CONF-8410142--11

HUMAN FACTORS REVIEW FOR SEVERE ACCIDENT SEQUENCE ANALYSIS (SASA)*

CONF-8410142--11

DE85 001670

P. A. Krois
P. M. Haas
J. J. Manning

Oak Ridge National Laboratory

C. R. Bovell

General Physics Corporation

Presentation To Be Made At:

12th Water Reactor Safety Information Meeting
National Bureau of Standards
Washington, D. C.

October 22-26, 1984

---

*Research sponsored by the U. S. Nuclear Regulatory Commission under DOE Interagency Agreement 40-550-75 with Martin Marietta Energy Systems, Inc. under Contract No. DE-AC05-840R21400 with the U. S. Department of Energy.

dsw

HUMAN FACTORS REVIEW FOR SEVERE ACCIDENT SEQUENCE ANALYSIS (SASA)*

P. A. Krois, P. M. Haas, J. J. Manning
Oak Ridge National Laboratory

C. R. Bovell
General Physics Corporation

Abstract

The paper will discuss work being conducted during this human factors review including: (1) support of the Severe Accident Sequence Analysis (SASA) Program based on an assessment of operator actions, and (2) development of a descriptive model of operator severe accident management. Research by SASA analysts on the Browns Ferry Unit One (BF1) anticipated transient without scram (ATWS) was supported through a concurrent assessment of operator performance to demonstrate contributions to SASA analyses from human factors data and methods. A descriptive model was developed called the Function Oriented Accident Management (FOAM) model, which serves as a structure for bridging human factors, operations, and engineering expertise and which is useful for identifying needs/deficiencies in the area of accident management.

The assessment of human factors issues related to ATWS required extensive coordination with SASA analysts. The analysis was consolidated primarily to six operator actions identified in the Emergency Procedure Guidelines (EPGs) as being the most critical to the accident sequence. These actions were assessed through simulator exercises, qualitative reviews, and quantitative human reliability analyses.

The FOAM descriptive model assumes as a starting point that multiple operator/system failures exceed the scope of procedures and necessitates a knowledge-based emergency response by the operators. The FOAM model provides a functionally-oriented structure for assembling human factors, operations, and engineering data and expertise into operator guidance for unconventional emergency responses to mitigate severe accident progression and avoid/minimize core degradation. Operators must also respond to potential radiological release beyond plant protective barriers, and this problem was addressed through detailed barrier diagrams identify potential fission product pathways along gaseous and liquid streams. Research needs in accident management and potential uses of the FOAM model are described.

---

*Research sponsored by the U. S. Nuclear Regulatory Commission under DOE Interagency Agreement 40-550-75 with Martin Marietta Energy Systems, Inc. under Contract No. DE-AC05-84OR21400 with the U. S. Department of Energy.

Introduction

The purposes of the project were to: (1) support the Severe Accident Sequence Analysis (SASA) Program with an assessment of operator actions, and (2) develop a descriptive model of operator severe accident management. Through coordination with SASA analysts studying the Browns Ferry Unit One (BF1) anticipated transient without scram (ATWS), part of this human factors study demonstrates contributions to accident sequence analysis from the assessment of factors shaping operator performance. A descriptive model was developed called the Function Oriented Accident Management (FOAM) model, which serves as a structure for bridging human factors, operations, and engineering data and expertise. The FOAM model is useful to identify needs and deficiencies in the area of accident management.

This paper describes both portions of the human factors work. Research supporting the SASA analysis is largely completed, and some preliminary results were previously reported in an appendix to the SASA ATWS report.[1] At the time of this writing, development of the descriptive model of accident management is in progress.

Assessment of Operator Actions During ATWS

The purpose of this section is to discuss the approach and results of both the qualitative and quantitative human factors assessments of operator actions during ATWS. A factor constraining this study was that the BF1 emergency procedures were being changed from event- to symptom-based procedures. The Emergency Procedures Guidelines (EPGs), developed by the BWR Owners Group, were undergoing review and adaptation by the Tennessee Valley Authority (TVA) for BF1. Both the SASA and human factors analyses were thus limited to using the best information available on the EPGs at the time the analyses were conducted. The section begins with a discussion of the EPGs and an identification of operator actions critical to the progression of ATWS. This is followed by a streamlined discussion of the qualitative review of these critical operator actions. In addition, a quantitative human reliability analysis (HRA) of some actions is presented.

The development of symptom-based procedures can be viewed as an attempt to reduce the cognitive workload of control room operators in diagnosing the type of transient. Through use of the EPGs during a transient, it is intended that operators verify and maintain the adequacy of critical safety functions. One advantage to an event-based procedure, however, is that operators may immediately relate causes and consequences of off-normal conditions and subsequently act directly to mitigate accident progression.

SASA analysts have made the recommendation in their ATWS report that the emergency procedures for ATWS be separated from the EPGs. The human factors analysis assisted in defining some of the problems operators may experience with the current structure of the EPGs. One of these problems is that certain operator actions called for in response to ATWS are substantially different from actions appropriate to virtually all other accidents. Some of these actions are also contrary to operational practices on which operators are trained. One example related to ATWS is the instruction in the EPGs to lower and maintain vessel level at the top of the fuel in order to reduce power. For all other accidents, low vessel level would be an off-normal condition and the EPGs would instruct operators to restore vessel level to within more acceptable bounds. SASA analysts noted their assumptions that the signature of ATWS is so distinguishable that operators would quickly diagnose the event, and that a separate ATWS emergency procedure would expedite operator response.

From a human factors standpoint, the structure of the EPGs presents some difficulties for operators in relation to ATWS. However, the solution proposed by SASA analysts to separate those instructions relevant solely to ATWS may or may not be entirely satisfactory. Operator performance during a transient would be based on several factors including training and operator aids, such as the safty parameter display system (SPDS), in addition to procedures. Currently, the SPDS at BF1 is in the design stage of development. These factors and others should be considered across a range of accidents to optimally guide operator response before deciding to restructure procedures in order to address problems related to one specific accident sequence.

Rather than assess operator actions throughout the ATWS, the analysis was consolidated to only those operator actions in the EPGs judged to be most critical to the accident sequence. The identification and selection of critical operator actions was coordinated with SASA analysts in response to their concerns with certain actions required by the EPGs. Inputs to the selection process included: (1) examination of the EPGs, (2) consideration of operator actions included in computer codes used for accident sequence analysis, (3) review of operator actions observed during simulator exercises conducted on perturbations of ATWS, and (4) review of an Operator Action Event Tree (OAET) developed for ATWS and based on the EPGs.[2] This OAET was modified based on input from SASA and operations personnel, and is shown in Fig. 1a.

Six operator actions were judged as being critical to the ATWS sequence. These actions included:

(1) Manual selection and insertion of individual control rods given complete failure to scram.

(2) Verification of conditions for use of the standby liquid control (SLC) system and initiation of poison injection into the reactor vessel.

(3) Initiation of pressure suppression pool (PSP) cooling through the residual heat removal (RHR) system.

(4) Operator control preventing overpressurization of the reactor vessel by manually operating safety relief valves (SRVs) before pressure setpoints are reached for automatic SRV actuation.

(5) Operator control of coolant injection systems in order to lower and maintain reactor vessel water level at the top of active fuel.

(6) Emergency depressurization of the reactor vessel in accordance with the PSP heat capacity temperature curve followed by control of low pressure injection.

Simulator exercises were conducted as part of this study to provide data to the human factors and SASA analyses. Exercises were videotaped to provide a record of operator actions and the videotapes were subsequently used in the task analysis supporting the HRA. Exercises were held on two occasions using two BWR SRO-instructors as operators.

The qualitative review was based on instructors' comments and analysts' observations resulting from simulator exercises, best information available on the EPGs, and a task analysis following NRC task analysis techniques.[3] For each of the six critical operator actions, the qualitative review included: (1) identification of problems/constraints affecting operator performance, (2) a description of actions required of the operator and constraints affecting performance, and (3) possible solutions to the problems. Problems/constraints included human engineering deficiencies in control room design and certain system responses to changes in reactor pressure and/or level. Suggested solutions included potential backfits to control room design and identified training needs corresponding to complex operator actions required by the EPGs.

The purpose of the quantitative HRA was to provide some clarification of uncertainties in operator response during ATWS. Whereas results of HRA are useful for PRAs, they are also useful for identifying potential performance deficiencies which may be alleviated through training and simulator practice, procedures development, improved plant communications, and so forth.

It is noted that whereas primary emphasis was on operator actions contained in the EPGs, input to the HRA included a task analysis of certain operator actions following the event-based Emergency Operating Instructions (EOIs). A general examination of the EPGs and EOIs suggested these actions would be performed in a closely similar manner. This similarity supports the assumption that results of the HRA, while based on the EOIs, were relevant to the EPGs.

Some of the six critical operator actions included in the qualitative review seemed suitable for the quantitative HRA since there was agreement by TVA and SASA analysts on the steps comprising the actions. However, other actions were the subject of some controversy, and the lack of consensus on what guidance should be included in the EPGs precluded their quantitative assessments.

The quantitative HRA was divided into four components. First, methods for HRA reported in the literature were identified and briefly described. Second, a task analysis of the four selected critical operator actions was completed. Third, the steps in conducting the HRA using the Technique for Human Error Rate Prediction, or THERP,[4] were completed resulting in a listing of the derived quantitative human reliability estimates. The use of THERP was primarily relevant to estimating operator reliability for each of the individual critical tasks. Fourth, results of the analysis using the Operator Personnel Performance Simulation (OPPS)[5] computer model were obtained. The uses of OPPS were to supplement the THERP analysis and compliment the SASA analysis by providing a time-reliability estimate across all operator actions throughout the ATWS.

For each of the four critical tasks, Task Data Forms (TDFs) were completed using the following resources: (1) BF1 emergency procedures, (2) videotapes of the simulator exercises on ATWS perturbations, (3) computer records of operators' switch manipulations during the simulator exercises collected through the Performance Measurement System,[6] (this system also provides continuous data on selected critical plant safety parameters), and (4) expert judgement from operations and human factors personnel.

Results of the task analysis were used to guide selection of nominal human error probabilities (HEPs) from the THERP human error data base (Chapter 20 of Ref. 4). It is noted that the level of refined task information provided in the NRC's TDFs is typically more detailed than the level called for in the THERP Handbook. An HEP worksheet was developed to organize and document the THERP analysis. Nominal HEPs were modified to reflect effects from performance shaping factors, such as stress, and the level of dependence among successive task elements. Modified HEPs comprising complete success paths were used to calculate final task success probabilities. Only actions for which errors would contribute to system failure were included in the calculations. Preliminary estimates of human failure probabilities and related uncertainty bounds are shown in Table 1.

Supplementary assessment of operator actions throughout the ATWS was provided through use of the OPPS computer model. The OPPS model was programmed in the simulation language known as SAINT (Systems Analysis of Integrated Networks of Tasks).[7] OPPS times the simulated control room crew progressing through major phases of pre-alarm detection, event diagnosis, execution of procedure steps, and error recovery. Based on 1000 iterations of simulated ATWS events, performance time for completion of all safety-related operator actions averaged 33.4 minutes. The minimum time was 23.0 minutes, and the maximum was 43.8 minutes. For comparison purposes, SASA analysts in their baseline worst case scenario of ATWS involving no operator actions reported that containment failure would occur at 36.8 minutes into the accident. These analyses suggest that operators should have sufficient time to complete all actions necessary to shut the reactor down. Moreover, not all safety-related actions would have to be completed within this time since the more critical actions which would likely be performed would slow accident progression and extend the time remaining for the operators to complete the remaining actions.

Operator Severe Accident Management

The Function Oriented Accident Management (FOAM) model is a descriptive structure which integrates data and expertise from operations, engineering, and human factors personnel. The purpose of the FOAM model is to structure guidance for operators in responding to severe accidents which exceed the scope of emergency procedures and necessitate a knowledge-based response.

Some industry and commercial training courses already exist for mitigation of core damage. Some progress has also been made by the French nuclear power industry for the prevention of severely degraded cores.[8] However, what seems to be lacking is a systematic technical guide for standardizing and linking operator training, emergency procedures, emergency response facilities, and other considerations important to emergency response. The FOAM model is a functionally-oriented approach for translating existing data and knowledge on accident phenomenology into technical guidelines supporting such concerns as training and procedures development for accident management.

The FOAM model consists of four components. Each component is subsequently described and exercised through a demonstration severe ATWS scenario assessed by SASA analysis. The first component is an assessment of the accident sequence with an identification of particular operator and/or system failures. The purpose of this assessment is to define the progression of the event and the potential end states resulting in core damage. An Operator Action Event Tree (OAET) is one method for identifying possible operator errors leading to a severe accident. For the demonstration ATWS scenario, a modified OAET is shown in Fig. 1a. The multiple failures of manual control rod insertion and initiation of the standby liquid control system lead to end state 18, although end states 14, 16, and 20 could also be considered depending upon the timing and success of other operator actions. Potential dominant causes identified from the PRA for BF1 of failure of manual control rod insertion were possible faults in the venting or in hydraulic mechanisms of the control rod drives, or possible rod sticking or binding due to mechanical stress; and failure of the SLC system due to valve misalignment following maintenance testing, or one or more SRVs fail open so that water from the SLC system tank quickly converts to steam as it enters the reactor vessel.

The second component involves a translation of the multiple failures identified in the first component using a functional classification developed to identify plant safety functions and control requirements.[9] The functional classification is being developed to identify hierarchical levels of safety functions and control requirements for both protection of the plant and protection of plant personnel and the public. One of the purposes of the translation is to identify potential alternate control requirements using redundant systems which would recover the off-normal safety function. The functional classification is intended to be a technical guide for extending symptom-based procedures which link safety functions, control requirements, and redundant plant systems.[10] A significant point is that when the functional classification does not identify redundant control requirements to meet the particular off-normal safety function, i.e., the multiple failures exceed the scope of the emergency procedures, the operators must develop one or more "unconventional emergency responses" (UERs) to either recover the failures or minimize/isolate their effects to plant safety. Specifications of UERs may use such resources as SASA analyses and recommendations, expert judgements from operations, engineering, and human factors personnel, and results of PRAs.

The cross-section of the functional classification most pertinent to the demonstration ATWS scenario is shown in Fig. 1b. Whereas negative reactivity can be inserted by several means, only insertion of rods or poison provides long-term shutdown of the reactor. SASA analysts report that manipulating inherent feedback in the reactor coolant serves to extend accident timing by several hours. During this time, operators must recover at least one of the failures in order to insert negative reactivity into the core and bring the reactor to hot standby.

The third component concerns modeling the UERs which the operator may devise for attempting to mitigate severe accident progression. For purposes of the FOAM model, UERs are modeled in an event tree format, which also permits an assessment of alternate end states. Each UER may be qualitatively assessed to systematically identify a range of information which, at the minimum, should include: (1) alarms and cues reflecting off-normal critical safety parameters associated with the system failure, (2) decision criteria such as identifying and weighing alternate actions, (3) an analysis of specific operator actions at some level of detail to either recover the failure or isolate its effects, and (4) consequences of the UER to the plant in terms of contribution to accident mitigation or extending the timing of accident progression.

For the demonstration ATWS scenario, an event tree containing potential UERs is shown in Fig. 1c. The event tree is entered through a transition from an analysis of the initial accident sequence, such as the OAET. The first two UERs pertain to the safety function of controlling reactivity, and recovery of either of the two failures will shut the reactor down by inserting negative reactivity. Recovery of these failures would depend upon their particular failure modes. SASA analysts and operations personnel have also suggested that the timing of accident progression may be extended through certain unusual operator actions. The remaining three UERs have been suggested as possible candidate UERs for protecting containment. Initiation of PSP sprays serves to protect containment by controlling torus temperature and pressure. Replenishing the PSP volume supports these same safety functions by replacing heated torus water with river water. A BF1 Operating Instruction (#74) guides normal adjustments to torus level. The UER of opening one main steam isolation valve (MSIV) is relevant only to the ATWS perturbation in which efforts to insert negative reactivity are unsuccessful. This UER could be considered if certain conditions existed (e.g., no fuel damage has occurred, technical limits of containment are severely challenged), and would then use the main condenser as a heat sink. In general, it would be desirable to assess all these actions in sufficient detail to develop corresponding technical guidelines. Such guidelines would support the development of procedures, specification of training objectives, and guidelines for the development of computer-based operator aids.

The fourth component of the descriptive model involves operator response to fuel damage and potential subsequent radiological release past plant protective barriers. The greatest hazard to the health and safety of plant personnel and the public is the release of fission products. Challenges to multiple barriers may occur along liquid and gaseous streams. As part of the model, fission product pathways are being identified through more detailed barrier diagrams[11] tailored to the ATWS at BF1, and a sample diagram is shown in Fig. 1d. Accompanying the barrier diagrams is a system description identifying such information as: (1) how fission products may breach plant barriers and be subsequently released to the environment, (2) the information (alarms and recorders) available to the control room operators for assessing whether a barrier has been violated, and (3) the possible actions the operator may take to mitigate a barrier breach and isolate the radiological release.

Potential applications of the FOAM model reflect regulatory, industry, and research perspectives. For each of these groups, the model provides guidance for structuring technical data and expertise and formulating potential requirements in order to improve responsiveness to degraded core conditions. The FOAM model provides such guidance for applications, including extended procedures development, training objectives and performance standards, technical support of emergency response facilities, guidelines for computer aids development and evaluation, and assessment of control room instrumentation and layout.

Conclusions and Recommendations

Results of this human factors study have fallen into two major categories. First, human factors support of the SASA Program has provided some resolution of uncertainties in operator response to severe accidents. Videotapes of the ATWS simulator exercises were notably useful to SASA and human factors analyses. Second, the descriptive FOAM model has suggested a structure for developing technical guidance for operator responses in mitigating both core damage and radiological release. The model provides a functional approach for standardizing procedures and training for accident management using operations, engineering, and human factors data and expertise.

Human factors support of other SASA studies is recommended to more thoroughly identify and assess operator actions effecting the accident sequence. Assessments of operator reliability, procedures, training, computer aids, and human engineering aspects of control room design are recommended to provide comprehensive determinations of operator actions, which in turn strengthens the SASA analysis by reducing uncertainties in operator response.

Further work in accident management should attempt to provide technical support for operators to mitigate degraded core conditions. The FOAM model is one approach for standardizing and extending procedures and training. Additional work is recommended to more comprehensively apply results from SASA and PRA studies to support NRC, industry, and research needs in accident management.

References

1. R. M. Harrington and S. A. Hodge, "ATWS at Browns Ferry Unit One - Accident Sequence Analysis," NUREG/CR-3470, ORNL/TM-8902 (June 1984).

2. W. A. Brinsfield, E. T. Burns, A. S. McClymont, S. E. Mays, and S. L. vonHerrmann, "Methods for Review and Evaluation of Emergency Procedure Guidelines Volume III: Applications to General Electric Plants," NUREG/CR-3177, Vol. III, EG&G Report EGG-2243, Vol. III (September 1983).

3. D. Burgy, C. Lempges, A. Miller, L. Schroeder, H. Van Cott, and B. Paramore, "Task Analysis of Nuclear Power Plant Control Room Crews Volumes I and II," NUREG/CR-3371, Vols. I and II, GPC Report GP-R1221020, Vols. I and II (September 1983).

4. A. D. Swain and H. E. Guttmann, "Handbood of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report," NUREG/CR-1278, SNC Report Sand80-0200 (August 1983).

5. E. J. Kozinsky, L. H. Gray, A. N. Beare, D. B. Barks, and F. E. Gomer, "Criteria for Safety-Related Operator Actions: Final Report, NUREG/CR-3515, ORNL/TM-8942 (March 1984).

6. E. J. Kozinsky, and R. W. Pack, "Performance Measurement System for Training Simulators," Electric Power Research Institute Report EPRI NP-2719 (November 1982).

7. P. Tanguy, "The French Apporach to Nuclear Power Safety," <u>Nuclear Safety 24</u>, 589-606 (1983).

8. D. B. Wortman, S. D. Duket, D. J. Seifert, R. L. Hann, and G. P. Chubb, "Simulation Using SAINT: A User-Oriented Instruction Manual," AMRL-TR-77-61 (July 1978).

9. "An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production," ALO-1011, Sandia National Laboratories (1982).

10. W. R. Corcoran, D. J. Finnicum, F. R. Hubbard, III, C. R. Musick, and P. F. Walzer, "Nuclear Power Plant Safety Functions," <u>Nuclear Safety 22</u>, 179-191 (1981).

11. "Mitigating Reactor Core Damage: BWR Version," General Physics Corporation Course Textbook, Columbia, Maryland (1983).

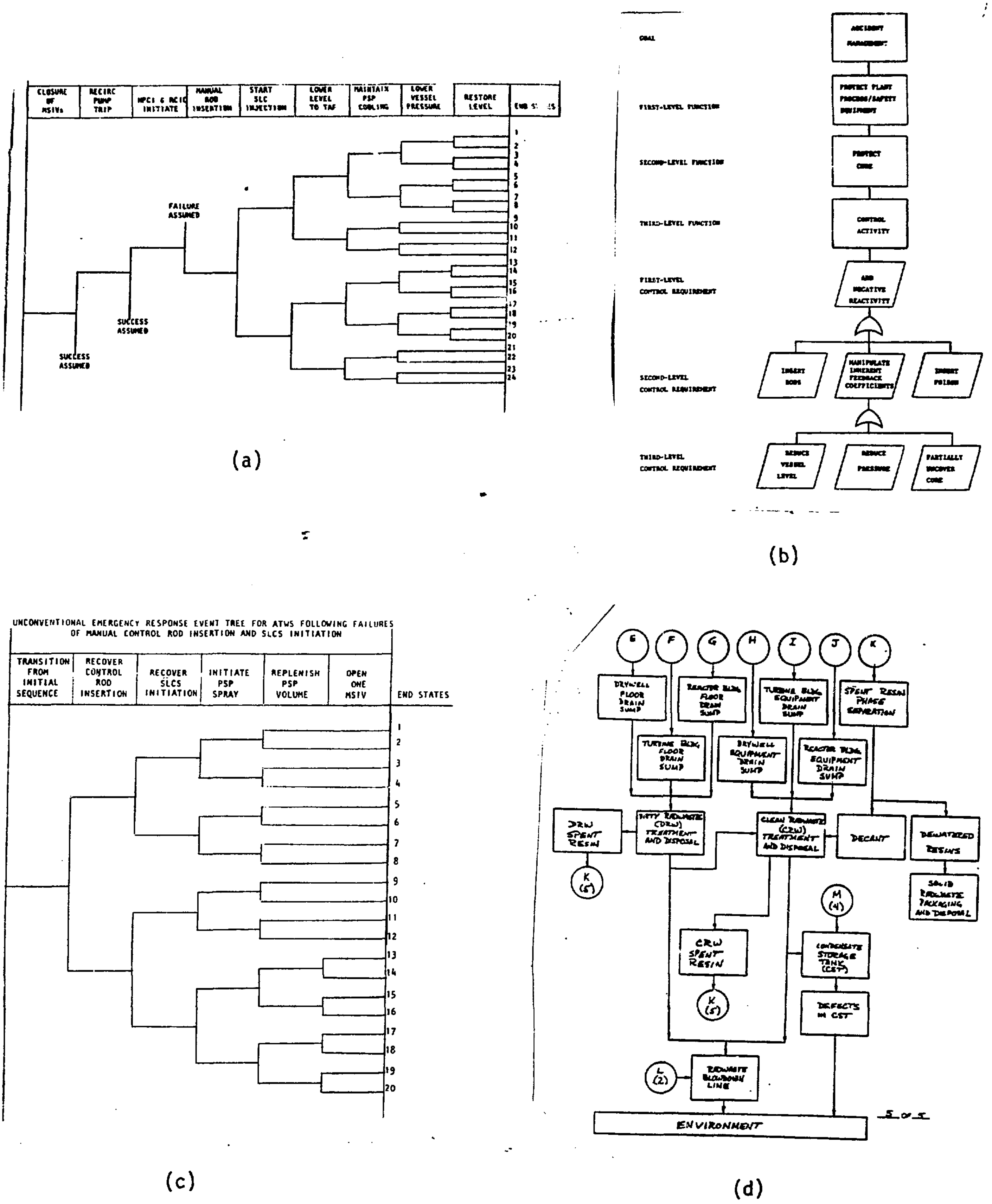

Figure 1. Representative components of the Function Oriented Accident Management (FOAM) model.

Table 1. Estimates of human failure probabilities for selected tasks during ATWS.

		Uncertainty Bounds	
Task Description	Nominal HEP	Upper	Lower
Manually operate SRVs before 1105 psig reactor pressure is reached	2.72E-02	2.61E-01	1.74E-02
Manual control rod insertion	1.82E-01	3.71E-01	1.63E-01
Initiate suppression pool cooling	1.27E-01	3.28E-01	3.92E-02
Verification of conditions for and initiation of SLC injection	3.69E-02	2.59E-01	1.47E-02