that may have wide applicability to the entire class of problems.

1 INTRODUCTION

This paper describes multiple versions of an existing fire analysis. Together, these versions present the range of approaches in current PSA. Our plans and suggestions for the future are described.

Fires in the control room involve conflicting considerations. The control room, as the nerve center of the plant, is continually manned and houses the bulk of the instrumentation and controls. Thus, fires, once started, are unlikely to propagate unnoticed. On the other hand, they can do significant damage to our ability to control and monitor the plant. Procedures have been written to assist operators in dealing with very severe fires that force evacuation of the control room but offer little guidance for the variety of more realistic fires that affect limited areas and impair operations. Procedure writers have not covered, and probably cannot cover, the full range of possible fire scenarios. However, risk analysts should consider all possibilities.

Analysis of the risk due to possible control room fire scenarios requires a mix of PSA talents--knowledge of plant design and operations, systems analysis, fire analysis, and human reliability analysis. In the following section, several versions of a control room fire analysis are reviewed in light of these criteria.

2 REVIEW OF EXISTING ANALYSES

The control room fire analysis begins with a screening task called the spatial interactions analysis (PLG, 1983). The two-step screening analysis identifies physical interactions among various power plant hazards. In the first step, the plant is broken down into fire areas, and each area is examined under the assumption that a fire could disable all equipment and cables within an area. For scenarios that have any significant chance of leading to core

SMiRT 11 Transactions Vol. M (August 1991) Tokyo, Japan, © 1991

damage under the first screen, the second step considers the equipment layout, cable routing and existing deterministic fire analysis to generate geometry and severity factors to determine the extent of equipment damage by the fire scenario. The scenario is screened from further study unless the equipment damage could lead to core damage not bounded by other causes of equipment damage, or if operator recovery action is required to prevent core damage.

The fire analysis we reviewed was performed for a Westinghouse PWR, and two of the key control room fire scenarios involved fires in panels that caused a loss of component cooling water (CCW). Such scenarios can lead to failure of reactor coolant pump (RCP) seal injection and thermal barrier cooling, and then progress to a seal LOCA with no high pressure injection. The relevant operator actions are to trip the RCPs (desirable, delaying the LOCA) and to restore CCW before core damage (necessary).

The analysis extends the screened fire scenarios by applying the method of PLG (1983).

Original Analysis. The first three factors were defined by the screening analysis. Suppression was conservatively ignored, and the operator actions were analyzed in a summary fashion. The human reliability analysis assumed that the control room would be evacuated and then asked if the operators would trip the reactor coolant pumps from the switchgear and restore CCW from the hot shutdown panel. The resulting quantification, based on many hidden assumptions, found that the scenarios were not significant (about 1×10^{-6} per year) compared to others.

Questions and Suggested Results. Reviewers of the analysis correctly pointed out that such fires might take some time before they would disable CCW, and if the operators had already evacuated the control room, they would have no immediate warning of the loss of CCW from the hot shutdown panel. They recognized that to assume guaranteed failure of the operators for all fires was overly pessimistic and suggested that perhaps only 1 in 10 such fires might require evacuation, implying a frequency of over 1×10^{-4}. The plant owner began thinking harder about the scenario and suggested including additional geometry factors to account for separation of panels and some credit for manual fire suppression.

Revised Analysis. On further reflection, the analysts developed an event sequence model that allowed for manual suppression, the chance that the control room remains habitable and, if not, the chance that CCW would be lost before evacuation, thus alerting the operators to the need to protect the RCPs. The frequency associated with the revised analysis was not so high as to be a dominant contributor.

Discussions indicated that while procedures were written to evacuate the control room when it becomes "uninhabitable," operators might evacuate in stages, depending on the dynamics of the fire: shifting operations to the hot shutdown panel, as required, but trying to maintain overall control from the much better-instrumented control room. In addition, recognizing that a fire in the vital electrical panel or the CCW panel could lead to RCP seal problems, they might observe CCW more closely or even trip RCPs in anticipation of a loss. However, no detailed analysis of the dynamic evolution of the scenarios was attempted, and the procedures have not been modified.

The three versions of the fire analysis reviewed fall short in one or more of the following areas. Fire analysts often oversimplify the fire scenarios to permit more straightforward calculations. Systems analysts ignore details of sequence timing affected by specific decisions about transferring control to alternate shutdown panels. Human factors analysts may not completely understand technical difficulties associated with abandoning the control room and the psychological factors arguing against it. All may be too willing to ignore the detailed dynamic effects that really control the evolution of control room fire scenarios.

3 A NEW INTEGRATED APPROACH

Severe control room fire scenarios involve three parallel, interacting stochastic processes: (1) the fire growth process, (2) the response of the plant, and (3) the operator crew actions.

The fire growth process causes damage to a variety of components distributed over time. This may lead to the loss of safety systems, spurious actuation of equipment, and faulty instrument readings. Furthermore, the growth process can create a smoky, hot environment and uncertainly with respect to the eventual extent of fire damage that limits the effectiveness of the operators in responding to the above problems. The physical plant, while not directly affected by the fire, responds to control signals (or loss of these signals) induced by the fire or by the operators in response to the fire. The operating crew must both keep the plant control and deal with the fire. In extreme cases, they may be forced to abandon the control room and use the more limited auxiliary shutdown panels outside of the control room. The results of interactions among these processes over the course of a scenario are difficult to predict *a priori*, and need to be dealt with explicitly.

Current fire risk analyses ignore, to a large extent, the interactions between the three processes mentioned above. In these studies, the fire growth process is modeled in order to determine the likelihood that certain "critical" components are damaged. Credit is taken for suppression efforts by the crew. Given that the critical components are damaged, the crew and plant response to the loss of components are then modeled. In other words, the effect of fire is treated as an initial shock to the system; i.e., in much the same manner as that used to treat hardware-caused initiating events.

The problem with this approach is that the time scale for fire growth can be of the same order as that for the operator actions to shut down the plant. (In many risk studies, damage is predicted some tens of minutes after fire initiation.) As a direct consequence, the possibility that a critical component may be damaged after the real need for that component has passed is not treated. There are potentially significant nonconservative consequences as well. For example, the fire suppression efforts of the operators are included in the growth analysis. Thus, the associated diversion of resources away from plant shutdown operations is not accounted for (due to the separation of the growth process from the plant and crew response processes). As another example, the current approach implies that a known, fixed set of equipment is damaged prior to the initiation of plant shutdown operations. In reality, there may be considerable uncertainty, as the fire damages components and creates a hazardous environment at the same time the operators are attempting to control the plant. The need for an integrated, dynamic model is apparent.

The general issue of modeling plant and crew dynamics in the context of an accident sequence analysis is discussed in Siu (1990). It is pointed out that in the case of complex scenarios, it is important to treat (in some manner) the operators' cognitive processes since these can provide a casual link between multiple failure events. It is also pointed out that two simulation-oriented dynamic analysis frameworks exist for integrating cognitive models into a PSA plant model.

The first approach, which has the potential for immediate use in the control room fire problem, uses dynamic event trees. A dynamic event tree is a multi-valued logic tree that models system evolution over time, rather than over top event state space. At discrete points in time, multiple branchings stemming from a single tree sequence may occur, depending on how the plant and operating crew change state. Siu and Acosta (1990) apply the dynamic event tree model to a steam generator tube rupture sequence, and show how operating crew behavior, as guided by emergency procedures, can be integrated into a PSA model.

Figure 1 illustrates the conceptual dynamic event tree implementation. (It is important to observe that 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 by this figure, the first task in the analysis is the deterministic computation of the plant process variables. The next task is to stop the branching process if an absorbing state, as defined by the needs of the analysis, is reached. Absorbing states can represent the successful completion of the scenario, or the achievement of a particular undesired physical state, e.g., primary coolant saturation. 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, or when operators start/stop equipment (based on the planning state from the previous time step.) Note that errors in executing actions are reflected at this step, rather than when determining the crew planning state. In the fourth through sixth tasks, branchings associated with the three substates defining the overall crew state (i.e., the crew diagnosis, quality, and planning states) are generated. The purpose of the seventh and eighth tasks is to limit the size of the analysis.

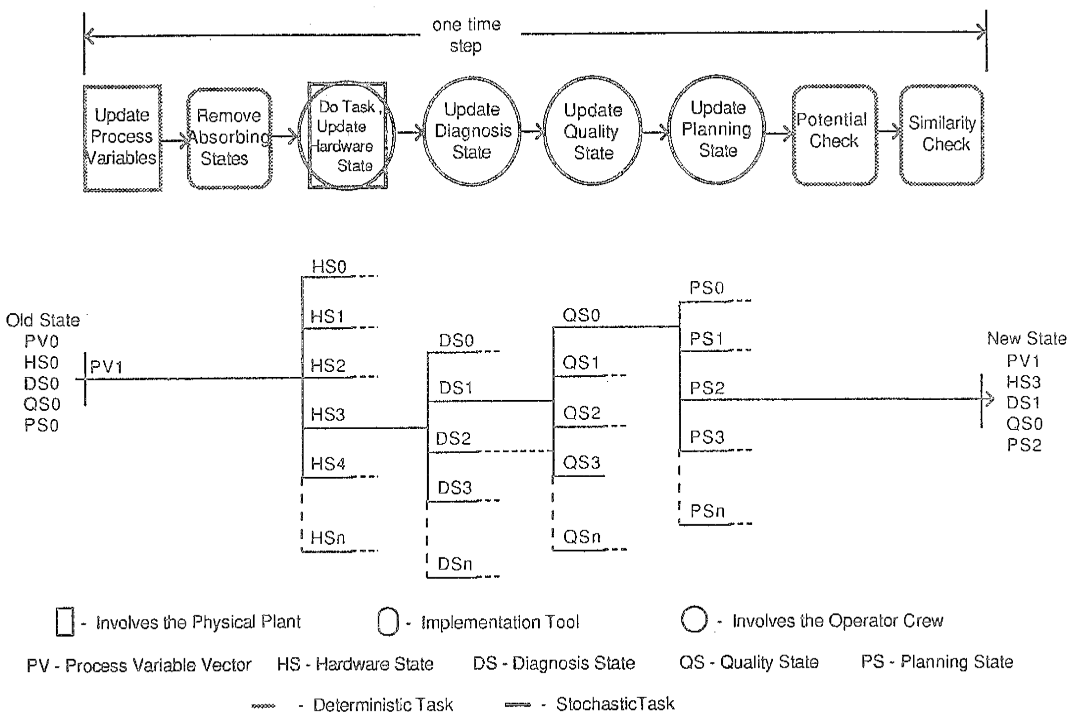

Fig. 1. Tasks Performed and a Sample State Transition during a Time Step

The definition of the crew state in terms of three substates is an important modeling step, and merits further discussion. The "diagnosis state" models the operators' understanding of the current accident situation. Although the representation of the diagnosis state can be quite complex, experimental observations/inferences of an operator's mental model during simulation exercises can 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 (Itoh et al., 1990).

The "quality state" models the internal condition of the crew; it is defined by such factors as time pressure, work load, and crew group structure. These factors can affect crew performance, and also can change over time. (Note that a variety of organizational factors (e.g., training) can affect crew performance but they are not explicitly included since they will remain static through the course of the scenario. These factors provide initial conditions for the analysis.)

The crew "planning state" models the actions planned by the operators. 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 also that the separate treatment of diagnosis and planning can lead to situations where the correct steps are taken, although an incorrect diagnosis has been made. (Such situations have been observed in simulator exercises.)

It is interesting to observe that the branching structure implied by Figure 1 bears some similarity with the operator action tree (OAT) model (e.g., Hall et al., 1982). Of course, the dynamic event tree employs this structure repetitively over time, and so the "re-diagnosis" branch in the OAT is accommodated by repetitive diagnoses in the dynamic event tree.

Although the model shown in Figure 1 was not developed with control room fires in mind, it can be modified without a great deal of conceptual difficulty to treat these scenarios. Some important modifications are: (a) a model for predicting fire growth must be integrated into the dynamic event tree (presumably in much the same manner as the thermal-hydraulic model for the plant), (b) the competing requirements for fire suppression and plant control must be treated, and (c) the effect on the crew members of the environmental effects caused by the fire must be treated. Note that the "quality state" can be a useful notion for treating the last two effects.

It should be noted that the most important drawback to the dynamic event tree approach, the possibility that the tree can grow in an unbounded fashion, need not be a problem in a control room fire analysis. In this case, the interesting dynamics may occur over a relatively short time span. (Chavez and Nowlen, 1988, describe a number of cabinet fire experiments in which room obscuration occurred roughly within 10 minutes of fire initiation.)

It has been previously mentioned that Siu (1990) identifies two frameworks for addressing the issue of scenario dynamics. The dynamic event tree approach is simple and appears to be adaptable to control room fires. However, as more advanced cognitive models for operators are developed (e.g., Huang et al., 1991), the simple definition of operating crew states will not be appropriate. In this case, the dynamic event tree approach is likely to lead to excessive branching; a more direct simulation approach, using Monte Carlo sampling, will be required. Of course, a primary disadvantage of a Monte Carlo approach is that intelligent sampling schemes are needed to treat rare events (Dang et al., 1991, and Vestrucci et al., 1991). A second disadvantage is that the scenario structural information traditionally provided by PSAs is not directly available from a straightforward Monte Carlo analysis. Thus, additional work is needed to determine the most important contributor to risk.

It should be pointed out that the key issue in the control room fire problem is not whether to use dynamic event trees or Monte Carlo simulation. Rather, it is to treat the scenario dynamics in an integrated fashion, including operator reasoning, which can strongly impact the course of the scenario, and the impact of the fire on the operators (which can affect their reasoning).

4 SUMMARY OF FINDINGS AND RECOMMENDATIONS

We find aspects of current analyses overly conservative and other aspects overly optimistic. Where the truth lies is unclear and may not be covered by existing uncertainty analyses. We believe that it is time to bring together an expert multidisciplinary team to study the control room fire problem. Ensuring full integration of the team will solve many problems of past analyses.

The fire analysis can be expanded to examine alternative progressions within the control room leading to impaired visibility and loss of limited equipment. Alternative procedures (such as shifting control of selected equipment to the alternate shutdown panel, while retaining overall direction of operations from the control room) can be evaluated. The key is to perform more thorough and dynamic human reliability analysis coupled with more realistic dynamic fire growth and systems analysis, as described in Section 3. Evaluation of the results of this multidisciplinary effort should indicate which of the enhancements are of real value and may indicate other aspects of existing PRAs that could be substantially improved by similar extensions of current analysis techniques.

REFERENCES

Pickard, Lowe and Garrick, Inc. [now PLG, Inc.] (1983). "Seabrook Station Probabilistic Safety Assessment," PLG-0300, prepared for Public Service of New Hampshire and Yankee Atomic Electric Company.

Siu, N.O., (1990). "Dynamic Accident Sequence Analysis in PRA: A Comment on Human Reliability Analysis--Where Shoulds't Thou Turn?", Reliability Engineering and System Safety, 29, 359-364.

Siu, N.O. and Acosta, C., (1990). "Modeling the Effects of Dependency Between Humans and Hardware on Overall System Performance," Proceedings of the 18th Water Reactor Safety Information Meeting, Rockville, MD.

Itoh, J., et al., (1990). "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.

Hall, R.E., Fragola, J.R., and Wreathall, J. (1982). "Post-Event Human Decision Errors: Operator Action Trees/Time Reliability Correlation," NUREG/CR-3010.

Chavez, J.M., and Nowlen, S.P., (1988). "An Experimental Investigation of Internally Ignited Fires in Nuclear Power Plant Control Cabinets, Part II: Room Effects Tests," NUREG/CR-4527, SAND86-0336, Vol. 2.

Huang, Y., et al., (1991). "Modeling Control Room Crews in Accident Sequence Analysis," to be published in Proceedings of 11th International Conference on Structural Mechanics in Reactor Technology, Tokyo, Japan.

Dang, V.N., Deoss, D.L., and Siu, N.O., (1991). "Event Simulation for Availability Analysis of Dynamic Systems," to be published in Proceedings of 11th International Conference on Structural Mechanics in Reactor Technology, Tokyo, Japan.

Vestrucci, P., Santucci, R., and Calern, R., (1991). "Monte Carlo Simulation of Crew Responses to Accident Sequences," Reliability Engineering and System Safety, 31, pp. 129-144.