NUCLEAR ENGINEERING

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Station Blackout: An Opportunity For Formulating Less Prescriptive Nuclear Safety Regulation

Vincent P. Manno

MITNE-261

Department of Nuclear Engineering

Massachusetts Institute of Technology

Cambridge, Massachusetts 02139

Station Blackout: An Opportunity For Formulating Less Prescriptive Nuclear Safety Regulation

Vincent P. Manno

MITNE-261

May 1984

Summary

MIT has proposed to the Nuclear Regulatory Commisssion (NRC) a project to help develop less prescriptive safety regulation in the licensing of advanced reactors. The proposal argues that a current outstanding Light Water Reactor (LWR) issue is a fruitful vehicle for achieving this goal. This paper addresses using the station blackout issue, which is currently classified as an Unresolved Safety Issue, as the trial example. The background, current regulation and present issue resolution are reviewed. The current state of acceptance criteria is then critiqued using as the principal criterion the usefulness of present approaches in licensing new designs. On the basis of some negative findings including overly prescriptive statutes and prejudices in favor of current LWR plant design, a new acceptance criteria framework is outlined. Finally, a cooperative MIT/NRC program to formulate and test this new regulatory approach in the future is described.

I. INTRODUCTION

A common criticism of current nuclear reactor safety regulation, as embodied in the Code of Federal Regulations (CFR), NRC Regulatory (Reg) Guides, Standard Review Plan (SRP), Branch Technical Positions (BTP's) and various licensing documents (such as NUREG reports, Safety Evaluation Reports (SER's) and Inspection and Enforcement Bulletins (IEB's)), is that it has become too prescriptive in nature. Thus, acceptable design solutions rather than acceptance criteria, are being specified. This tendency in turn retards the introduction of new and innovative designs since the proposal of a novel approach assures a more lengthy and less predictable licensing process. Further, the bulk of the regulations focus nearly exclusively on the problems and features of the current generation of LWR design (and design basis). As such, it is ill-suited for the assessment of advanced reactor designs such as next generation LWR's, HTGR's, liquid metal reactors, and other options which are receiving increased attention during the current nuclear ordering hiatus.

In the interest of trying to learn from the LWR history and set the stage for a more efficient licensing process, MIT has proposed a modest project [1] with the NRC to begin to address these concerns. A major aspect of the proposed effort falls under a subtask entitled, "Evolution of a Nonprescriptive Safety Regulation Approach." This effort would utilize a LWR safety issue for which the nature of safety requirements is well established but which also has applicability to other reactor designs. Of the major issues currently under active NRC resolution, the Unresolved Safety Issue A-44 (USI-A-44) concerning station blackout seems particularly appropriate as a vehicle for carrying out this preliminary work since the concern for plant stabilization during electric power losses is generic to any power station.

The purpose of this report is to define the problem in a clear way and set the direction of this work. Following these introductory remarks, the current regulations affecting electrical power systems are reviewed. This discussion is centered upon three specific regulatory documents - General Design Criteria (i.e., Appendix A to 10CFR50), Reg. Guides, and SRP (as delineated in NUREG - 0800 [2]). As alluded to earlier, the station blackout issue is currently classified as an Unresolved Safety Issue (USI). An action plan to address this issue was formulated in 1980 by the NRC. The highlights of this plan, the current research efforts being performed and the possible direction (short term) of new regulations are addressed in the next discussion. The USI resolution discussion is followed by a general critique of the new and existing regulations using the criterion of their usefulness in the licensing of new designs. As this analysis shows some serious deficiencies, a different approach formulated specifically to improve electrical power system acceptance criteria and plant safety in general is proposed. The specification of an alternative strategy is followed by a program plan which describes how the MIT/NRC program can develop the approach into a usable licensing mechanism.

II. CURRENT REGULATIONS

Anything more than a cursory review of the current body of regulations affected electrical power systems would be a major report unto itself. This point is reinforced by a review of Table 8-1 of Chapter 8 of NUREG-0800. This table is included in this report as Appendix A. The design of electrical power systems involve conformance to at least 6 design criteria, 12 Reg. Guides, 7 BTP's, 7 IEEE standards and the recommendations of an existing NUREG report [3]. Of the various GDC, number 17 deals specifically with electrical power system design and is the subject of the next subsection. The applicable Reg. Guides are described in the subsequent subsection. Finally, the SRP is reviewed in the final portion of this section. Further review of the IEEE standards as well as NUREG-0660 would be fruitful and these are planned as future work.

1. GDC 17

A copy of General Design Criteria 17 entitled, "Electric Power Systems" is included as Appendix B to this report. The first paragraph is general in nature and requires the inclusion of an electrical power system capable of maintaining core cooling and assuring fuel and containment design limits. The second paragraph requires an onsite power system that is independent, redundant, and testable. This system must perform its vital functions assuming a single failure. The third paragraph contains more detailed requirements for the offsite sources including two incoming circuits which may share a common switchyard. At least one of these circuits must be designed to be available within a few seconds following a large LOCA. The final paragraph contains a call for designing against common cause failures.

Three noteworthy observations can be made. First, an explicit consideration of reliability is lacking with redundancy and the single failure criterion acting as surrogates. This reflects the inadequate state of knowledge in the reliability engineering area at the time this guidance was formulated. Second, the allowance of common switchyards regardless of design specifics increases the potential for common cause failure without any justification. Third, the requirement of A.C. availability with a few seconds of a LOCA has two important ramifications. First, it is indiciative of the emphasis upon large double-ended near-instantaneous breaks as the chief design basis events. Second, it indicates an implicit assumption of the plant being a current generation LWR since a specific accident response time frame is required.

2. Regulatory (Reg) Guides

Reg Guides are documents issued by the NRC staff which describe in great detail how licensees should formulate their designs in order to assure conformance to applicable safety regulation. These documents vary in specificity from general endorsements of established design practices or industry standards (such as IEEE Standards and ASME codes) to the requirement of specific analytical models and input assumptions. The 12 Reg Guides related directly to electircal power systems reflect this variation. Five of these have system level implications and address separation, independence, testing, and maintenance. The remainder are narrower in scope in that they address specific components such as electrical penetrations, lead storage batteries, and diesel generators. The predisposition to diesel generators is important since it reinforces their choice as the emergency power source of the inconsistent performance of these devices. Of course, the choice of

diesel generators also mirrors the requirement for rapid power restoration typical of large LWR LOCA analysis.

3. Standard Review Plan (SRP)

The SRP, which is designated presently as NUREG-0800, is prepared for the guidance of NRC staff reviewers as they analyze applicants' designs. Its stated principal purpose is to assure the quality and uniformity of review and establish a well-defined design basis. The document itself is two-volumes (each over 2 inches thick) and is structured to correspond to FSAR chapters. Chapter 8 concerns electric power and has been reviewed in some detail. The chapter is divided into three sections and two appendices. The first section is introductory and describes the general format of the review as well as referencing other related regulatory statutes (e.g., 10CFR50, Reg. Guides, BTP's). The second section describes the review of offsite electrical power systems while the final section which addresses onsite systems is further divided into A.C. and D.C. power systems. The first appendix contains the important BTP's while the second describes the performance of site inspections.

A review of Chapter 8 leads to a general observation that its contents are prescriptive in nature as will be demonstrated by the following citation of specific instances. A second major point is the bias towards diesel generators. No general criteria or even presciptive design constraints for non-diesel generator systems are presented save for a general caveat that such instances will be addressed on a case by case basis. The potential problems arise from the fact that the staff is not given any guidance in their general review documents - the SRP.

Some specific instances of design prescription are:

- 2 redundant single-failure proof offsite circuits with a common switchyard allowable (pg. 8.2-1),
- design specification of switchyard breaker control schemes (pg. 8.2-5),
- no loading of non-safety loads on emergency buses (pg. 8.3.1-2),
- detailed diesel generator design suggestions (based on NUREG-0660) including (pgs. 8.3.1-6 to 8.3.1-7):
    i) loading testing specs
    ii) formal maintenance training program structure
    iii) preventative maintenance program structure
    iv) placement of control and monitoring equipment,
- prohibition of onsite multiunit power system crossconnections (pg. 8.3.1-9),
- design of interconnections between load control centers to include two tie-breakers connected in series (pg. 8.3.1-9),
- emergency diesels cannot be used for power peaking (pg. 8A-6),
- design specification of undervoltage protection system (pg. 8A-13),
- seven day supply of diesel fuel for each engine (pg. 9.5.4-2). Day or "integral" tank overflow line, low level alarm, tanks designed for water removal (pg. 9.5.4-5),
- diesels must have independent circulating heated water loop to increase "first try" reliability. Also, 3-way thermostatically controlled bypass value required (g. 9.5.5-5),
- diesel starting system to include air system of compressor, dryer, air receivers, piping, and other components. Diesel must be able to crank cold engine 5 times without charging receivers (pg. 9.5.6-3), and

• design remedies for assuring lube oil flow (pg. 9.5.7-5).

If applicants choose not to conform to these specifications, they must propose "an acceptable alternative method for complyling" with regulations but no acceptance criteria save for GDC 17 are provided.

III. UNRESOLVED SAFETY ISSUE (A-44) RESOLUTION

Station blackout is designated USI A-44 by the NRC in their Congressionally-mandated program of resolving such issues on a timely basis [4]. As identified in NUREG-0510 [5], station blackout is the complete loss of all alternating current (A.C.) power (i.e., both offsite and onsite sources). Without station A.C., the coolability of the core depends upon systems which do not require A.C. power and the subsequent restoration of power. As such the issue has both system performance and reliability aspects. As outlined above, current regulations require diverse and redundant offsite and onsite power supplies and the principal design criterion is that of adequate performance in spite of a single failure. At the time this issue was raised it was the NRC staff's opinion that despite these requirements, electrical power reliability was not assured. The action plan for resolving USI A-44 is reviewed in brief below. In addition to the NRC staff, technical assistance contracts have been awarded to Oak Ridge National Laboratory (ORNL) and Sandia National Laboratory (SNL). The information generated to date as well as future directions are then highlighted. Since most of the technical background studies are complete, the NRC staff is formulating a final issue resolution package which will include new rules [6]. Though these regulations have not been officially published, the NRC staff has offered some general features of the new regulations and these are outlined in the final discussion of this section.

1. Action Plan

A Task Action Plan for this issue was issued in 1980 and the current status of it is reviewed in Reference 7. A figure depicting the historical progression is reproduced as Figure 1 in this report. Though this figure is

somewhat confusing, three important features are discernible. First, the resolution process is behind schedule in that the present final resolution date is 2/85 as opposed to the original proposal of 6/82. Second, three sets of analyses define the research effort. These are:

1) loss of offsite power at nuclear power plants,
2) reliability of emergency A.C. power supplies, and
3) station blackout accident sequence probabilities and consequences.

The third important point is that the proposed resolution direction is rulemaking and subsequent additions to the current set of regulations in conjunction with the issuance of a new Reg Guide specifying how an applicant can satisfy the new criteria. If past experience is indicative of how this Reg Guide is formulated, very specific design constraints can be expected. A final note is that the schedule reported in Reference 7 is itself probably slipping but no revised information is available at this time.

2. Current Research Efforts

Two of the three research activities mentioned above have ben completed and documented. The investigation of loss of offsite power is complete but a formal report has not been issued. Some internal NRC documentation of this effort exists [8]. However, an approximate occurrence rate for loss of offsite power of 0.1/reactor-year has been mentioned in informal conversations with knowledgeable parties. The historical record has shown that a few complete station blackouts have occurred but, except for one, their duration was a few minutes at most. The one exception was an incident at the Ft. Saint Vrain HTGR where power was lost for over a half hour. The

three major contributors to offsite power loss are switchyard failures, grid stability, and external event outages such as those due to severe weather. Grid problems and switchyard failures are the most benign since they can usually be restored in a short time. Weather-related damage is of greater concern due to the duration of their impact. Figure 2 which is extracted from Reference 9 demonstrates these points quantitatively.

ORNL has issued a report on emergency A.C. power supply relilability [10]. Onsite power system reliability was calculated for 18 power plants and 10 generic configurations. The three objectives of the study were:

1) assess the range of onsite A.C. system reliabilities at nuclear plants,
2) determine major factors affecting reliability, and
3) incorporate loss of offsite power data to determine station blackout frequency range.

Some of the major findings of the study are:

- diesel generator failure probability ranged from 0.008 to 0.1 with a mean value of 0.025,
- common cause (both human and hardware) failures contributed to unavailability in the range 0.0001 to 0.0042,
- scheduled maintenance unavailability ranged from 0 to 0.037 with a mean of 0.006,
- diesel repair time ranged from 4 to 92 hours with an average of 20 hours,
- plant service water contributed significantly to unavailability,
- overall demand unreliability for onsite power systems ranged from 0.00022 to 0.048 per demand.

The "Highlights" section as well as a few informative figures and tables from the report are included as Appendix C. A general conclusion is that independent diesel generator failures are important contributors to total system unavailability. This finding is in agreement with an earlier study [11] of LER (Licensee Event Report) data. Therefore, redundancy is of major importance. Some modest gains are possible in maintenaence and operation areas to decrease common cause failures. No single design area could be identified as a primary problem and hence generic recommendations are not made. However, in plants where redundancy is high (e.g., 1 of 3 generators needed for success path), unavailability is dominated by common cause failures.

SNL has issued a report documenting their analysis of station blackout accident sequences [12]. Thus, this effort will be combined with the ORNL findings to establish a technical basis for future regulatory requirements. The goals of the SNL study were:

1) determine core damage probabilities,
2) provide insights into reducing core damage frequencies, and
3) provide perspectives on risks associated with such events.

The "Executive Summary" as well as a few informative excerpts are included as Appendix D to this report. The most important plant features with respect to risk were found to be:

- ability and timing of power restoration,
- standby reliability of decay heat removal systems following A.C. power loss,
- reliability of onsite emergency power,
- D.C. power reliability especially impact on instrumentation and decay

heat removal equipment,

- common service water dependencies,
- RCP seal leakage potential,
- likelihood of relief valve opening and malfunction during event,
- containment design,
- operator training and performance, and
- external event impact.

Plant analyses were found to be plant design-specific in that PWR's and BWR's of various basic configuration exhibited different susceptibilities. For example, in the PWR, the most important equipment involved auxiliary feedwater (i.e., turbine-driven, non-A.C. dependent pumps), battery depletion, possible A.C. dependence of RCS isolation controls, common service water dependencies and the potential for pump seal leakage. The external event contribution sets a limit on achieving lower core damage frequencies through system improvements.

3. Potential New Regulations

The regulatory resolution of this safety issue has not been formally presented but the direction of the new approaches are known. In all likelihood, the NRC will propose new rules which would be applicable to both existing and new plants. It is expected that the new rules will be in addition to the existing body of regulation. The major thrust of the requirements will be the establishment of the ability to do without any A.C. power for a given period of time. The exact time period would be inversely proportional to the level of onsite diesel generator redundancy. A possible requirement matrix is:

diesel redundancy	no A.C. survivability period
2 out of 3	16 hours
1 out of 2	8 hours
1 out of 3	4 hours

The construction of this matrix implies a certain range of acceptable reliabilities and risks but these are not explicitly given.

The most significant impact of such a rule would be on operating plants due to backfit requirements. The most important element for PWR plant response is non-A.C. dependent auxiliary feedwater flow to assure decay heat removal. Nearly all plants have some capability to accomplish this function through turbine-driven auxiliary feedwater pumps (TDAFWP's) which require only D.C. power for operation. Other areas which may require more substantial work are D.C. power systems including longevity and reliability of storage batteries, capability of equipment to operate in moderately harsh environments caused by the lack of ventilation, integrity of reactor coolantpump seals during extended periods without seal flow and availability of plant auxiliary service systems such as cooling water and compressed air.

IV. USEFULNESS OF CURRENT AND PROPOSED REGULATIONS FOR LICENSING ADVANCED DESIGNS

Assuming the general directions for new regulation outlined in III.3 are correct, the resultant body of rules will remain prescriptive in nature. The validity of this approach for determining backfit requirements and judging current LWR plant design is itself questionable. The ORNL analysis of current designs, which was formulated using the existing regulatory structure, shows that this approach was not overly successful in promoting acceptably reliable electrical power systems. A wide range of reliability existed despite a fine level of design guidance contained in the regulations (see section II). One may then argue that a continuation of this type of approach does not present the most useful path. Nevertheless, the most important deficiencies of the established (albeit soon to be modified) regulatory statutes is their limited usefulness in assessing new plant designs where system characteristics are not constrained by existing plant layout or design criteria.

The present set of guidelines (present implies existing rules plus proposed rules) do not focus on reliability but instead require redundancy. The two are not synonomous. Further, the required levels of redundancy is not validated by experience. Minute design constraints such as those involving switchyard breaker design and diesel engine lube oil system characteristics removes the engineering function from the manufacturer. In effect, the rules set the design which in turn stifles innovation. The onsite emergency power systems are assumed to be diesel generators. This confines new designs to an alternative that the NRC itself has identified to be less than optimal. Further, the linkage of plant performance to

redundancy is again based on the false assumption that redundancy assures reliability. In short, a more clearly based and flexible set of criteria would provide a more efficient and reliable mechanism to judge new plant designs as to their characteristics during electrical system transients. An outline for such an alternative structure is described in the next section.

V. DEVELOPMENT OF FLEXIBLE LESS PRESCRIPTIVE CRITERIA

The previous discussions demonstrate the potential benefits of a different regulatory approach in the station blackout area especially if the licensing of advanced designs is considered as important. Despite the criticism made in the preceding critique, the goal of the regulations to assure safety during electrical system upsets remains a valid constraint. As such, the following framework is suggested in order that this design goal can be achieved with greater certainty and such that new solutions are encouraged or at least judged in a reasonable way. The proposed tack involves three related criterion areas. The extent to which these criteria can be determined is partially dependent upon the status of a number of interfacing safety issues. Therefore after these three directions are described, the most important related safety issues will be delineated.

1. Explicit Reliability Design Goals

Reliability is clearly the central concept in judging a system's design. The current regulations themselves are structured around some undetermined and unstated reliability goals. The practices of quantitative reliability assessment have advanced to the point today that they can be used to judge the adequacy of a system. This is especially true in the analysis of electrical components and systems for which large data bases and a number of demonstrated analysis techniques exist. Given this situation, the bulk of the design-related regulations could be replaced by an explicit set of reliability goals. The acceptance critreria should also define the important considerations which must be taken into account in the analysis such as common cause failures, human actions, external events and repair/testing

strategies. The onus of design would then be placed on the applicant. For example, redundancy may be preferred over individual component reliability or vice versa. The regulatory review would focus on asssuring that the goals are met. If they are not, the redesign is the applicant's concern.

2. Non-endorsement of Specific Onsite Power Sources

Despite disclaimers, the current regulations assume diesel generators are the onsite emergency power source. This is based on the fact that nearly all of the present LWR plant onsite power supplies rely on diesel generators. The sudden break non-mechanistic large break LOCA design basis prejudices the choice of emergency power supplies due to the need for near-instantanious emergency (A.C. - dependent) equipment response to such events. Further, the imposed assumption of offsite power loss at the time of a LOCA forces the design choice even further. Advanced designs need not abide by the same constraints due to a number of factors including slower accident time constants (see V.3), refined safety criteria (see V.4), and demonstratably reliable preferred power sources (see V.1). In short, the removal of diesel generator design requirements would assist the review process in that overall safety and performance will be emphasized more than compliance to individual component restraints.

3. Reducing A.C. Dependence

The design details associated with reducing a nuclear plant's dependence in both immediate and long term time frames are not the responsibility of the regulatory authorities. Possible areas of fruitful research are more reliance on D.C. dependent systems, emphasis of passive heat removal

mechanisms and minimization of active components which require rapid changes of state. Nevertheless, the safety criteria used to judge new designs should allow and perhaps encourage such approaches.

One avenue for accomplishing this goal is to develop the explicit reliability criteria discussed in V.1 in a way which gives credit to designs that minimize A.C. dependence. The new rules currently under NRC consideration are a step in this direction except that they reward redundancy not reliability. The degree to which advanced designs can achieve A.C. independence is determined in part by a number of other regulations which impact design choices. The most important issues in this category are discussed in the next subsection.

4. Interfacing Safety Issues

The usefulness of safety regulations is analogous to the operation of a nuclear plant in that neither can be adequately judged on the merits of individual parts. A valid assessment is achieved only when the integrated structure is analyzed. Hence, the station blackout issue cannot be discussed in a vacuum. Five issues of particular relevance are identified as requiring explicit attention.

First, the overall content and structure of all current regulation contain a strong bias towards conventional LWR design. This came about due to the natural tendency to codify solutions to past problems to avoid their repetition. Nevertheless, this tendency in itself may stifle development of effective designs for non-LWR plants. Second, and more immediately germane to station blackout, the current large LOCA instantaneous break assumption has fostered the design choice of diesel generators. Experience and analysis

has shown that the outcome has been a decrease in real safety since station blackout events given diesel generator systems are larger contributors to risk than are large LOCA's. In fact, while an instantaneous double-ended break may not be physically possible, diesel failures occur frequently. Developing safety criteria which aremechanistically based such as "leak before break" would allow the utilization of systems which are more reliable in expected events.

The single failure criterion permeates nuclear safety regulation. Its development was not flawed in that it reflected the state of knowledge in the reliability area over 20 years ago. However, its usefulness may be fading as systems become more complex and reliability assessment techniques become more standardized and credible. In some instances, such as the requirement for offsite power circuits, its imposition may have caused design which did not enhance reliability. There are surely other examples of this kind of effect. The fourth issue is that of seismic design. This is a monumental and complex issue unto itself but the employment of less conservative design assumptions could encourage the use of more passive systems.

The final issue is that of safety goals. The proposed new regulations for the resolution of the station blackout issue reflect an unofficial internal NRC target risk limit of 10^{-5} core damage events per reactor year given the occurence of a station blackout. The utilization of any value must be based on the overall safety goals rather than setting limits on each potential occurence. Second, improvements in electrical power system reliability must be taken into account. For example a goal based on the probability of an event times its consequences should be used. As such if one design has a blackout probability of 0.001/R-yr and a core damage

frequency of 10^{-5} given a blackout has occurred, its composite index is 10^{-8}/R-yr. A second plant may have an improved design such that blackout frequencies are 10^{-5}/R-yr but a core damage frequency given a blackout of 10^{-4}. The second plant has the lower risk. The point is that regulation of individual issues cannot be performed without considering the bigger picture.

VI. MIT/NRC PROGRAM

The following summarizes the approach to evolving non-prescriptive regulation as proposed recently by MIT to the NRC [1]. Even if all involved parties agreed with the general content of the arguments advanced in the previous section, formulating this new criteria set and process is itself a major task. The following discussion outlines a framework for NRC and MIT to work together to begin this concrete development. The suggested program would involve two major tasks to be performed sequentially - criteria development and test case assessment.

The first task would involve transforming the ideas outlined in section V into a useful regulatory framework. This development would be based on the explicit acknowledgement that station blackout is a substantial safety issue for the plant operator as well as an item of licensing demand from the NRC. As such, the past and present regulations as well as the experience base accrued to date cannot be put aside. The first step of the process would involve a careful reveiw of the relevant material by MIT to distill the central safety concerns imbedded in the current regulations. This effort would build upon the recent ORNL and SNL work as well as other available information.

The second step would use these central concerns coupled with the guidance detailed in section V to devise a new streamlined, less prescriptive and more flexible criteria set. This effort would involve the development of credible reliability goals and guidance for system assessment. Design information and equipment performance data bases would be reviewed to provide confidence that a realistic criteria set is developed. As mentioned earlier, there are major interfacing issues. The degree to which possible changes in

their assessment should be incorporated in this work is an open question. Nevertheless, at this point, all other current regulations (such as large LOCA requirements) would be assumed to be in force. The degree to which current regulations can be relaxed in this exercise should be addressed by the NRC and MIT when the project commences. While it is assumed this development would be performed in an interactive mode with the NRC staff, the final part of this task will be a thorough review of the proposed criteria and a resolution of outstanding issues. The product of this first task would be an acceptance criteria specification.

The second task is the formulation of a design example which satisfies the acceptance criteria in MIT's judgment. This design would then be "submitted" for an informal NRC review. This process provides a useful exercise in that it would test both the criteria structure and the staff's ability to utilize it as a licensing tool. A complicating aspect of this task is that an electrical system design (even a less-detailed version as would be produced by MIT) cannot be developed without specifying the plant characteristics. Therefore, a choice of plant type must be made. The proposed option is an advanced LWR since its performance characteristics are better established in both operational and accident scenarios.

VII. REFERENCES

1. M.W. Golay et al., "Safety Regulation Of Advanced Reactors," proposal to U.S.N.R.C., March 1984.

2. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," U.S.N.R.C., July 1981.

3. G.L. Boner and H.W. Hanners, "Enhancement of Onsite Emergency Diesel Generator Reliability," NUREG/CR-0660, January 1979.

4. Energy Reorganization Act of 1974, Amended December 1977, Section 210.

5. NUREG-0510, "Identification Of Unresolved Safety Issues Relating To Nuclear Power Plants," U.S.N.R.C., January 1979.

6. Personal communication with K. Kniel (U.S.N.R.C.)

7. NUREG-0606, Volume 5, No. 4, "Unresolved Safety Issue Summary," U.S.N.R.C., November 1983.

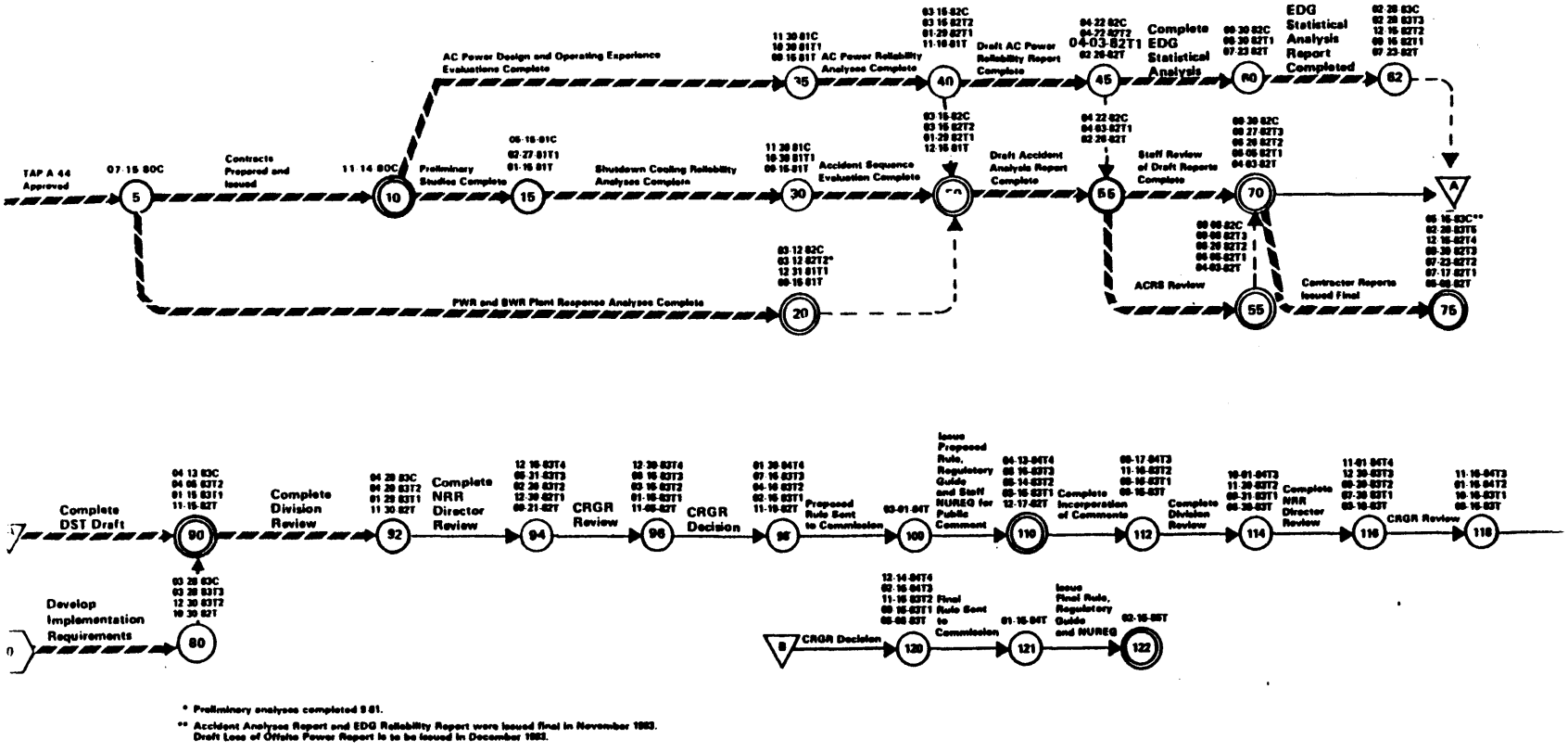
8. F.H. Clark, "Loss of Offsite Power at Nuclear Power Plants," letter report to NRC March 2, 1982.

9. E.W. Hagen, ed., "Loss of Electric Power Coincident With LOCA," Nuclear Safety 18 (1), January-February 1977, pg. 53.

10. R.E. Battle and D.J. Campbell, "Reliability of Emergency A.C. Power Systems at Nuclear Power Plants," NUREG/CR-2989, ORNL/TM-8545, July 1983.

11. T. Mankamo and U. Pulkkinen, "Dependent Failures of Diesel Generators," Nuclear Safety, 23 (1), January-February 1982, pg. 32.

12. A.M. Kolaczkowski and A.C. Payne, Jr., "Station Blackout Accident Analyses (Part of NRC Task Action Plan A-44)," NUREG/CR-3226, SAND82-2450, May 1983.



* Preliminary analyses completed 9-81.

** Accident Analyses Report and EDG Reliability Report were issued final in November 1983. Draft Loss of Offsite Power Report is to be issued in December 1983.

FIGURE 1: NRC TASK ACTION PLAN SCHEDULE (from[7])

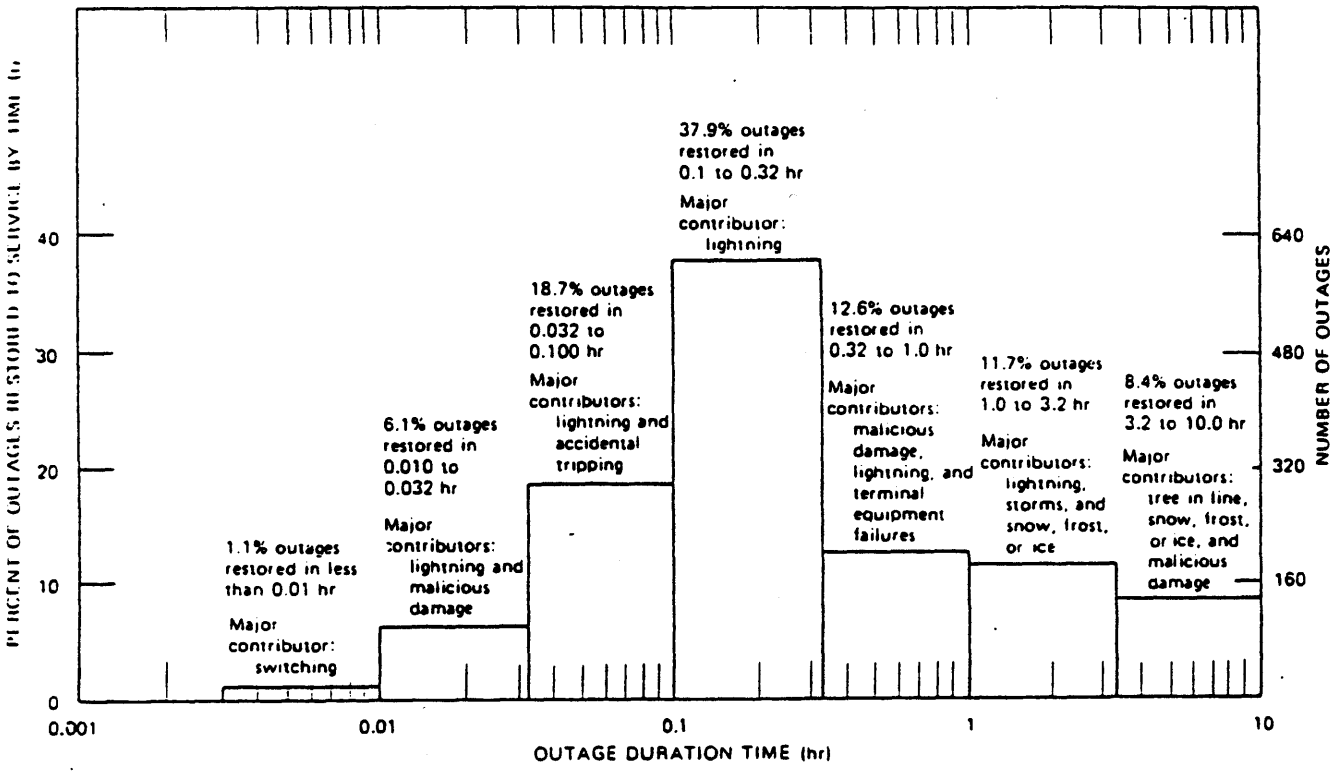


Fig. 2 Histogram: restoration of transmission-line outages. (from [9])

APPENDIX A

Table 8-1 of Standard Review Plan

ATTACHMENT

STANDARD REVIEW PLAN

TABLE 8-1

ACCEPTANCE CRITERIA AND GUIDELINES FOR ELECTRIC POWER SYSTEMS

The matrix of Table 8-1 identifies the acceptance criteria (denoted by "A") and the guidelines (denoted by "G") and their applicability to the various sections of Chapter 8.0. The acceptance criteria define the requirements established by the Commission for power systems important to safety; the guidelines amplify these requirements and provide more explicit basis for evaluation of the conformance of the power systems to these Commission requirements. Acceptance criteria and guidelines are not included herein when the primary review responsibility for these aspects of power systems are reviewed in accordance with sections other than Chapter 8.0 of the SRP.

The Branch Technical Positions listed herein are contained in Appendix 8-A to Section 8.1 of the SRP.

ACCEPTANCE CRITERIA AND GUIDELINES FOR ELECTRIC POWER SYSTEMS - TABLE 8-1

CRITERIA	TITLE	APPLICABILITY (SAR Section) 8.2	8.3.1	8.3.2	REMARKS
1. General Design Criteria (GDC), Appendix A to 10 CFR Part 50					
a. GDC 2	Design Bases for Protection Against Natural Phenomena		A	A	
b. GDC 4	Environmental and Missile Design Bases		A	A	
c. GDC 5	Sharing of Structures, Systems, and Components	A	A	A	
d. GDC 17	Electric Power Systems	A	A	A	

TABLE 8-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY (SAR Section) 8.2	8.3.1	8.3.2	REMARKS
e. GDC 18	Inspection and Testing of Electrical Power Systems	A	A	A	
f. GDC 50	Containment Design Bases		A	A	
2. Regulatory Guides (RG)					
a. RG 1.6	Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems		G	G	
b. RG 1.9	Selection, Design, and Qualification of Diesel-Generator Units Used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants		G		See IEEE 387
c. RG 1.32	Use of IEEE Std 308, "Criteria for Class 1E Power Systems for Nuclear Power Generating Stations"	G	G	G	See IEEE 308
d. RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	G	G	G	
e. RG 1.63	Electric Penetration Assemblies in Containment Structures for Light-Water-Cooled Nuclear Power Power Plants		G	G	See IEEE 317
f. RG 1.75	Physical Independence of Electric Systems		G	G	See IEEE 384
g. RG 1.81	Shared Emergency and Shutdown Electric Systems for Multi-Unit Nuclear Power Plants	G	G	G	
h. RG 1.106	Thermal Overload Protection for Electric Motors on Motor-Operated Valves		G	G	

TABLE 8-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY (SAR Section) 8.2	8.3.1	8.3.2	REMARKS
i. RG 1.108	Periodic Testing of Diesel Generators Used as Onsite Power Systems at Nuclear Power Plants		G		
j. RG 1.118	Periodic Testing of Electric Power and Protection Systems		G	G	See IEEE 338
k. RG 1.128	Installation Design and Installation of Large Lead Storage Batteries for Nuclear Power Plants			G	See IEEE 484
l. RG 1.129	Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Nuclear Power Plants			G	See IEEE 450
3. Branch Technical Positions					
a. BTP ICSB 4	Requirements on Motor-Operated Valves in the ECCS Accumulator Lines		G		
b. BTP ICSB 8 (PSB)	Use of Diesel-Generator Sets for Peaking		G		
c. BTP ICSB 11 (PSB)	Stability of Offsite Power Systems	G			
d. BTP ICSB 18 (PSB)	Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves		G		
e. BTP ICSB 21	Guidance for Application of RG 1.47	G	G	G	
f. BTP PSB-1	Adequacy of Station Electric Distribution System Voltages		G		

TABLE 8-1 (CONTINUED)

CRITERIA	TITLE	APPLICABILITY (SAR Section) 8.2	8.3.1	8.3.2	REMARKS
h. BTP PSB-2	Criteria for Alarms and Indications Associated with Diesel-Generator Unit Bypassed and Inoperable Status		G		
4. NUREG Reports					
a. NUREG/CR 0660	Enhancement of Onsite Diesel Generator Reliability		G		

APPENDIX B

General Design Criteria 17 from Appendix

A to 10CFR50

Criterion 2—Design bases for protection against natural phenomena. Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena, and (3) the importance of the safety functions to be performed.

Criterion 3—Fire protection. Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Firefighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.

Criterion 4—Environmental and missile design bases. Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

Criterion 5—Sharing of structures, systems, and components. Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

II. Protection by Multiple Fission Product Barriers

Criterion 10—Reactor design. The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

Criterion 11—Reactor inherent protection. The reactor core and associated coolant systems shall be designed so that in the power operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.

Criterion 12—Suppression of reactor power oscillations. The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

Criterion 13—Instrumentation and control. Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

Criterion 14—Reactor coolant pressure boundary. The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.

Criterion 15—Reactor coolant system design. The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.

Criterion 16—Containment design. Reactor containment and associated systems shall be provided to establish an essentially leaktight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

Criterion 17—Electric power systems. An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

Criterion 18—Inspection and testing of electrical power systems. Electric power systems important to safety shall be designed to permit appropriate periodic inspection and testing of

important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically (1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses, and (2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among the nuclear power unit, the offsite power system, and the onsite power system.

Criterion 19—Control room. A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

III. Protection and Reactivity Control Systems

Criterion 20—Protection system functions. The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

Criterion 21—Protection system reliability and testability. The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Criterion 22—Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in

APPENDIX C

Highlights and Selected Excerpts from

NUREG/CR - 2989

HIGHLIGHTS

Reliability of emergency onsite ac power systems at nuclear power plants has been questioned within the Nuclear Regulatory Commission (NRC) because of the number of diesel generator failures reported by nuclear plant licensees and the reactor core damage that could result from diesel failure during an emergency. Because of these considerations, the NRC classified the loss of all ac power (station blackout) at a nuclear plant an unresolved safety issue. The NRC requested Oak Ridge National Laboratory (ORNL) to develop a technical basis to help resolve this issue. This report contains the results of a reliability analysis of the onsite ac power system, and it uses the results of a separate analysis of offsite power systems to calculate the expected frequency of station blackout.

Included is a design and operating experience review. Eighteen plants representative of typical onsite ac power systems and ten generic designs were selected to be modeled by fault trees. Operating experience data were collected from the NRC files and from nuclear plant licensee responses to a questionnaire sent out for this project. A total of 1526 events are categorized by failure type for 120 diesel generators, along with data on the number of starts, scheduled maintenance, and repair times for 86 diesel generators.

Important contributors to onsite power system reliability vary from plant to plant, but among the important contributors are the following:

(1) diesel generator failure probability, for which the industry-average is 2.5×10^{-2} and the range is 8×10^{-3} to 1×10^{-1},

(2) human-error and hardware failure common-cause failure, for which the unavailabilities range from 1×10^{-4} to 4.2×10^{-3},

(3) scheduled maintenance unavailability during reactor operation for which the industry-average is 6×10^{-3} and the range is 0 to 3.7×10^{-2},

(4) diesel repair time, for which the average is 20 h and the range is 4 to 92 h,

(5) plant service-water system unavailability, for which the independent failure probability is 2×10^{-3}, the common-cause failure probability is 8×10^{-5}, and the unavailability for scheduled maintenance is 2×10^{-3}.

For the 18 plants modeled, the median probabilities that the onsite power system will fail on demand vary from 2.2×10^{-4} to 4.8×10^{-2}. Sensitivity of the onsite system unreliability to contributors 1-3

listed above is analyzed, and costs of decreasing the probabilities of failure for these contributors are estimated. The important factors affecting onsite ac power system reliability are dependent upon plant-specific features. These features may be independent diesel failure, scheduled diesel downtime, service water unavailability, or common-cause failure of the diesels.

Independent failure of diesel generators is an important contributor to the probability of failure of an onsite ac power system, but significantly reducing the industry-average probability of independent diesel failure will be difficult because there is no single subsystem that dominates the failure probability. Common-cause failure probability may be reduced inexpensively by improving operating and maintenance procedures and eliminating some design features which have a common-cause failure potential. Plants which have two reactors and which require two-of-three diesels to cool both reactors after a loss of offsite power have the least reliable diesel configuration. By adding a diesel, such a plant could improve the onsite ac system reliability by a factor of 5 to 10. However, the approximate cost to add a 3000-kW diesel is $20-$30 million. The costs and reliability improvement for other, less expensive modifications are also included in this report.

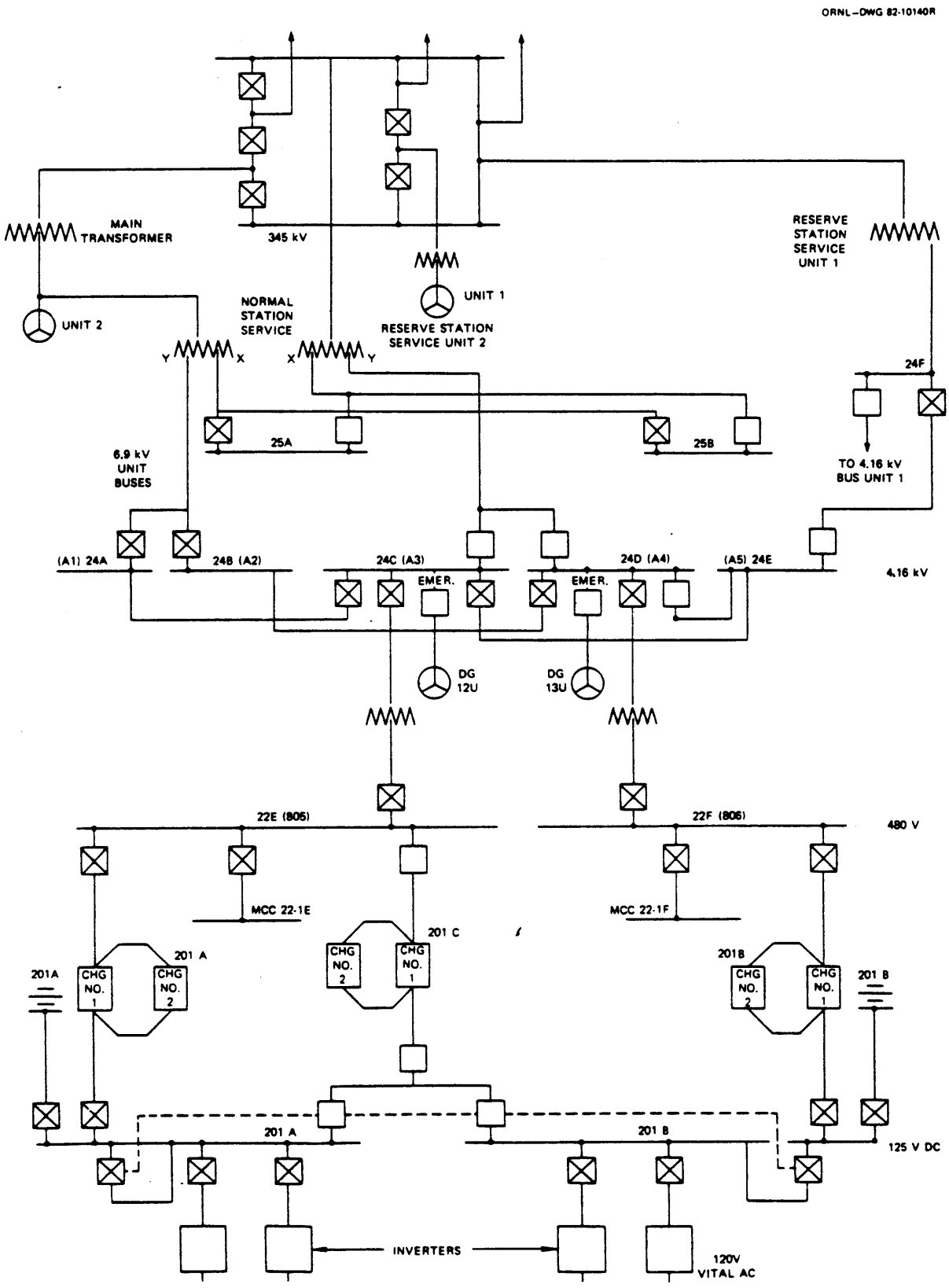


Fig. 2.1. Typical power distribution system.

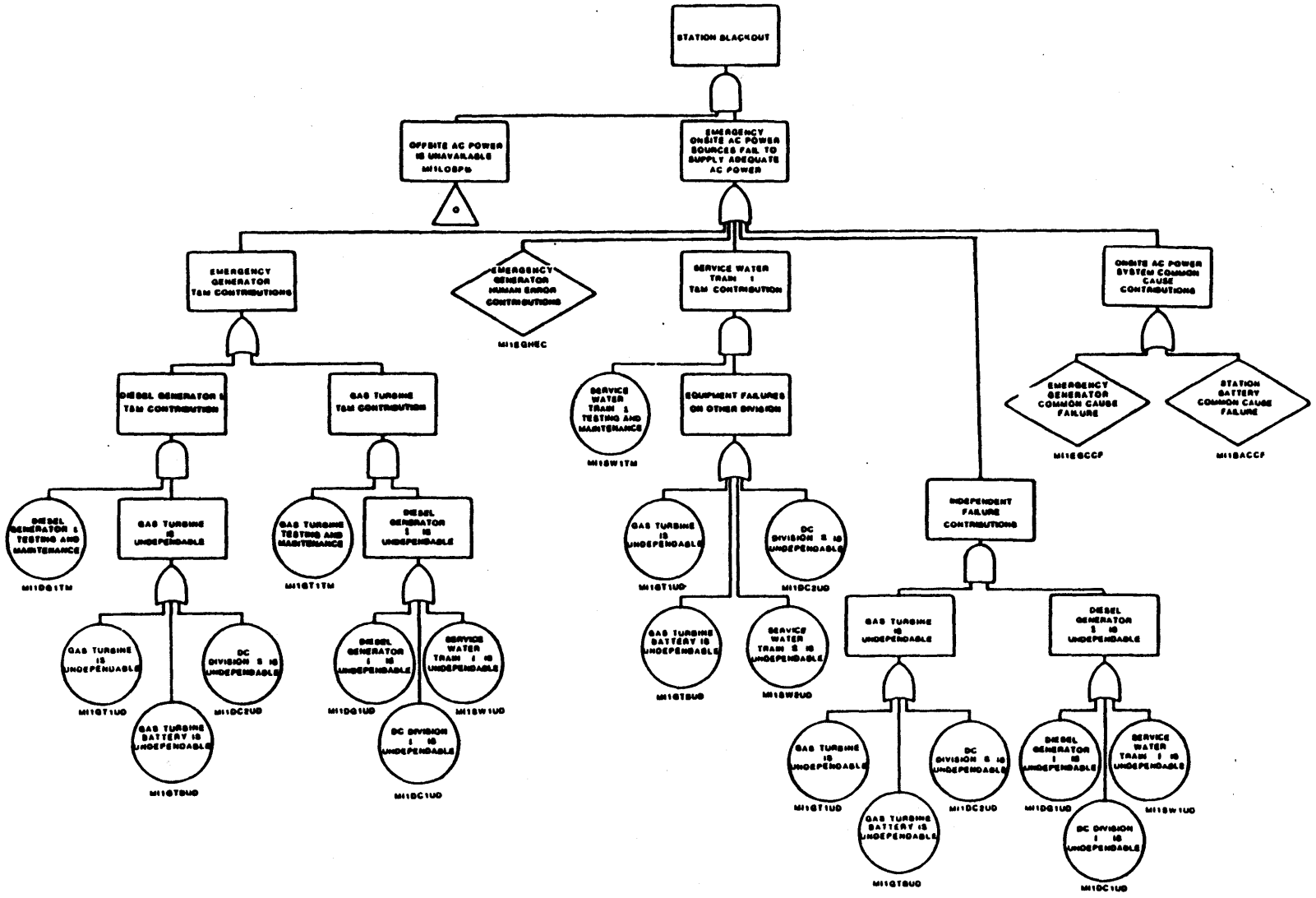


Fig. 3.2. Millstone 2 fault tree.

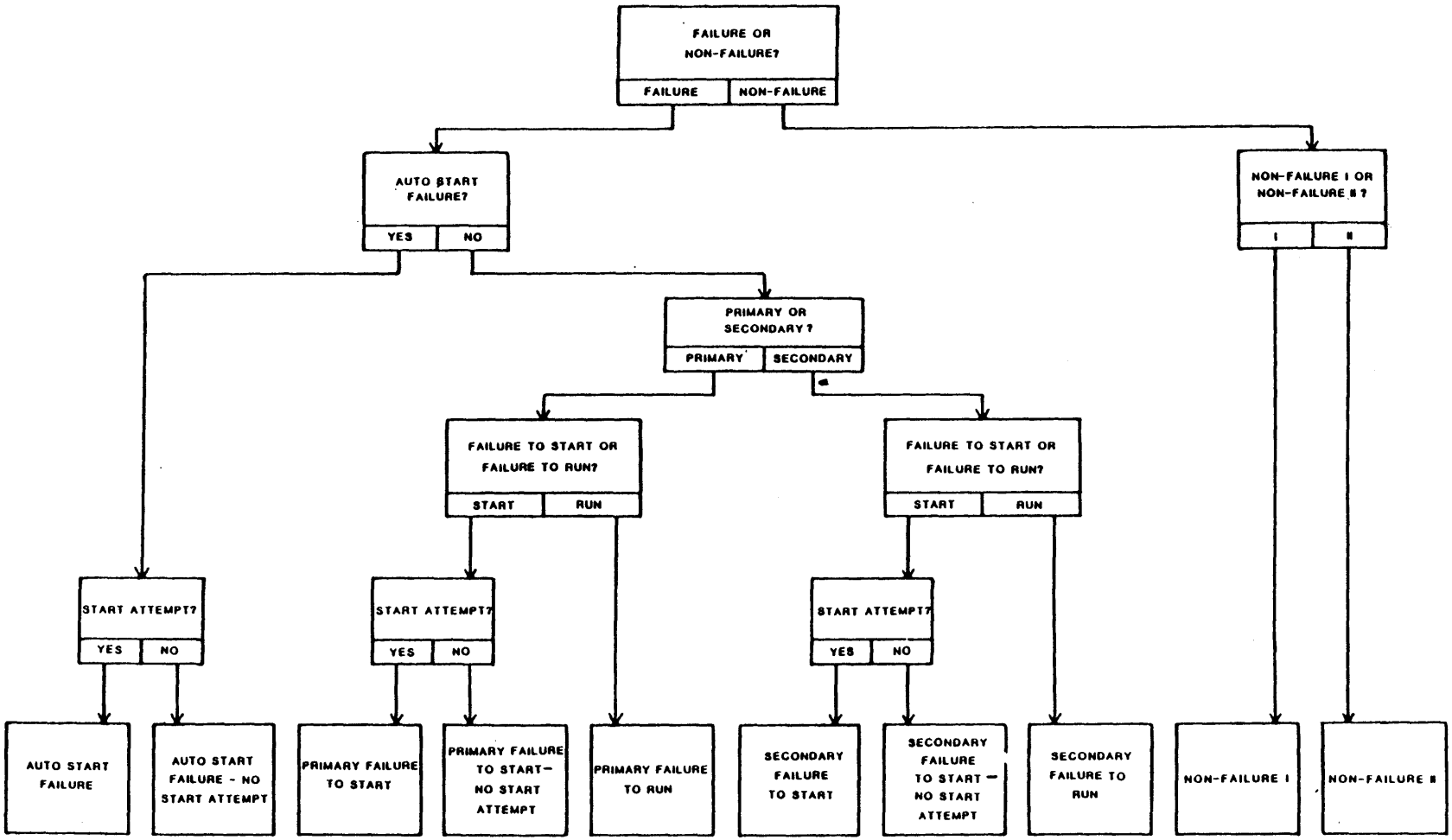


Fig. 4.1. Event classification flowchart.

ORNL-DWG. 82-20504

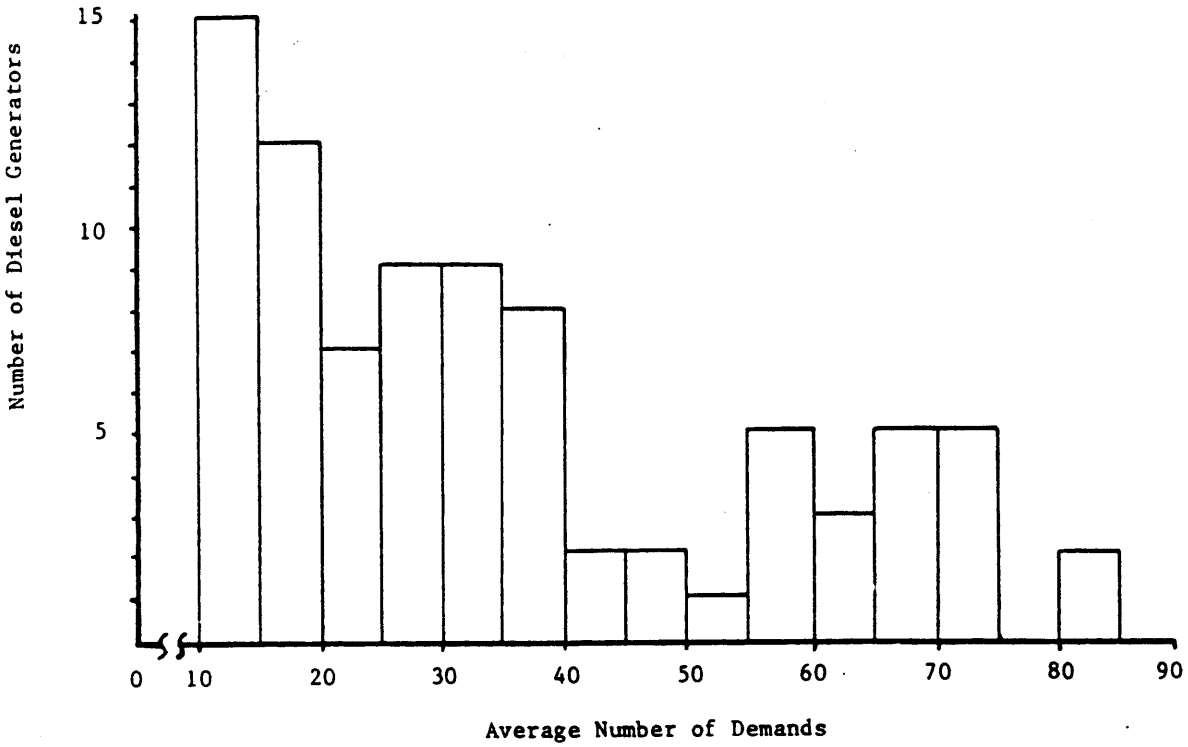


Fig. 4.2. Number of diesel generators vs number of demands per year (1976-1980).

APPENDIX D

Executive Summary and Selected Excerpts

from NUREG/CR - 3226

1.0 EXECUTIVE SUMMARY

The complete loss of AC electrical power to the essential and nonessential switchgear buses in a nuclear power plant is referred to as a "Station Blackout." Because many safety systems required for reactor core decay heat removal are dependent on AC power, and since a number of precursor events to station blackout have occurred, the importance of this issue was raised to that of an "unresolved" safety issue.

This work coupled with a companion report by Oak Ridge National Laboratory (ORNL) [1] provides a technical basis for resolving the station blackout issue. This report focuses on the accident sequence analysis portion of the program by (1) determining core damage probabilities, (2) providing insights and sensitivity reviews for lowering the core melt frequency of accidents, and (3) providing perspectives on the risk from such an event.

The scope of this program covers virtually all existing or near-term operating plants with just a few exceptions due to their unique design features. This was accomplished by performing probabilistic safety analyses on a few generic "base" plant configurations and then providing additional information to assess plant design and/or operational features different from the "base" configurations.

Those plant features found to be important overall, as a result of our analyses, are summarized below:

- The effectiveness of actions to restore offsite power once it is lost,
- The degree of redundancy and reliability of the standby AC power system,
- The standby reliability of decay heat removal systems following loss of AC power,
- DC power reliability and battery capacity including the availability of instrumentation and control for decay heat removal without AC power,
- Common service water dependencies between the emergency AC power source and the decay heat removal systems,
- The magnitude of reactor coolant pump seal leakage and the likelihood of a stuck open relief valve during a station blackout,
- Containment size and design pressure,
- Operator training and available procedures,

- External events which cause plant responses similar to an actual station blackout (but may be better analyzed independent of the station blackout issue).

Since the generic "base" plant configurations have differing susceptibilities, a summary of the important features for each configuration is given below:

(1) Pressurized Water Reactors (PWRs): Initial Auxiliary Feedwater System (AFW) unavailability, battery depletion effects, possible AC dependency for Reactor Coolant System (RCS) isolation, common service water dependencies in AC/makeup systems and the likelihood of a large RCS pump seal leak.

(2) Boiling Water Reactors (BWRs) with isolation condenser(s): loss of RCS integrity due to stuck-open relief valve or large RCS pump seal leak, isolation condenser(s) unavailability, and common service water dependencies in AC/makeup systems.

(3) BWRs with High Pressure Coolant Injection - Reactor Core Isolation Cooling (HPCI-RCIC): ability to operate HPCI-RCIC under a prolonged blackout.

(4) BWRs with High Pressure Core Spray - Reactor Core Isolation Cooling (HPCS-RCIC): initial HPCS-RCIC unavailability and ability to operate RCIC under a prolonged blackout.

In addition to the station blackout accident sequences initiated by system failures, current estimates [9,10,63] of the frequency of major seismic, fire, and wind events which could cause blackout-related core damage are in the range of 1E-4 to less than 1E-6 per year. The likelihood depends on plant features such as the plant's susceptibility to seismic activity and the effects on the switchyard and control systems, susceptibility to fire and the degree of cable separation, and susceptibility to wind or storm events and the effect on offsite power, the switchyard, and on other plant equipment. While not necessarily causing a station blackout, the plant could lose the ability to supply power from the onsite electrical buses to the AC/DC loads. If this should happen, plant responses similar to an actual station blackout event would occur.

These external events may limit the degree to which station blackout core melt frequencies can be lowered by improving the features summarized in the preceding paragraphs.

In view of these results, one can see that the important factors that determine a plant's susceptability to a station blackout can be plant unique. This report provides the analysis which will enable one to compare specific existing plant features against the

important factors identified in this report and to decide upon the importance of station blackout at each plant. This comparison and the sensitivity analysis will provide part of the input for future Nuclear Regulatory Commission (NRC) decisions on the Station Blackout issue.

Figure 1 GENERIC PWR EVENT TREE FOR STATION BLACKOUT

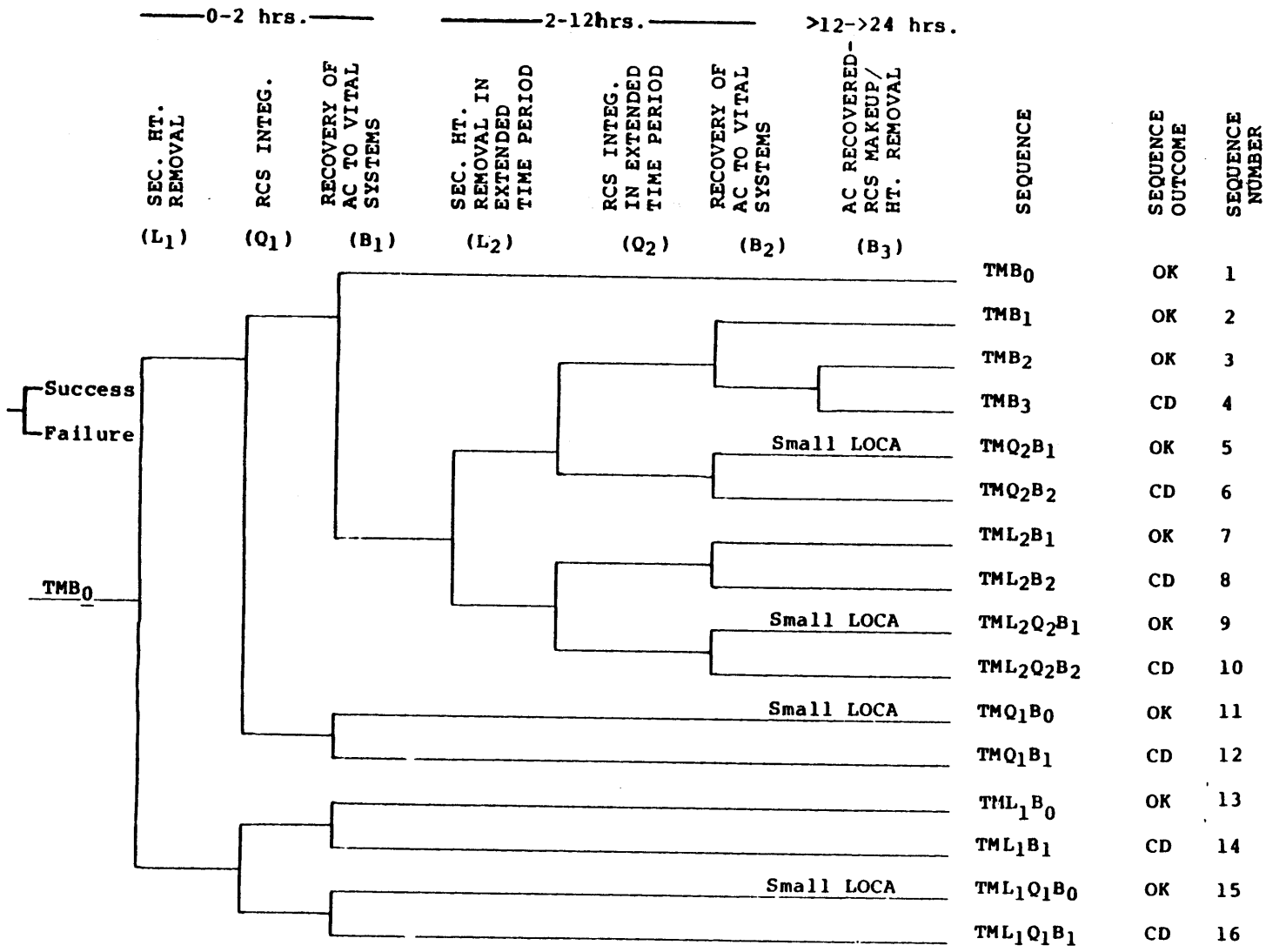
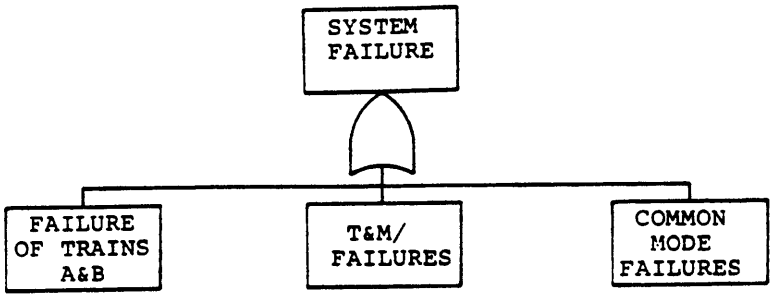
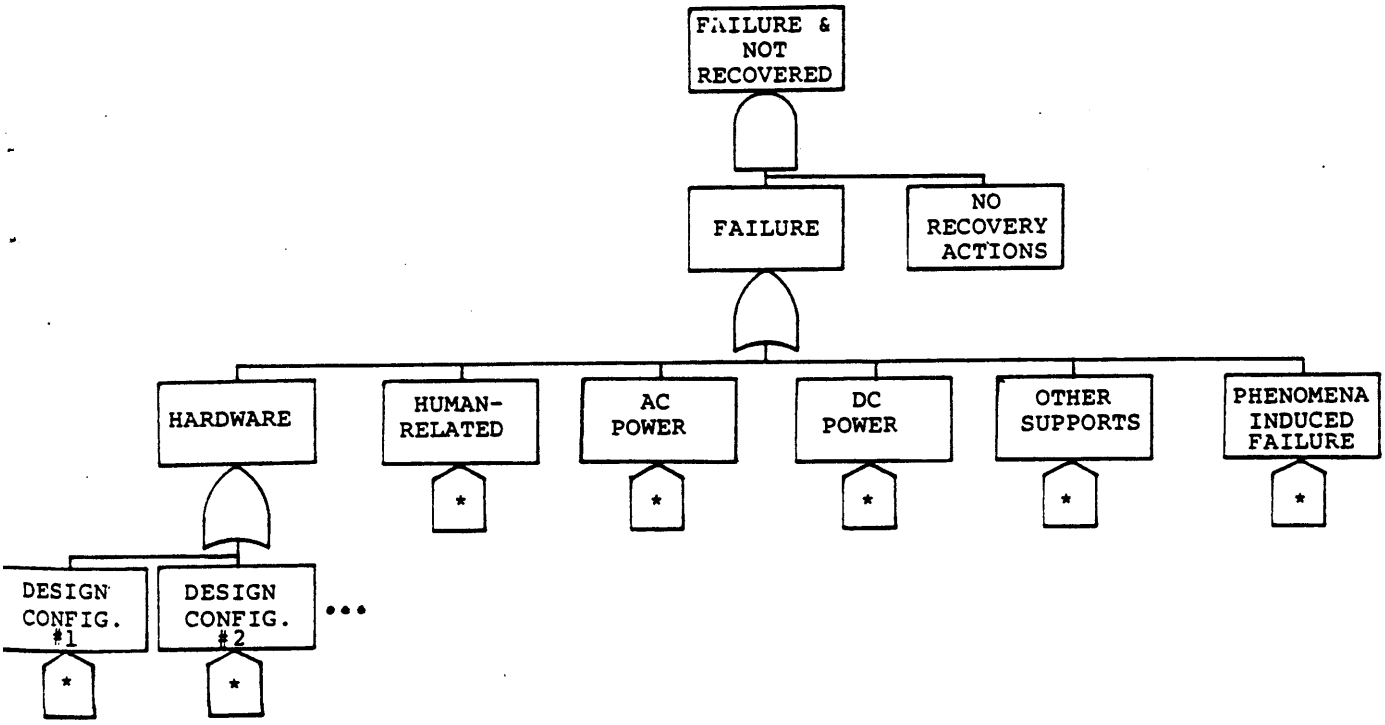


FIGURE 4. TYPICAL FAULT TREE STRUCTURE

OVERALL TOP LOGIC:



FAILURES TYPICALLY DEPICTED AS:



*Turn "on" and "off" to select design variations and to introduce failure modes at specific times following the initiating event.

Table 1

PWR Base Configuration 1*
Station Blackout - Core Damage Sequence Probabilities

(See Figure 5)

Sequences (See Fig. 1)	Point Value	Probability/Reactor Year			
		Mean	5%	50%	95%
TML_1B_1 & $TML_1Q_1B_1$	6.5E-6	3.0E-5	2.5E-6	1.5E-5	9.5E-5
TML_2B_2 & $TML_2Q_2B_2$ (battery depletion)	1.5E-5	5.0E-5	4.0E-6	2.5E-5	1.5E-4
TQ_2B_2	1.0E-5	6.0E-5	2.5E-6	2.0E-5	1.5E-4
TML_2B_2 & $TML_2Q_2B_2$ (CST depletion)	3.5E-6	1.0E-5	2.5E-8**	6.0E-6	3.5E-5
TQ_1B_1, TMB_3	1E-7	were not further evaluated			
Approximate Total	3.5E-5	1.5E-4			

*B&W With 1 Steam Train AFWS, 1 PORV, High Head AC Dependent HPI pumps, 2 AC Divisions)

*If the plant design is such that the operator cannot run the AFWS steam driven pump without electrical power, then this sequence is not possible and its frequency goes to zero while the frequencies of the other sequences increase slightly.

Table 7. Containment Failure Insights

Containment Type	Approximate Time to Containment Failure Following Onset of Core Damage	Most Probable Containment Failure Modes
Ice Condenser	1 hr.	Hydrogen burn, steam spike
	2 hrs.	Overpressure
	At or following AC recovery	Hydrogen burn
Subatmospheric or Small Dry	2 hrs.	Hydrogen burn, steam spike
	6-12 hrs.	Overpressure
	Following AC recovery	Hydrogen burn
Large Dry	10 hrs.	Overpressure
	Following AC recovery	Hydrogen burn
Mark I, Mark II	2-4 hrs.	Electrical penetration failure
	4-8 hrs.	Overpressure
Mark III	10-15 hrs.	Overpressure
	1 hr. following AC recovery	Hydrogen burn

6.0 OBSERVATIONS, INSIGHTS, AND SENSITIVITIES

6.1 GENERAL OBSERVATIONS AND INSIGHTS

From the results of this study and particularly from a review of the dominant sequence cutsets, there are a number of general observations and insights which can be made and which apply uniformly to large groups of plants. These are listed below and pertain to those factors which are important to most, if not all, the accident sequences resulting from station blackout for a particular group of plants.

PWRS

1. Core damage probabilities due to system failures in the 2-12 hour time period following station blackout could be just as great if not greater than core damage probabilities due to early system failures following station blackout. This is due to subsequent important AC/DC dependencies in the AFWS or due to the loss of RCS integrity by reactor coolant pump seal failure in the longer time periods.

2. Offsite power loss, diesel generator unavailability and the nonrecovery of either offsite or onsite power are important to virtually every station blackout core damage sequence. Thus, improvements in the reliability and recovery of both these systems has direct impact on the entire core damage probability from all sequences.

3. The major importance of DC power to station blackout sequences is with regard to how long DC power can be maintained before it is depleted without battery charging or otherwise made unavailable due to prolonged loss of AC effects. Maintaining DC power allows for a system's possible, continued, AC-independent operation, provides needed instrumentation for monitoring plant status, provides necessary lighting in vital plant areas, and plays an important role in defining those periods when diesel generator recovery will become very difficult if not virtually impossible due to the DC dependencies of field flashing, etc. Loss of DC power can also somewhat hinder the ease with which offsite AC power can be restored due to the need for local manual closing of breakers.

4. Based on past judgments as well as current judgments by analysts, containment failure by either H_2 burn or overpressure failure seem rather likely although the large dry containment designs in particular may have a reasonable chance of survivability due to their large volumes and high design pressures. Containment failure may even be induced by AC power recovery in some situations (see Section 5.2).

5. Though not analyzed in detail in these analyses, external events could play a sizable role in inducing station blackout or similar acting scenarios (e.g., loss of vital control power) which could then result in severe core damage. (See Appendix J.)

BWRs (with isolation condensers):

1. Core damage probabilities due to failures in the 2-12 hour period could be greater than core damage probabilities due to early system failures particularly for those plants with no AC-independent system capable of providing primary system makeup. This is highly dependent on the recirculation pump seal LOCA probability.

2 & 3. Same as for PWRs.

4. Overpressure failure appears to be the most likely containment failure mode and may happen rather quickly depending on the electrical penetration seal design. (See Section 5.2.)

5. Same as for PWRs.

BWRs (with HPCI-RCIC systems)

1. Core damage probabilities due to system failures in the 2-12 hour time period appear to dominate the overall core damage probability from station blackout accident sequences. This is due primarily to the fact that two AC-independent systems are available for early success of decay heat removal, but both systems suffer from important AC/DC/ventilation dependencies in the later time periods following station blackout.

2 & 3. Same as for PWRs.

4. Same as for BWRs with isolation condensers.

5. Same as for PWRs.

BWRs (with HPCS-RCIC systems)

1. Core damage probabilities due to late system failures in the 2-12 hour time frame could be just as great if not greater than core damage probabilities due to early failures of the HPCS and RCIC systems.

This is due primarily to the subsequent AC/DC/ventilation dependencies suffered by RCIC coupled with early unavailability of the HPCS system. Overall, however, BWRs with this third redundant train of shutdown heat removal (in the form of HPCS and its dedicated AC/DC/support system configuration) appear to have the least susceptible design of all the "base" plant configurations to station blackout.

2 & 3. Same as for PWRs.

4. Plants of this group with Mark II containment designs will respond in a similar way with regard to containment failures as the previous two BWR plant groups have. BWRs with HPCS-RCIC systems with Mark III containment designs are more susceptible to H_2 burn failure as well as eventual overpressure failure of containment. AC restoration could also induce containment failure. (See Section 5.2.)

5. Same as for PWRs.

All Plants Fitting the "Base" Plant Configurations

With the exception of BWRs with HPCS and RCIC systems, core damage probabilities due to station blackout and caused by internal plant system failures can be summarized in the following way for plants which are like the "base" plant configurations of this study. A "best guess" point estimate in the low 1E-5/reactor year range appears to apply for all the "base" configurations while the mean value is approximately 1E-4/reactor year. External event caused loss of AC accident sequences appear to fall in the 1E-4-1E-6/reactor year range or lower depending on the specific plant's susceptibilities to seismic, fire, wind, and other external event phenomena. These are in comparison to the proposed safety goal figure of 1E-4/reactor year for all core damage sequences caused by both internal and external plant failures. (See Appendix F.)

Not all plants fit the "base" plant configurations of this study. Differences in the number of diesel generators and onsite system power trains, in the AC system success criteria, and in shutdown cooling system designs, can all affect the core damage probability and ultimate risks associated with station blackout. These differences are examined by reviewing the specific accident sequence factors which affect each sequence's importance and by performing simple sensitivity analyses which demonstrate the effects of these differences. These topics are discussed in the following section.