CONF-850996--3

HUMAN FACTORS REVIEW FOR NUCLEAR POWER PLANT SEVERE ACCIDENT SEQUENCE ANALYSIS*

CONF-850996--3

TI85 017081

P. A. Krois
P. M. Haas

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

Presentation To Be Made At:

29th Human Factors Society Meeting
Baltimore, Maryland
September 29 - October 3, 1985

*Research sponsored by U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research with Oak Ridge National Laboratory operated by Martin Marietta Energy Systems, Inc. under contract #DE-AC05-84OR21400 with U.S. Department of Energy.

HUMAN FACTORS REVIEW FOR NUCLEAR POWER PLANT SEVERE ACCIDENT SEQUENCE ANALYSIS

P. A. Krois and P. M. Haas

Oak Ridge National Laboratory
Oak Ridge, Tennessee

ABSTRACT

The paper discusses work conducted to: (1) support the severe accident sequence analysis of a nuclear power plant transient based on an assessment of operator actions, and (2) develop a descriptive model of operator severe accident management. Operator actions during the transient are assessed using qualitative and quantitative methods. A function oriented accident management model provides a structure for developing technical operator guidance on mitigating core damage and preventing radiological release.

INTRODUCTION

The purposes of this project, which was sponsored by the U.S. Nuclear Regulatory Commission (NRC), were to: (1) support the nuclear power plant severe accident sequence analysis (SASA) program, and (2) develop a descriptive model of operator response in accident management. The first goal was accomplished by working with SASA analysts on the postulated boiling water reactor (BWR) anticipated transient without scram (ATWS) at Browns Ferry Unit One and providing a systematic assessment of critical operator actions. This assessment demonstrates potential contributions to SASA analyses from human factors data and methods. The second goal was accomplished by developing a function oriented accident management (FOAM) model, which serves both as a conceptual structure for identifying needs and deficiencies and as a method for developing technical operator guidance in accident management.

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 an ATWS. The human factors assessment was focused to some extent by concerns of SASA analysts in their accident sequence analysis (Harrington and Hodge, 1984). The SASA analysis considered operator actions in the context of new symptom-based Emergency Procedure Guidelines (EPGs). Because the EPGs were still in the review process, both the SASA and human factors analyses were limited to using the best information available on the EPGs at the time the analyses were conducted.

The following discussions describe the EPGs with an identification of operator actions critical to the progression of an ATWS, show how these critical operator actions underwent a systematic qualitative review, and summarize a quantitative human reliability analysis (HRA) of some of these actions.

Critical Actions in the EPGs

Event-based emergency procedures require control room operators to first diagnose the type of transient before taking corrective actions. The symptom-based EPGs attempt to reduce the cognitive workload associated with

event diagnosis by having operators verify and maintain the adequacy of important safety functions. One advantage of an event-based procedure, however, is that operators may immediately relate causes and consequences of off-normal conditions and subsequently act to directly mitigate accident progression.

SASA analysts made the recommendation that the emergency procedures for an ATWS be separated from the EPGs. The human factors analysis assisted in defining some of the problems operators may experience with instructions in the EPGs. One of these problems is that certain operator actions called for in response to an ATWS are substantially different from actions appropriate to other accidents. Some of these actions are also contrary to operational practices on which operators are trained. SASA analysts noted their assumption that the signature of an ATWS is so distinguishable that operators would quickly diagnose the event and that a separate ATWS procedure would expedite operator response.

One specific example of a problem related to an ATWS is the instruction in the EPGs to manually lower and maintain reactor vessel water level at the top of the active fuel (TAF) 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.

From a human factors standpoint, the instructions in the EPGs present some difficulties for operators in relation to an ATWS. However, the solution proposed by SASA analysts to separate those instructions relevant solely to an ATWS may or may not be entirely satisfactory. Operator performance during a transient would be based on several factors including training and operator aids. These factors and others should be considered across a range of accidents before targeting the restructuring of procedures to address problems related to one specific accident sequence.

The identification of critical operator actions was coordinated with SASA analysts. Inputs to the selection process included: (1) review of the EPGs, (2) consideration of operator actions included in computer code models used for accident sequence analysis, (3) review of operator actions observed during exercises of ATWS perturbations on the

full-scope Browns Ferry control room simulator, and (4) review of an operator action event tree (OAET) developed for an ATWS and based on the EPGs (Brinsfield, Burns, McClymont, Mays, and vonHermann, 1983). However, comparison of this OAET with results from the SASA analysis suggested several modifications, and a modified OAET is shown in Figure 1.

Six operator actions were judged as being critical to the ATWS sequence as follows:

1. Manual selection and insertion of individual control rods given complete failure of the reactor to automatically scram.
2. Verification of conditions for use of the standby liquid control (SLC) system and initiation of poison injection into the reactor vessel in order to shut the reactor down.
3. Initiation of pressure suppression pool (PSP) cooling by manual operation of the residual heat removal system in order to maintain the PSP as a heat sink.
4. Control of reactor vessel pressure 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 level at TAF.
6. Emergency depressurization of the reactor vessel in accordance with the PSP heat capacity temperature curve followed by control of low pressure injection.

Qualitative Review

The qualitative review was based on instructors' comments and analysts' observations resulting from the simulator exercises and on a task analysis using NRC task analysis techniques (Burgy, Lempges, Miller, Schroeder, Van Cott, and Paramore, 1983). For each of the six critical operator actions, the review included: (1) identification of problems/constraints affecting operator performance (e.g., human engineering deficiencies in control room design), (2) a description of performance required of the operator and constraints to success, and (3) possible solutions to the problems so as to improve performance reliability (e.g., potential backfits to control room design and identified training needs).

As an illustration of the qualitative review, the operator action involving reactor vessel water level control presents several problems. For an ATWS, the EPGs instruct the operator to lower and maintain reactor vessel water level at TAF while the SLC system injects a neutron absorber into the reactor. This instruction conflicts with intuition and training for virtually every other accident situation. Further, in the process of executing this instruction, operators must rely on level indicators which may be inaccurate, have insufficient range, or are located on distant panels, Operators may also experience difficulty with use of the high pressure coolant injection (HPCI) system because of automatic interlocks. Very briefly, the performance description includes the purpose of this operator action, which is to provide a temporary reduction in reactor power until control rods or sufficient poison are inserted. Human engineering deficiencies are that the level instrumentation in the control room show differences in their readings at different reactor vessel pressures, that because range at the bottom end for some indications is so restricted operators must check other displays for the vessel level, and that display locations force operators to verbally relay display readings to one another. The potential loss of HPCI is due to a suction shift from cool to hot water which eventually damages the HPCI pump lube oil, and leads the operators into a more difficult branch of accident progression. Resolutions of these problems would include: (1) providing operator simulator training on ATWS conditions; (2) introducing human engineering fixes of level instrumentation, although operator use of a safety parameter display system, once it is installed, should alleviate many of these particular problems; and, (3) inserting in the EPGs an instruction that during an ATWS operators should manually trip HPCI before it fails so that it may be restarted at a later point if necessary.

Quantitative HRA

The purpose of the quantitative HRA was to provide some clarification of uncertainties in operator response during an ATWS. The first four of the six critical operator actions seemed suitable for the HRA since there was

agreement among nuclear engineering analysts on the steps comprising the actions.

One method used in the HRA was the Technique for Human Error Rate Prediction, or THERP, which results in human error probability (HEP) estimates (Swain and Guttman, 1983). The THERP analysis provides some additional understanding on how respective operator actions were deterministically incorporated into the computer code used by SASA analysts to study ATWS. A second method used in the HRA was the Operator Personnel Performance Simulation (OPPS) computer model (Kozinsky, Gray, Beare, Barks, and Gomer, 1984). The uses of OPPS were to supplement the THERP analysis and complement the SASA analysis by providing a time-reliability estimate based on operator actions during an ATWS.

For each of the four critical operator tasks, a task analysis using the NRC task data form (TDF) was completed. Inputs to the task analysis included: (1) plant emergency procedures, (2) videotapes of the simulator exercises involving ATWS perturbations, (3) computer records of operators' switch manipulations and plant systems data collected during the simulator exercises through the Performance Measurement System (Kozinsky and Pack, 1982), and (4) expert judgment of operators.

The task analysis data were used to guide selection of nominal HEPs from the THERP human error data base. It is noted that the level of refined task information provided in the TDFs is typically more detailed than the level called for in the THERP Handbook. A 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 from the level of dependence among successive task elements. Modified HEPs comprising complete success paths were used to calculate human failure probabilities. Only actions for which errors would contribute to system failure were included in the calculations. Estimates of HEPs and related uncertainty bounds for the four tasks are shown in Table 1.

Supplementary assessment of operator actions during an ATWS involved the OPPS computer model. The OPPS model was programmed in the SAINT (Systems Analysis of Integrated Networks of Tasks) language (Wortman, Duket, Seifert, Hann, and Chubb, 1978). 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 (minimum of 23.0 and maximum of 43.8 minutes). For comparison purposes, SASA analysts in their baseline worst case scenario for ATWS involving no operator actions reported that containment failure would occur at 36.8 minutes into the accident. This corresponds to about 85th percentile in the OPPS distribution. The analysis suggests that most 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 period since the more critical actions which would likely be performed early in the sequence would slow accident progression and extend the time remaining for the operators to complete the remaining actions.

ACCIDENT MANAGEMENT

The FOAM model was developed both as a conceptual structure for systematically describing operator response in accident management and as a method for standardized development of technical guidance supporting operator decision making and response. Guidance is necessary because accident conditions are assumed to exceed the scope of existing emergency procedures. Technical guidance may be developed through expertise compiled from operations, engineering, and human factors personnel and integration of data from SASA and probabilistic risk analysis (PRA) studies. This guidance is central for extending emergency procedures, systematic operator training, and defining information requirements for computer-based operator aids.

Some industry and commercial training courses already exist for mitigation of core damage. Some progress has also been reported by the French nuclear power industry for the prevention of severely degraded core conditions (Tanguy, 1983). 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 was developed, then, as a function-oriented approach for translating existing data and knowledge on accident phenomenology into technical operator guidelines. The FOAM model consists of four components. Each component is subsequently described and exercised through a demonstration severe ATWS scenario that was assessed by SASA analysts.

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 OAET is one method for identifying possible operator errors leading to a severe accident. For the demonstration ATWS scenario, the multiple failures of manual control rod insertion and initiation of the SLC system would 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 for these failures have been identified through SASA and PRA studies, and it is noted that this scenario is a very unlikely event.

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. The functional classification was 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 (Corcoran, Finnicum, Hubbard, Musick, and Walzer, 1981). A significant point is that when the functional classification does not identify redundant control requirements to meet the particular off-normal safety functions, i.e., when 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 judgments from operations, engineering, and human factors personnel, and results of PRAs. Relative to the demonstration ATWS scenario, only insertion of control rods or poison provides stable shutdown of the reactor. SASA analysts reported that manipulating reactor vessel water level would extend accident timing by several hours. During this time, operators must recover at least one of the failures or take additional actions to further extend the timing of the accident.

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. End states may be classified according to expected possible plant conditions, and some end states may necessitate identification of additional UERs. 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 UERs, (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 extension of the timing of accident progression.

For the demonstration ATWS scenario, an event tree containing potential UERs is shown in Figure 2. 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. The UER of opening one main steam isolation valve (MSIV) is relevant

only to the ATWS perturbation in which all efforts to insert negative reactivity are unsuccessful. This UER could only 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. End states in Figure 2 are classified according to a qalitative logic. In general, it would be desirable to assess all these actions in sufficient detail to develop corresponding technical operator guidelines.

The fourth component of the descriptive model involves operator response to fuel damage and potential subsequent radiological release past plant protective barriers. Beyond the mitigation of core damage, 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 identified through detailed barrier diagrams tailored to the BWR ATWS, and a sample diagram is shown in Figure 3. 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 for formulating potential requirements in order to improve responsiveness to degraded core conditions. The FOAM model provides a structure for applications in accident management, 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

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 core damage and preventing 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 affecting the accident sequence. Assessments of operator reliability, procedures, training, computer aids, and human engineering aspects of control room design are recommended to provide comprehensive assessments of the operator's contribution in the accident sequence.

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

Brinsfield, W.A., Burns, E.T., McClymont, A.S., Mays, S. E., and vonHerrmann, S. L. (1983). Methods for review and evaluation of emergency procedure guidelines Volume III: Applications to General Electric plants (NUREG/CR-3177, Vol. III). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Burgy, D., Lempges, C., Miller, A., Schroeder, L., Van Cott, H., and Paramore, B. (1983). Task analysis of nuclear power plant control room crews Volumes I and II (NUREG/CR-3371, Vols. I and II). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Corcoran, W.R., Finnicum, D.J., Hubbard, F.R., III, Musick, C. R., and Walzer, P. F. (1981). Nuclear power plant safety functions. Nuclear Safety 22, 179-191.

Harrington, R. M., and Hodge, S. A. (1984). ATWS at Browns Ferry Unit One - Accident Sequence Analysis (NUREG/CR-3470). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Kozinsky, E. J., Gray, L. H., Beare, A. N., Barks, D. B., and Gomer, F. E. (1984). Criteria for safety-related operator actions: Final Report (NUREG/CR-3515). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Kozinsky, E. J., and Pack, R. W. (1982). Performance measurement system for training simulators (EPRI NP-2719). Palo Alto, CA: Electric Power Research Institute.

Swain, A. D., and Guttman, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications: Final Report (NUREG/CR-1278). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Tanguy, P. (1983). The French approach to nuclear power safety. Nuclear Safety, 24, 589-606.

Wortman, D. B., Duket, S. D., Seifert, D. J., Hann, R. L., and Chubb, G. P. (1978). Simulation using SAINT: A user-oriented instruction manual (AMRL-TR-77-61). Wright-Patterson Air Force Base, OH: Aeromedical Research Laboratory.

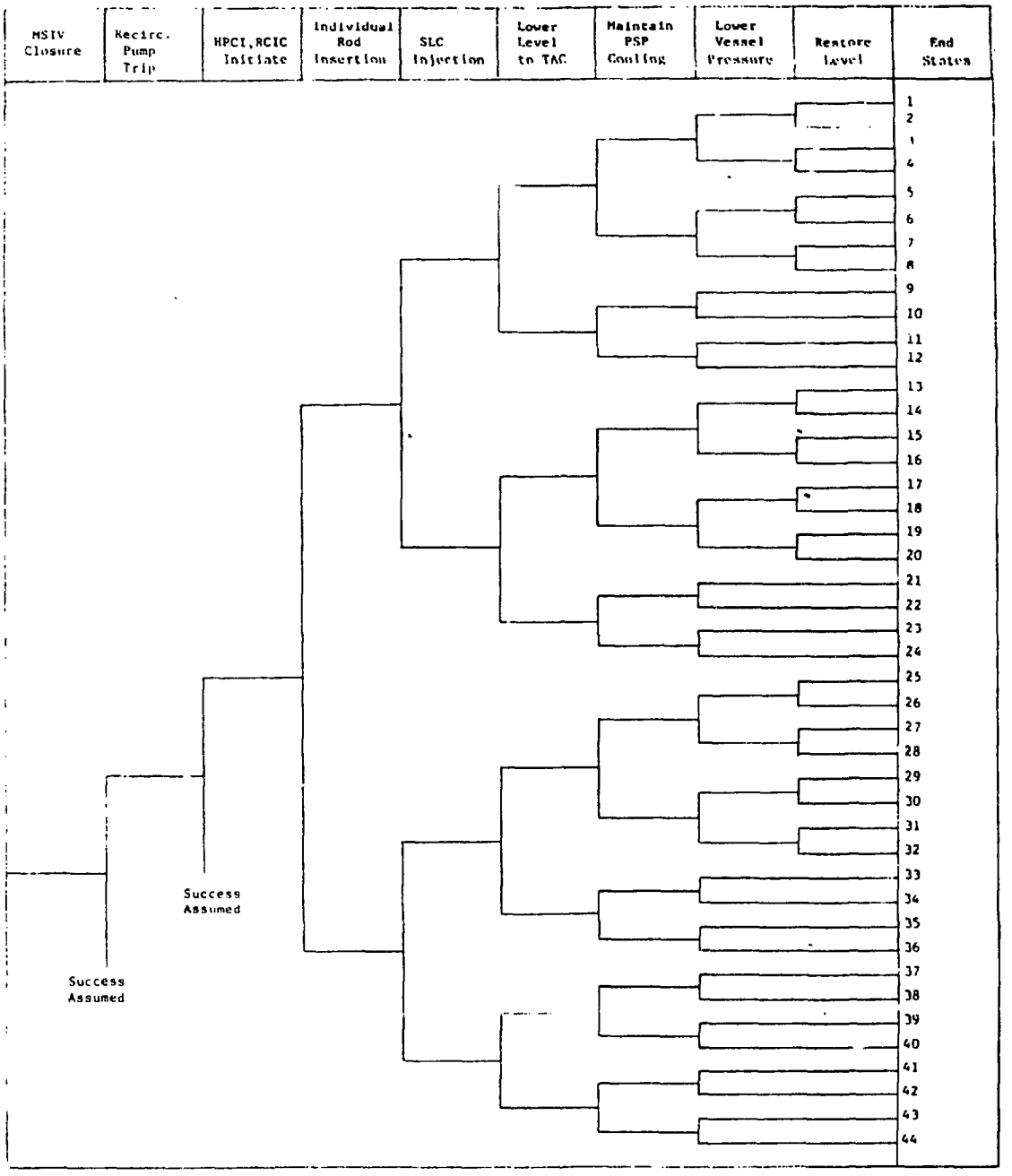

Figure 1. Modified OAET in accordance with SASA analysis.

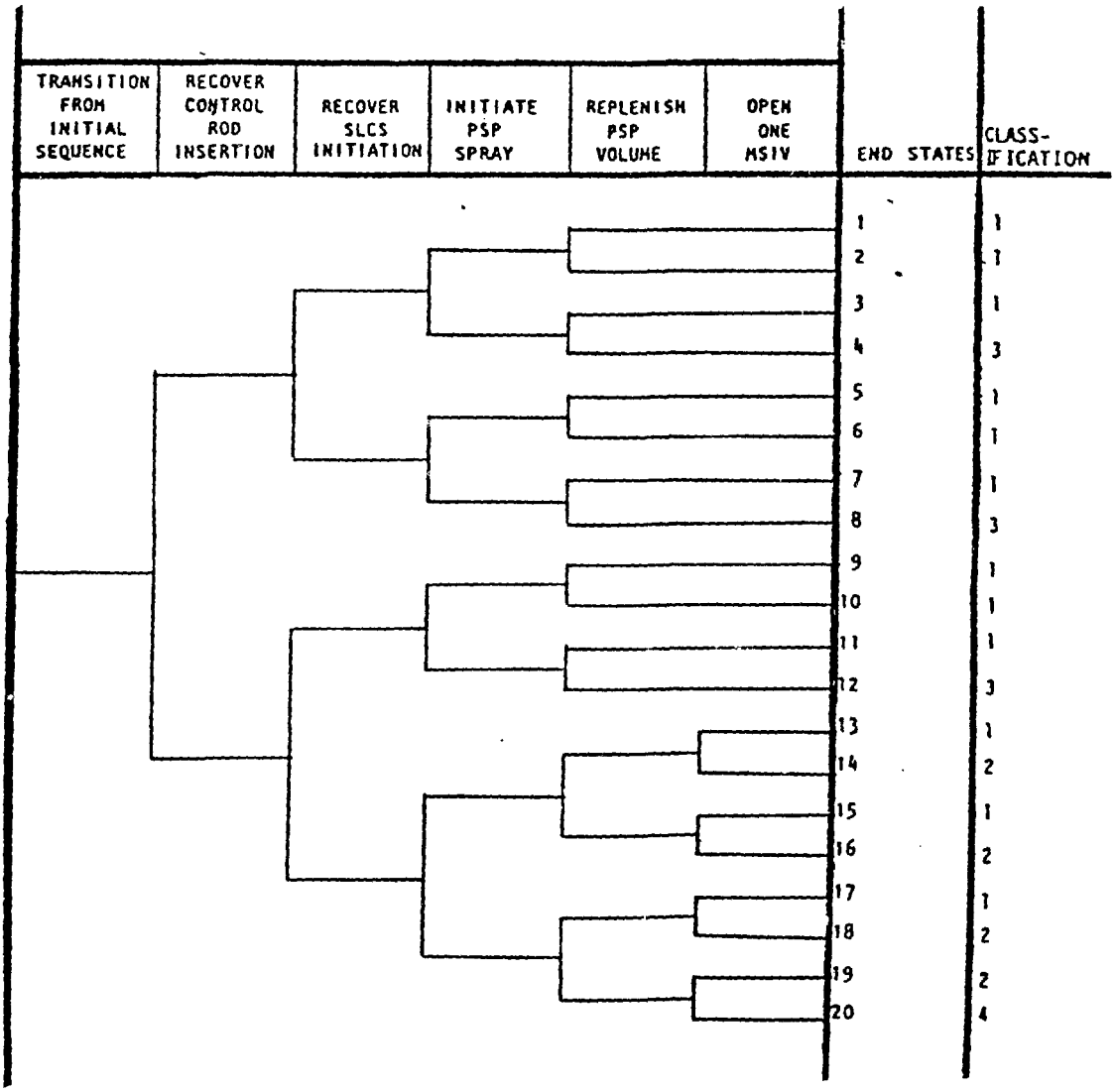

Figure 2. Unconventional emergency response event tree for ATWS following failures of manual control rod insertion and SLCS initiation.

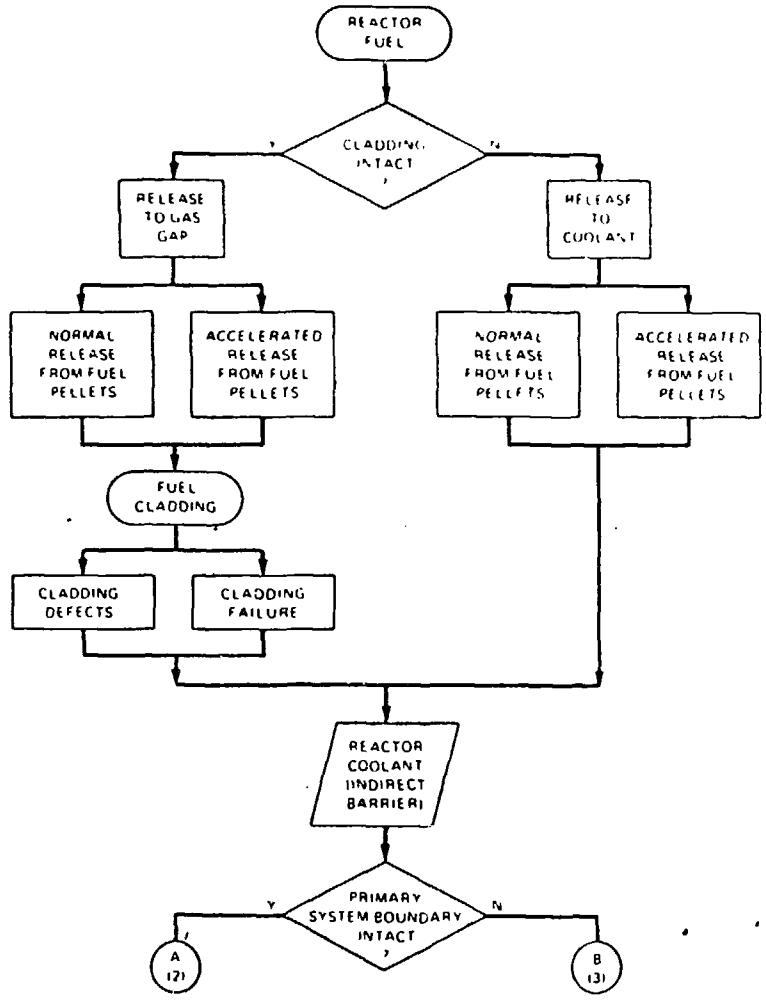

Figure 3. Pathways for release of radionuclides in liquid stream from a BWR during ATWS.

Table 1. Estimates of Human Failure Probabilities for Selected Tasks During ATWS

Task Description	Nominal HEP	Uncertainty Bounds	
		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