

## Idaho National Engineering Laboratory

Operated by the U.S. Department of Energy

# Methods for Review and Evaluation of Emergency Procedure Guidelines Volume I: Methodologies

James L. vonHerrmann

March 1983

Prepared for the

**U.S. Nuclear Regulatory Commission**

Under DOE Contract No. DE-AC07-76IDO1570



Available from

GPO Sales Program  
Division of Technical Information and Document Control  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555

and

National Technical Information Service  
Springfield, Virginia 22161

#### NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

**NUREG/CR-3177  
EGG-2243  
VOL. I  
Distribution Category: RX**

**METHODS FOR REVIEW AND EVALUATION OF  
EMERGENCY PROCEDURE GUIDELINES VOLUME I:  
METHODOLOGIES**

**James L. vonHerrmann**

**Published March 1983**

**Wood-Leaver and Associates, Inc.**

**Prepared for EG&G Idaho, Inc.  
Under Subcontract No. C29-007729-MOD-3  
and the U.S. Nuclear Regulatory Commission  
Under DOE Contract No. DE-AC07-76IDO1570  
FIN No. 6331**

## ACKNOWLEDGEMENTS

The acquisition and evaluation of the ongoing industry programs in emergency procedure guideline development were an essential part of this report. In this regard, the efforts and guidance of Milan Stewart of EG&G Idaho, Inc. are gratefully acknowledged. We would also like to thank the many individuals involved in the various Owners Groups' programs for their efforts to explain the basic concepts and present status of their respective programs.

## ABSTRACT

Systematic methods for reviewing and evaluating improved emergency procedure guidelines are presented. The deficiencies of existing "event-oriented" emergency procedures are discussed and the industry efforts to produce improved guidelines in the aftermath of TMI are summarized. It is concluded that the function- or symptom-oriented approaches which have evolved since TMI have, in theory, the potential to produce effective guidelines. However, when attention is focused on a limited number of critical safety functions (or symptoms indicative of the performance of these functions), the concern arises that diverse accident conditions which exhibit common or similar symptoms can result in ambiguous operator diagnosis and ineffective response. Methods for systematically examining potential accident sequences using "operator action event trees" are developed in this first volume which can help ensure that functional or symptomatic guidance can, in reality, lead to unambiguous and effective diagnosis and response regardless of the specific failure events. Subsequent volumes of this report will apply these methods to Westinghouse, General Electric, Babcock & Wilcox, and Combustion Engineering plant designs.

## SUMMARY

Subsequent to the accident at Three Mile Island (TMI), industry groups have endeavored to develop emergency procedures which do not require the operator to diagnose a specific event or series of events before guidance is provided. The function - or symptom-oriented approaches which have evolved since TMI are summarized and discussed.\* It is concluded that these alternate approaches to guideline development - as exemplified by the programs of groups associated with each of the four major U.S. vendors - have, in theory, the potential to produce effective guidelines. However, when attention is focused on a limited number of critical safety functions (or symptoms indicative of the performance of these functions), the concern arises that diverse accident conditions which exhibit common or similar symptoms can result in ambiguous diagnosis and ineffective response.

Thus, the potential pitfalls which must be avoided in the practical application of these alternate approaches to guideline development are closely linked with the primary motivation for their development. The pre-TMI procedures required the operator to know too much before he could be assured of taking the right action. The proposed remedy is to provide guidance based on much less information (a limited number of key symptoms associated with the performance of a few critical functions). However, whenever guidance is based on limited information, extreme care must be taken to assure that it is always correct and unambiguous.

In this first volume, systematic methods are developed which can help assure that functional or symptomatic guidance can, in reality, lead to unambiguous and effective diagnosis and response regardless of the specific failure events. These methods are based upon the premise that a practical way of examining whether guidelines can provide unambiguous guidance regardless of the specific event(s) is to

---

\*This summary and discussion is based on those versions of Owners Group guidelines available in late 1981. It is recognized that the guidelines associated with some of the Owners Groups have since evolved considerably. However, the evolution has not affected the conclusions or recommendations presented in this report.

systematically examine their ability to provide such guidance for a wide variety of known specific events. Thus, these methods represent a framework for systematically and efficiently applying the best available information concerning specific accident sequences to the evaluation of guidelines which are intended to be able to "handle" all such sequences. Risk significant multiple failure accident sequences are focused upon in this report, although the methodology is applicable to any sequence which the analyst believes is important.

The methods are based on the use of Operator Action Event Trees (OAETs) which logically depict the role of the operator throughout the progression of any postulated accident sequences. These OAETs systematically document the required operator actions and key symptoms exhibited by the plant at the various stages of the accident sequences. This information base provides the technical foundation upon which the guidelines can be reviewed.

The OAET-based review methods which are presented can be applied in three basic ways:

- (1) Preliminary or incomplete guidelines can be fine-tuned and finalized using input gained from a systematic OAET-based investigation of the incomplete guidelines.
- (2) Complete guidelines can be systematically reviewed and any inadequacies corrected.
- (3) Guidelines can be developed based upon the technical framework provided by the OAETs.

The OAET-based methods presented in this volume could potentially be used in the regulatory process in the following ways:

- (1) They could be used as a systematic demonstration that a set of guidelines provides unambiguous guidance under all important accident conditions; alternatively, they can be used by NRC to independently review submitted guidelines.
- (2) They can be cited by a specific utility as an integral part of their program to customize the Owners Group's generic guidelines to their specific plant.

- (3) They can be used as the technical foundation for guideline and procedure development by utilities which do not plan to use the Owners Group's generic guidelines.

It is suggested that these methods could potentially play a valuable role in the regulatory process because:

- o From the regulatory side, they provide an easily audited process which also provides very high assurance that the guidelines submitted by the Owner's Groups and implementation plans submitted by the individual utilities will result in unambiguous operator guidance under all important accident conditions.
- o From the industry side, they provide a well defined process by which regulatory concerns over the technical content of guidelines and procedures can be systematically satisfied.

It is recognized that the development of effective emergency procedures entails inputs from a wide variety of sources, ranging from plant transient analyses to human factors analyses. In order to produce effective guidelines, there must be a strong interaction between the human factors analysts, the plant thermal-hydraulics analysts and the plant operations staff. The OAET-based methodologies presented in this volume appear to provide a mechanism by which information concerning the realistic thermal-hydraulic response of plants to risk significant accident sequences and the actions required of the operations staff can be systematically presented in a form which can be readily integrated into human factors engineering analyses.

## LIST OF ACRONYMS

ATOG	Abnormal Transient Operating Guidelines
B&W	Babcock & Wilcox
BWR	Boiling Water Reactor
C-E	Combustion Engineering
CSF	Critical Safety Function
EPG	Emergency Procedure Guideline
ESAS	Engineered Safeguards Actuation System
GE	General Electric
HPCI	High Pressure Coolant Injection (System)
HPI	High Pressure Injection
ICC	Inadequate Core Cooling
LOCA	Loss of Coolant Accident
NRC	Nuclear Regulatory Commission
OAET	Operator Action Event Tree
PORV	Power Operated Relief Valve
PSM	Plant Status Monitoring (Program)
P-T	Pressure - Temperature
PWR	Pressurized Water Reactor
RCIC	Reactor Core Isolation Cooling (System)
RDS	Reactor Depressurization System
RPV	Reactor Pressure Vessel
SASA	Severe Accident Sequence Analysis (Program)
SI	Safety Injection
SLBIC	Steam Line Break Instrumentation and Control
TMI	Three Mile Island
<u>WOG</u>	Westinghouse Owners Group

## CONTENTS

	<u>Page</u>
Section 1. INTRODUCTION AND BACKGROUND	1-1
Section 2. EMERGENCY PROCEDURE DEVELOPMENT IN THE AFTERMATH OF TMI	2-1
2.1. REQUIRED CHARACTERISTICS	2-1
2.2. FUNCTIONS, SYMPTOMS, AND EVENTS	2-3
Section 3. SUMMARY OF OWNERS GROUPS' APPROACHES	3-1
3.1. WESTINGHOUSE OWNERS GROUP PROGRAM	3-2
3.2. COMBUSTION ENGINEERING OWNERS GROUP PROGRAM	3-10
3.3. GENERAL ELECTRIC OWNERS GROUP PROGRAM	3-18
3.4. BABCOCK & WILCOX OWNERS GROUP PROGRAM	3-26
Section 4. DISCUSSION OF OWNERS GROUPS APPROACHES	4-1
4.1. PRACTICAL APPLICATION OF BASIC CONCEPTS	4-2
4.2. VALIDATION OF OWNERS GROUPS' GUIDELINES	4-9
Section 5. PLANT STATUS MONITORING APPROACH	5-1
5.1. PSM METHODS, TOOLS, AND INFORMATION BASE	5-1
5.2. APPLICATION OF PSM APPROACH TO THE REVIEW AND EVALUATION OF EXISTING EMERGENCY PROCEDURES	5-5
5.3. APPLICATION OF THE PSM APPROACH TO THE DEVELOPMENT OF EMERGENCY PROCEDURES	5-10
5.4. DISCUSSION OF PSM APPROACH	5-21
Section 6. CONCLUSIONS	6-1
REFERENCES	R-1

## LIST OF TABLES

	<u>Page</u>
Table 3.1. Plant Status and Trending Table	3-16
Table 3.2. Summary of Actions to Assure Adequate Core Cooling	3-17

## LIST OF FIGURES

Figure 2.1. Hierarchy of Events and Functions	2-6
Figure 2.2. General Diagnostic Structure of Event and Function-Oriented Procedures	2-7
Figure 3.1. Use of <u>WOG</u> "Mixed" Guidelines	3-4
Figure 3.2. Illustration of Mixed Function- and Event-Oriented Approach	3-5
Figure 3.3. Example of <u>WOG</u> CSF Status Tree	3-7
Figure 3.4. C-E Emergency Procedure Guideline System	3-11
Figure 3.5. Operational Information	3-12
Figure 3.6. Structure of GE Guidelines	3-21
Figure 3.7. Functional Guidance in GE Procedures	3-25
Figure 3.8. ATOG Functional Framework	3-28
Figure 3.9. ATOG P-T Diagram	3-30
Figure 3.10. ATOG Flow Diagram	3-33
Figure 3.11. Accident Mitigation Approach	3-35
Figure 5.1. An Example Operator Action Event Tree	5-4
Figure 5.2. Emergency Procedure Review Flowchart for PSM Approach	5-7
Figure 5.3. Emergency Procedure Development Flowchart for PSM Approach	5-11
Figure 5.4. PSM Emergency Procedure Development: Expansion of Step #1	5-14
Figure 5.5. PSM Emergency Procedure Development: Expansion of Step #2	5-15

LIST OF FIGURES (Continued)

	<u>Page</u>
Figure 5-6. PSM Emergency Procedure Development: Expansion of Step #3	5-16

Section 1  
INTRODUCTION AND BACKGROUND

The events at Three Mile Island (TMI) in 1979 emphasized the need for improved emergency operating procedures to guide the operator under accident conditions. Substantial industry effort has since been devoted to alleviating the perceived deficiencies in the form and content of the procedures which existed prior to TMI. On the regulatory side, the post-TMI investigations culminated in the requirements described under Item I.C.1 of NUREG-0737.<sup>[1]</sup> In response to these requirements, groups associated with each of the four major U.S. reactor vendors have developed, or are in the process of developing, guidelines for improved emergency procedures.

Coincident with these activities, the NRC-funded Plant Status Monitoring (PSM) Program has been in the process of developing and validating methodologies to address a number of operations-related safety problems. Much of the work being performed under the PSM Program was also motivated by the events at TMI and the subsequent investigations and resultant recommendations.

The PSM Program has produced a set of methodologies to systematically investigate the role of the operator under accident conditions. The information generated in these investigations has been applied to a number of issues related to enhancing the operator's ability to efficiently respond to accident conditions (see References 2, 3, and 4). One of the conclusions that resulted from this PSM activity is that the methods, tools, and information base developed in the program appear to provide a logical basis for systematically reviewing and evaluating guidelines and procedures which are being produced in response to Item I.C.1 or for generating internally consistent emergency procedure guidelines which are consistent with requirements of Item I.C.1.

The major purpose of the investigations and analyses reported here is to determine if the methods, tools, and information base generated in the PSM program can support the review and evaluation of such emergency procedure guidelines.

## Section 2

### EMERGENCY PROCEDURE DEVELOPMENT IN THE AFTERMATH OF TMI

As previously noted, the events at TMI and the subsequent investigations and analyses of that accident resulted in the conclusion that the existing emergency procedures were deficient in a variety of ways. In this section, these perceived inadequacies are reviewed and the required characteristics of improved procedures which would alleviate these shortcomings are discussed.

#### 2.1 REQUIRED CHARACTERISTICS

Prior to the incidents at TMI, the emergency operating procedures in use throughout the nuclear industry were essentially "event-oriented" procedures. These procedures described the steps which the operator should take given the occurrence of certain pre-selected, pre-analyzed events. Further, the events for which these procedures existed were typically limited to transient events or loss-of-coolant events followed by successful operation of all safety systems designed to respond to these events.

The accident at TMI pointed out a number of serious problems with the form and content of the existing emergency procedures. Among the most important of these evident deficiencies were:

- (1) The procedures did not address accidents which involved multiple failures or provide guidance under conditions of inadequate core cooling.
- (2) It is difficult for the operator to diagnose with confidence which specific event procedure to follow because of the common symptoms exhibited by many different events, especially those involving multiple failures.
- (3) Accidents do not, in reality, progress exactly as predicted in pre-analyzed events.

Thus, the pre-TMI "event-oriented" procedures were perceived to be both lacking in sufficient breadth (important events are not addressed) and too proscriptive with respect to the events which are addressed. Unless the operator

is confronted with an event or sequence of events for which a specific procedure exists, and this sequence evolves just as the procedure predicts, the emergency procedures may be of little assistance to the operator. In fact, rather than providing aid to the operator, the procedures could easily confuse the operator, significantly increase the chance of erroneous response, and thereby compound the operator's problem.

Investigations performed subsequent to TMI have resulted in a number of recommendations concerning improved emergency procedures. Item I.C.1 of NUREG-0737 specifically addresses this issue. The principal underlying theses of most of these recommendations and directives are that improved emergency procedures are needed and that these improved procedures should have the following characteristics:

- (1) They should allow the operator to respond to multiple failure sequences.
- (2) They should allow the operator to quickly respond to maintain critical safety functions without the necessity of knowing the specific events which have occurred.
- (3) They should allow the operator to efficiently and unambiguously diagnose what specific actions are required.
- (4) They should allow the operator to be able to maintain critical safety functions throughout the evolution of the accident even if the accident takes unexpected directions.
- (5) The operator should be able to quickly and clearly diagnose the onset of inadequate core cooling (ICC).
- (6) The procedures should explicitly detail the required operator response to ICC conditions.
- (7) The procedures should provide a clear and logical transition to the ICC procedures.

It has been the goal of a variety of industry programs to produce guidelines for the development of emergency procedures which would exhibit those characteristics. The basic direction that these programs have taken is discussed in Section 3.

## 2.2 FUNCTIONS, SYMPTOMS, AND EVENTS

As noted above, many of the deficiencies associated with the pre-TMI emergency procedures were attributed to the event-specific nature of the procedures. Accordingly, much of the post-TMI emergency procedures activity has been devoted to the development of an alternative procedure framework which does not require the explicit diagnosis of specific events. The major result of this development activity has been the emergence of "function-oriented" or "symptom-oriented" procedures to replace or at least significantly augment the event-specific procedures. The virtually universal perception is that these alternate approaches to procedure development provide the means to remedy the pre-TMI deficiencies discussed in the previous section and can result in procedures which possess the required characteristics described above.

The basic assumption underlying these alternate approaches is that there is a limited set of key safety functions which, if successfully performed automatically or through manual action, result in a "safe" condition for the plant. Thus, the basic design goal of the plant safety systems and the ultimate goal of all operator actions is to ensure the performance of these critical functions.

The attractiveness of this "critical functions" concept evolves from the implication that the operator need only to monitor a relatively few pieces of information to ascertain the status of the plant. While there are a limited number of critical functions, or parameters which indicate the performance of these functions, there is a virtually unlimited number of events (with a wide variety of symptoms) which can affect the performance of these functions. Theoretically, since events are significant only with respect to their impact on these functions, and since the purpose of all operator actions is to perform these functions, the operator can carry out his duties by focusing on these critical functions without regard to the specific events which have occurred. Thus, procedures which are based on the monitoring and maintenance of these critical functions should possess most, if not all, of the required characteristics listed in Section 2.1.

Because these alternate approaches to procedure development form the foundation for much of the post-TMI activity and will be discussed at some length in subsequent sections, it is beneficial at this point to briefly summarize the basic differences between functional or symptomatic procedures and the pre-TMI event-specific procedures. The value of this comparison is heightened by the fact that there are not clear and obvious distinctions among the various approaches. Furthermore, whatever distinctions do exist are often blurred to some extent in actual practice.

The first point to recognize is that the term "event" can be (and often is) used to describe the occurrence of any off-normal plant condition. Thus, "the reduction of primary coolant inventory below level x" and "a cold leg break in excess of y sq. inches," could both be termed events. This broad interpretation of the term "event" is responsible for considerable confusion. If the usage of this term is restricted to describing the occurrence of particular failure modes of specific components, the distinction between event-oriented approaches and the proposed alternative approaches becomes more clear and most of the confusion can be avoided. Thus, under the more restrictive definition "valve xyz fails to open" is an event while "lack of flow to reactor" or "inadequate coolant inventory" are effects of that event. Procedures which require the operator to determine what specific components have failed and how they have failed before any mitigative actions can be performed can clearly be referred to as "event-oriented" procedures.

The effect of any event (or combination of events) can be expressed in terms of its impact on the performance of various plant safety functions. Thus, the relationship of an event to the non-performance of a safety function is that of cause to effect. The confusion caused by a too liberal interpretation of the term "event" is compounded by the fact that "functions" can be (and are) defined at various levels of detail. For example, "maintenance of emergency injection flow to the reactor" and "maintenance of adequate coolant inventory" can both be referred to as functions. However, emergency coolant injection can be just a single example of a way to maintain inventory (or, conversely, failure of injection can be a contributing cause to the failure to maintain inventory). Therefore, there can also be a cause and effect relationship between functions, with the more specifically defined functions being the "causes" of more general functions.

These cause and effect relationships can, therefore, be extended from a specific event to the performance of the most generally defined function. Figure 2.1 illustrates this hierarchical cause and effect relationship.

Theoretically, any procedure which does not require the determination of which specific components have failed can be referred to as "function-oriented." The operator focuses on the performance of a set of functions and does not need to be concerned with what caused the failure of any of these functions to be performed.

Any complete set of functions can be used, and therefore any level above the event level in Figure 2.1 can support functional procedures. However, since the principal motivation behind function-based procedures is to allow the operator to monitor a relatively few key functions, these functions need to be defined at a fairly general level (i.e., near the top of Figure 2.1).

The difference between a function-oriented procedure and an event-specific procedure can become blurred if the functions are defined in fairly detailed terms and/or the events are described in broader terms. In actual practice, the sub-function level depicted in Figure 2.1 often forms the bases for both event- and function-oriented procedures with the difference being only the degree of resolution within that level.

A second key point to recognize is that symptoms can be associated with the occurrence of specific events as well as the performance of general functions. Since operators actually respond to symptoms and not to events or functions, all procedures are, in reality, symptom-based. Event-specific procedures call for the operator to translate the observance of certain sets of symptoms into the occurrence of specific events and respond accordingly. Function-oriented procedures require the operator to translate symptoms into decisions related to the performance of critical functions. These diagnostic processes are illustrated in Figure 2.2. The distinction between symptom-oriented procedures and function-oriented (or event-specific procedures) can, therefore, be merely one of semantics if the sets of key symptoms are linked in a one-to-one correspondence with either the critical functions, specific events, or the associated operator tasks.

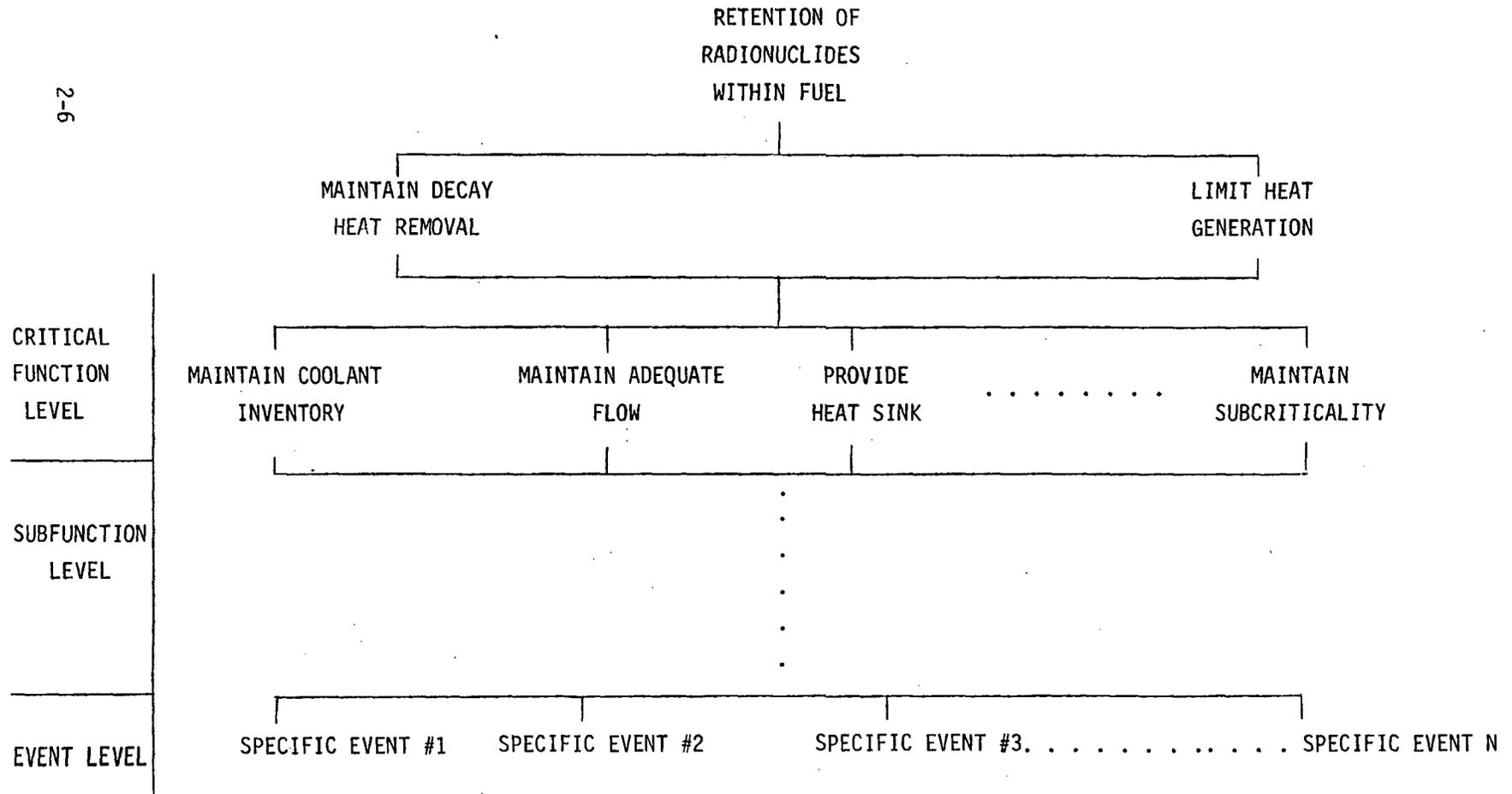
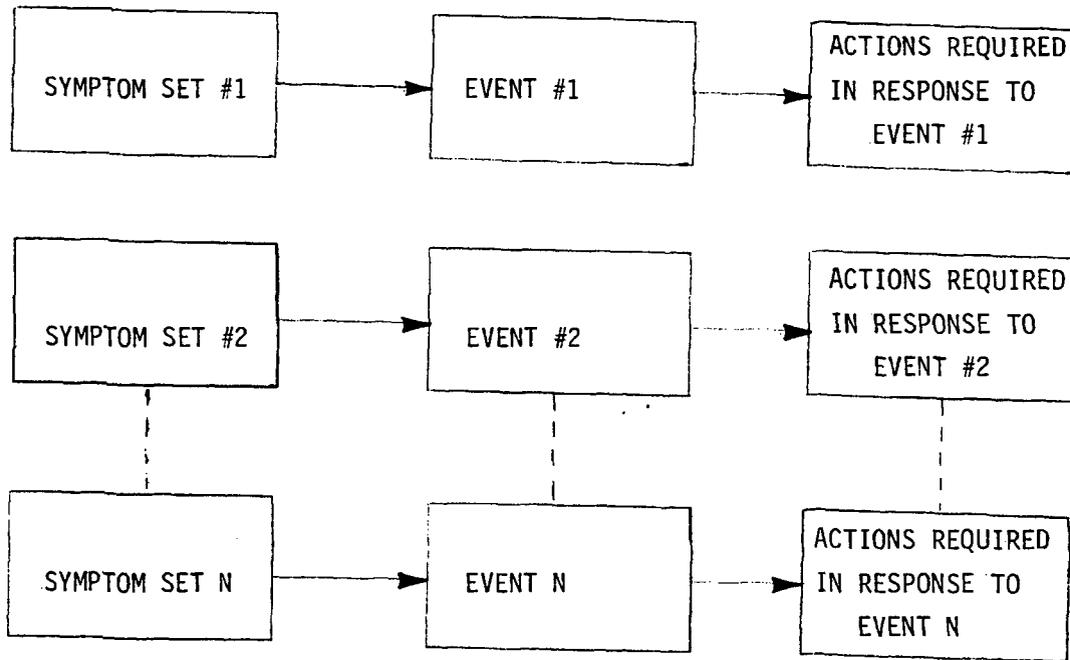
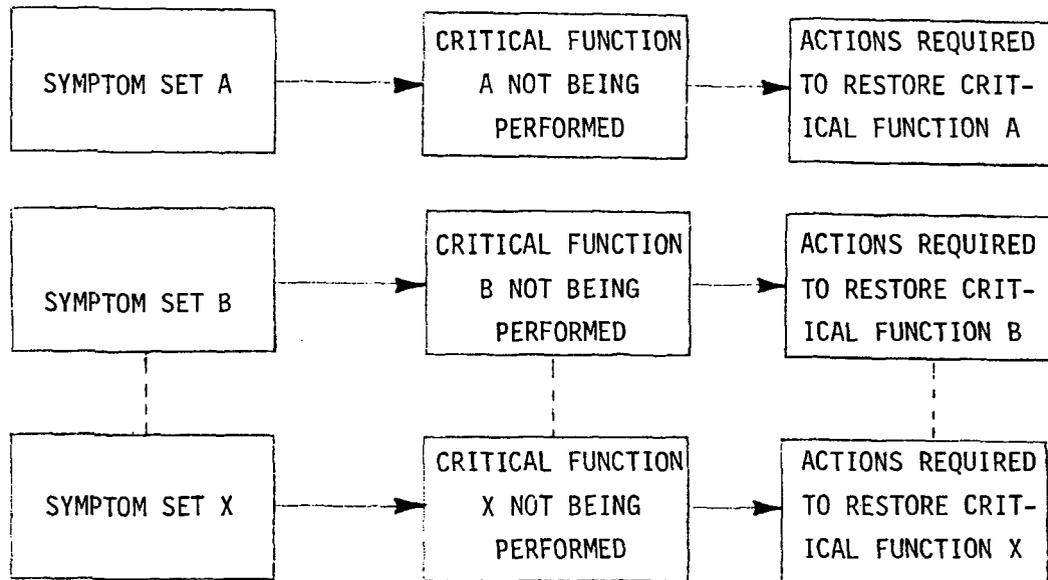


Figure 2.1 Hierarchy of Events and Functions



EVENT-SPECIFIC PROCEDURES



FUNCTION-ORIENTED PROCEDURES

Figure 2.2. General Diagnostic Structure of Event and Function-Oriented Procedures

However, the distinction can gain substance in two basic ways. In the first, the procedures are presented in such a way that the operator is no longer required to explicitly associate symptoms with either the performance of critical functions or the occurrence of specific events. Thus, the second column of Figure 2.2 can be removed by prior analysis and the operator can translate symptom sets directly into actions. The functions being affected or the events which caused the upset become "invisible" to the operator.

Once the need to link symptoms and actions to the performance of particular functions or the occurrence of specific events is removed, it is possible to gain additional substance by investigating in more depth the relationships between the symptom sets and the associated sets of actions. The goal of these investigations is twofold:

- (1) to identify specific actions (or sets of actions) which are always associated with particular symptoms (or sets of symptoms) regardless of the affected function or causal event, and
- (2) to identify a minimal set of symptoms which can be used to identify the need to undertake any set of actions.

In this way, the monitoring activities can be focused on fewer parameters and more efficient diagnostic/action algorithms can be derived.

In the following section, the manner in which each of the four Owners Groups have attempted to develop these basic concepts of functional, symptomatic, and event-specific guidance into practical Emergency Procedure Guidelines will be summarized. In subsequent sections, potential pitfalls of the functional and symptomatic approaches will be discussed and the degree to which the Owners Groups have addressed these problems will be summarized. The basic information presented above should provide the necessary foundation for these discussions.

Section 3  
SUMMARY OF OWNERS GROUPS' APPROACHES

In response to Item I.C.1 of NUREG-0737, groups associated with each of the four major U.S. vendors have endeavored to produce a set of Emergency Procedure Guidelines which alleviates those deficiencies identified in pre-TMI procedures and possesses the necessary characteristics required by the NRC. As previously noted, these efforts have all resulted in the replacement or significant augmentation of event-specific procedures by guidelines based on critical safety functions or the key symptoms indicative of these functions.

In this section, each of the four Owners Groups' approaches is reviewed. The particular manner in which each group uses function- or symptom-oriented guidelines to address the existing procedural deficiencies is summarized.

It should be emphasized that the following summaries are not intended to be detailed critiques of each approach or even a complete presentation of each approach. Each group's efforts are examined with respect to only a few key aspects which are important to the issues addressed in this report. The final submittal of each group should be referred to for more complete information. (This section is based on information available in late 1981 and final versions of the guidelines could differ significantly from those presented here.) In addition, it should be noted that the amount of available information regarding each of the four programs varied considerably. However, the general features of each program relevant to this investigation could be obtained from the available documentation.

### 3.1 WESTINGHOUSE OWNERS GROUP PROGRAM<sup>[5]</sup>

The Westinghouse Owners Group (WOG) Procedures Development and Evaluation Program has produced a set of Emergency Response Guidelines which utilizes a combination of functional and event-specific guidance. The function-based guidance is supplied by what are referred to as Critical Safety Function (CSF) Status Trees and Critical Safety Function Restoration Guidelines. The event-specific guidance is provided by Optimal Recovery Guidelines.

#### 3.1.1 Guideline Structure

As discussed in Section 2.2, functional guidance is based on the premise that there are certain key safety functions, which, as a set, indicate overall plant safety status; that is, if these critical functions can be performed, the plant will necessarily be in a "safe" condition. In the WOG Guidelines, the CSF Status Trees are the primary guidance tools used by the operator to monitor these key safety functions. If the use of these Status Trees indicates that one or more of these critical functions is not being performed, the operator is referred to the appropriate CSF Restoration Guidelines. These Guidelines are designed to allow the operator to successfully restore the critical functions to acceptable values without the need to diagnose the specific event(s) which produced the upset condition.

The inclusion of this function-based guidance in the overall Emergency Recovery Guidelines is designed to address the problems associated with event-specific guidelines discussed in Section 2. However, WOG states that there are practical limitations to the use of these function-based Guidelines. Since the use of these CSF Status Trees and Restoration Guidelines is independent of the specific events which caused the upset condition or the status of plant equipment, they would not necessarily be adequate to permit full plant recovery from an emergency condition. This implies the need for ultimate reversion to a set of event-specific guidelines to fully recover the plant. Additionally, if diagnosis of the event is possible from the start, event-specific guidelines can provide the operator with a more direct, efficient means of responding to the emergency. Therefore, the functional guidance supplied by the CSF Status Trees and Restoration Guidelines is supplemented by a set of event-specific

Optimal Recovery Guidelines which permit plant recovery following event identification and determination of plant equipment status and plant state.

Figure 3.1 illustrates how the operator uses the resultant "mixed" set of functional and event-specific Guidelines. If diagnosis of the event(s) is possible, the operator proceeds with the appropriate Optimal Recovery Guideline until plant recovery is attained. During recovery from a known event, the operator continually monitors the critical safety function. If a challenge to a critical safety function occurs during the recovery (implying the original diagnosis may have been incorrect, or an additional failure has occurred), the Status Trees direct the operator to actions designed to restore the critical function. Upon restoration of all critical safety functions, the plant condition is rediagnosed and the appropriate optimal recovery actions are taken.

If no diagnosis of the specific event can be made, the CSF Status Trees direct the operator to the appropriate CSF Restoration Guidelines. The critical functions are then continuously monitored as the sequences evolve. While the operator is restoring the critical safety functions, diagnosis of the specific event is simultaneously being attempted. When the safety challenge is removed by the operator acting under guidance of the CSF Restoration Guidelines, the plant may then be fully recovered by performing the steps of the appropriate Optimal Recovery Guideline.

Thus, the integrated set of both functional and event-specific guidelines is designed to not only provide for optimal recovery of the plant during identifiable emergency conditions but to also permit the operator to maintain safe plant conditions for all other situations, including non-diagnosed events and for cases where multiple failures or subsequent failures limit the applicability of the pre-defined optimal recovery steps. The basic concept of this "mixed" approach to emergency procedure guidelines is illustrated in Figure 3.2.

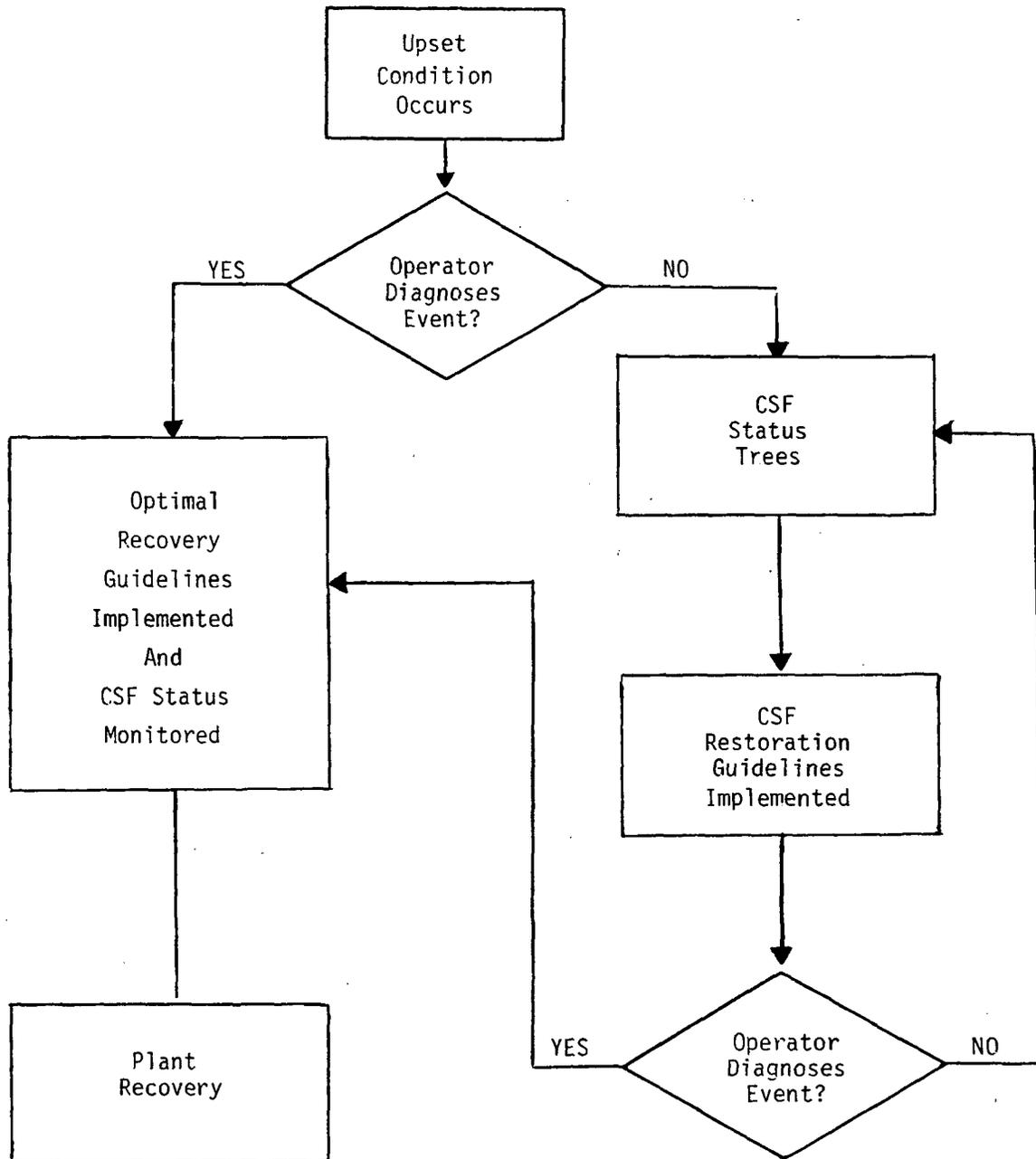


Figure 3.1 Use of WOG "Mixed" Guidelines

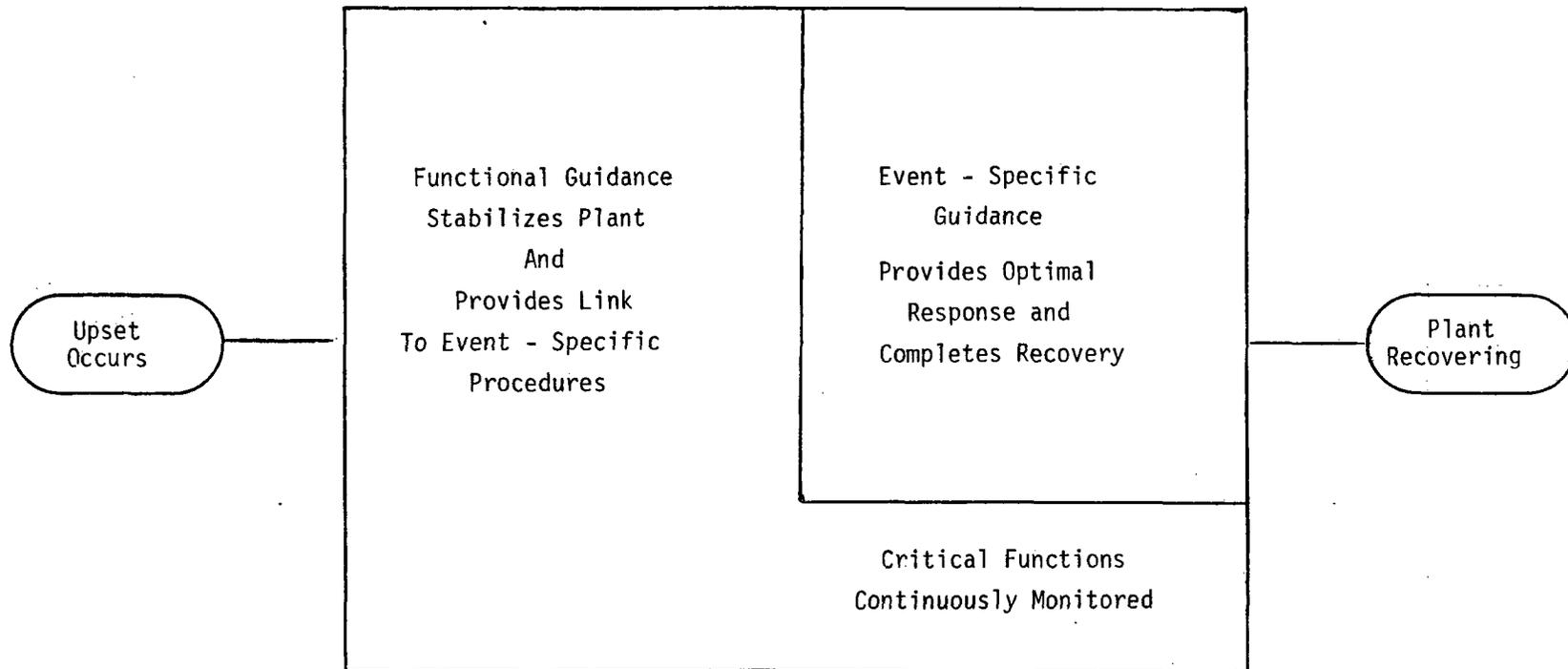


Figure 3.2 Illustration of Mixed Function - and Event - Oriented Approach

### 3.1.2 Functional Guidance

The set of functions that must be performed in order to fully protect the public from the risks of plant operation are referred to by WOG as Critical Safety Functions. The set of Critical Safety Functions selected by WOG for emergency response guideline development is comprised of the following:

- Maintenance of Subcriticality
- Maintenance of Reactor Coolant System Integrity
- Maintenance of Core Cooling
- Control of Reactor Coolant Inventory
- Maintenance of a Heat Sink
- Maintenance of Containment Integrity.

Status Trees are generated for each of these six Critical Safety Functions.

These Status Trees are produced by associating a few key symptoms with the performance (or non-performance) of each Critical Function. The trees are then structured in such a way that each pathway through the tree corresponds to a particular combination of symptoms. For example, Figure 3.3 presents a Reactor Coolant System Integrity Status Tree. The format of this tree implies that the status of this particular function can be evaluated by monitoring two key parameters - RCS pressure and Cold Leg Temperature - and depicts the plant conditions relevant to the performance of this function in terms of these two parameters.

By monitoring a few key parameters, the operator can then determine if the particular Critical Safety Function is being successfully performed and, if not, which CSF Restoration Guideline should be utilized.

# REACTOR COOLANT SYSTEM INTEGRITY

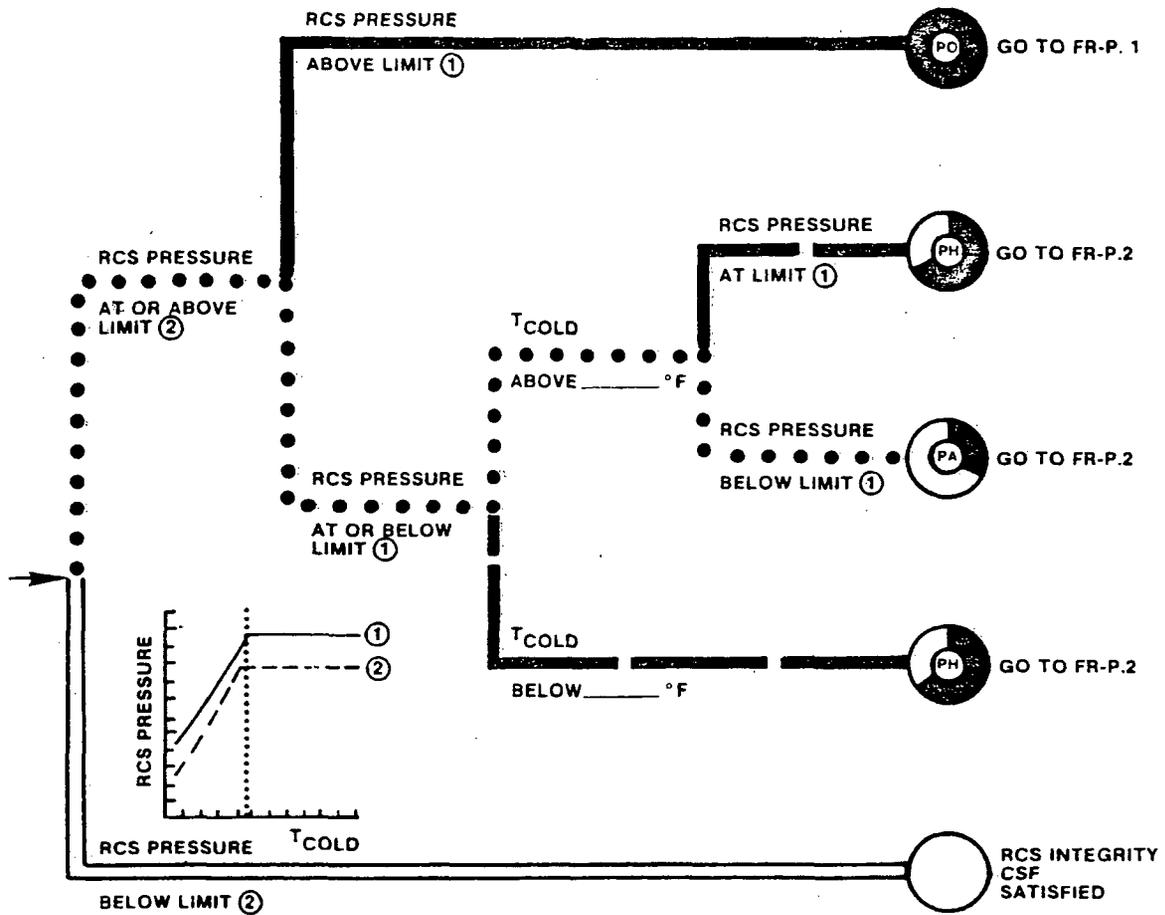


Figure 3.3 Example of WOG CSF Status Tree

The development of CSF Status Trees for each of the six functions listed above resulted in the need for eighteen (18) separate CSF Restoration Guidelines. For example, the RCS Integrity Status Tree discussed above resulted in two CSF Restoration Guidelines: "Response to RCS Overpressurization "and" Response to High RCS Pressure."

Each of these CSF Restoration Guidelines instructs the operator to take a variety of diagnostic steps and particular actions to bring the parameters indicative of the critical function back to acceptable values. The diagnostic steps involve determining the status of various components and systems and monitoring the values and trends of plant parameters. These monitored parameters are not necessarily limited to, and are often far more extensive than, the limited number of parameters associated with the CSF Status Trees.

### 3.1.3 Event-Specific Guidance

Each of the CSF Restoration Guidelines also refers the operator to one or more of the Optimal Recovery Guidelines. This referral to the event-specific procedures is made when sufficient diagnostic steps have been carried out to unambiguously identify the specific event. This may, depending on the observed conditions, occur in the middle of the CSF Restoration Guideline prior to actual function restoration, or at the end of the CSF Restoration Guideline when the critical function has been restored and the plant is in a stable condition. The Optimal Recovery Guidelines are then used to bring the plant to a fully recovered condition.

The WOG Program has developed, or is in the process of developing, twenty-one (21) separate Optimal Recovery Guidelines which can be grouped into seven basic categories. For example, the two CSF Restoration Guidelines to which the operator can be directed from the RCS Integrity Status Tree ultimately refer the operator to the event-specific guidance contained in the Loss of Secondary Coolant Optimal Recovery Guideline or to one of two other related Guidelines (SI Termination Following Loss of Secondary Coolant or Transfer to Cold Leg Recirculation Following Loss of Secondary Coolant).

The Optimal Recovery Guidelines are essentially restructured versions of the original (pre-TMI) Westinghouse Emergency Guidelines and certain of the original Westinghouse Abnormal Guidelines. Reformatting and internal restructuring of the original Guidelines has been performed to provide guidance for situations in which the accident does not progress as anticipated and to facilitate transitions between the guidelines.

## 3.2 COMBUSTION ENGINEERING OWNERS GROUP PROGRAM<sup>[6]</sup>

Combustion Engineering (C-E) has produced an Emergency Procedure Guidelines System in response to Item I.C.1 of NUREG-0737 which is intended to be, with minor modifications, generic to all C-E plants. In a manner similar to that of Westinghouse, the C-E System represents a combination of functional and event-specific guidance. The information contained in this section is based upon descriptions of the C-E program as of late 1981. Since the C-E guidelines are expected to continue to evolve, the latest available (or final) version of the guidelines should be referred to.

### 3.2.1 Guideline Structure

The general structure of the C-E Emergency Procedure Guidelines System (as of late 1981) is depicted in Figure 3.4. Event-oriented emergency procedure guidelines form the core of the C-E System. These event-oriented guidelines are supplemented by an Inadequate Core Cooling (ICC) Guidance Package which provides tabulated information which is intended to allow the operator to determine (1) parameters indicative of the status of the critical safety functions, (2) definitions of acceptable performance and trending of these parameters for each function, and (3) the appropriate response(s) associated with the loss of each safety function.

The combination of the event guidelines with the plant status and trending diagnostics included in the ICC Guidance Package is intended to provide the operator two general diverse paths for implementing the emergency procedures. A simple flow chart depicting how the operator uses the C-E guideline system is presented in Figure 3.5.

Given the occurrence of any upset event, the operator first attempts to associate the symptoms being exhibited by the plant with events for which guidelines exist. The operator would do this by attempting to match symptom sets observed in the control room with symptom sets listed in the emergency procedure guidelines. If the operator believes he understands what is happening due to his perceived ability to match these symptom sets, he will begin to implement the immediate actions of the event guidelines to which he is led.

EMERGENCY PROCEDURE GUIDELINES SYSTEM SUMMARY DESCRIPTION

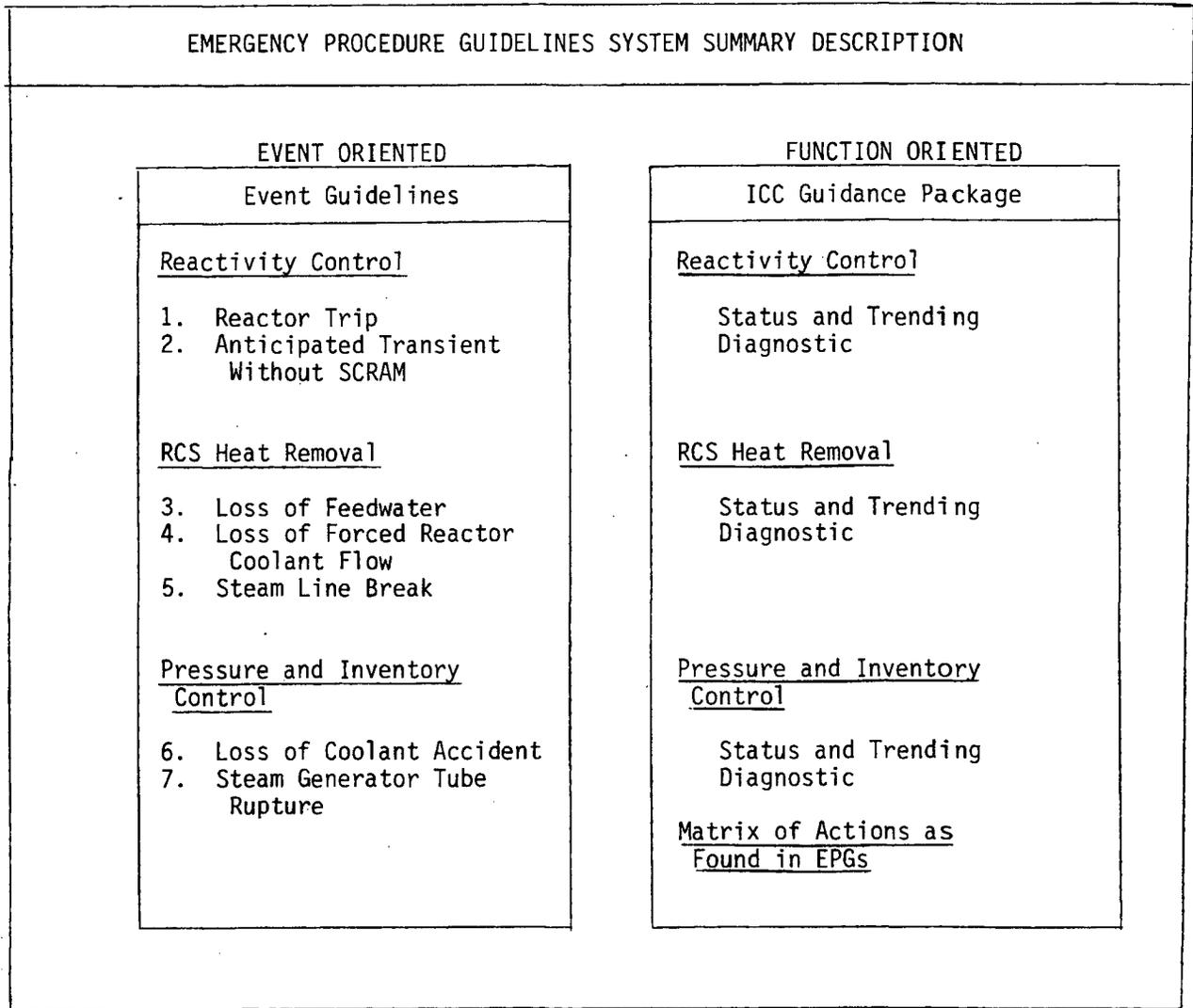


Figure 3.4 C-E Emergency Procedure Guideline System

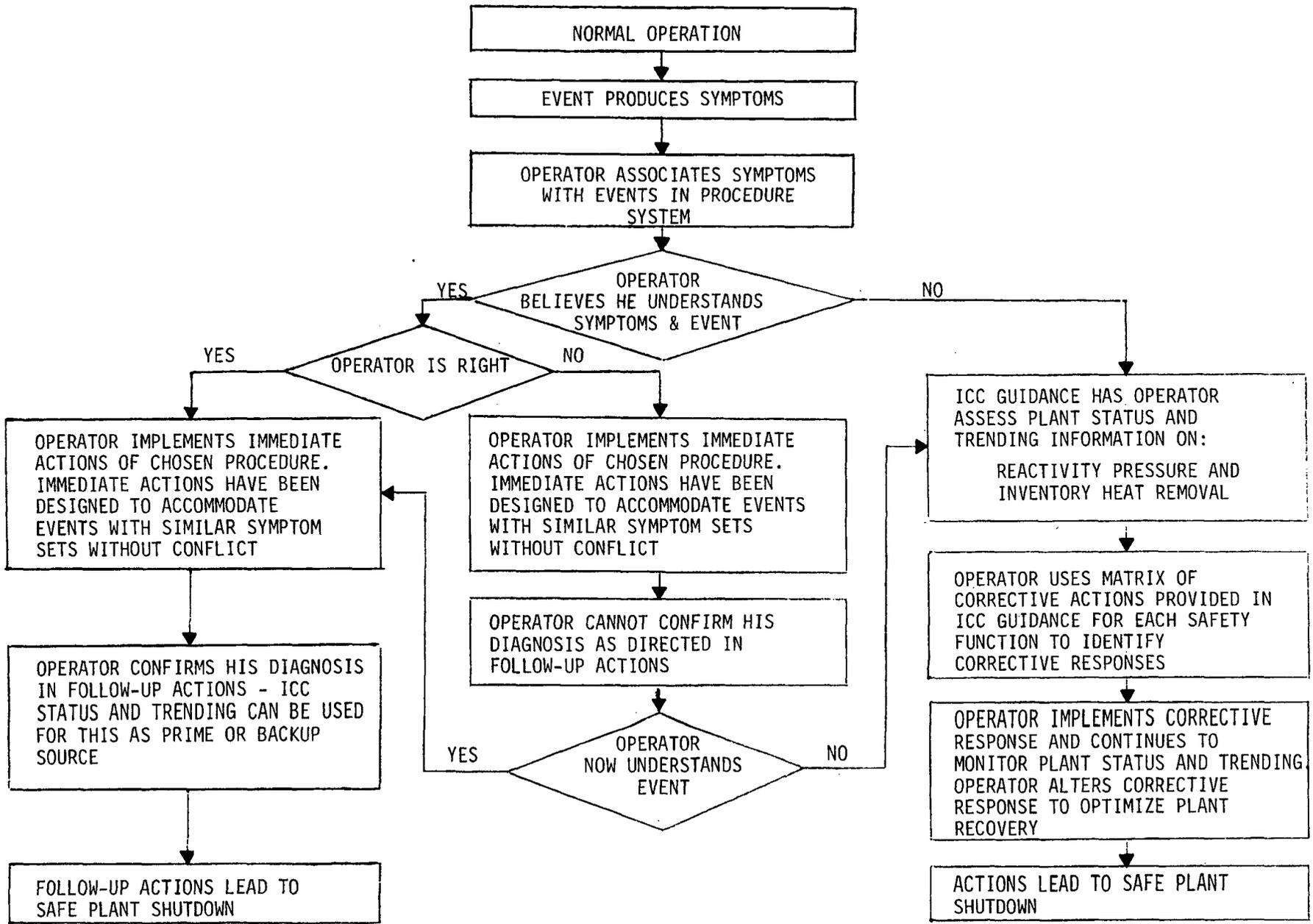


Figure 3.5 Operational Information

If the operator does not feel confident in his diagnosis of the event, or if the initial diagnosis path has failed to produce the desired plant response and he therefore cannot confirm his diagnosis, he is directed to the functionally oriented status and trending diagnostic provided in the ICC Guidance Package.

### 3.2.2 Functional Guidance

The C-E System provides function-oriented guidance to the operator which is intended to be used when the operator does not understand the symptoms being exhibited by the plant or when he is unable to find a good fit between these symptoms and symptom sets provided for each event guideline. This functional guidance is provided in the form of two tables in the ICC Guidance Package.

The first is a Plant Status and Trending Table. A portion of this table is presented for illustrative purposes as Table 3.1. For each of four critical safety functions (Reactivity Control, RCS Heat Removal, RCS Inventory and Pressure Control, and Containment Integrity) the Plant Status and Trending Table lists the following:

- Various normal and emergency methods for controlling the function
- A set of parameters which are intended to provide an indication of the performance of the function
- A definition of the acceptable status and trend for each parameter
- A general description of the plant condition implied by unacceptable status or trending of each parameter
- A reference to the guideline(s) which address these plant conditions.

The second table provided by C-E in their ICC Guidance Package summarizes, in a matrix format, the corrective actions associated with a loss of each safety function and a checklist of the procedure guidelines which address these responses. A portion of this table is presented for illustrative purposes as Table 3.2.

Thus, when confronted with a plant condition that is not readily diagnosed or if the actions taken by the operator in accordance with a particular event guideline do not produce the anticipated plant stability, the operator is instructed to use these two tables (or, presumably, a procedure developed by the individual utility based on these tables) to ascertain the status of the critical safety functions (by examining the behavior of the listed parameters), take the actions associated with each function, and proceed to the indicated event guidelines for further guidance.

Function-oriented guidance is also integrated into the event guidelines in a variety of ways, including:

- (1) the guidelines themselves are defined and grouped in accordance with the critical safety functions,
- (2) within each guideline, the operator is instructed to confirm his diagnosis using the Status and Trending Table, and
- (3) the supporting documentation accompanying each guideline (see below) discusses the anticipated plant response and required corrective actions with respect to the performance of the critical safety functions.

### 3.2.3 Event-Specific Guidance

The C-E System provides event-oriented guidelines for the seven specific events listed in Figure 3.4. The operator is expected to implement these procedures by matching observed symptom sets with symptom sets provided in each guideline. Each of these seven guidelines is comprised of five essential parts:

- Bases: This section provides the operator with a substantial amount of information concerning the plant response to the particular event and an explanation of the required corrective actions. This information is presented as a condensation of realistic transient analysis, licensing analysis, hardware data, incident reports, sequence of events diagrams, etc. This section will primarily be used in training. The development of the bases section is accomplished in parallel with the symptoms and corrective action sections (discussed below) to assure internal consistency.

- Symptoms: A list of plant parameters and their anticipated behavior given the event are provided to allow the operator to choose the appropriate guideline. These symptom sets were generated by surveying symptoms currently used in existing emergency procedures for each event and adding symptoms identified in the realistic analyses of the event. The combined list was then analyzed to determine a "best judgment" set of symptoms and these symptoms were then prioritized. A comparison of the event-specific symptom sets was then made in an attempt to ensure that each set was unique to a specific event. Where symptom sets were found to be similar for diverse events, specific symptoms were highlighted to help the operator distinguish between the events.
- Immediate Actions: This section lists those actions required to place the reactor in a safe condition. The list was generated by a survey of the immediate actions for each event found in the existing procedures, preparation of a "best judgment" listing, and analysis and adjustment of this listing. If a set of immediate actions is applicable and these events exhibit common or similar symptoms, these events were combined to facilitate operator diagnosis and response. The guidelines were reviewed to assure that guidance for the control of all critical safety functions appropriate to the event was addressed.
- Follow-up Actions: This section provides the operator with additional guidance subsequent to the performance of the immediate actions. This guidance is intended to place the plant in a stable condition, permit problems to be corrected, and allow recovery operations (hot standby, hot shutdown, or cold shutdown) to commence. These actions tend to contain more information and cover a greater range of possible failures and alternative actions. If a particular failure, taken in conjunction with an initiating event, places the plant in a position from which recovery is possible by following the actions of another guideline, the follow-up action refers the operator to that guideline.
- Precautions: This section provides additional information to the operator to alert him to measures that can enhance his response. This information is generated by examining the immediate and follow-up actions and noting special circumstances associated with specific events, actions which should be performed only after certain specific conditions exist, potentially confusing symptoms, etc.

Table 3.1  
Plant Status and Trending Table

RCS INVENTORY AND PRESSURE CONTROL

METHOD FOR CONTROL	PARAMETER	ACCEPTABLE STATUS AND TREND*	IF UNACCEPTABLE, IMPLIED CONDITION	GUIDELINE
1. Auto or Manual Control of CVCS	A. Charging pump flow	A. Maint. press. level between 42% and 56% and constant	A. Loss of RCS coolant replacement Loss of chem/ reactivity control	A. Reactor trip
	B. Letdown flow	B. Maint. press. level between 42% and 56% and constant	B. Loss of chem/ reactivity control	B. Reactor trip
	C. Pressurizer Level	C. Maint. press. level between 42% and 56% and constant	C. Loss of RCS coolant replacement Loss of chem/ reactivity control	C. Reactor trip
	D. RCS subcooled	D. > 20°F subcooled and constant or increasing	D. Voids in RCS	D. LOCA, loss of flow/NC
	E. T <sub>H</sub>	E. < 620°F and constant or decreasing	E. Loss of liquid phase coolant reduces effectiveness of pressurizer	E. LOCA, loss of flow/CS
	F. Core exit thermocouples	F. < 620°F and constant or decreasing	F. Core heating up	F. LOCA, loss of flow/NC
2. SIS Operating	A. HPSI flow	A. > 600 gpm and constant or decreasing	A. Loss of coolant replacement	A. LOCA, S/G tube rupture
	B. LPSI flow	B. < 4000 gpm pre RAS and constant or decreasing	B. Loss of coolant replacement	B. LOCA
	C. RCS subcooled	C. > 20°F subcooled and constant or increasing	C. Voids in RCS	C. LOCA, S/G tube rupture, loss of flow/NC
	D. T <sub>H</sub>	D. < 20°F and constant or decreasing	D. Loss of liquid phase coolant	D. LOCA, loss of flow/NC
	E. Core exit thermocouples	E. < 620°F and constant or decreasing	E. Core heating up	E. LOCA, loss of flow/NC
3. Automatic or Manual Control of Pressurizer Heater or Spray Valve	A. Heaters	A. Maint. PZR. press. between 2010 psia and 1975 psia	A. Pressure decreasing	A. Reactor trip
	B. Spray flow	B. Maint. PZR. press. between 2010 psia and 1975 psia	B. Pressure increasing	B. Reactor trip
	C. Auxiliary spray	C. Maint. PZR. press. when spray flow is not available	C. Pressure increasing	C. Loss of flow/NC
	D. RCS subcooled	D. > 20°F and constant or increasing	D. Voids in RCS	D. LOCA, loss of flow/NC

Table 3.2

## Summary of Actions to Assure Adequate Core Cooling

RCS INVENTORY CONTROL	REACTOR TRIP	ANTICIPATED TRANSIENT WITHOUT SCRAM	LOSS OF FEED WATER	LOSS OF COOLANT ACCIDENT	STEAM GENERATOR TUBE RUPTURE	STEAM LINE BREAK	LOSS OF FORCED REACTOR COOLANT FLOW
1. ISOLATE THE BREAK IF POSSIBLE			X	X	X	X	X
2. VERIFY THAT THE PLCS IS AUTOMATICALLY RESTORING PRESSURIZER LEVEL	X	X	X	X	X	X	X
3. IF NECESSARY, MANUALLY OPERATE CHARGING AND LETDOWN TO RESTORE AND MAINTAIN NORMAL PRESSURIZER LEVEL	X	X	X	X	X	X	X
4. MAINTAIN RCS INVENTORY USING THE SIS							
A. IF PRESSURIZER PRESSURE FALLS BELOW (1600 PSIA), VERIFY INITIATION OF SAFETY INJECTION. IF NECESSARY, MANUALLY INITIATE SAFETY INJECTION	X	X	X	X	X	X	
B. IF THE SIS IS OPERATING, IT MAY BE STOPPED IF THE FOLLOWING CONDITIONS ARE SATISFIED:	X	X	X	X	X	X	
1. RCS HOT AND COLD LEG TEMPERATURE ARE AT LEAST 20°F + (INACCURACIES) BELOW SATURATION TEMPERATURES FOR PRESSURIZER PRESSURE	X	X	X	X	X	X	
2. A PRESSURIZER LEVEL IS INDICATED	X	X	X	X	X	X	X
3. ONE STEAM GENERATOR HAS AN INDICATED LEVEL AND IS REMOVING HEAT FROM THE RCS	X	X	X	X	X	X	X
C. IF 20°F + (INACCURACIES) OF SUBCOOLING (REFER TO FIGURE 2) CANNOT BE MAINTAINED AFTER THE SIS HAS BEEN STOPPED, THE HPSI SYSTEM MUST BE RESTARTED	X	X	X	X	X	X	X

### 3.3 GENERAL ELECTRIC OWNERS GROUP PROGRAM<sup>[7]</sup>

The General Electric (GE) Emergency Procedure Guidelines are intended to provide generic guidance for BWR 1 through 6 designs. In contrast to the W and C-E programs discussed previously, the GE guidelines do not explicitly contain event-specific guidance. They do not explicitly allow the operator to "short-circuit" the function-based guidance if diagnosis of the specific event is possible. The GE guidelines therefore are intended to replace and not merely augment event-specific procedures. The implication of this approach is that the functional guidance provided to the operator is sufficient by itself to allow efficient response to all events and bring the plant to cooldown conditions and that a reversion to event-specific procedures when deemed appropriate by the operator can only raise the possibility of inapplicability of the procedure due to initial misdiagnosis or the occurrence of subsequent additional failures.

#### 3.3.1 Guideline Structure

There are two basic levels of guidance provided in the GE Emergency Procedure Guideline package. The more general level is constructed around three emergency procedures guidelines\*:

- Level Control Guideline
- Cooldown Guideline
- Containment Control Guideline

The Level Control Guideline is intended to restore and stabilize reactor pressure vessel water level. This guideline is entered when certain symptoms indicative of a need to restore level are observed. Once the reactor pressure vessel water level has been stabilized, the operator is directed to the Cooldown Guideline. The Cooldown Guideline maintains vessel water level while depressurizing the reactor to cold shutdown conditions.

---

\*This section is based on Revision 1 of the guidelines. Revision 2 utilizes only two guidelines, the RPV Control Guideline and the Containment Control Guideline.

The Containment Control Guideline is intended to maintain the primary containment temperature, pressure, and level within acceptable limits. This guideline is utilized whenever key symptoms indicative of unacceptable containment conditions are observed. The Containment Control Guideline is essentially composed of five "sub-guidelines" addressing:

- suppression pool temperature control
- drywell temperature control
- containment temperature control
- drywell pressure control
- suppression pool water level control.

If during the process of implementing these general guidelines or sub-guidelines, the operator is unable to successfully accomplish and confirm the stabilization of the vessel level or the containment parameters due to failures in the systems designed to perform these functions, he is directed to a more detailed level of guidance provided in six contingency procedures. A contingency procedure is entered from either one of the guidelines or from another contingency procedure. For example, the operator is directed to the Contingency #1 procedure if his actions outlined in the Level Control guideline have not resulted in a water level above the top of active fuel; this procedure instructs the operator to take a number of alternate measures to maintain level (e.g., use of Fire System) and, in turn, directs the operator to the Contingency #2 procedure (Rapid Depressurization) if the HPCI and RCIC are not available and RPV pressure is increasing.

These more detailed Contingency Procedures might be considered to be event-specific guidelines. As discussed in Section 2.2, the border between functional and event-specific guidance becomes very hazy when sub-functions or broadly defined events are addressed (see Figure 2.1). This portion of the GE Guidelines falls into that hazy area between obviously functional and clearly event-specific guidance.

The basic structure of the GE guideline package is illustrated in Figure 3.6.

In addition to the three general guidelines and the associated contingency procedures, GE has provided the operator with twenty (20) Operator Precautions\* which are intended to alert the operator to special considerations of plant physical response and necessary constraints on operator emergency response.

Finally, GE has included a section which provides the basis for certain steps in the procedures and for the operator cautions. This basis is primarily intended to be used in training, but may be referred to under emergency conditions in order to clarify the guidance.

### 3.3.2 Functional Guidance

As noted above, the GE guidelines package provides guidance on two basic levels - a set of three general guidelines and a set of six more detailed contingency procedures. The three general guidelines are essentially based upon six critical safety functions:

- (1) Maintenance of vessel water level
- (2) Limitation of suppression pool temperature
- (3) Limitation of drywell temperature
- (4) Limitation of containment temperature
- (5) Limitation of drywell pressure
- (6) Maintenance of suppression pool water level.

The first function is addressed in the Level Control Guideline; the remaining five functions are addressed in the five "sub-guidelines" contained in the Containment Control Guideline.

In the GE guidelines, the operator's first responsibility is to ascertain the need to take action to perform one or more of these six critical functions.

---

\*Revision 2 contains 25 cautions.

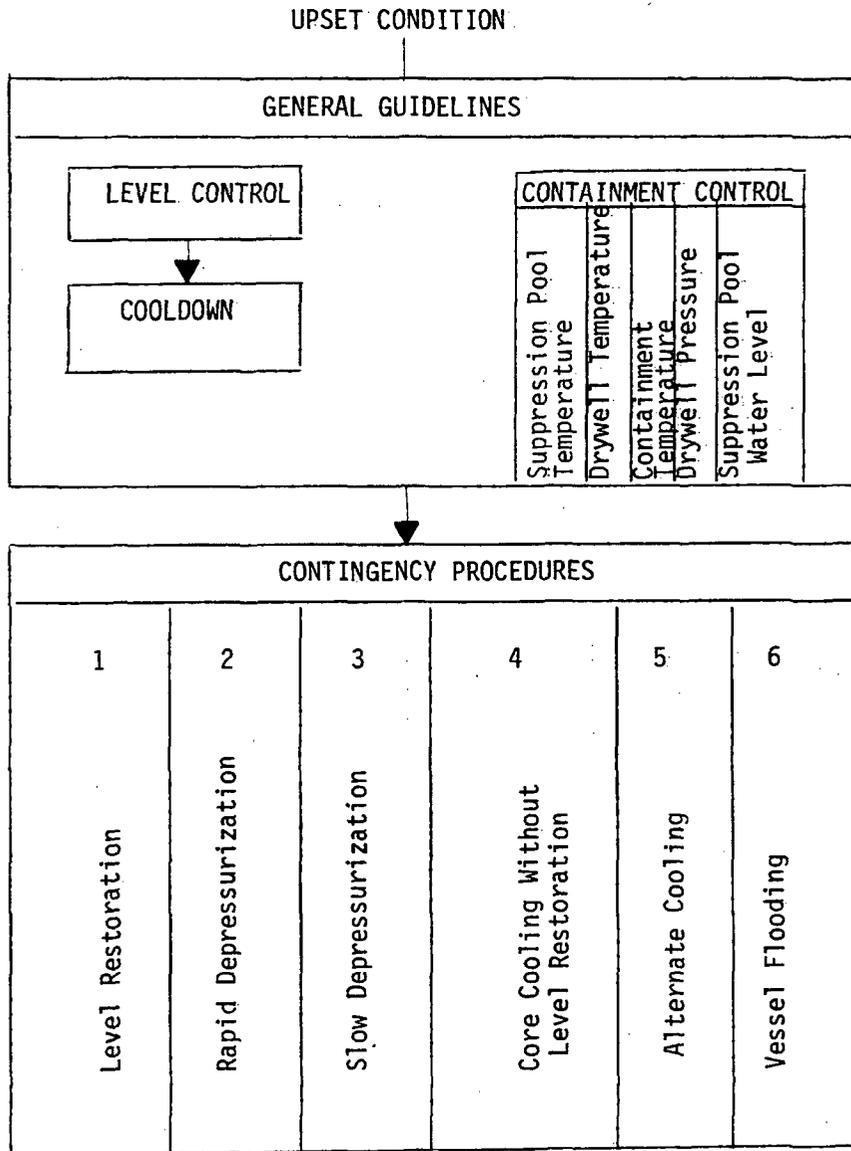


Figure 3.6. Structure of GE Guidelines

He is instructed to make this determination by matching symptoms observed in the control room to the entry conditions for each of the six general guidelines (Level control plus five Containment Control guidelines). These entry conditions are expressed in terms of the behavior of parameters indicative of the status of the critical functions. The operator determines that the Level Control Guideline should be implemented by observing RPV water level, the drywell pressure, or indication of an isolation which requires or initiates reactor scram. The operator is instructed to implement the Containment Control Guidelines based on the observance of five key parameters, each associated with one of the critical functions addressed in this Guideline (i.e., suppression pool temperature, drywell temperature, etc.). The Cooldown Guideline is implemented after completion of the Level Control Guideline when vessel water level is observed to be stable. Thus, the operator is called upon to monitor only seven distinct key parameters to ascertain the status of the critical safety functions and determine the appropriate general procedure(s) to carry out.

This very simple functional guidance scheme is illustrated in Figure 3.7: Six critical safety functions are defined; a procedure guideline (or "sub-guideline") is provided for maintenance of each function; for each of the five "sub-guidelines," a single symptom is listed which is intended to allow the operator to determine that he should implement the actions of that guideline; the observance of any one of three symptoms should cause the Level Control Guideline to be implemented.

Once the operator has entered one of the general guidelines, he will either successfully achieve the goal of the guideline or he will be directed to one of the contingency procedures. The operator is directed to these contingency procedures in those cases where the critical function has not been restored and the key parameter(s) are still not within acceptable limits. The operator can, therefore, determine the need to move from the general guideline to a particular contingency plan based on the same seven key symptoms he initially used to enter the general guideline. The operator will be directed to one of three of the contingency procedures. The other three contingency procedures can only be entered from another contingency procedure.

The six contingency procedures represent six fundamental sets of operator actions:

- Contingency #1: Use of alternate injection systems to restore level
- Contingency #2: Rapid Reactor Depressurization  
(when injection system available)
- Contingency #3: Slow Reactor Depressurization  
(when injection systems unavailable)
- Contingency #4: Use of core spray systems for core cooling without level restoration
- Contingency #5: Alternate Shutdown Cooling by establishing flowpath through open safety/relief valve
- Contingency #6: Reactor Flooding

The implication of the GE guidelines is that, regardless of the specific events which caused the initial upset or prevented the operator from stabilizing the plant with the general guidelines, the appropriate operator response is represented by one (or more) of these sets of actions.

The operator is directed to contingencies #1, #2, or #5 from the general guidelines; he uses the seven key parameters plus reactor pressure and level to determine which of these contingency procedures (if any) to implement. The actions contained in Contingency #1 procedure can, in turn, result in the operator being directed to contingencies #2, #3, or #4. The operator decides whether to enter these contingency procedures based on the behavior of these same seven key parameters, reactor pressure, and indicators of injection system(s) status. During the implementation of contingency #2, the operator may be directed to Contingency #6; the symptoms which indicate the need to implement Contingency #6 include the seven key parameters plus suppression chamber pressure, reactor pressure, and cold leg temperature.

Thus, the operator can determine which general guideline to implement by monitoring seven key parameters. He can determine which specific contingency procedure to carry out by monitoring the seven key parameters plus reactor pressure, cold leg temperature, suppression chamber pressure, and indicators of the status of each injection system.

Due to the inherent interdependence of the critical safety functions, the operator will often be called upon to simultaneously implement multiple procedures. For example, an elevated drywell pressure will cause the operator to enter the procedure produced from the Level Control Guideline as well as that portion of the containment control procedure which addresses drywell pressure limitation. In more general terms, virtually all transient events leading to isolation or most LOCAs will cause the simultaneous implementation of five of the six containment control procedures, the level control procedure, and, subsequently, the cooldown procedure. Thus, the interdependence of the critical safety functions and associated symptoms will often result in the situation where the operator's initial diagnostic task is not to differentiate the appropriate procedure to carry out but to determine that (virtually) all procedures should be carried out. This implies that a great majority of postulated BWR accidents are very similar in their basic effects on the plant and in their general requirements for operator response.

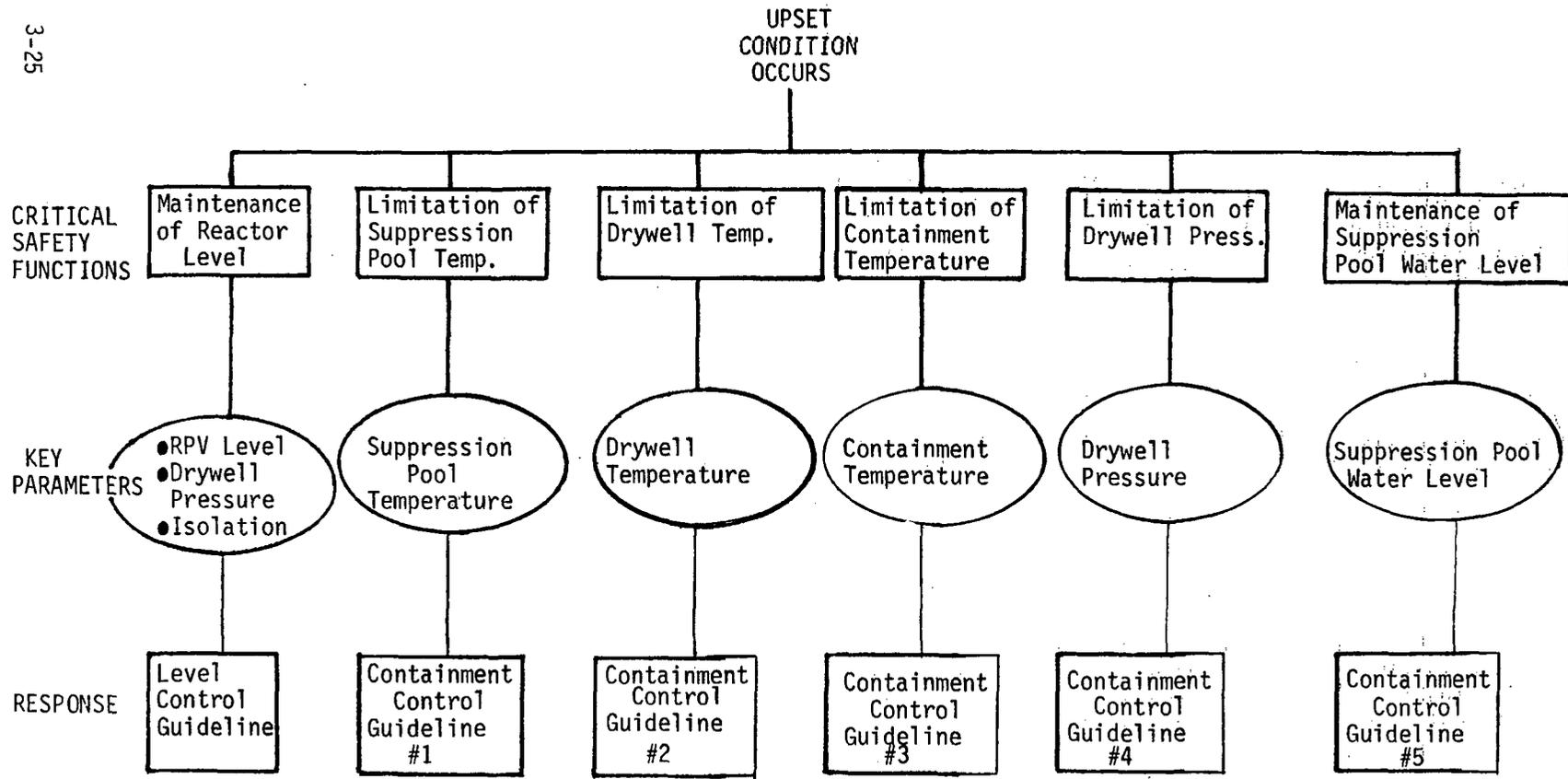


Figure 3.7. Functional Guidance in GE Procedures

### 3.4 BABCOCK & WILCOX OWNERS GROUP PROGRAM [8]

Babcock & Wilcox (B&W) has established the Abnormal Transient Operating Guidelines (ATOG) Program to serve as a basis for the development of emergency procedures for B&W plants. Based on the discussion found in Section 2.2 which compared the basic approaches to guideline development, the ATOG approach can be more clearly characterized as "symptom-oriented" than the approaches utilized by the other three vendors. As such, the form of the ATOG-based guidelines differs considerable from that of the other groups. As will be discussed below, the ATOG program has moved beyond that basic concept of functional guidance and has introduced methods and tools which clearly differentiate it from other procedure development programs.

#### 3.4.1 ATOG Approach

The Abnormal Transient Operating Guidelines are based on the principle that there are only two general accident "types":

- Excessive primary to secondary heat transfer through the steam generators ("overcooling")
- Inadequate primary to secondary heat transfer through the steam generators ("overheating")

Accidents involving a loss of subcooling margin can be combined with or caused by either overheating or overcooling. Thus, at the most general level, the ATOG program is based on one critical safety function -- "maintenance of acceptable primary to secondary heat transfer through the steam generators". On a slightly more detailed level, all operator actions are directed at the performance of three critical safety functions:

- maintenance of minimally acceptable heat transfer
- avoidance of excessive heat transfer
- maintenance of a sub-cooling margin

These three critical functions provide the basic framework for the B&W guidelines. As will be discussed below, one of the operator's key responsibilities in the B&W Guidelines is to quickly determine if one or more of these critical functions is not being performed and to thereby diagnose the basic accident "type".

Just as all potential events (or combinations of events) with which the operator might be confronted can be grouped into a few basic accident types, ATOG recognizes that all potential operator actions to mitigate these accidents can be grouped into a few basic modes of operator response. The general goal of controlling heat transfer from the primary to secondary system can be accomplished by five fundamental methods:

- Reactivity Control
- Reactor Pressure Control
- Reactor Inventory Control
- Steam Generator Pressure Control
- Steam Generator Inventory Control

These "types" of operator response form the framework for the development of the instructions to the operator for each of the accident types.

These methods of heat transfer control can be viewed as an alternative set of critical safety functions which is derived from the triad of functions presented previously. Thus, a hierarchy of critical safety functions, as depicted in Figure 3.8, has been developed which forms the framework for both accident diagnosis and operator action definitions.

A key element of the ATOG approach is an integrated diagnostic scheme which was evolved from the functional framework depicted in Figure 3.8. As stated above, one of the operator's first duties is to determine the basic accident type (with the different type corresponding to the three critical functions in Figure 3.8). Rather than merely listing a large array of symptoms

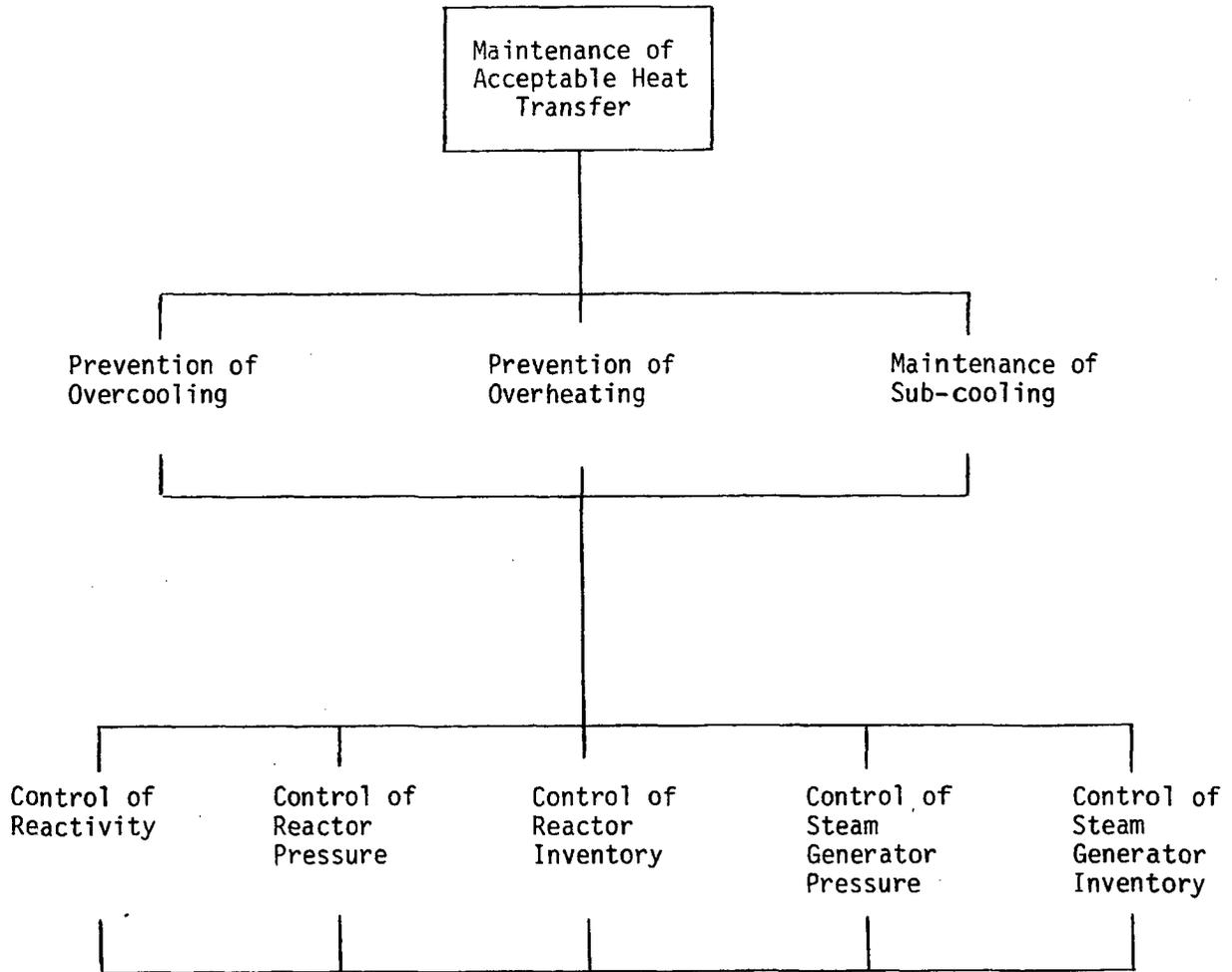


Figure 3.8 ATOG Functional Framework

for each of the accident types, ATOG has examined the expected symptom sets associated with each type and has developed a relatively simple diagnostic tool which is intended to allow efficient determination of the basic accident type.

This tool is based on the control functions depicted in Figure 3.8. Since these control functions are both an alternate representation of the three critical functions and a delineation of the basic modes of operator response, they can provide an effective framework for the process of determining the accident type and identifying corrective actions.

The tool, referred to as a "P-T diagram", is illustrated in Figure 3.9. As displayed in Figure 3.9, the P-T diagram is used to depict the time dependent behavior of both the primary and secondary pressure and temperature (thus "P-T"). From just these few basic parameters, the operator can determine a substantial amount of information concerning the type of accident which is occurring and the appropriate corrective action. The key pieces of information which the operator can derive from plotting the trends of reactor coolant pressure vs. temperature and steam generator pressure vs. temperature are:

- The occurrence of overheating transients which produce a reactor coolant P-T trend line which moves upward and to the right.
- The occurrence of overcooling transients which produce a trend line which moves lower and to the left.
- The degree of subcooling and the approach to loss of subcooling.

Thus, the operator can quickly categorize the basic accident type by using the P-T diagram.

The P-T diagram can also provide a considerable amount of more detailed information concerning key accident characteristics. In fact, P-T diagram trendlines can be used as the basic accident indicators instead of sets of individual symptoms. By analyzing potential events or combinations of events and

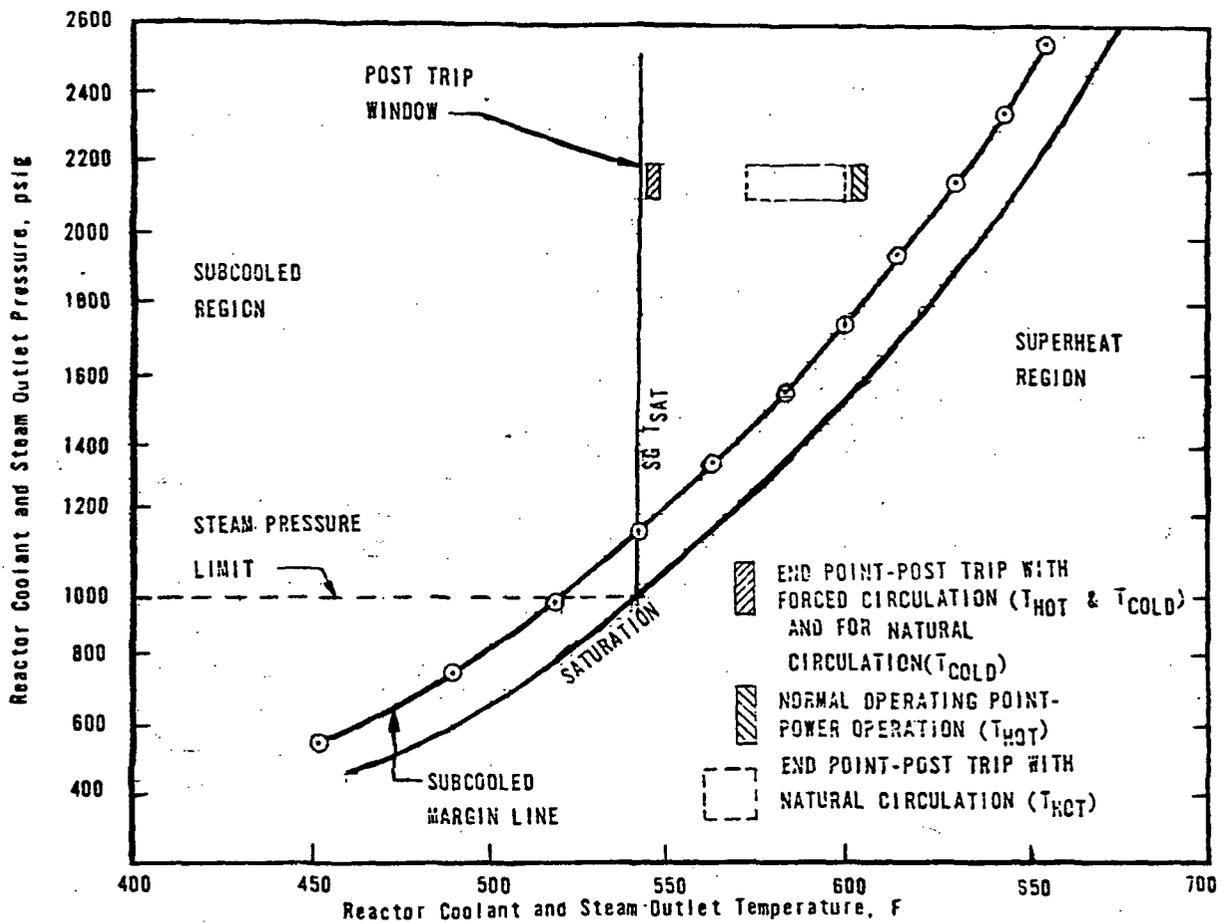


Figure 3.9 ATOG P-T Diagram

describing the resultant plant response in terms of the P-T trendline instead of sets of individual symptoms, the ATOG Program has provided the operator with a symptom-based diagnostic procedure. Thus, by consolidating much of the symptom information necessary for effective diagnosis into P-T trendlines, the ATOG approach has moved beyond the "critical function - symptom set - required response" format illustrated in Figure 2.2.

#### 3.4.2 ATOG Structure

Presented in Figure 3.10 is a general flow diagram which illustrates how the operator utilizes the B&W guidelines in response to potential accident conditions. Figure 3.11 represents an expanded version of this accident mitigation approach. The operator response sequence depicted in Figure 3.11 is initiated by an automatic or manual reactor trip.

The operator is first called upon to take a set of "Immediate Actions" after the reactor trip. Included in these initial information gathering actions are: (1) a determination if a reactor trip, Engineered Safeguards Actuation System (ESAS), or Steam Line Break Instrumentation and Control (SLBIC) actuation signal was initiated; special actions must be taken depending on which signal was initiated, and (2) a quick determination of the status of various plant safety systems. This information will later assist the operator in carrying out his required duties and will allow him to determine if either of two accidents which require fast identification and response have occurred. These two accidents are excessive main feedwater and steam generator tube failures. If either of these have occurred, the operator will take immediate action to mitigate their effects.

The next major block of Figure 3.10 is the P-T diagram check. As discussed previously, the P-T diagram is the foundation for accident diagnosis and corrective response. This diagram is used to identify the general accident type. If the P-T diagram shows that the plant is successfully responding to the initiating event, the operator is called upon to perform follow-up actions which are designed to bring the plant to a stable condition. If the P-T diagram shows that the plant is not responding as expected, the operator can identify the basic

type of accident and is directed to the appropriate portion of the guidelines. In all cases the operator checks for loss of subcooling and, if observed, follows a "Loss of Subcooling Rule" to start the high pressure injection pumps.

After taking the corrective actions prescribed for the accident type, the operator reviews the P-T diagram to see if primary/secondary heat transfer has been adequately restored. If not, core heat removal through the steam generators may not be possible and Backup Cooling Methods must be used. The operator is directed to these Backup Cooling Methods in the B&W Guidelines based upon the P-T trendlines and a few additional symptoms.

The ATOG Program also provides a few additional aids to the operator as part of its overall guidelines package:

- A section which provides guidance for the operator to assess plant stability which is obtained outside the normal "post-trip window" on the P-T diagram
- Guidance for diagnosing LOCAs and differentiating such events from other transients
- A set of post-stabilization cooldown procedures
- A set of "Rules" addressing loss of subcooling.

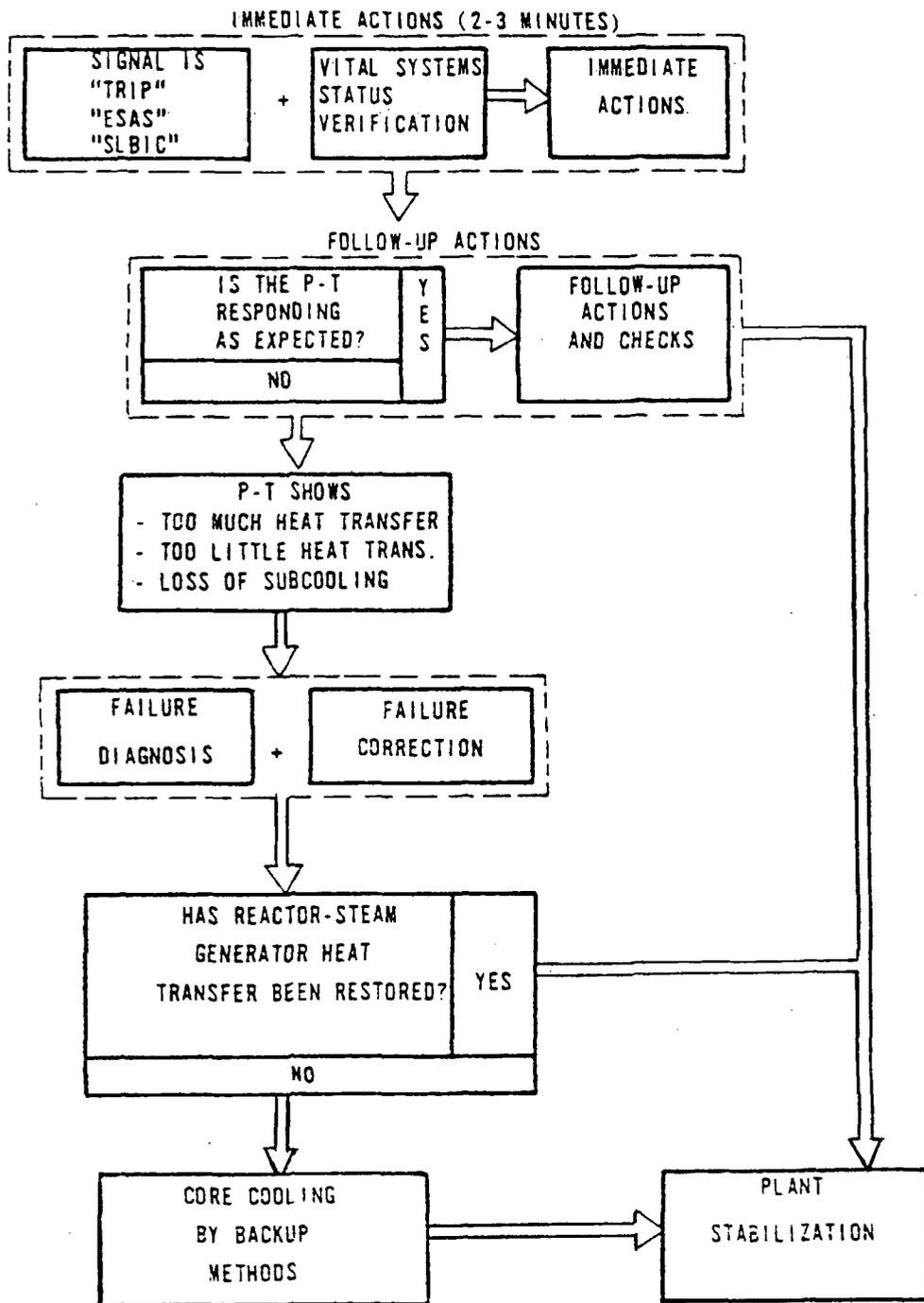


Figure 3.10 ATOG Flow Diagram

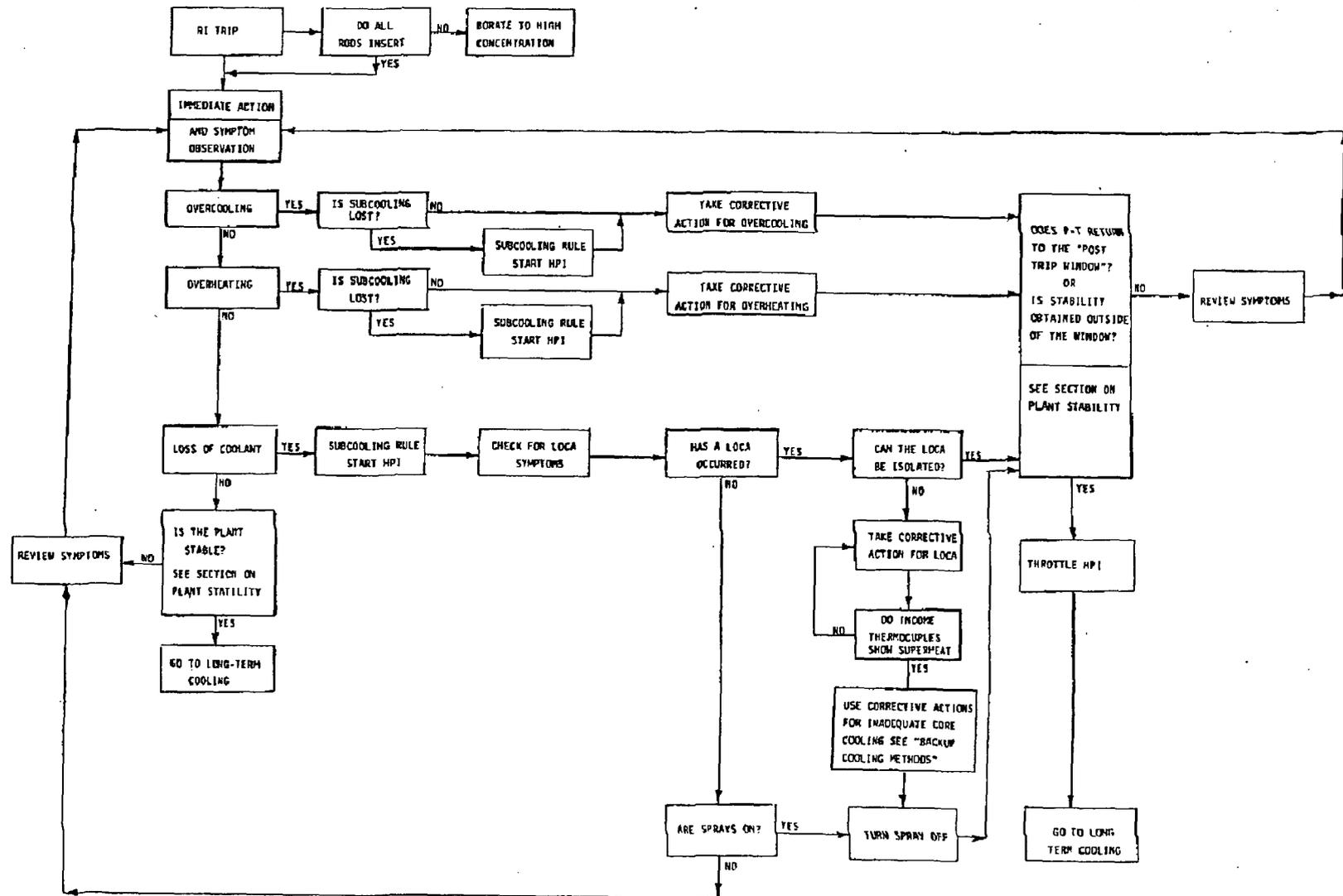


Figure 3.11 Accident Mitigation Approach

Section 4  
DISCUSSION OF OWNERS GROUPS APPROACHES

The preceding section provided a summary of the four Owners Groups' programs to produce improved emergency procedures. A key feature common to each Group's approach is the replacement or significant augmentation of event-specific procedures with function-based or symptom-based guidance. As discussed in Section 2, these alternate approaches are all designed to alleviate the problems associated with the pre-TMI event-specific procedures by focusing on a few critical safety functions or symptoms indicative of the performance of these functions.

While the basic concept behind all of these approaches is the same, there are significant differences in the guidelines which resulted from each program. The W and C-E programs resulted in "mixed" guidelines in which both functional and event-specific guidance is explicitly provided to the operator. However, when the operator cannot diagnose the specific event, W provides functional guidance through color-coded Status Trees and Critical Safety Function Restoration Guidelines; whereas, in the same situations, C-E provides two tables delineating arrays of symptoms and actions associated with critical functions. The GE guidelines contain no explicit event-specific procedures and are based on a totally functional approach. The B&W ATOG Program uses P-T diagrams and trendlines as the foundation for their guidance instead of the "function-symptoms-actions" format used by the other groups.

In spite of these evident differences, each program is based on a concept which appears to be sound. All of these approaches can, in theory, provide the means to remedy the problems associated with purely event-specific procedures. However, as is always the case, the translation of these basic concepts into actual practice requires that a number of specific steps be taken to ensure that the ultimate product can, in reality, achieve the intended goals.

It is the primary purpose of this section to examine these alternate approaches and identify the key steps which must be taken in their application to produce efficient unambiguous guidance for the operator under all accident conditions. Further, this section will briefly examine the extent to which these necessary steps have been taken by the four Owners Groups.

#### 4.1 PRACTICAL APPLICATION OF BASIC CONCEPTS

The primary motivation behind the development of the alternate approaches is to provide guidance to the operator without requiring the operator to explicitly identify the specific events which caused the upset condition. As discussed in Section 2.2, Functions, Symptoms, and Events, the underlying thesis of these alternate approaches is that it is possible to provide efficient unambiguous guidance to the operator for all accident conditions based on a relatively small set of critical safety functions (or symptoms indicative of the performance of these functions).

The validity of this thesis is dependent upon a few key interrelated assumptions. The first of these is that all events or combinations of events can be encompassed by a limited set of critical functions and the significance of any event can be described in terms of its impact on the performance of one or more of these critical functions. Thus, as depicted in Figure 2.1, the failure to perform any of these critical functions is the more general effect caused by the occurrence of specific events or sets of events.

The second assumption is that operator actions designed to restore a general critical function will accomplish the same basic goal as those actions designed to respond to the specific events which caused the failure of that critical function. Thus, the identity of the specific events can be invisible to the operator and not impede his ability to restore the plant to a stable condition (although perhaps not as efficiently as if he knew the precise cause).

The third assumption is that there exists a set of a limited number of symptoms which is always indicative of the performance of each critical function. Therefore, the observation of these "critical" symptoms will always indicate that the operator should take the actions specified to restore that critical function regardless of the specific events which have occurred.

A fourth assumption made by the four Owners Groups is that the critical functions and key symptoms necessary to make the first three assumptions valid are the same (with minor modifications) for all plants which plan to use the guidelines.

The third assumption, in combination with the first two assumptions above, implies that the effects of any specific event can be expressed in terms of a small number of symptoms which will allow the operator to take actions which will accomplish the same general goals (plant stability) as those which would be taken if the operator could diagnose the specific event. Thus, if these assumptions are valid, a limited set of symptoms, indicative of a limited set of critical functions, can be used to successfully guide the operator in his response to all accident conditions regardless of the specific events which caused the accident condition to exist. The practical application of these alternative approaches, therefore, requires that critical functions be selected and key symptoms identified which will make the above assumptions valid and thereby produce effective unambiguous guidance to the operator under all accident conditions. These requirements will be discussed in more detail below.

#### 4.1.1 Selection of Critical Functions

The definition of the critical functions is obviously an important element in the functional approach and many sets of critical functions can be and have been proposed. The main practical problem lies in the definition of the level of resolution of a function. What is called a function by one group might be considered a sub-function by another. For example, is "heat removal through the steam generators" a critical function or merely a subset of the more general "decay heat removal" function? The answer obviously depends upon the inclination of the analyst.

Figure 2.1 illustrated the concept of a hierarchy of functions. As shown in Figure 2.1, it is possible to just define one critical function - "retain fission products in core"; if this function is performed, the plant presents no risk to the public. All operator actions are designed to accomplish this function as are all safety systems. Of course, this function is much too general to be of any practical use. On the other hand, a continued breakdown of functions into subfunctions will ultimately produce specific events which were initially deemed unacceptable as a framework for operating procedures.

The goal, therefore, is to select a set of critical functions somewhere between these two extremes which satisfies two general criteria:

- (1) the functions must be sufficiently general so that a relatively few functions comprise a complete set
- (2) the functions must be specific enough so they can practically be translated into effective responses.

#### 4.1.2 Key Symptom Identification

While the identification of a complete set of critical functions satisfying the criteria cited above is often a fairly simple task, the task of identifying the key symptoms which should be monitored to determine the status of these critical functions can be significantly more difficult.

Since the operator will be instructed to carry out a specific set of actions based upon certain key symptoms, it is essential that these actions are always appropriate given these particular symptoms and that these symptoms can always be unambiguously determined. If the critical functions are too general and/or the number of key symptoms too few, there is increased danger that the specified actions will not always be appropriate or that the operator will not be able to clearly determine the correct set of actions. In such circumstances the basic premise that, regardless of the specific causal event, there are appropriate actions which can be taken based on key symptom behavior has not been effectively translated into practice; events could occur which require actions contrary to those indicated by the procedures or which exhibit symptoms similar to those which indicate the need for contrary actions.

Thus, just as the pre-TMI event-oriented procedures were prone to problems of misdiagnosis or incorrect response due to their over-specific nature, the alternative function- or symptom-oriented guidance is susceptible to the same problems in their attempt to generalize.

#### 4.1.3 Criteria for Effective Application

The preceding sections have pointed out a number of basic considerations which must be addressed in the practical application of the functional or symptomatic approaches to emergency procedure guideline development. These considerations are primarily concerned with the selection of critical functions and associated key symptoms in such a way that the guidance provided is always appropriate and unambiguous.

Because the basic value of these alternative approaches lies in their ability to efficiently provide appropriate and unambiguous guidance to the operator regardless of the specific causal event(s), the guidelines produced by these approaches must satisfy all of the following criteria:

- (1) The set of critical functions and/or key symptoms must be comprised of a relatively few elements.
- (2) Actions associated with any given set of key symptoms must be appropriate for any postulated event(s) which produces those symptoms; that is, there must be no two postulated events which, while requiring different actions of the operator, exhibit common key symptoms.
- (3) The key symptoms must be defined well enough so that criterion (2) is met even for events that exhibit only similar symptoms; the symptoms produced by any postulated events must be able to be unambiguously translated into the appropriate response.
- (4) The above criteria must hold for all specific plants which plan to utilize the guidelines.

The potentially conflicting nature of criterion (1) to criteria (2) and (3) is the primary source of problems in the practical application of the alternative approaches to emergency procedure development. The fewer the symptoms, the more difficult it is to assure that the guidance is always appropriate and unambiguous. Thus, the potential pitfalls which must be avoided in the practical application of these alternate approaches are closely linked with the primary motivation for their development. The pre-TMI procedures

required the operator to know too much before he could be assured of taking the correct action. The proposed remedy is to provide guidance based on much less information (a limited number of key symptoms associated with performance of a few critical functions). However, whenever guidance is based on limited information, extreme care must be taken to assure that it is always correct and unambiguous.

#### 4.1.4 Implications of Criteria to Owners Groups

The general criteria listed in Section 4.1.3 must be met by each of the Owners Groups Guidelines. However, as noted above, there is significant variation in the form and content of each Group's guidelines. Therefore, in this section, some of the major implications of these general criteria to each Group's guidelines will be examined. This examination will help illustrate the practical meaning of the above criteria and will assist in the determination of whether the four Owners Groups' have demonstrated the validity of their respective programs.

The WOG Program utilizes Critical Safety Function (CSF) Status Trees and Restoration Guidelines to provide guidance to the operator when the specific event(s) cannot be readily diagnosed. These Status Trees use the behavior of a few key parameters to direct the operator to the appropriate Restoration Guideline. In order for the WOG Guidelines to achieve their goal of providing effective unambiguous guidance to the operator under all accident conditions, the following criteria must be met for all plants to which the Guidelines apply:

- The operator actions associated with each CSF Restoration Guideline must be appropriate for every postulated event or combination of events which exhibits the particular symptoms associated with the branch(es) of the Status Trees which direct the operator to that Restoration Guideline. For example, the Status Trees direct the operator to the Core Cooling Restoration Guideline #3 whenever the reactor coolant is not subcooled, the core exit thermocouples indicate below 1200°F, at least one coolant pump is operating, and the wide range vessel level indicates above 100%; the actions delineated in this Guideline must be appropriate for all postulated events or combinations of events which can produce these symptoms.

- Any postulated event or combination of events must exhibit symptoms that can be readily associated with one or more of the branches on the Status Trees. That is, the combinations of symptoms associated with the Status Tree branches must form a complete set and each branch point on the Status Trees must be sufficiently defined so that the operator can unambiguously determine the correct branch(es) for any postulated event.
- If an event or combination of events can exhibit symptoms which are consistent with more than one Status Tree branch and these branches direct the operator to different Restoration Guidelines, the actions associated with these Guidelines must be mutually compatible.

The C-E Guidelines, as discussed in Section 3.2, direct the operator to the function-based ICC Guidance Package when a clear diagnosis of the event(s) is not possible. The guidance provided by C-E in these situations is in the form of two tables which delineate an array of symptoms, appropriate actions, and relevant event-specific procedures for each critical safety function. Presumably, C-E intends that these tables be used by individual utilities to develop procedures to diagnose and respond to failure of the critical functions. Such procedures will have to be developed in such a way as to meet the criteria listed in Section 4.1.3. For these tables to be directly used by the operator, it must be demonstrated that the actions listed for each function are always appropriate for any event or combination of events which exhibits the "unacceptable" symptoms associated with loss of this function. Although it is unclear how the operator is expected to use the cross-references to event-specific guidelines provided in both tables, he should very carefully diagnose the situation before implementing any of these event-specific procedures. For example, if a subcooling margin of less than 20°F is observed, Table 3.1 references the LOCA, Steam Generator Tube Rupture, and Loss of Flow event-specific guidelines while Table 3.2 references six distinct event-specific procedures. Efficient and unambiguous guidance will be difficult to obtain in this situation. The procedures which are developed from these tables must provide a clear transition to the event-specific guidelines.

In the GE Guidelines, as described in Section 3.3, the operator's first task is to ascertain the need to implement one or more of the six general Guidelines (one Level Control Guideline and five Containment Control Guidelines). The GE

Guidelines provide three indications of the need to implement the Level Control Guideline and one indication for each of the five Containment Control Guidelines (see Figure 3.7). If the plant is not stabilized by these general Guidelines, the operator is directed to one or more of six Contingency procedures.

In order for the GE Guideline package to meet the criteria listed in Section 4.1.3, the following must be demonstrated:

- All postulated events or combinations of events must exhibit at least one of the key symptoms used for general Guideline entry conditions.
- The actions delineated in these general Guidelines must be compatible with all events that exhibit the necessary entry symptoms. Since some accident conditions can simultaneously meet the entry conditions for more than one Guideline, the actions associated with these Guidelines must be mutually compatible (for example, some LOCAs will cause the implementation of the Level Control Guideline, five of the six contingency procedures, and subsequently the cooldown procedure).
- The appropriate operator response for all postulated events or combinations of events must be included in the general Guidelines or one of the six Contingency procedures.
- The symptoms which direct the operator to the Contingency procedures must be such that the operator is efficiently and unambiguously directed to the appropriate procedure for all postulated events; no event(s) should exist that exhibit symptoms that can lead to contingency procedures with incompatible actions.

The B&W ATOG Program utilizes the P-T diagram as the foundation for accident diagnosis and corrective operator response. Since this diagram only charts four basic parameters, it is crucial that any actions based on the P-T diagram be appropriate for all postulated events that exhibit a similar P-T chart. For example, the corrective actions described for overcooling transients in ATOG must be appropriate for all events or combinations of events which can exhibit the P-T trendline associated with overcooling. Further, each Backup Cooling Method must be appropriate for all events which exhibit those symptoms

which direct the operator to that method. In addition, the ATOG Program provides a few rules whenever subcooling is lost: (1) Start both HPI pumps, (2) Trip Reactor Coolant pumps, (3) Raise Steam Generator Level to 95%. Obviously, it should not be possible to postulate an event or combination of events for which these rules do not apply.

#### 4.2 VALIDATION OF OWNERS GROUPS' GUIDELINES

In this section, the manner and degree to which the four Owners Group's programs have demonstrated that their Guidelines satisfy the three criteria listed in Section 4.1.3 will be briefly discussed.

All four groups use a combination of arguments to demonstrate the rationale for their approaches and the validity of the resultant guidelines (although these arguments are more often implied than explicitly stated).

The deductive portion of their argument is primarily based on an examination of basic engineering principles relevant to the physical plant response under accident conditions.\* Using these principles, each group either (1) categorized all potential accident conditions into a limited number of accident types or (2) identified a limited number of critical functions which, if performed, would leave the plant in a "safe" condition. The deductive analysis which was performed in these essentially identical tasks was either sufficiently documented or could be readily reconstructed to conclude that the resultant sets of accident types or critical functions were logically complete.

However, as noted above, given any complete set of functions or accident types, the task of integrating the key symptoms and appropriate actions with these functions or accident types into a set of guidelines which satisfies the criteria listed above is a very difficult one. While most groups provided considerable background information or supporting discussion regarding the integration of symptoms and actions, none attempted to deductively prove that the resulting guidelines meet these criteria for all plants to which the guidelines apply.

---

\*The Babcock and Wilcox ATOG Program documented the most extensive analysis in this regard.

The absence of such a proof was undoubtedly due to a recognition that such a proof would be extremely difficult to perform, and its credibility would be low. Instead, each of the groups depended (in varying degrees) on (1) the apparent reasonableness of their results, and (2) an examination of a number of postulated accident sequences.

The first method of validation can add considerable weight to the credibility of any product if the reasonableness is judged by experts. However, when the basic value of the product is based on its ability to effectively handle all situations, "apparent reasonableness" is not sufficient and a more systematic demonstration of its validity is required.

The second method, examination of specific accident sequences can be used as this more systematic approach. However, to be truly effective in demonstrating the ability of the guidelines to provide effective and unambiguous under all accident conditions, this examination must contain two essential elements:

- (1) A systematic identification of all significant accident conditions in order to provide as broad a base for the inductive argument as possible, and
- (2) A systematic comparative symptoms analysis of the different postulated accidents to confirm that different accidents requiring different operator actions do not exhibit common or similar symptoms.

Most of the Owners Groups' programs have performed and documented investigations which, at least, address accident identification and symptoms comparison. For example, the ATOG program performed extensive event tree analysis to select important accidents and studied six initiating events (each compounded by a variety of additional plant failures) while developing their guidelines. The results of these studies were documented to demonstrate the validity of their guidelines and how their guidelines are applied to specific accident conditions. The Westinghouse Program used a Probabilistic Risk Assessment (PRA)- based approach to examine whether all risk significant accident sequences were covered by the WOG guidelines. All groups performed and documented realistic computer analyses of their plants'

response to a wide spectrum of transients and LOCAs with multiple failures. Symptoms information derived from these computer analyses was integrated into each group's guidelines.

However, there is no evidence that any group performed both a systematic identification of important accident conditions and a systematic comparative symptoms analysis adequate to clearly demonstrate the validity of their guidelines. Thus, despite the substantial effort associate with the production of these alternative guidelines and the supporting analyses, a clear demonstration that they have met the criteria listed in Section 4.1.3 is still lacking\*.

---

\*Recent changes in the various Owners Groups' programs do not affect the conclusions cited here.

Section 5  
PLANT STATUS MONITORING APPROACH

In the preceding section, the criteria which must be met in the practical application of the alternative function- or symptom-oriented approaches to emergency procedure development have been identified. Further, the essential elements of a review program which must be carried out to ensure that these resultant guidelines do, in fact, meet these criteria have been discussed. In this section, the ability of the methods, tools, and information base generated in the Plant Status Monitoring (PSM) Program to review and evaluate guidelines to ensure that they meet these criteria will be investigated.

5.1 PSM METHODS, TOOLS, AND INFORMATION BASE

The Plant Status Monitoring Program was initiated by NRC to develop and validate methods to systematically address a number of important safety issues concerned with enhancing the operator's ability to respond to potential accident conditions. In the flurry of post-TMI activity related to investigating the role of the operator in overall plant safety, the need was perceived for a logical framework to address these various issues in a manner which would ensure that any resultant conclusions and recommendations would be firmly anchored to a thorough physical understanding of the plant response to important potential accident conditions.

The basic thesis of the PSM program is that, while there are numerous facets of the overall man/machine interface problem, any efficacious changes to plant design and/or operation must be based on a firm foundation consisting of:

- An explicit identification of potential accident sequences and the plant states comprising these sequences.
- A careful delineation of the actions required of the operator at each plant state.
- A clear understanding of the physical phenomenon associated with each plant state.

Without this foundation, the course of the accident sequences cannot be effectively charted, the information flowing to the operator as the sequence evolves cannot be realistically determined, and the role of the operator in response to the accident cannot be properly analyzed and optimized. Simply stated, it is impossible to significantly enhance the operator's ability to respond to accidents without a clear understanding of the plant conditions under which he must respond, and the tasks with which he will be confronted.

One of the primary goals of the Plant Status Monitoring (PSM) Program was to develop and demonstrate the use of the tools necessary to systematically construct this essential foundation. A further goal of the PSM Program was to develop and verify methods utilizing this foundation to address a variety of operator/plant interface issues including the selection of adequate instrumentation and the development of effective monitoring schemes.

Event trees were chosen as the logical framework upon which this foundation could be constructed. These event trees are based upon the fundamental functions which must be performed by the plant safety systems either automatically or through operator action (e.g., maintenance of coolant inventory, decay heat removal, etc.). The event trees allow a systematic identification of the various combinations of component or system failures which result in an inability to perform one or more of these fundamental functions.

The development of these models begins with the trees as they appear in completed probabilistic risk assessments. The events in each sequence which involve operator action can be identified and in some cases broken down into additional events in order to separate out and highlight individual operator tasks. In addition, the sequences can be expanded (events added to the event tree) to include additional operator actions which could be performed to prevent core melt, but which were neglected or conservatively omitted from the original analysis. The result of these efforts is an "operator action event tree" which logically displays the role of the operator throughout the progression of the accident. Figure 5.1 presents an illustrative example of an operator action event tree developed for a particular sequence associated with a loss of offsite power initiating event for the Big Rock Point BWR. Note that in Figure 5.1, the key plant states which can evolve from this initiating event are individually

enumerated. These operator action event trees can thus systematically provide the first element of the foundation described above and also provide the logical framework for producing the two remaining elements.

For each of the key plant states of each operator action event tree, the specific actions required of the operator can be explicitly identified. These actions can range from passive tasks associated with verification of successful automatic plant responses (e.g., verification of successful reactor scram) to rather creative responses to plant conditions resulting from multiple system failures (e.g., use of low pressure condensate pumps following loss of both main and auxiliary feedwater in a PWR).

Each plant state will exhibit a variety of "symptoms" which are defined as the resultant time dependent behavior of measurable plant parameters. The next step in the analysis is to obtain accurate and representative information about the plant response to the postulated accident conditions and develop a list of symptoms for each plant state.

Thus, the development of a fully documented set of operator action event trees can systematically provide a listing of the appropriate operator actions and the key plant symptoms associated with every known significant plant condition. This package of information can provide a logical way to determine the necessary diagnostic procedures which allow the operator to unambiguously and efficiently respond to upset conditions and to review and evaluate the effectiveness of existing procedures or guidelines. In the following subsections, a more detailed discussion of the methods by which these tasks can be performed using the PSM methods, tools, and information base will be presented.

LOSP	RPS	EMERGENCY POWER (EMERGENCY DIESEL GENERATOR)	OPERATOR STARTS EDG OR STANDBY DIESEL, PROVIDES EMERGENCY POWER	PRIMARY SYSTEM ISOLATION	EC SHELL SIDE MAINTAINED	OPERATOR PROVIDES MAKEUP TO SHELL SIDE	POWER RESTORED	RDS/CS	OPERATOR MANUALLY DEPRESURIZES AND/OR PROVIDES COOLANT TO CORE	LONG-TERM COOLING
------	-----	----------------------------------------------	-----------------------------------------------------------------	--------------------------	--------------------------	----------------------------------------	----------------	--------	----------------------------------------------------------------	-------------------

5-4

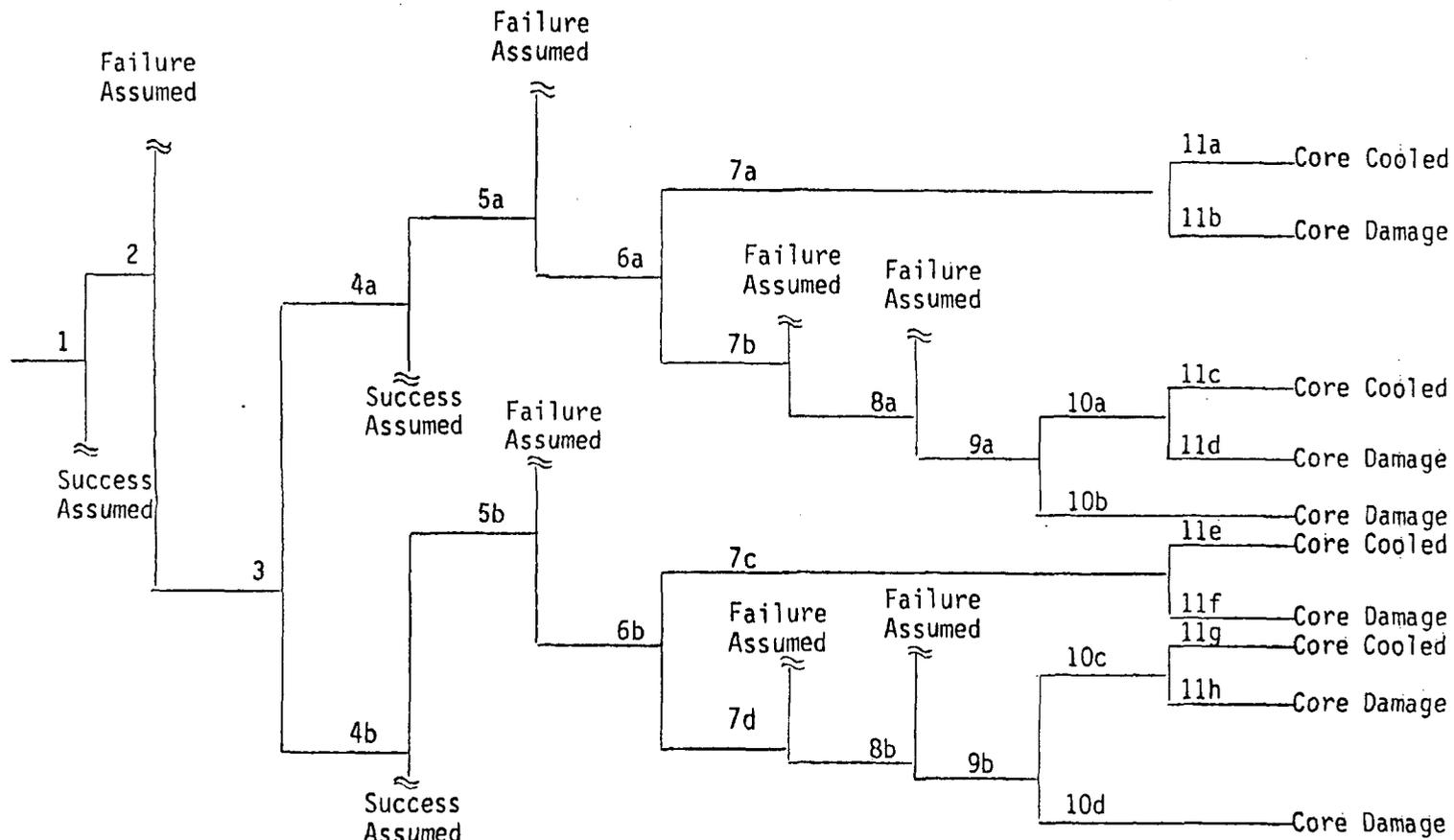


Figure 5.1. An Example Operator Action Event Tree

## 5.2 APPLICATION OF THE PSM APPROACH TO THE REVIEW AND EVALUATION OF EXISTING EMERGENCY PROCEDURE GUIDELINES

As discussed in Section 4, any set of functional or symptomatic emergency guidelines should be systematically examined with respect to all known important accident conditions to ensure that they actually do provide unambiguous guidance regardless of the specific event or combinations of events that have occurred. A fully documented set of Operation Action Event Trees can provide the information base necessary to efficiently perform this systematic examination.

To begin with, the OAETs provide a tool for systematically identifying the key plant states with which the operator might be confronted under accident conditions. The event trees upon which the OAETs are based identify the probabilistically significant ways by which the critical safety functions can fail to be performed. The key states of the OAETs therefore represent the set of probabilistically significant accident conditions to which the operator could potentially be required to respond. This set of key OAET states therefore provides the broadest practical base for any validation process. If the guidelines can provide efficient and unambiguous guidance for all of these OAET states, they will represent significant improvement over the pre-TMI emergency procedures.

Secondly, the documented OAETs, by providing a comprehensive listing of the operator actions required for each plant state and the key symptoms exhibited by the plant at each of these states, supply the necessary information by which this systematic examination can be performed.

The review methodology is based on the recognition that emergency procedure guidelines can be viewed as a collection of instructions, each of which relates a "symptom set" to an "action set". For example, one instruction might be in the form:

"when you observe Symptom Set A (comprised of symptoms  $a_1, a_2, a_3$ ), take Action Set P (comprised of actions  $p_1, p_2, p_3$ )."

The review process entails asking four basic questions regarding these instructions:

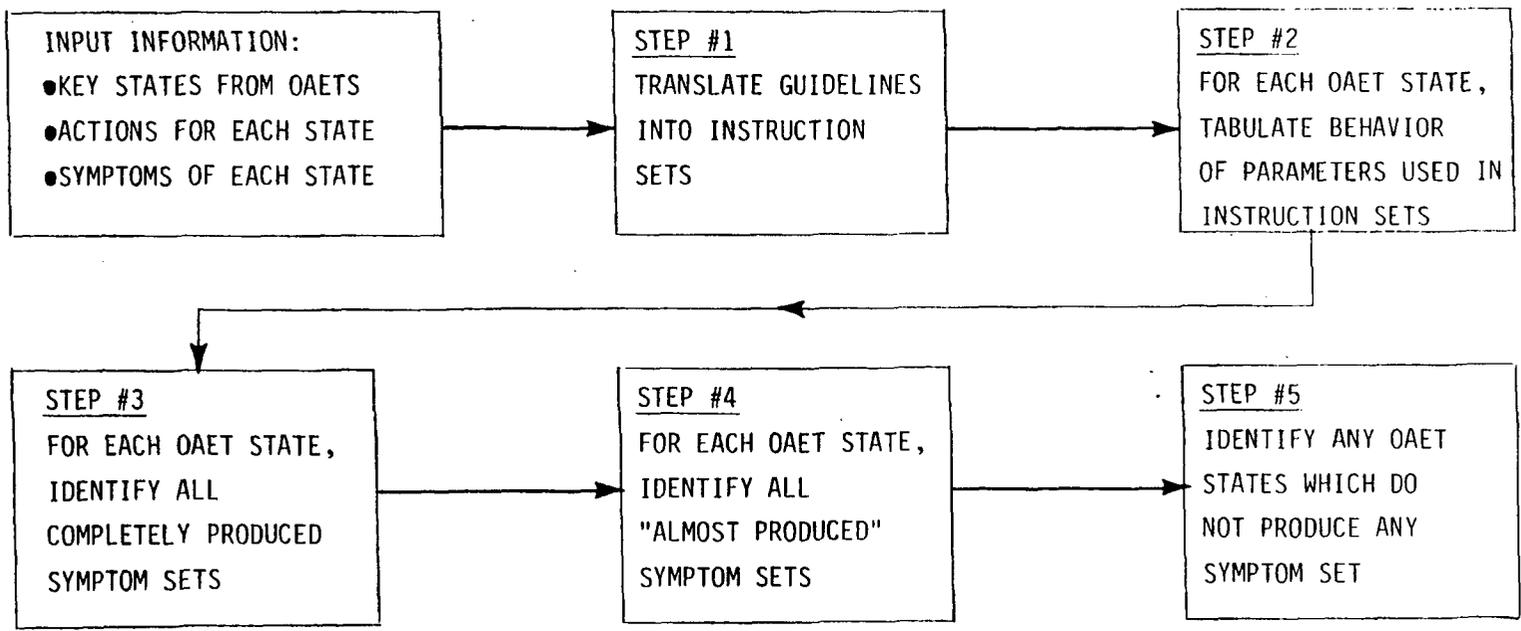
- (1) Is the collection of symptom sets complete?  
That is, are there risk significant states requiring operator action which could occur but for which no guideline instruction applies?
- (2) Are the instructions always right?  
That is, if the guidelines say "when you see Symptom Set A take Action Set P," is Action Set P always appropriate for every situation that can produce Symptom Set A?
- (3) Are the action sets always complete?  
That is, are there important actions which should be carried out at a particular state which are not included in the action set indicated at that state?
- (4) Are the instructions always unambiguous?  
Are there plant states which produce symptom sets which the operator might confuse with guideline symptom sets and thereby take inappropriate action?  
This confusion might arise due to similar looking symptoms or a faulty control room indication.

These four questions can be answered by performing the systematic OAET-based symptoms comparison outlined in Figure 5.2.

As depicted in Figure 5.2, the input information is again a description, for each key plant state identified in the OAETs, of the symptoms exhibited by the plant at that state and the necessary operator actions associated with that state.

In Step #1, attention is focused on the guidelines and the goal is to translate these guidelines into a collection of instructions, each of which relates a well defined symptom set to an action set. This can be accomplished by performing three tasks:

- (1) Generate a complete listing of the specific symptoms which are used in the guidelines.



5-7

Figure 5.2. Emergency Procedure Review Flowchart for PSM Approach

- (2) Make these specific symptoms (e.g., hot leg temperature rising above  $X^\circ$ ) into general symptoms (e.g., hot leg temperature rising), and produce a list of "generalized symptoms." This is done to facilitate comparison between the guideline symptoms and the OAET symptoms. If this comparison points out potential ambiguities involving the "generalized symptoms" then these few cases can be re-examined using the specific guideline symptoms.
- (3) Translate the guidelines into instruction sets using the generalized symptom sets and action sets. These instructions should be in the form:

Symptom A + Symptom B  $\longrightarrow$  Action P

These tabulated instruction sets will be used as input to the systematic comparison steps discussed later.

In Step #2, attention is focused on the OAETs. For each OAET state, the behavior of each of the generalized parameters listed in Step #1 should be tabulated. For some of these states, the behavior of some of the parameters may be uncertain. In these cases, several different symptoms (e.g., pressure rising, pressure stable) may be assigned to the same state. If any of these symptoms is later found to result in potential ambiguities, that particular state and symptom can be looked at more closely. These tabulated symptoms will be used as input to the systematic comparison steps discussed below.

In Step #3, the comparison process begins. The first task is to identify, for each OAET state, any and all guideline symptom sets listed in Step #1 which are completely produced. The guideline action sets associated with these symptom sets should also be identified.

In Step #4, the task is to identify, for each OAET state, any and all guideline symptom sets listed in Step #1 which are almost produced. For example, if an OAET state exhibits all but one of the symptoms in a guideline symptom set, this state should be noted here.

In Step #5, any OAET states which do not completely produce any guideline symptom set are identified.

The information generated in the above five steps can be used to systematically address the four basic questions listed above.

The first question - Is the collection of symptom sets complete? - can be directly addressed using the results of Step #5 which identifies any OAET states which does not produce any symptom set in the collection. Should any such states be identified, the guidelines must be examined to ascertain whether they are indeed incomplete (i.e., plant conditions requiring operator response were overlooked or intentionally ignored in the guidelines) or that certain plant states which were intended to be covered by the guidelines actually exhibit symptoms different from those listed in the guidelines due to 1) inaccuracies in the guidelines' symptom descriptions, or 2) the existence of subtle system interactions which can alter the symptoms perceived by the operator and which were overlooked in the guideline development process. This last possibility is by far the most likely cause of identifying OAET states which do not produce a symptom set in the guideline collection. The OAET-based review procedure provides a systematic way to search for such states and "fine-tune" the guidelines to handle them. Usually, all that is required is a slight alteration in a symptom description or a "caution" added to the guidelines.

The second question - Are the instructions always right? - can be addressed using the results of Step #3. For each OAET state, there will be one or more action sets identified in Step #3. The indicated action sets must be compatible with each other and they must be compatible with the actions associated with that OAET state. Problems identified in this step are often due to multiple failure plant states which simultaneously affect multiple critical functions. Such situations can usually be handled with a clear presentation of priorities within the guidelines.

The third question - Are the action sets always complete? - can also be addressed using the results of Step #3. There may be important actions which must take place which are indicated in the OAET but are not included in the indicated guideline action set. It should be recognized here that functional guidelines are not necessarily intended to provide all the detailed steps required to bring the plant to a safe shutdown condition, but rather, are focused on those actions which will restore the critical safety function. Accordingly, this third question should also focus on actions related to restoration of critical safety functions.

The fourth question - Are the instructions always unambiguous? - can be addressed using the results of Step #4. Each OAET state will have associated with it an "almost indicated" guideline symptom set and the associated guideline action set. First, the guideline action set should be compared with the appropriate action set for that OAET state to see if they are compatible. If they are not compatible, then the question arises whether the operator might confuse the two symptom sets (the actual symptom set exhibited by the plant and the "almost indicated" guideline symptom set leading to inappropriate actions). The "missing" symptoms should be examined and a judgment made whether the operator will be able to clearly and unambiguously notice their absence and not take the wrong action.

It should be noted that this fourth question can also be used to examine the potential impact of instrumentation failure on the adequacy of the emergency procedures. Since it is certainly possible for the operator to be provided with a faulty parameter reading in the control room under accident conditions (due to instrument failure, physical phenomena associated with the accident which produces false instrument readings, etc.), it is important to know how sensitive the written procedures are to a bad reading. Since the functional guidelines look at a relatively few symptoms, the impact of one bad reading on the quality of the guidance provided by the procedures could be significant. The results of Step #4 can be used to examine this question and in effect can provide a "single failure analysis" of the guidelines with respect to faulty symptoms.

### 5.3 APPLICATION OF THE PSM APPROACH TO THE DEVELOPMENT OF EMERGENCY PROCEDURE GUIDELINES

In the previous section, the use of the OAET information base in reviewing and evaluating existing guidelines was discussed. In some cases, however, adequate existing guidelines might not exist. In those cases where unique plant design or other considerations make it impossible to adapt existing guidelines, alternate guidelines must be developed. In this section, the steps which can be taken to translate the information contained in the documented operator action event trees (OAETs) into emergency procedure guidelines will be discussed. Figure 5.3 presents a flow diagram of the proposed methodology. Figures 5.4, 5.5, and 5.6 present expanded versions of key steps in the methodology.

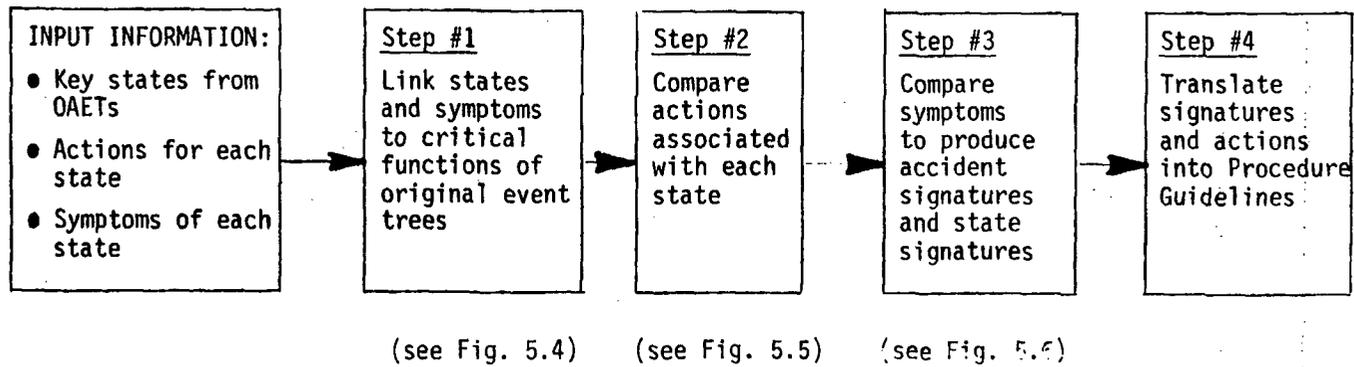


Figure 5.3 Emergency Procedure Development Flowchart for PSM Approach

As shown in Figure 5.3, and discussed previously, the necessary input information to this methodology is comprised of three main elements:

- (1) A listing of all the key states identified in the OAETs.
- (2) A description of the necessary operator actions associated with each state.
- (3) A description of the symptoms exhibited by the plant at each state.

The first step in processing this input information into effective guidelines (Figure 5.4) is to explicitly link all of the above information to the performance of the critical safety functions upon which the original event tree analysis was performed. Each of the OAETs' states can be associated with the critical safety function which is most threatened at that state (which group a state is put in if two or more are affected is not important at this point). This will allow all states to be grouped into a limited number of categories based on these critical functions. In addition, those parameters whose behavior provides the most direct indication of the status of each critical function can be identified (e.g., the reactor vessel coolant level can be associated with the maintenance of coolant inventory function in BWRs). The key symptoms for each state can then be described in terms of the behavior of these key parameters. Thus, each state at this point has been placed into a category associated with one of the critical functions and has been described in terms of the parameters most directly indicative of these critical functions.

The second step (Figure 5.5) is to compare the required actions associated with each OAET state within each category. Since the ultimate goal of all operator actions is to restore or maintain these critical functions, the required set of actions should be very similar for all OAET states within the same category. The goal of this comparison of actions is twofold. The first objective is to identify any specific OAET states which require actions that are not compatible with other states in the same category. If such actions exist which are contrary to the actions required for other states in the same category (i.e., produce effects which could worsen the situation), then it can be concluded that the operator can not determine the correct response based solely on a diagnosis of the states' functional category. In these cases, the particular states must be removed from that category, and placed in either another category (in which

its required actions are compatible with those of all other states in that category) or placed in a totally new category. At the end of the action comparison, a revised set of categories will have been produced; the OAET states which comprise each of these categories will all have mutually compatible actions associated with them.

The second objective of this comparison of actions is to delineate those states which have different, but not incompatible, operator action requirements associated with them. These particular states will be the result of the different ways by which a certain critical function can fail to be performed and the variations in the required action are merely reflections of the specific failures associated with the OAET states. For example, consider two BWR OAET states grouped together in the category associated with the "Maintenance of Primary Coolant Inventory" critical function. The first state might be that associated with a small LOCA; the appropriate operator response could be to ensure adequate high pressure injection. The second state might be that associated with the same small LOCA in combination with the failure of high pressure injection. In this case, the appropriate operator response could be to depressurize and utilize low pressure systems to maintain inventory. These actions are not really incompatible with each other. They are merely a more precise description of the correct operator actions required in response to the specific failures or combinations or failures associated with the different OAET states. At the end of this second step of the action comparison, the different ways which each critical function can fail to be performed which require different operator actions will have been identified.

The third step in the procedure (Figure 5.6) is to perform a comparative symptoms analysis. This step, like the comparison of actions, is performed for two basic reasons. The first objective of this symptoms comparison is to determine the minimum set of symptoms by which each of the critical function categories can be unambiguously diagnosed. As discussed above, each of these categories will, at this point, be comprised only of OAET states with mutually compatible actions. Each of these states will also have been described in terms of the behavior of the key symptoms associated with each critical function. By comparing these key symptoms it should be possible to identify for each category a set of symptoms which uniquely and clearly defines that category. These unique sets of symptoms can be referred to as accident "signatures" because they allow the operator to identify the particular accident type.

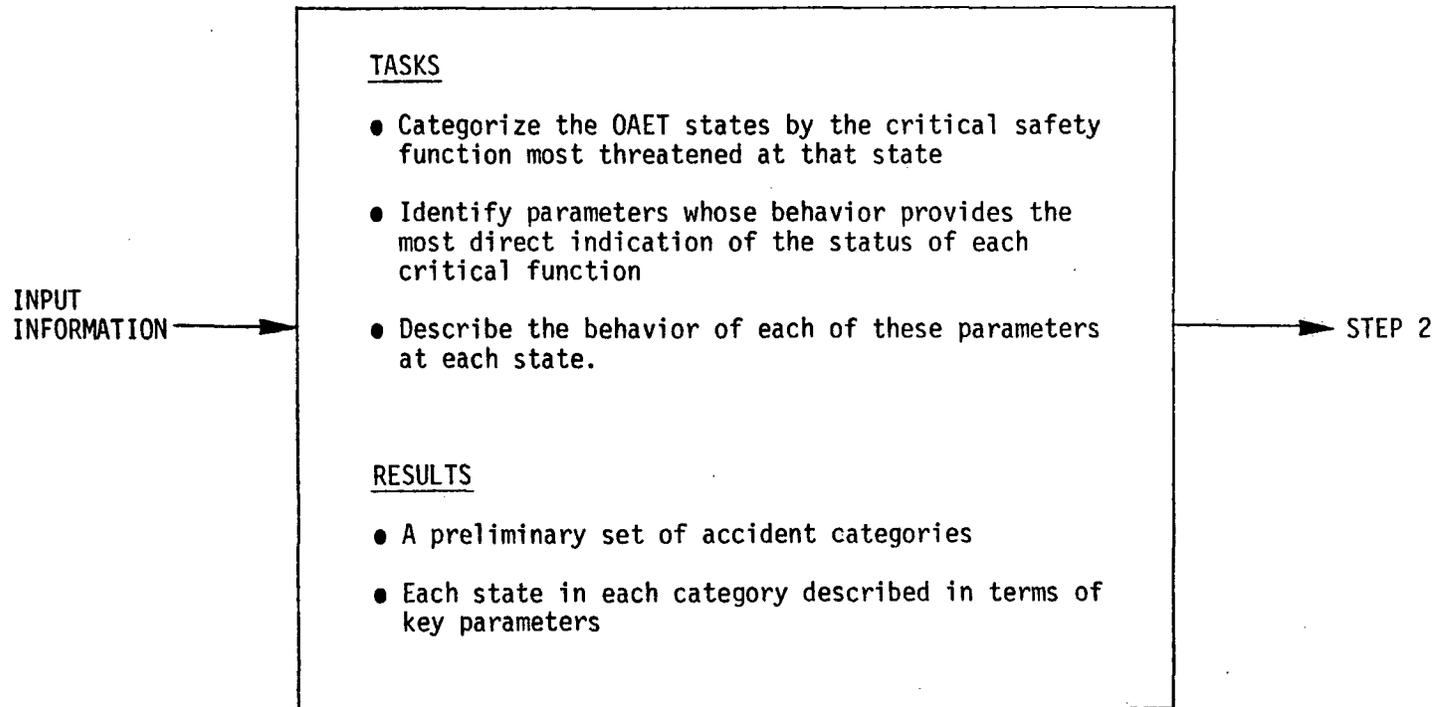


Figure 5.4. PSM Emergency Procedure Development: Expansion of Step #1 (Figure 5.3).

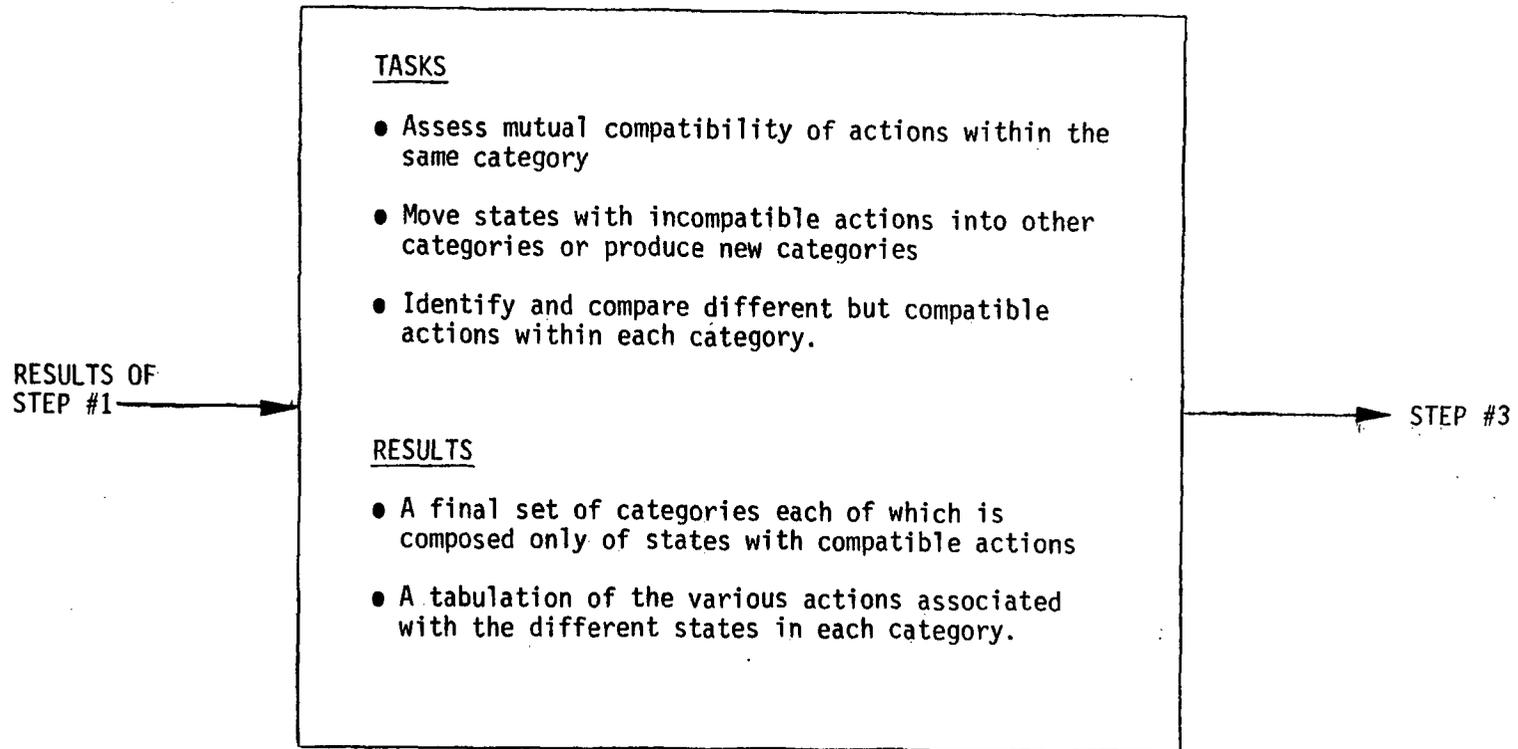


Figure 5.5. PSM Emergency Procedure Development: Expansion of Step #2 (Figure 5.3).

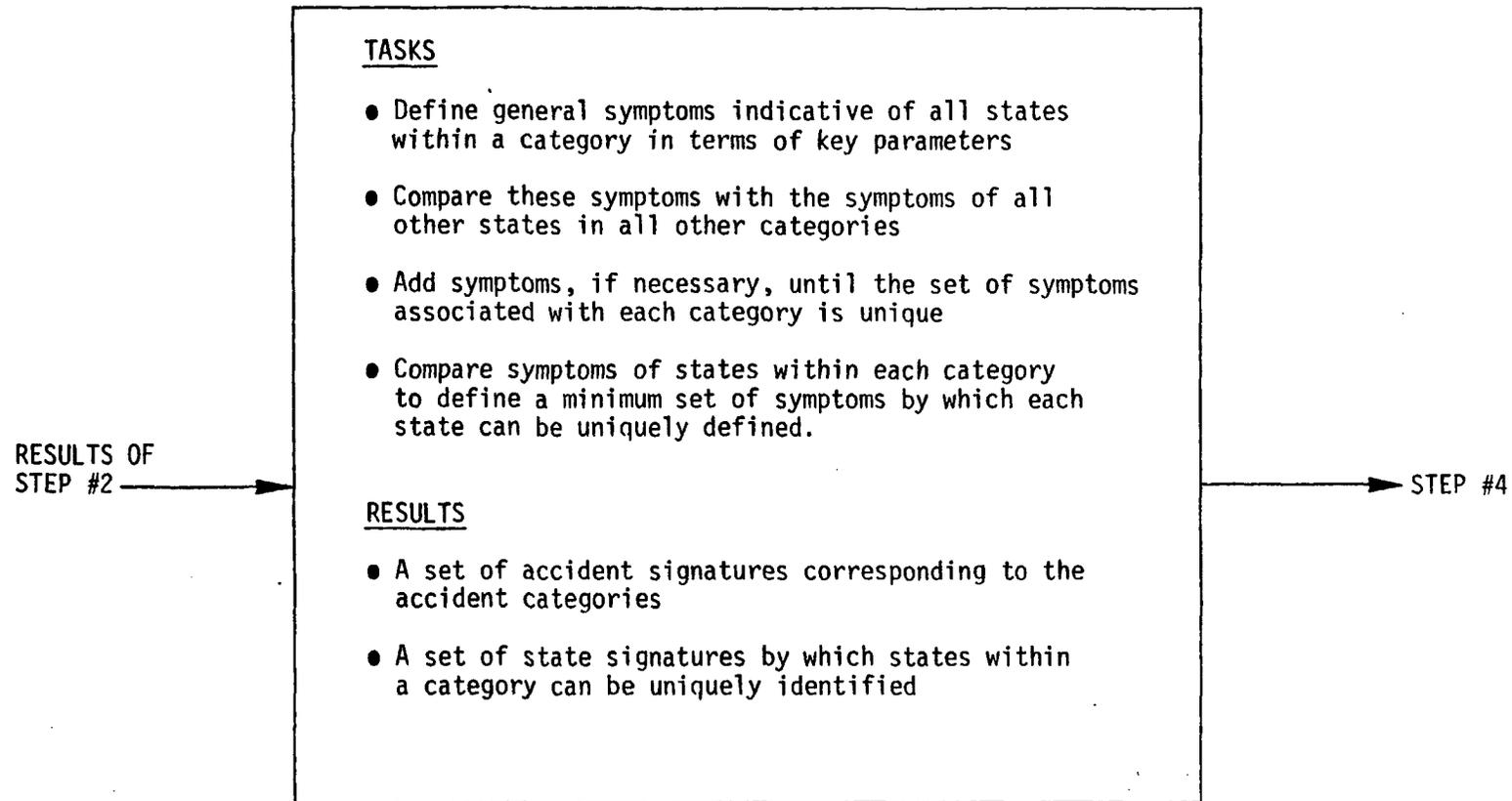


Figure 5.6. PSM Emergency Procedure Development: Expansion of Step #3 (Figure 5.3).

These signatures can be constructed in a fairly straightforward systematic way. The most efficient process is to choose one category and first look at behavior of the key parameter previously chosen to be most indicative of the critical function associated with that category. For example, one category of states might be associated with the critical function "Limitation of Primary Pressure." All states in that category represent plant conditions identified in the OAETs in which this critical function is threatened and all the actions associated with these states are mutually compatible ways of limiting the primary pressure. The key parameter associated with this function will undoubtedly be primary pressure and the behavior of the primary pressure has been described for all states within this category as well as all states in all other categories (this was done in Step 1). The behavior of the primary pressure can be compared at all states within this category and a general description of this behavior which holds for all these states can be determined (e.g., pressure rapidly rising to relief valve setpoint might be a general symptom for all states within the category although the rate of rise might vary from state to state).

This general symptom exhibited by all states in this category can then be compared to the behavior of the primary pressure at all other states in all other categories. If no other state exhibits the same symptom (or a sufficiently similar symptom to confuse the operator), then this general symptom can be used as the signature for this category of states (and actions). Thus, whenever the operator observes this symptom, he can confidently take the (mutually compatible) actions associated with this state without fear that other states might exist which also exhibit this symptom but require a different response.

However, it will often be the case that other states in other categories will also exhibit symptoms at least similar to this general symptom. In this case, additional symptoms must be added to the signature until a unique combination of symptoms can be associated with the category. It is often the case that the additional symptoms necessary to produce a unique signature are associated with the lack of change in key parameters (e.g., a steam-line break outside containment in a BWR and a LOCA inside containment can both produce rapid reduction in pressure, but the steam-line break can be diagnosed by the lack of change in containment parameters such as temperature, humidity, radiation level, etc.).

At this point, the sets of symptoms or "accident signatures" by which the operator can unambiguously determine the category of event(s) that has occurred have been identified. The second goal of the symptoms analysis is to provide the information necessary to allow the operator to take the most efficient response once the general category of accident has been determined. Thus, this portion of the symptoms comparison is directed at differentiating between the various states within each category (this differentiation is not required between states requiring identical actions). As noted above, the different states in each category represent the different events or combinations of events which can produce that particular accident type. For example, a category might be comprised of all states leading to a failure to maintain adequate coolant inventory. This category might include states caused by a large coolant pipe break, a small coolant pipe break, a stuck open PORV, a small break with failure of high pressure injection, a loss of feedwater (in BWRs), etc. In addition to identifying an accident signature which can be used to differentiate these states as a group from all other states, it is possible to identify symptoms or sets of symptoms by which these states can be differentiated from each other. These "state signatures" will be used in the following step to develop the procedure by which the operator can efficiently focus on the most effective response.

The logical format of the OAETs can be used as a guide to systematically produce these state signatures. Each state represents the occurrence of a particular OAET initiating event or an initiating event coupled with one or more subsequent failures. The process of developing these signatures should start with identifying the symptoms which can be used to differentiate between the various initiating events associated with the states within each category. For example, the rate of level reduction or the behavior of the primary pressure can be used to differentiate a large LOCA from a small LOCA; containment conditions can be used to differentiate between (some) LOCA's and a loss of feedwater. When this is accomplished preliminary "initiating event signatures" will have been produced.

The next step in the process of developing state signatures is to examine and differentiate the individual states associated with each initiator. For example, one state might be associated with a large LOCA with successful emergency coolant injection, another might be associated with a large LOCA coupled with failure of low pressure injection and a third involve a large LOCA with subsequent failure of emergency recirculation. Symptoms indicative of additional failure(s) must be identified. This process should be carried out very systematically as follows:

- (1) Select an initiating event.
- (2) Examine one of the OAET states associated with this initiator.

- (3) Identify the symptom(s) indicative of the additional failure(s) associated with this state.
- (4) Produce a preliminary state signature comprised of the symptoms necessary to identify the initiating event together with these symptoms necessary to identify the occurrence of the additional failures.
- (5) Compare this preliminary state signature to the preliminary initiating event signatures to assure that the signatures are still unique (i.e., assure that the additional failure will not produce symptoms which could be confused with those of another initiating event).
- (6) Repeat steps (3), (4), and (5) for each of the states associated with each initiating event ensuring that each signature is indeed different from all others; previously defined signatures may have to augmented with additional symptoms if subsequent states can produce identical or similar symptoms.
- (7) Repeat steps (2) through (6) for each initiating event. As each state signature is developed it must be compared to all previously developed signatures to ensure its uniqueness.

At this point, accident signatures have been developed which can be used to identify the accident category and state signatures have been developed which allow the diagnosis of the particular state within that category.

The fourth, and final, step of the process depicted in Figure 5.3, is the translation of these documented OAETs and accident signatures into emergency procedure guidelines, or diagnostic/action algorithms, which allow the operator to efficiently translate the observed symptoms into required responses. The fundamental task is to select and logically order the specific symptoms at which the operator should look to unambiguously and efficiently determine and carry out the required response. The form and content of the documented OAETs and signatures allow this task to be carried out in a straightforward manner. The accident and state signatures have been explicitly developed to minimize the ambiguity; the only remaining task is to optimize the procedures, or diagnostic algorithm, by ordering the symptom monitoring process to produce the most efficient diagnosis of the required action.

To a great extent, this task has also already been accomplished by the production of the accident and state signatures. These accident signatures are the minimum set of symptoms by which the accident category can be determined. Thus, by monitoring the relatively few symptoms comprising these signatures, the operator can quickly focus on the type of accident which is occurring. Once the operator determines what category of upset is occurring, he can then use the state signatures to identify the most effective response. Again, since a state signature represents the minimum set of symptoms necessary to unambiguously identify the need for a particular action, the appropriate response is readily identified.

This efficiency of the diagnostic process can be further enhanced by a closer examination of the constituents of the individual signatures and the specific actions associated with each state. In many cases it may not be strictly necessary to observe all elements of a signature before any of the required actions can be taken. The need for some specific action might be always indicated by one of the symptoms comprising a signature while the other elements of the signature are needed to determine which additional actions should be taken. For example, assume that OAET state #1 has a state signature comprised of symptoms  $S_1$  and  $S_2$  and requires actions  $A_1$  and  $A_2$ , and that OAET state #2 has a signature comprised of symptoms  $S_1$  and  $S_3$  and require actions  $A_1$  and  $A_3$ . If symptom  $S_1$  is not produced by any state for which action  $A_1$  is incompatible, the operator can first look for symptom  $S_1$ , take action  $A_1$  immediately if  $S_1$  is observed, and then look for symptoms  $S_2$  and  $S_3$  to decide whether to take action  $A_2$  or  $A_3$ .

This restructuring of the diagnostic process to produce more efficient responses will usually provide the most benefits once the particular accident category has been established. Since each category has been explicitly constructed to contain only states with mutually compatible actions there are often one or more actions common to all states within the category which can be, and should be, taken as soon as the category is determined (i.e., these actions can be based solely on the accident signature without the need to identify a specific state). The additional elements in the state signatures can be used to determine what additional actions are required in response to the different individual states.

## 5.4 DISCUSSION OF PSM APPROACH

The two preceding sections have demonstrated how the PSM generated methods, tools, and information base (represented by the fully documented OAETs) can be used to systematically determine whether the various Owners Groups' guidelines meet the criteria listed in Section 4.1.3 or to develop such guidelines. In this section, a few important points concerning the application of the PSM approach are discussed.

Perhaps the most important point concerning the process of developing the guidelines is that the efficient application of the PSM approach is dependent upon high quality OAETs. Since these OAETs form the foundation upon which the guidelines are evaluated, poorly constructed trees or inadequate analysis or documentation of the actions and symptoms associated with the states in these trees can obviously have an adverse impact on the ability of the OAETs to support guideline review. The quality of the OAETs can be maximized by three basic methods:

- (1) The logic structure of the trees should be developed in an iterative manner by continually assessing the adequacy of the tree structure as the symptoms and operator actions are developed for each state. Each state must be sufficiently defined so that the symptoms of that state and required actions can be clearly defined. For example, it is not adequate to define a tree heading "LOCA" because the symptoms of a LOCA can be widely divergent depending upon the size and location of the break. Clearly defined symptoms would not be possible to identify, and the heading should either be broken down into better defined events or additional trees should be developed.
- (2) The knowledge and judgement of operators should be applied to the determination of the actions associated with each state. Operators should either be used to define the actions or, at least, should carefully review this aspect of OAET documentation.
- (3) The definition of the symptoms exhibited by the plant at each state should be based on best-estimate computer analysis. The availability of such analyses has increased substantially over the last few years. The various Owners Groups' have documented a considerable amount of new information concerning the response of their respective plants to transients and accidents with multiple failures. The NRC-funded Severe Accident Sequence Analysis (SASA) Program is also performing and documenting best-estimate computer analyses of risk significant accident sequences. These sources of information should be extensively utilized in the construction and documentation of the OAETs.

Another key point which should be noted is the flexible nature of the PSM approach; the PSM tools, methods, and information base can be effectively utilized in a variety of ways to produce emergency procedure guidelines which meet the required criteria. The PSM-based approach can be used systematically to:

- (1) Fine-tune and finalize completed or nearly-completed guidelines.
- (2) Modify existing generic guidelines so that they provide effective, unambiguous guidance to the operators of a specific plant.
- (3) Provide the basis for production of self-validated guidelines independently of other programs.

This variety of capabilities will allow the benefits of the PSM-based approach to be gained in virtually any guideline development program.

The final point which should be addressed concerns the notion of "completeness." Since it was the inherent incompleteness of the pre-TMI event-specific procedures which provided the primary motivation for the development of alternative functional or symptomatic guidelines, any proposed methodology should be examined with respect to its completeness. The fact that the PSM-based approach uses event trees and a tabulation of event tree states which is inherently incomplete, might suggest that the approach is deficient in this regard. In reality, as discussed below, application of the PSM approach can enhance the completeness of any set of guidelines.

As discussed previously, the various Owners Groups' guidelines are intended to be able to provide guidance regardless of the specific event(s) that have occurred because they are based on a complete set of critical safety functions or types of accidents. However, the PSM-based methodology also uses these same critical functions to generate the OAETs and subsequently produces categories of accident states based on these critical functions. Therefore, at this level there is no difference between the PSM approach and the Owners Groups' approaches with respect to completeness.

But the mere identification of a complete set of functions or accident types does not produce emergency procedure guidelines. It is still necessary to define the appropriate operator actions when these functions are not automatically performed or these accident types occur, and to identify the symptoms by which the

operator can efficiently and unambiguously determine that these actions should be taken. Selecting a complete set of functions or accident types is easy. However, producing guidelines based on these functions or accident types which meet the criteria discussed in Section 4 is much more difficult.

The Owners' Groups apply their considerable experience and substantial computer analyses of multiple failure accident sequences to produce an integrated set of functions, actions, and symptoms. Some also explicitly validate their results against a number of specific accident conditions. Others use event tree techniques to demonstrate that their guidelines address all important accident conditions.

The PSM approach uses OAETs to systematically identify all known ways that a particular function can fail to be performed or all known events (or combinations of events) that comprise a certain accident type and also to identify the symptoms and actions associated with these states. By systematically integrating the information from all of these known plant conditions into the review or development of guidelines, maximum possible assurance is gained that the resultant guidelines provide unambiguous guidance regardless of the specific event(s) that occurred. It should also be noted here that the OAET techniques are applicable to any accident scenario whether high risk or high frequency. High risk, multiple failure sequences have been emphasized here only because of the inherent difficulties in providing unambiguous guidance under those conditions.

Once any investigation proceeds beyond the critical function level it becomes difficult to guarantee completeness. The more detailed the investigation becomes, the greater the chance of "missing something" becomes until it becomes a virtual certainty at the specific event level. However, credible procedure guidelines cannot practically be developed by remaining at the critical function level. The complexities of individual plant response to multiple failure accidents and the inherent interdependence of these critical functions demand that procedures based on a limited number of symptoms indicative of the status of a limited number of critical functions be, at the very least, validated against a list of specific accident conditions (even if this list is inherently incomplete). The PSM-based approach systematically examines the broadest possible spectrum of important accident conditions.

Thus, the PSM approach is complete at the same level that the Owners Groups' approaches are complete. In addition, when the investigation is, by necessity, forced beyond the complete functional level, the PSM approach provides the "most complete" examination of the plant response specific accident conditions and their implications to the form and content of the emergency procedure guidelines.

Section 6  
CONCLUSIONS

By examining the required characteristics of practical emergency procedure guidelines, and by comparing the approaches utilized by the four Owners Groups to develop such guidelines<sup>\*</sup> with an approach that utilizes the methods, tools, and information base generated in the PSM Program, it can be concluded that the PSM approach can offer considerable benefits either in conjunction with or independent of the Owners Groups approaches. The key elements of the investigation that led to this general conclusion are the following:

- The pre-TMI event-specific procedures have serious deficiencies with respect to their ability to provide unambiguous guidance for multiple failure accident sequences (see Section 2)
- Alternative approaches (such as those used by the four Owners Groups) which focus on a limited number of critical safety functions or symptoms indicative of the status of these functions have the potential to remedy most of these deficiencies and provide effective guidance regardless of the specific event(s) which produce the upset condition (see Sections 2 and 3)
- The practical application of these alternative approaches can, however, produce other problems because different accident conditions requiring different operator responses can "look the same" to the operator if attention is focused on only a few key parameters (see Section 4)
- A systematic process is therefore necessary to gain maximum assurance that the guidelines provide effective unambiguous guidance to the operator regardless of the specific event(s) that occur (see Section 4)
- A fully documented set of operator action event trees (OAETs), by systematically tabulating the key plant states, the operator actions required at each state, and the symptoms exhibited by the plant at each state, can provide the tools and information necessary to finalize or review existing guidelines to ensure that they provide correct and unambiguous guidance (see Section 5)
- These OAETs can also be effectively used to alter generic guidelines so that they can be assured of providing unambiguous guidance to the operator of any specific plant (see Section 5)

\*Recent changes on these guidelines do not affect the conclusions cited here.

- The OAETs and supporting information can also be used to directly produce emergency procedure guidelines independently of other approaches; the process of producing guidelines in this manner will be self-validating (see Section 5).

The various approaches used by the four Owners Groups are all essentially sound and the guidelines produced by each group potentially represent a substantial improvement over the pre-TMI procedures. However, as is often the case, the process of solving one problem can produce other compensating problems which must be addressed. The potential pitfalls which must be avoided in the practical application of the functional or symptomatic approaches are closely linked with the primary motivation for their development. The pre-TMI procedures required the operator to know too much before he could be assured of taking the correct action. The proposed remedy is to provide guidance based on much less information (a limited number of key symptoms associated with the performance of a few critical functions). However, whenever guidance is based on limited information, extreme care must be taken to assure that it is always correct and unambiguous. The PSM-based approach using OAETs and supporting information can be effectively used to assure that the function- or symptom-oriented guidelines do, in fact, solve the problems associated with event-specific procedures uncovered at TMI and do not merely replace those problems with others.

## REFERENCES

1. "Clarification of TMI Action Plan Requirements," NUREG-0737, November 1980.
2. J. vonHerrmann, R. Brown, T. Tome, "Light Water Reactor Status Monitoring During Accident Conditions," NUREG/CR-1440, EGG-EA5153, June 1980.
3. R. Brown, J. vonHerrmann, "Light Water Reactor Engineered Safety Features Status Monitoring," NUREG/CR-2278, EGG-2122, August 1981.
4. R. Brown, J. vonHerrmann, "Boiling Water Reactor Status Monitoring During Accident Conditions," NUREG/CR-2100, EGG-2099, April 1981.
5. "Summary of Westinghouse Owners Group Program to Address NUREG-0737, Item I.C.1," Letter from Robert W. Jurgensen (WOG) to Stephen H. Hanauer (NRC), November 30, 1981.
6. "Combustion Engineering Emergency Procedure Guidelines," CEN-152, June 1981.
7. "Emergency Procedure Guidelines - BWR 1 through 6, Revision 1," General Electric Company, January 30, 1981.
8. "Abnormal Transient Operating Guidelines," (DRAFT), Babcock & Wilcox, July 1980.





**EG&G Idaho, Inc.**  
**P.O. Box 1625**  
**Idaho Falls, Idaho 83415**