DEVELOPMENT OF A METHODOLOGY FOR ANALYZING PRECURSORS TO SEVERE CORE DAMAGE ACCIDENTS IN NUCLEAR POWER PLANTS

by

Jaime K. Salas

B.S. Mechanical Engineering (1991)

Military Polytechnical Academy, Chile

Submitted to the Department of Nuclear Engineering in Partial Fulfillment of the Requirements for the Degree of Master of Science in Nuclear Engineering

at the

Massachusetts Institute of Technology

January 1997

[February 1997]

Signature of Author ....

Department of Nuclear Engineering
January 15, 1997

Certified by... ....

George Apostolakis
Professor of Nuclear Engineering
Thesis Supervisor

Certified by... ....

Michael Golay
Professor of Nuclear Engineering
Thesis Reader

Accepted by............ ....

Jeffrey Freidberg
Chairman, Department Committee on Graduate Students

DEVELOPMENT OF A METHODOLOGY FOR ANALYZING PRECURSORS TO SEVERE CORE DAMAGE ACCIDENTS IN NUCLEAR POWER PLANTS

by

JAIME K. SALAS

Submitted to the Department of Nuclear Engineering on January 15, 1997 in partial fulfillment of the requirements for the Degree of Master of Science in Nuclear Engineering

Abstract

A methodology is developed for analyzing precursors to severe core damage accidents, consistent with the Accident Sequence Precursor [ASP] program, sponsored by the US Nuclear Regulatory Commission. The results of this thesis are a) an overall step-by-step methodology for analyzing precursors to fire-initiated potential accidents, b) several stylized case-studies demonstrating how the methodology works in practice, and c) recommendations for the development of additional information and models that will enhance the ASP analyst's ability to carry out the methodological guidance given herein.

Thesis Supervisor : George Apostolakis

Title: Professor of Nuclear Engineering

TABLE OF CONTENTS

CHAPTER 4. Methodology for screening and analysis

Chapter 5. Case studies

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

ES.1. Introduction

The NRC Office for the Analysis and Evaluation of Operational Data [AEOD], established shortly after the TMI accident, has been the principal focus at NRC and indeed for the U.S. as a whole for analyzing operating data and operating events to understand their safety significance. One of AEOD's principal vehicles for performing their analysis has been the NRC-supported Accident Sequence Precursor [ASP] project. However, the current ASP methodology does not include precursors to fire-initiated accident sequences, which is a significant gap in its coverage. Filling this gap is the subject of the work reported on this thesis. Specifically, the objective of the thesis is to develop a methodology for analyzing precursors to internal-fire-initiated core damage accidents.

This gap in ASP's coverage is significant in light of the broadly accepted finding from the PRA literature that external events generally, and internal fires specifically, are often major contributors to the overall core-damage frequency and overall offsite risk from nuclear power plants. Obviously, there are numerous "precursor events" at the more-than-a-hundred US operating power reactors in the fire areas, just as there are in other areas such as events initiated by LOCAs and internal-plant transients. However, the analysis of fire precursors to obtain useful insights requires the development of different types of analytical tools and data-collection tools, tools specifically directed toward fire-initiated accident sequences.

The benefits from the present methodology are especially timely now, because in earlier years, many nuclear power plants did not have a plant-specific PRA. Now, however, each plant has (or soon will have) a plant-specific PRA, many of them developed under the Individual Plant Examination [IPE] program. This makes the application of the new methodology simpler and more effective, so that the potential for enhancing the benefits of the ASP insights is likely to be great.

ES-2. Categories of Precursors

The methodology that has been structured, which relies on a PRA-type model, enables the ASP analyst to analyze the following different categories of precursors:

- Precursor fires as initiating events
- Precursor fire-configuration compromises
- Precursor non-fire failures

ES-3. Structure of the Methodology

The methodology includes a pre-screening step, Step 1 (to screen out the unimportant precursor candidates prior to detailed analysis), followed by an intermediate-screening step, Step 2, requiring preliminary analysis, followed if necessary by a detailed-analysis step, Step 3. In this Executive Summary, only the structure of the methodology will be discussed: the details are in the chapters. The three steps are described as follows:

1) Step 1 -- "Screening", whose aim is to sort out (eliminate from further evaluation) an Licensee Event Report [LER] that clearly will not ultimately be designated as a precursor. Other LERs are passed on to Step 2. This step is envisioned as requiring no actual analysis but rather merely a comparison of the information in the LER to certain specific Step-1 criteria. Screening an LER in in Step 1 only implies that one cannot conclude without further evaluation whether or not it is worthy of ultimate designation as an Accident Sequence Precursor.

2) Step 2 -- "Preliminary Analysis", whose aim is to perform enough analysis to decide whether a given LER can be screened out (eliminated) based on comparison with specific Step-2 criteria, or requires additional analysis to ascertain whether or not it is an Accident Sequence Precursor.

3) Step 3 -- "Detailed Analysis", whose aim is to subject a limited fraction of the LERs to detailed analysis if, based on specific Step-2 criteria, it is judged that Step-3 analysis is justified.

The NRC's ASP program, which currently studies only internal-initiated events, only documents Step-3-type precursors.

The conception is that of the LERs that reach the Step-2 preliminary-analysis stage, it is still only expected a modest fraction of them (rather than most or all of them) to be passed to the Step-3 stage. Specifically, of those that survive the Step-1 screening, the Step-2 "preliminary analysis" **(i)** may indicate that no new safety insights are obtainable from the LER; or **(ii)** may reveal those insights; or **(iii)** may indicate that the extensive analysis of Step 3 will be required to probe at a deeper level. In fact, some LERs that get to Step 3 will, upon in-depth analysis, be found not to meet the precursor criteria. This situation is fully acceptable.

ES-4. Considerations in Developing the Screening Criteria

1) Conservative

During the Step-1 screening, LERs will be retained unless they can be affirmatively screened out, not the other way around. This is consistent with current ASP practice for internal faults.

2) Equivalence

The methodology has been developed considering as a basic guideline to be roughly equivalent to the internal-faults ASP screening criteria where feasible. This criterion uses the conditional core damage probability of 1.0×10^{-6} , given the precursor, as a screening level.

3) Ease of discrimination

The Step-1 screening criteria enables the analyst to discriminate easily between those LERs that are obviously not of much ASP interest and the others.

4) Rigor

The screening criteria cannot be rigorous and should not pretend to be. The methodology has been established so that considerable analyst judgment must be involved. In fact, it is envisioned that no workable screening criterion can avoid such analyst judgment in the fire area.

ES-5. Additional Information

The chapters also contain the following important sections:

- A multi-sheet block-diagram flow sheet for each of the individual methodologies to guide the analyst/user.
- Several stylized case studies, derived from actual LERs, that illustrate how the methodological steps work in actual practice.
- From the study of the cases, recommendations for information and tasks to be performed to implement the various methodological steps effectively. Specifically:

  a) The documentation that the analyst requires to perform his job.

  b) The required effort that should be carried out to evaluate the consistency between the methodologies applied for fire risk analysis.

  c) A list of future tasks that, under the judgment of the author, should be performed in the near future.

ACKNOWLEDGMENTS

The present thesis was sponsored by the US Nuclear Regulatory Commission [NRC] through contract with Future Resources Associates [FRA, Inc.] and Advanced System Concepts Associates [ASCA, Inc.].

My very special thanks go to Professor George Apostolakis, for his permanent support, guidance and advice all through this research effort. With his always friendly and supportive attitude, Professor Apostolakis transformed my job in a great experience.

I would also like to thank Dr. Robert Budnitz, from FRA, Inc. and Dr. Jya Syin Wu, from ASCA, Inc., for their permanent support, comments and suggestions. Working with them as a team was a valuable experience.

A special thanks go to BGL Luis Iracabal L., President of the Military Polytechnical Engineering Committee of the Chilean Army. Without his support and decisive effort, my specialization at MIT would not have been possible.

A special mention and deepest thanks go to CRL Claudio Rubio B. His participation on the efforts made to allow me attend MIT was crucial.

My thanks go also to all those people who had different levels of responsibility on my attendance to MIT. My special thanks to CRL Julio Baeza B., CRL Jorge Nunez M., TCL Renato Canales R., CC Julio Vergara A and MAY Walter Araya M.

Finally, I would like to dedicate this thesis to my spouse, Nita, and to our two children, Jaimito and Javierita. They always supported me with love and patience.

Chapter 1. Introduction

1.1. Background.

Nuclear power plant risk assessments have established that health risk is dominated by accidents involving severe core damage as well as early containment failure. However, in order for that event to occur, it would be required an initiating event of the protective safety features designed first to prevent severe core damage and second to mitigate consequences for the environment. In order to predict the corresponding event scenarios, Probabilistic Risk Assessment [PRA] is a well established and powerful tool.

PRA is a standard method used for assessing, maintaining, assuring and improving the nuclear power plant safety. This holds for all phases of the nuclear power plant life cycle: from design, start up and various modes of nuclear power plant operation, although it is primarily used for the normal operation.

A PRA can be characterized, in this context, as a fully systematic tool for identification and quantification of possible accident scenarios modeled on the basis of the design and operating characteristics of the facility and on data gained from the past experience at similar technical installations.

Probabilistic approaches analyze the plant design utilizing statistical data on plant, component and human performance to determine which accident scenarios are most likely to result in a significant threat to plant safety, regardless of the apparent levels of redundancy and diversity provided. Probabilistic methods have resulted in a number of regulatory additions since the original deterministic framework was established.

One of the possibilities for supporting PRAs by operational experience is the use of precursor studies. Such studies are based on the precursors reported in reactor operation and use probabilistic methods for the prediction of the safety-related importance of these precursors. An accident sequence precursor is an observed event, identified as either an operational event or a configuration change at a nuclear power reactor that represents a significant potential to develop into a severe accident, had other failures occurred that in fact did not occur. As a matter of fact, the notion of a precursor is that no actual severe core damage accident has actually occurred.

The precursor methodology is based to the highest extent possible degree on event combinations observed in operational experience. The precursor methodology has a particular strength in that it can use data on combinations of events instead of the single basic event normally used in a PRA. Thus, while a PRA synthesizes the frequency of event combinations from the frequencies of the different initiating events and the failure probabilities of individual components, a precursor study can directly take combinations of events into account, as far as observed, without making assumptions on the synthesis process. Precursor studies are also a powerful tools to obtain a deeper understanding of the safety-related importance of the precursors collected in abnormal occurrence reporting systems or to optimize these systems using such insights. Events which rarely happen and have not been observed so far, naturally can not be verified using the precursor methodology.

1.2. Identification of the problem.

The NRC office for the Analysis and Evaluation of Operational Data [AEOD], established in 1979 shortly after the Three Mile Island accident, has been the principal focus at NRC and indeed for the U.S. as a whole for analyzing operational data and operating events at nuclear power plants to understand their safety significance. One of AEOD's principal vehicles for performing their analyses has been the Accident Sequence Precursor [ASP] Program [Minarick, 1990; NRC, 1994a]. The ASP program that NRC has supported for the past decade and a half has been one of the major beneficial applications of PRA methods.

The fundamental objective of the program is the development of information related to risk from operational events. The process of identification of accident sequence precursors within the database of operational events involves several steps aimed at the efficient identification of precursors from the large number which must be reported to the US NRC, through the Licensee Event Reports.

The IPE [NRC, 1988] and the Individual Plant Examination for External Events [IPEEE] [NRC, 1991] efforts over the past years at all U.S. nuclear power plants have resulted in PRA-type internal-initiator analyses for each operating plant, and in similar evaluations for the external initiators.

In January 1992 NRC sponsored a workshop in Annapolis entitled "NRC workshop on the use of PRA methodology for the analysis of reactor events and operational data" [NRC, 1992]. At that workshop, one recommendation was that the ASP program should be extended to cover precursors to external events, among them those to internal fire-initiated-events, which are not presently covered within ASP's scope.

The fact that internal fires are currently out of the scope of the ASP program is a significant gap on its coverage. Filling this gap is the objective of this thesis.

1.3. Objective of the thesis.

The objective of the thesis is to develop a methodology for analyzing precursors to internal fire-initiated accidents at commercial nuclear power plants and thus incorporate fires as external events to the Accident Sequence Precursor Program.

1.4. Significance of the problem.

The gap in ASP's coverage is significant in light of the broadly accepted finding from the PRA literature that external initiating events, in general, and internal fires, specifically, are often major contributors to the overall core damage frequency and overall offsite risk from nuclear power plants. Obviously, there must be numerous "precursor events" at the U.S's more than a hundred operating power reactors in the fire areas, just as there are in other areas such as events initiated by pipe breaks, power interruptions, operator errors and various other internal plant transients. However, the analysis of fires as precursors to potential core damage accidents requires the development of data collection tools and analytical tools that are specifically directed to fire-initiated accident sequences.

1.5. Benefits from the implementation of the methodology.

With the improvement to the ASP methodology that will result from incorporating internal fires, several different types of insights will become available. The major insights will be:

1) *Insights about initiating events*

There are numerous precursor fires annually at commercial nuclear power plants. Some of these fires have potential safety significance as precursors, but most of them do not. Identifying whether any potentially important fires occur with greater frequency or greater potential severity than anticipated by current PRAs will be a major benefit.

2) *Insights about important components and systems*

Although the types of components and systems that contribute to the potential fire accident sequence may be available from the PRAs and IPEEE analyses, it is possible that an examination of which components and systems show increased precursor failures or participate in unusual operational events may reveal insights not yet appreciated. Precursor analyses can identify, if any, important contributors that have not yet been identified in the existing PRAs and IPEEE analyses.

3) *Insights about human errors*

The importance of human errors have been recognized since the first PRA studies such as WASH 1400 [WASH, 1975]. Much effort has been devoted over the years to quantifying human error rates for different category of errors, different sequence types, and so on. From the PRAs, we know that human errors are one important aspect of fire-initiated sequences. Insights into possible human errors in precursor situations will be important.

4) *Insights about common cause failures*

Common cause failures are a feature of all PRA analyses generally, but based on the PRAs they are of event greater importance in fire initiated sequences. Discovering whether precursors of this type exist will be very important. Certain types of common-cause failures, especially involving support systems [AC, DC, instrument air, HVAC, etc.] turn out to be important in the external event PRAs and should be the focus of particular attention in precursor studies.

5) *Insights about regulatory requirements*

It is broadly recognized that the body of NRC regulations, developed before risk-based information was available, can benefits from perspectives of PRA. The broad examination of plat-specific fire precursor information may reveal trends in certain safety areas that can best be addressed by modifying the regulations, regulatory guides or other NRC positions.

6) *Insights about new research topics*

Research, broadly defined, means "developing" new knowledge. Insights from studying the precursors to fire-initiated accident sequences may suggest new research topics or alter the relative emphasis among existing research areas.

CHAPTER 2. Background

2.1. Introduction

This chapter presents the current ASP program developed for internal events. The objectives of the program and the basic methodology are shown, with emphasis in the quantification process and the criteria of report of operational events as precursors. A background about the methodology for analysis and evaluation of risk from fires in nuclear power plants, using the systematic tools provided by Probabilistic Risk Assessment [PRA] techniques is given. It is also presented what is called the fire protection system, group of engineered systems and procedures, designed to prevent and/or fight the effects of internal fires. Finally, the basic methodologies that nuclear power plants have applied for complying with the IPEEE requirement is detailed briefly.

2.2. The current ASP program

2.2.1. Introduction

The methodology developed and used for the ASP program is intended to produce a reasonable estimate of the safety significance of operational events at nuclear power plants, including observed human and system interactions. The collection of operational events from a unique database of historical system failures, multiple losses of redundancy, and infrequent core damage initiators. These events are useful in identifying significant weaknesses in design and operation. Thus, the primary focus of the ASP program is the development of risk-related information from events reported in the LERs.

The ASP methodology from the U.S. has had influence on the development of similar programs in other countries. One significant example, as described by Hoertner et al. [Hoertner, Kafka and Reichart, 1990] is provided for the German Precursor Study [GPS], whose objectives can be summarized as follows:

- To gain a deeper understanding of the safety-related importance of the event scenarios, reported during the operation of the plant.
- To identify and evaluate possible weak points
- To compare the results with those from a previous phase, called the German Risk Study.

The ASP methodology was plant-specifically applied, using the nuclear power plant Biblis, with the two units A and B as the reference plants. The verification of probabilistic results from PSAs, making use of the plant-specific experience with system trains was among the most significant results from the application of the program. One of the main advantages was the evidence of the importance of potential system failures and potential multiple failures, from a plant-specific point of view. Moreover, an annual trend for the frequency of potential severe core damage was verified, along with the identification of weak points in the systems and the impact of erroneous manual actions, mainly in the frequencies of initiating events.

The application of system-analytic tools and especially probabilistic methods on the evaluations of the event reports and other records of operational experience contributed to:

- A deeper understanding of the safety-related importance of the events reported in reactor operations
- The importance ranking of the different safety features
- The expansion of the scope and content of the abnormal occurrences reporting systems

2.2.2. Objectives of the ASP program

The following quotation from the NRC's 1994 "ASP Program Plan" [ASP Plan, 1994] provides a good overview of the current ASP Program objectives:

- "Identify and rank risk significance of operational events: Historically, this was the purpose of the ASP Program and it remains the primary objective."
- "Determine generic implications of an operational event/characterize risk insights: ASP events provide insight into potential problems at other plants and bring to light generic issues. This can be done by analyzing the trends and patterns of the ASP events as a whole, and it can be done on an event-by-event basis. Most importantly, any risk insights need to be fed back to nuclear power plants and to the nuclear industry.
- "Provide supplemental information on plant specific performance: ASP data is often used along with other performance data to report on plants at the Senior Management Meeting and in various agency studies. Distribution of event analyses to a wider audience and conducting ASP seminars with the staff will increase the understanding and usage of ASP."
- "Provide a check on PRAs: ASP data and insights should be compared with expectations based on PRAs and IPEs. This will gauge some of the uncertainties and will help identify some modeling errors or areas with important completeness problems."
- "Provide an empirical indication of industry risk and associated trends: ASP can be used as one input into trending of industry risk implications of operating reactor experience. The degree to which ASP can be used to support this objective is limited because of the limited models and data."

2.2.3. ASP methodology approach

The following discussion, adapted from NRC's annual ASP compilation [NRC, 1994a], is a good introduction to the methodology:

Two types of events are analyzed in the current ASP program. The first type is a precursor that includes an initiating event, such as a small-break loss-of-coolant accident [LOCA] or a loss of offsite power [LOOP]. The second type is a precursor that involves a failure condition over a period of time during which an initiating event could (but, in fact, did not) occur. The first type is referred to as an Initiating Event Assessment and the second one as a Condition Assessment.

The current ASP methodology for analyzing operational events is developed in two steps. The first step, the screening process, is performed in order to select the events that appear to deserve a detailed review and to eliminate those events that are clearly unimportant. In the second step, those events retained in the first step are subjected to a detailed analysis, which is intended to identify those considered to be precursors to potential severe core damage accidents.

2.2.4. Quantification process

The following quotation from the NRC's 1994 "ASP Program Plan" [ASP Plan, 1994] provides a good overview of the current ASP Program quantification process:

"The effect of a precursor on accident sequences is assessed by reviewing the operational event specifics against system design information. The quantification of an accident precursor significance involves determination of a conditional probability of subsequent severe core damage [CCDP], given the failures observed during an operational event. This is estimated by mapping observed failures observed during the event onto the ASP accident sequence models, which depict potential paths to severe core damage and calculating a conditional probability of core damage through the use of event trees and linked fault trees modified to reflect the event."

"The conditional probability estimated for each precursor is useful in ranking because it provides an estimate of the measure of protection against core damage that remains once the observed failures have occurred. An incremental risk has to be considered, in order to evaluate the effective significance and so permit comparison among different events."

2.2.5.Criteria utilized in the screening process

The NRC ASP compilation [NRC, 1994a] states as follows: "Events are identified for further consideration if they include:

- All CD initiators (LOOP, LOCA, steam pipe breaks {in PWR})
- All events where a trip was demanded
- All failures in support systems (cooling water systems, instrument air, instrumentation and control, electric power systems).
- All events where two or more failures occur
- Any event or operating condition different from that expected according to design
- Any other that, according to reviewer's experience, could have resulted in or significantly affected a sequence of events leading to potential severe core damage".

"Events are eliminated from further consideration as precursors if they involved, at most, only one of the following:

- A component failure with no loss of redundancy,
- A loss of redundancy in only one system,
- A seismic design or qualification error,
- An environmental design or qualification error,
- A structural degradation,
- An event that occurred prior to initial criticality,
- An event impact bounded by a reactor trip or LOFW,
- An event with no appreciable impact on safety systems, or
- An event involving only post-core damage impacts."

Note that among the items in this long list that are "eliminated from further consideration as precursors" are configuration problems that might lead to vulnerabilities in large earthquakes and fires. It is precisely those potential safety concerns that are the subject of this thesis.

2.2.6. Event sequences requiring calculation

The NRC ASP compilation [NRC, 1994a] provides the following guidance to the ASP analyst:

"If an initiating event occurs as part of a precursor (i.e., the precursor consists of an initiating event plus possible additional failures), then use the accident sequence model associated with the initiator; otherwise, use all accident sequence models impacted by the observed unavailability".

"Initiating event probability: If an initiating event occurs as part of a precursor, then the initiating event probability used in the calculation is 1.0. If an initiating event does not occur as part of the precursor, then the probability used for the initiating event is developed assuming a constant hazard rate. Event durations (the period of time which the failure existed) are based on information included in the event report, if provided. If the event is discovered during testing, then one-half of the test period is typically assumed, unless a specific failure duration is identified."

"Component failure probability estimation: For components that are observed failed during the precursor, the associated basic event is set to "true". Associated common-cause basic events are revised to reflect the type of failure that has occurred. For components that are observed to operate successfully, or are not challenged during the event, a failure probability equal to the nominal component failure probability is utilized."

"Non-recovery probability: If an initiating event or a total system failure occurred as part of the precursor, the basic event representing the probability of not recovering from the failure is revised to reflect the potential for recovery of the specific failures observed during the event. For condition assessments, the probability of non-recovery is estimated under the assumption that the initiating event has occurred."

"Failures in support systems: If the support system is not included in the ASP model, the impact of the failure is addressed by setting impacted components to failed. The modeling of a support system recognizes that as long as the failure remains unrecovered, all impacted components are unavailable, but if the support system failure is recovered, all impacted components are also recovered. This can be modeled through multiple calculations which address the impact of failure and success of the failed component. Calculated core damage probabilities for associated cut sets for each case are normalized based on the likelihood of not recovering the support system failure."

2.2.7. ASP criteria for documenting an event as a precursor.

The criteria for when the ASP analysis leads to actually reporting of certain events as "Accident Sequence Precursors" are discussed as follows [NRC, 1994a]:

"Events were selected and documented as precursors to potential severe core damage accidents (accident sequence precursors) if the conditional probability of subsequent core damage was at least 1.0×10^{-6}. Events of low significance are thus excluded, allowing attention to be focused on the more important events."

"Other events that provided insights into unusual failure modes with the potential to compromise continued core cooling but were determined not to be precursors were also identified. These are documented as 'interesting events."

Note that if the Conditional Core Damage Probability [CCDP] corresponding to the operational event does not exceed the screening value of 1.0×10^{-6} established for use in the ASP program, then the LER is screened out.

2.3. PRA background and tools.

A PRA is performed by systematically considering the likelihood of all possible scenarios for accidents of a system in operation. By doing that PRA could reveal any faults on design, as well as the possibility of common cause or mode failures or adverse system interactions in the nuclear power plant.

PRA identifies and delineates the combinations of events that could lead to an accident. It also estimates the frequency of occurrence for each combination and then the consequences. For doing that, it integrates into a uniform methodology the relevant information concerning the plant design and construction, operation, operating practices, operating maintenance, component reliability, human reliability and the physical progression of core-melt accidents, then the potential environmental and health effects in a realistic manner. PRA makes use of both logic models and physical models. Logic models represent the combinations of events that could result in a core-damage accident, and in conjunction with physical reliability data, logic models can also be used to determine the frequencies associated with each combination. Physical models represent the progression of the resulting accidents and damage.

The analysis performed by a PRA involves developing a set of possible accident sequences and then estimating their outcomes. Several sets of models are developed, according to the scope and objectives of the study. Among them there are models related to plant systems, to the response of the containment and to off-site consequences.

Plant-system models generally consist of event trees, which depict initiating events and combinations of systems failures and successes, and fault trees, which depict the ways in which the system failures represented as top events of the event trees can occur. This event tree-fault tree [ET/FT] methodology is widely used in technological system applications. It is useful because it focuses on a key characteristics of many such systems: accident scenarios typically involve a chain of failure events involving hardware, human action and software. Interruption of the chain at any point can reduce the consequences of the accident or even prevent it from occurring at all.

The ET/FT approach employs discrete logic diagrams (generally based on success/failure modeling) to explicitly show the causal and correlation between model elements and to determine the probability of different accident scenarios. These models are analyzed and evaluated by making use of existing reliability data of systems and components to estimate the frequency of each accident sequence. The failure probability for most safety systems is usually estimated using fault trees and failure probabilities for the individual system components. This is necessary because there is very little directly measured data for the entire system: There are few demands and very few failures.

In the quantification process, damage probabilities of components and structures are evaluated at first and minimal cut sets for accident are generated. In order to quantify accident sequences, a minimal cut set upperbound approximation is used [NRC, 1995]:

$$\mathbf{P_k = 1-\Pi[1-P_i]} \qquad [2.1]$$

where:

$\mathbf{P_k}$: Occurrence probability of accident sequence k

$\mathbf{P_i}$: Probability of i-th minimal cut set for k-th accident sequence.

An event tree for a loss of coolant accident and a fault tree for the High Pressure Coolant Injection [HPCI] system are shown in Figures 2.3.1 and 2.3.2, respectively [NRC, 1994a].

2.4. Fire Protection systems in nuclear power plants [NPP]

Because fires can damage front-line systems together with support systems (AC, DC, instrument air, HVAC, etc.), their potential to cause sequences dominated by common-cause failures is greater than for sequences initiated by internal plant faults. The main concern and point of interest in fire analysis is the effect of fire on structures, systems, cables (power, instrumentation and control), equipment and components that are designed to achieve and maintain sub-critical conditions in the reactor, maintain reactor coolant inventory and maintain safe and stable shutdown conditions following a fire initiated event. Passive components, such as pipes, tanks, heat exchangers and manual valves are usually excluded from the analysis, except that they are known to be affected by an environment related to a fire. As a result, the analysis usually involves electrical components such as power control and instrumentation cables.

There are many types of extinguishing systems installed in nuclear power plants. They are collectively referred as the Fire Protection System [FPS]. The term refers to the integrated complex of components and equipment provided for detection and suppression of fires. In addition to this system, the "fire protection program" includes the concepts of design and layout implemented to prevent or mitigate fires, administrative controls and procedures, and personnel training. The fire protection program uses a defense-in-depth approach aimed at preventing fires, minimizing the effect of any fires that occur, providing appropriate fire detection and suppression equipment, and training personnel in fire prevention and fire fighting.

The defenses interact on four levels to protect nuclear power plants against the impact from fires:

1) Keeping low the amount of combustible material in areas having vital safety equipment or its cabling, as well as using fire resistant insulation material for electrical equipment.

2) Providing equipment for fire detection and fire fighting, both manual and automatic, that prevents small fires from propagating to large, safety-related fires.

3) Protecting vital cabling and safety equipment by a suitable physical distribution, involving separation of redundancies and by fire resistant barriers. The purpose of the separation is to prevent fire damage to multiple safety system trains and to preserve the availability of the redundancies needed for safe shutdown following fire induced events.

4) Providing backup to safety equipment that has been disabled by fire events and establishing management procedures to preserve the retention capability of the containment.

2.5. Fire risk analysis methodologies used in NPP.

NRC issued Generic Letter 88-20 [NRC, 1988] in November of 1988, on Individual Plant Examination [IPE] to address severe accident risk because of internal events, including internal floods. In June of 1991, Supplement 4 to Generic Letter 88-20 [NRC, 1991] was issued requesting each licensee to perform an Individual Plant Examination of External Events [IPEEE] to address not only for internal events but also for external events: seismic activity, high winds and tornadoes, external floods and internal fires.

In response to that letter, three types of methodologies used for fire IPEEEs were: FIVE [EPRI, 1993] standard fire PRA [NRC, 1983] and an aggregate of FIVE and PRA. The majority of licensees have taken some advantage of various features of the FIVE methodology.

The FIVE methodology was developed by EPRI to address the fire portion of the IPEEE, as an alternative to the fire PRA. It is directed at implementation by plant personnel experienced with overall plant operation, fire hazards and protection features, as opposed to being conducted by the PRA analyst. The methodology provides plant personnel with walkdown guidelines to identify potential fire-related vulnerabilities for plant equipment, cabling and components necessary to achieve safe shutdown.

The following sections describe briefly the most important characteristics of the methodologies in use.

2.5.1. Standard fire PRA

The traditional fire PRA is done in two phases. The first screening phase identifies fire locations that could be potentially significant to the risk of the plant. It culminates in a conservative assessment of the frequency of potential fire-induced accident scenarios in each area of the plant. The second or detailed phase provides a more realistic assessment of the plant damage frequency associated with the fire scenarios that are not screened out, and is achieved by relaxing some assumptions of the first. The risk from fires in a nuclear power plant, according to this method, is analyzed in four steps [Apostolakis, 1993; Kazarians, Siu and Apostolakis, 1985]:

1) Identification of "important" fire scenarios.
2) Assessment of the frequency of fires.
3) Assessment of the fraction of fires that damage critical components of fires.
4) Assessment of the frequency of plant damage states, given fire and damaged components.

Based on these steps, the frequency, $\Phi_{y,j}$, of the plant damage state **y** (e.g. Core damage) due to fire scenario **j** in room **z** can be written as

$$\Phi_{y,j}=\lambda_z * f_{G,j} * f_{S,j} * f_{ns} * Q_{y,j} \qquad [2.2]$$

where:

λ_z	:	Annual frequency of fires in room **z**.
$f_{G,j}$	:	Fraction of those fires in room **z** that are initiated in a specified area within the room, which is defined by fire scenario **j** [geometric factor].
$f_{S,j}$	:	Fraction of those fires that are initiated in the area defined by fire scenario **j** that have an initial severity great enough to potentially damage the critical components in scenario **j** [severity factor].

$\mathbf{f}_{ns,j}$: Fraction of scenario-**j** fires that are not suppressed before component damage [non-suppression factor].

$\mathbf{Q}_{y,j}$: Conditional frequency of reaching damage state **y** due to failure of equipment exposed to a fire. The frequency of failure is a combination of random cause and fire-induced causes. The frequency of reaching damage state **y** also includes possible recovery of equipment.

The factors in the equation [2.2] account for the possibility that a number of physically distinct fires within one room may cause component damages. Some fires may be relatively close to the critical component and of a relatively small size, while other fires may be much farther away and much more severe. Some fires start in cabinets, some in cable trays and some in other locations due to the ignition of flammable materials. Therefore, these factors are modifying the initiating fire frequency, referring specifically to a location. The product of the fractions, $\mathbf{f}_{G,j}$ and $\mathbf{f}_{S,j}$, in above equation, quantifies the relative likelihood of representative scenario **j**, given a fire in room **z**. COMPBRN-IIIe fire code calculates the fire growth time [or damage time] from a deterministic reference model and an uncertainty factor which are related directly to obtain the $\mathbf{f}_{ns,j}$ value.

The risk due to fires in nuclear power plants, similar to the risk from other potential accident initiators, is highly dependent upon the detailed configuration of each plant. The exact routing of power and control cables, the location of barriers and fire protection systems and the equipment available to mitigate the losses caused by a serious fire all help determine the magnitude of the risk.

The model described employs parameters such as the frequency of fire occurrence in a given room, and the frequency of successful suppression system actuation. Each of the parameters in a fire risk model must be quantified for the model to be of use. Because serious fires in nuclear power plants are not frequent events, the statistical evidence from those fires that have occurred is relatively weak. Therefore, in order to estimate many of the parameters, we must supplement the occurrence data with other types of information. Estimation means, here, developing probability distributions for the parameters.

It is important to note that as more factors for a fire scenario are considered, less data are available for the specific fire-class of interest and our uncertainty in the frequency increases. Thus, while the frequency of fires anywhere in the plant is known fairly well, the frequency of fires in other zones may be known to a lesser degree. That will be reflected in the spread of the distribution for some of the factors. The definition of the number of fires in the plant can be taken from historic data from the plant or, if adequate, from generic industry data.

The Geometric factor and Severity factor

The first two factors, the geometric factor and the severity factor, take into account the frequency of fires in a specific location. It can be seen that these factors represent increasing levels of detail and that assigning a value to unity to any of the fractions is conservative. These two factors tend to specialize the information so that a specific frequency can be determined for the specific scenario.

These factors are usually be assessed using expert judgment, since they are highly situation-specific and statistical evidence does not exist. While the use of judgment may give very different results for particular situations, it is true that the use of formal methods can improve the process to a significant degree. Some guidelines for helping the application of judgment can be summarized as:

- The number of rooms that the building of a particular class have
- The contents of the room
- The frequency of visits of personnel to the room.
- The nearness of specific items, such as cable trays, to ignition sources or propagation paths inside the room.

The non-suppression factor

The probability of component damage during the occurrence of a fire scenario in a nuclear power plant is a primary factor in defining the contribution of that scenario to the total fire risk. This probability is largely dependent on the hazard time $\mathbf{T_h}$, the time the component is exposed to the fire hazard.

$\mathbf{T_h}$ can be defined as the sum of the time to detect the fire, $\mathbf{T_D}$, and the time to suppress the fire, $\mathbf{T_S}$, once it has been detected. Both $\mathbf{T_D}$ and $\mathbf{T_S}$ are random variables whose distributions depend on the type of fire protection equipment (if any) installed in the room. Since both detection and fire fighting stages of the suppression process can include a number of different modes of action, a diversity of fire suppression scenarios can be anticipated for a fire in any given location. Thus, to construct the distribution of $\mathbf{T_h}$ it is required to analyze both the fire detection process and the fire suppression process in greater detail and then evaluate that time in relation to the time to growth.

Eventually, $\mathbf{f_{ns}}$, the non suppression factor, will be a function of the hazard time, $\mathbf{T_h}$, the growth time, $\mathbf{T_G}$, and the equipment available in the location. The growth time, determined for the specific conditions of the scenario by using a fire model, such as COMPBRN IIIe, is defined in the absence of suppression efforts. The fire growth calculations help define which pilot fires have the potential to initiate the critical fire scenario.

A model and the analytical description for the non suppression factor is presented by Siu and Apostolakis [Siu and Apostolakis, 1985]. According to that, the non suppression factor corresponds to the fraction of fires causing damage to the critical components before the fire is suppressed, therefore given by:

$$\mathbf{f_{ns} = F_r(T_G < T_h)} \qquad [2.3]$$

and the analytical model for the competition between growth and suppression is given by:

$$\mathbf{f_{ns} = exp\ (-T_G/\xi_c)^{\gamma c}} \qquad [2.4]$$

where ξ_c and γ_c are functions of the hazard time and the equipment available in the location for fire protection, including detection and suppression means.

Detection time. [Siu and Apostolakis, 1986]

A fire in a nuclear power plant can be detected by a number of means. If the fire is not initiated by human action, or it is initiated by human action but not detected immediately, it may be detected by three modes:

- Automatic, by detectors located in the scenario of the fire, at time $\mathbf{T_{D1}}$
- Local, by personnel who happen to come upon the fire, at time $\mathbf{T_{D2}}$
- Remote, via indications of abnormal instrument or control behavior, at time $\mathbf{T_{D3}}$

The delayed detection of a fire can be modeled as the result of a process of competition between the three detection modes. If $\mathbf{T_D}$ is the time to detection, then

$$\mathbf{T_D = min\ (T_{D1}, T_{D2}, T_{D3})} \qquad [2.5]$$

Of course, if there are no detectors in the area, then $\mathbf{T_D}$ is the minimum between $\mathbf{T_{D2}}$ and $\mathbf{T_{D3}}$. Both $\mathbf{T_D}$ and $\mathbf{T_{di}}$ are random variables, for they depend on such random process as the behavior of the fire, the arrival of personnel in the affected area and the specific room characteristics at the time of the fire.

The methodology proposed for the detection time of fires in nuclear power plants differentiates between these competing modes of detection and between different initial fire severities. The methodology makes use of data or evidence, **E**, from different sources, as indicated below. In this model, the $\mathbf{T_D}$ is assumed as having an exponential distribution, with parameter λ_D, according to:

$$\mathbf{f(t) = \lambda_D \exp(-\lambda_D t)} \qquad [2.6]$$

Where $\lambda_d = \lambda_1 + \lambda_2 + \lambda_3$

The assumptions for the model can be summarized as follows:

- The modal detection times, $\mathbf{T_{Di}}$, are conditionally independent exponential random variables with means $(1/\lambda_i)$
- The three detection means are competing
- The data consist of the mode of detection for each event as well as actual detection times, or probability distributions for the detection times.

Thus, the parameter λ_d must be determined in order to evaluate the time to detection. λ_d is, of course, a random variable and its distribution was modeled by using the Bayes' theorem, according to:

$$\pi_1(\lambda / E) = \frac{\mathbf{L(E/\lambda)\,\pi_o(\lambda)}}{\int \mathbf{L(E/\lambda)\,\pi_o(\lambda)d\lambda}} \qquad [2.7]$$

The prior distribution for λ, $\pi_o(\lambda)$ quantifies the state of knowledge prior to the evidence **E**, while the posterior distribution $\pi_1(\lambda$ **/E**) quantifies our state of knowledge upon acquisition of **E**. The likelihood function **L(E/** λ) is the conditional probability of observing **E**, given λ.

The evidence, in the form of detection times, may consist on several data sets. On the model of the reference, three separate sets of data were used: nuclear power experience (E1), EPRI database (E2) and a supplemental source of information, as the fire hazard report of the plant of interest (E3).

The Bayesian approach, which arises naturally from the subjective notion of probability, will allow the analyst to maximize his use of available information. However, to aid the analyst properly, sensitivity analyses will be usually applied. An adequate use of the information, combined with the proper use of expert judgment would decrease the spread of the distribution for the uncertain parameters to be used in detection, when applying the Bayes' theorem. By using a combination of quantitative and qualitative information from industry experience, it is possible to derive joint probability distributions for the detection rates, which includes the effect of that industry experience on the understanding of the detection rates of actual fires.

Some of the important characteristics that may affect the automatic detection time are: the fire magnitude at the time of detection, the fire growth rate, the distance from the fire to the detectors and the resistance of the room air mass to changes in composition. On the other hand, the local detection time is affected primarily by the volume of the traffic passing through the given room, while the remote detection time is dependent on the fire severity, growth rate, and location and on the room contents.

Suppression.

Basically, the suppression modes can be classified into two groups: human suppression, usually by the fire brigade and automatic suppression, usually by sprinkler-based systems located in the susceptible locations.

In the case of the automatic systems, three related aspects are typically important:

1. Failure to actuate on demand
2. Capability of the automatic system to put out the fire
3. Put out the fire before significant damage

It is reasonable to expect that the suppression time distribution will be dominated by the unavailability of the automatic suppression system. However, it has to be noticed that the other factors, activated when the system has not failed on demand, are also important and they must be considered. In this context, aspects of growth time and characteristics of the propagation process will be very significant.

A methodology [Siu and Apostolakis, 1988] was developed for determining the probability distribution of the demand unavailability of sprinkler-based suppression systems. The methodology incorporates the expert judgment in the treatment of numerical data and partially relevant information.

The distribution for the unavailability of the sprinkler-based system on demand, ψ, was derived directly from the Bayes' theorem, according to:

$$\pi_1(\psi / \mathbf{E}) = \frac{\mathbf{L}(\mathbf{E}/\psi)\,\pi_o(\psi)}{\int \mathbf{L}(\mathbf{E}/\psi)\,\pi_o(\psi)\,d\psi} \qquad [2.8]$$

Where $\pi_0(\psi)$ is the prior distribution for ψ, and $\pi_1(\psi/\mathbf{E})$ the posterior distribution, quantifying the state of knowledge upon acquisition of **E**, as defined earlier in this chapter.

Data for suppression system successes and failures under conditions typical of nuclear power plants exist. However, the total number of these events is so small that any estimates derived from these data alone will have large uncertainties. Perhaps more importantly, these estimates will not include the rather substantial amount of evidence available from tests and from other industrial applications of the fire protection systems in question.

The data available for the analysis of sprinkler system demand unavailability can be usually grouped into three categories:

- Data from actual nuclear plant experience (E1)
- Data from tests of systems similar to those used in nuclear plants (E2)
- Relevant data from other industrial activities (E3)

The test and non-nuclear data may not be exactly equivalent to the nuclear operating data but are relevant at least to a degree, and should be accounted for in some manner.

Thus, the indirect evidence from tests and non-nuclear applications is incorporated using an expert opinion likelihood model and applied in the use of the Bayes' theorem.

It should be pointed that the distribution for ψ quantifies the probability that the suppression systems will fail upon demand. However, the success on demand for the automatic systems is not a sufficient condition to eliminate the effects of the fire, for two factors must also be considered. The fact that even with success on demand, it is necessary to put out the fire, and, that it is required to put out the fire before significant damage has been reached.

2.4.2. FIVE Methodology

The FIVE methodology is a screening technique based on conservative assumptions using historical experience and plant specific data for evaluating fire event sequences. The methodology considers all plant areas and focuses on the availability of 10 CFR 50 Appendix R [CFR 50, 1993] Safe Shutdown equipment remaining free of fire damage.

2.4.2.1. Phase I : Area Screening [Qualitative Analysis]

This phase provides a method for quickly screening plant areas whose loss due to fire will have no impact on the ability to achieve and maintain safe shutdown. The evaluation is performed on a fire area by fire area basis. An exposure fire is assumed to occur within each fire area, and all safe shutdown components within the fire area are considered damaged by the fire. The normal redundant or alternate shutdown path outside the fire area is assumed to be unavailable. The fire is confined to the boundaries of the fire area. The project for safe shutdown functions while damaging safe shutdown components in the fire area at the same time. Then, this fire area can be screened out.

2.4.2.2. Phase II: Fire Compartment Screen [Quantitative Analysis]

Basically, this phase involves a five-step progressive probabilistic evaluation containing a sequence of events which occurs to create the loss of shutdown functions. The first three steps [step 1: Ignition Source Frequency, step 2: Redundant/Alternate Shutdown Path Unavailability and step 3: Fire Hazard Evaluation Basis and Combustible Material Evaluation] can be used as a progressive screening approach based on quantifying the following 5 items, from which the core damage frequency [CDF] for each fire compartment [NRC-CFP, 1994] is calculated according to:

$$\mathbf{CDF} = \prod_{i=1}^{5} \mathbf{Pi} \qquad [2.9]$$

where

$\mathbf{P_1}$: Fire ignition frequency in the specific plant compartment.

$\mathbf{P_2}$: Failure probability of redundant/alternate success paths.

$\mathbf{P_3}$: Probability of critical combustible loading damage.

$\mathbf{P_4}$: Failure probability of automatic suppression systems

$\mathbf{P_5}$: Failure probability of manual suppression recovery actions

These steps are arranged progressively. If at any point in the process, the frequency of losing a safe shutdown function is less than 1.0×10^{-6} per reactor-year, the compartment can be screened out from further evaluation.

Step 4 is the evaluation of potential fire vulnerabilities. Different approaches include: evaluating the implementation of administrative and/or hardware modifications, or further evaluating the subject fire compartment with more detailed analysis than those proposed in the Phase II screening method. Step 5 involves the evaluation of the potential impact on containment heat removal and isolation.

2.4.2.3. Phase III: FIVE Methodology Walkdown/Verification

This phase can be performed before or after phase I/II. Its purposes are to walkdown/verify the plant to gather data and confirm information and assumptions used or while performing phase I and II and complete the Sandia Fire Risk Scooping Study Evaluation. The Sandia Fire Risk Scooping Study will address six issues, which include: seismic/fire interactions, fire barrier qualifications, manual fire fighting effectiveness, total environment equipment survival, control system interactions, and improved analytical codes. Its implementation of the FIVE methodology should be documented in a traceable manner to provide the basis for findings. This can be dealt with most efficiently by a two-tier approach. The first tier consists of the results and conclusions of the plant-specific application of the FIVE methodology that will be reported to the NRC for review. The second tier is the documentation of the process itself, which should be retained by the licensee for the duration of the license.

Figure 2.3.1. Event tree for a loss of coolant accident [LOCA]

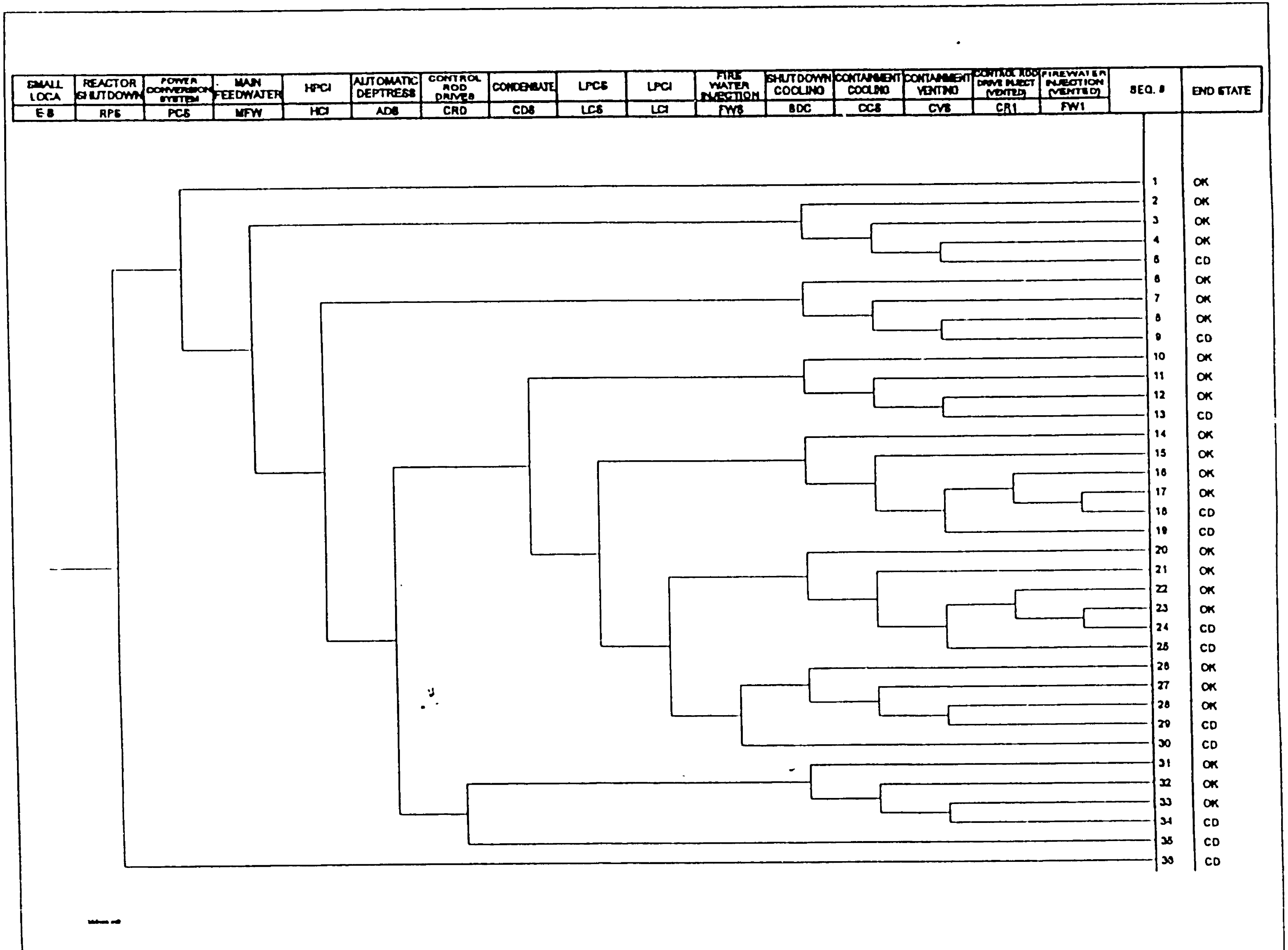
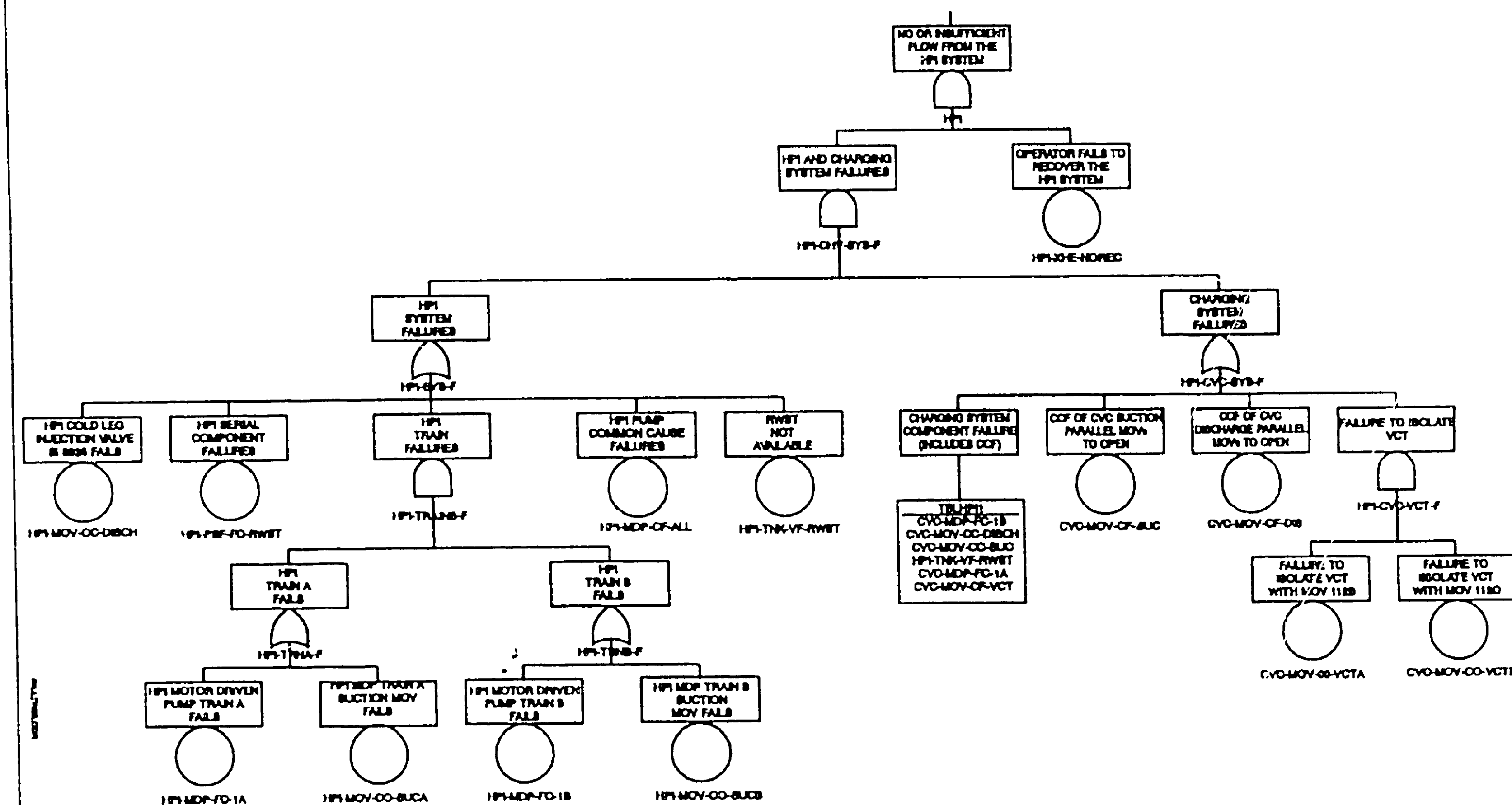


Figure 2.3.2. Fault tree for the high pressure cooling injection system [HPCI]



Chapter 3. Technical approach

3.1. Introduction

This chapter establishes the structure and the technical approach for screening and analysis of LERs relevant to internal fires. The structure comprises a series of steps or levels of screening followed by analysis. The considerations taken into account to develop the screening criteria are presented, along with the basic steps that the nuclear power plants should carry out in order to incorporate the fire ASP methodology.

3.2. Basic approach

The fire PRAs reveal that the most vulnerable parts of the plants are usually the few areas -control room, cable spreading room, electrical control panels, etc., where multiple trains of safety-related systems come together, so that a single fire could compromise more than a single plant division. The PRAs also reveal that the non-fire failures, together with the fire initiator, are important contributors to many of the significant cut sets. The core damage frequency from a stylized fire cut set can be written as:

$$\mathbf{CDF = IE_f * A_f * B_{nf}} \qquad [3.1]$$

where

CDF : Core damage frequency [events/year]

$\mathbf{IE_f}$: Fire Initiating event frequency [Fires/year]

$\mathbf{A_f}$: Probability of fire-initiated failures of equipment A

$\mathbf{B_{nf}}$: Probability of non-fire-initiated failures [NFF] of equipment B.

Where * represents the Boolean connection “and”.

Thus, for this cut set to occur and lead to core damage, there must be both fire-caused failures like $\mathbf{A_f}$ and non-fire failures like $\mathbf{B_{nf}}$. Non fire failures are assumed here to be failures-on-demand, for example a failure to start, an unavailability because of a maintenance outage or an undiscovered broken part, or a human error. Events like $\mathbf{B}_{nf}$ are similar or identical to events in the internal-initiators part of the PRAs, and are entered into the PRA model based on data and fault tree analysis from the internal events PRA. Some events like $\mathbf{B}_{nf}$ may be not very important in the internal events PRA but become important after an internal fire initiating event, because the structure of a fire-initiated sequence may be different.

Therefore, it is concluded that there are three places to look for significant plant-specific precursors from fire-related events:

1) One should examine whether there has been an increase in the population of one or more of the categories of fire initiating frequencies, either in the number of fires or in their severity.

2) One should look for configuration compromises that would make the consequences of a fire in the equipment of the locations more severe than it is assumed in the fire PRA.

3) One should examine whether the non-fire portions of the accident sequences occur more frequently or with greater severity in precursor events and data than assumed in the fire PRA.

3.3. Classification of fire-related operational events

Consistent with the basic approach from above, the fire-related operational events will be classified into three categories:

1) Real fires

In this category are classified those operational events where a real fire has occurred. Notice that the fire may be the cause of the main problem reported in the LER or be incidental to the occurrence of other operational events.

2) Configuration compromises

A configuration compromise is defined as a detected condition that is different from that assumed in the original fire risk analysis and that affects the ability of safety related equipment to survive a fire. This type of accident precursor is one in which the configuration of a fire location has been altered or differs from the original plant walkdown and prior safety evaluations. This change to the fire safety situation may not only compromise the original fire safety analysis, but may also indicate a potentially increased fire risk.

The following conditions can be classified as configuration compromises:

- Differences in regulated separation distance for redundant trains.
- Evidence of new ignition sources, not considered in previous fire analyses.
- Presence of transient fuels.
- Modification of physical properties or distribution of fire barriers or materials involved in a fire scenario.
- Modification of physical properties in seals, leading to fire spread from one location to another.
- A detected condition or new mode of failure related to equipment that could increase the risk due to fires in a location.
- Modifications on ventilation systems, that could change the physical configuration considered in the fire modeling for affected locations.

3) Non-fire failures

A non-fire failure is defined as a failure, including a maintenance unavailability, an operator error, such that, if a fire were to occur, the availability of the required safety related function would be degraded. That could be a complete loss or a decrease in the level of redundancy of a required safety function. Since any loss or degradation of a safety system that is required for plant shutdown after a fire could be considered a precursor, the issue is whether the degradation is significantly different from the degradation assumed in the plant's safety basis or in the plant PRA. That is, if an LER indicates that a reduction of a safety system redundancy has occurred, this event should be analyzed with respect to its increased fire hazard.

3.4. A three-step process

The fire methodology is based on a screening/analysis process in a three-step process: an initial screening step, followed by a second step that requires some analysis, followed by a more detailed analysis only if appropriate (more details in section 4.7, rationale). The three broad steps in the overall structure are:

3.4.1. Step 1. Initial screening

This step is designed to eliminate clearly unimportant operational events from the ASP point of view in general and from fires in particular. The goal of step 1 is to sort out, i.e., eliminate from consideration, those LERs that require no further evaluation. Other LERs are passed on to step 2. This step is envisioned as requiring no actual analysis but rather merely a comparison of the information contained in the LER to certain specific step-1 criteria.

3.4.2. Step 2. Preliminary analysis

The goal of step 2 is to perform enough analysis to decide whether a given LER is likely to be designated as an accident sequence precursor or is otherwise likely to contain important new safety insights, or can be screened out based on a comparison with specific step-2 criteria. This step is intended to reduce the number of operational events and gain insights into the detailed analysis, for which the step 1 is not designed. In this step the analyst makes a more detailed use of the documentation from the plant, such as the Individual Plant Examination [IPE], the fire PRA and any other relevant documentation considered useful to understand the safety significance of the event.

3.4.3. Step 3. Detailed analysis

The goal of step 3 is to subject a limited number of LERs to detailed analysis if, based on specific step-1 and step-2 criteria, it is judged that step-3 analysis is justified. This step constitutes the crucial part and the culmination of the analysis in the process. Its output will be the definition of those operational events that will be reported as accident sequence precursors.

Designation as an accident sequence precursor means that the LER meets the ASP criterion of CCDP>1.0 x 10^{-6} established for the ASP program [Minarick, 1990] Only a few LERs will meet this criterion and therefore will be so designated.

3.4.4. Considerations applied in developing the screening criteria

1) Conservative

During both the step-1 and step-2 screening, LERs should be retained unless they can be affirmatively screened out, not the other way around. This is consistent with current ASP practice for internal faults.

2) Ease of discrimination

The step-1 screening criteria are intended to enable the analyst to discriminate easily between those LERs that are obviously not of much ASP interest and the others.

3) Equivalence

The internal-faults ASP screening criterion uses a level of about 1.0 x 10^{-6} for CCDP. For steps 2 and 3 below, the logic for fire-related LERs is structured to be consistent with that screening criterion.

4) Rigor

The screening criteria cannot be rigorous and there is no pretense that they are. As the criteria are applied, considerable analyst judgment is necessary: In fact, it is important to emphasize that no workable screening criterion can avoid such analyst judgment in the fire area (of course, there is also considerable judgment necessary to apply the ASP approach to internal-plant-fault LERs). It is important to point out that an element of conservatism, embedded in the ASP procedures here, compensates somewhat for this.

5) Models

It is assumed here that a plant-specific PRA exists and is available for fire-initiated scenarios. The methodology here explicitly requires the analyst to use these models, and to adapt them as appropriate (see Section 3.7.2 for a more extensive discussion of these issues).

3.5. Scope of the methodology

The methodology discussed herein is intended for the review of Licensee Event Reports [LERs] that are reported by U.S. nuclear power plants to the U.S. Nuclear Regulatory Commission, under NRC rules in Title 10, Part 50.73 of the Code of Federal Regulations (see also [NRC, 1994b]). LERs report operational situations that are out-of-the-ordinary and that have at least a modicum of safety significance. There are specific reporting rules, including thresholds below which the situation as discovered need not be reported; this will not be discussed here. Suffice it to say that over a thousand LERs are reported each year to the NRC, and that their analysis for precursor insights through NRC's ASP program is the subject here.

Throughout this report, LERs will be referred as the sole source of the reported abnormalities. However, it is recognized that the ASP program also analyzes information from other sources. Nevertheless, for brevity's sake, the methodology will be written as if the LERs are the sole source of input to the ASP analysis, and will often refer to what an LER reports without due recognition that other sources of relevant information exist.

3.6. Plant-specific preparation to incorporate the ASP methodology

It is required that the following steps be taken by the plants in order to incorporate the ASP methodology.

1) Fire Step 1

Identify the 10 or 20 leading fire-initiated core damage sequences [cut sets] in the plant specific PRA, taking care of including cut sets that have non-fire failures and human errors.

2) Fire Step 2

Identify any other fire-initiated sequences in the fire PRA that could be significant contributors if any non-fire failure were significantly larger than previously thought.

3) Fire Step 3

Identify the type of fire initiator (Control-room fire, electrical cabinet fire, etc.) involved in each of these sequences identified in steps 1 and 2 and for each, identify the numerical value of its annual rate [probability per year] in the fire PRA.

4) Fire Step 4

Identify the non-fire failures and human errors in each of the sequences identified in steps 1 and 2, and for each identify its numerical quantification value in the fire PRA (based on either data, or fault tree analysis, or both).

CHAPTER 4. Methodology for screening and analysis

4.1. Introduction

This chapter establishes a structure for screening and analysis of LERs relevant to internal fires. The structure comprises a series of steps or levels of screening followed by analysis.

4.2. The meaning of screening

The notion of "screening" as used in step 1 below is that a quick, non-labor-intensive evaluation should be able to sort those LERs that require or merit further evaluation from those that do not. Screening an LER out means that it will not be designated as an Accident Sequence Precursor [ASP] and that no important new safety insights can be gained from evaluating it further. Screening an LER in during either step 1 or 2 only implies that one cannot conclude without further evaluation whether or not it will be designated as an accident sequence precursor.

4.3. Safety insights vs. designation as a precursor

Designation as an accident sequence precursor means that the LER meets the ASP criterion of CCDP> 1.0×10^{-6}. Only a few LERs will meet this criterion and therefore will be so designated. However, in the guidance here the ASP fire analyst is sometimes directed to develop and document a "safety insight" even for an LER that does not end up being designated as a precursor.

For some LERs, safety insights can be derived during the step-2 phase, even if the event is screened out there, so that there is no need for further step-3 precursor analysis. For some other LERs, step-3 analysis will be required to ascertain if the LER is actually an accident sequence precursor, and separately if any other safety insights can be gained.

4.4. Screening and analysis guidance for a fire Configuration Compromise LER

Under consideration here is an LER that reports a "configuration" abnormality that could affect risk of a fire-initiated accident. It is necessary to note first that to be reported as an LER such an abnormality must cross a reporting threshold that should eliminate the completely trivial issues. Presumably, the reporting threshold is related to violations of the operating basis.

A flow diagram in block form for analyzing these LERs is presented in Figure 4.4.1.

4.4.1. Step-1. Screening Criterion

For this initial step, the analyst should postulate a fire that destroys everything within the fire zone where the configuration abnormality is reported to have occurred, or the two or more zones if multiple zones are affected by the configuration abnormality.

The LER can be screened out if all of the following four criteria are met (see Section 4.7.1 for a discussion of the rationale for these four criteria). Otherwise, the LER is screened in.

1) If the fire damage would not have caused a plant trip.

2) If the fire damage would be limited to the net effect of compromising at most only a single train of a multi-train front-line safety system or function.

3) If the fire damage would not have compromised the functioning of any one train of a support system (cooling water, instrument air, electrical power, instrumentation and control, etc.) that supports a safety-relevant front-line system or function.

4) If the fire damage would not have caused one accident-sequence initiators (LOCA, LOFW, loss of offsite power, turbine trip, etc.) used in the internal-faults ASP analysis methodology.

Notwithstanding the above four criteria, the LER should be retained for step-2 analysis if an evaluation of the LER reveals an important compromise of the effectiveness of either the automatic suppression system or the ability of the fire brigade (or other manual suppression) to perform its function.

4.4.2. Step-2. Preliminary-Analysis Criterion and Guidance

For LERs that have not been screened out during the step-1 screening, the analyst should continue with the postulate that everything in the entire fire zone in which the problem is located has been destroyed by a fire. In step 2, a quasi-realistic analysis but based on a conservative scenario should be performed, the guidance for which is as follows:

1) As mentioned, continue with the postulate that everything in the entire fire zone in which the configuration abnormality in the LER is located has been destroyed by a fire. If more than one zone is a factor for this LER, then the analyst should postulate that all equipment in all involved zones has been destroyed.

2) Assess whether or not the loss of the equipment in (1) would cause an automatic plant trip (see Section 4.7.5 for a more extensive discussion of the rationale for the guidance below under (3A) and (3B)).

Case A. Plant would not trip:

3A) Assume that the postulated fire damage in (1) above would cause the operators to initiate a manual trip (see Section 4.7.9 for a discussion of the rationale for assuming a manual trip). For the PRA analysis in (4) below, use the appropriate internal-events PRA event tree for that manual trip. For the initiating event frequency, use the frequency, taken from either the plant-specific data base or, if necessary, a generic data base, of fires in the zone under consideration.

Case B. Plant would trip:

3B) Assume that the frequency of the plant-trip initiating event, to be used in the PRA model in (4) below, is the frequency, taken from either the plant-specific data base or, if necessary, a generic data base, of fires in the zone under consideration.

4) Run the plant-specific internal-events PRA model, but with the failures from (1) put into the model, and with the plant-trip initiating event and its frequency taken from either (3A) or (3B).

5) Work out the conditional core damage probability [CCDP] according to the usual PRA methods and using the appropriate assumptions for the plant-specific internal-events PRA under consideration.

6) If the CCDP is below about 1.0×10^{-6}, the LER is screened out. If this criterion is exceeded, the LER is screened in and passed on to Step 3 (Detailed Analysis) for further evaluation.

4.4.3. Step-3. Detailed-Analysis Criterion and Guidance

In this step, the analyst will perform either full or partial, but detailed, probabilistic modeling of the postulated event. The guidance for this modeling is as follows:

1) Based on the information in the LER, the analyst should identify each of the specific equipment items whose fire capability has been compromised by the inadequate configuration.

2) Earlier Step-1 screening or Step-2 preliminary analysis may have screened out some of the items in (1). The analyst should reduce the equipment list to only those items that have survived the earlier screening so that they require the detailed analysis in this Step 3. The fire area(s) or zone(s), from the PRA analysis, should be identified for all of the affected equipment on this reduced list.

3) For each equipment item on the reduced list from (2), the analyst should define the fire scenario associated with that equipment in its actual location. This includes the identification of the potential source of the postulated fire, the target for the fire, and other items that may be affected by the fire once it were to start.

Note that it is possible that some of the equipment identified in (2) may represent the potential source of the fire; alternatively some or all of the equipment may be the fire's target. The fire source may be modeled as arising elsewhere such as due to transient fuels present in the vicinity.

The product of this substep is a list of fire scenarios involving safety-related equipment that can potentially be affected by the configuration-compromise change from the LER, such that a deeper analysis is necessary.

4) For each scenario from (3), the analyst should define the fire-PRA model(s) that capture the accident sequence(s) in which the fire scenario may be involved. There are two different cases here, depending on whether or not each identified fire scenario and its associated accident sequence has or has not been included in the prior PRA analysis.

Case A. Scenario not included:

4A) If any of the fire scenario(s) is not modeled in the existing fire analysis (presumably because it was screened out of the base-case fire analysis on a valid basis), then it must be modeled before it can be analyzed (see Section 4.7.6 for a discussion of the rationale for the guidance here). This involves going back to the internal-events PRA model, identifying where the affected equipment enters into the PRA, and modifying the fire PRA model to account for the previously absent equipment. When this modification has been accomplished, go to (5).

This work may be difficult: the analyst must perform an in-depth review of the plant's fire-related documentation, so as to identify those fire scenarios that may have been examined by the earlier fire analysts as part of the development of the existing fire analysis, but were screened out for some valid reason. For these, the analyst here must determine if the conditions that allowed for the earlier screening-out are still applicable given the configuration-compromise situation from the LER. This work can reduce considerably the analyst's need for new modeling effort here.

Case B. Scenario Included:

4B) Even if a fire scenario is already in the existing analysis model, it is necessary to assess whether that existing model adequately accounts for the affected equipment in its compromised state from the LER. If so, go to (5). If not, the analyst should modify the existing analysis to take account of the different situation from the LER. Then go to (5).

5) Assess whether or not the configuration compromise from the LER would affect any of the fire initiation frequencies used in the base-case PRA fire analysis (see Section 4.7.7 for a discussion of fire initiating-event-frequency issues). If not, proceed. If so, modify the relevant fire-initiation frequencies before proceeding.

6) Re-do the plant-specific fire analysis (fire PRA) using the fire scenarios (including the relevant fire initiating events and frequencies) from (4) and the frequency modifications from (5), but assuming that the postulated fire(s) cause the greater damage that is indicated by the LER, compared to the base-case situation. Use the earlier base-case-analysis assumptions and data, except if the base case should be modified to account for compromises as indicated in the LER.

This part of the analysis should be done in two stages: an "intermediate-screening" stage, that is followed, if necessary, by a "final-analysis" stage.

6A) Perform an intermediate-screening analysis. This consists of the following sub-elements:

i) Assume, for each scenario identified in (1) above, that all of the safety-related equipment identified in (1) above would be destroyed by the postulated fire, with 100% probability.

ii) Using this assumption, re-run the plant-specific fire analysis.

iii) Work out the conditional core damage probability according to the usual ASP methods and using the appropriate assumptions for the plant-specific PRA under consideration. In this analysis, use the full spectrum of fire initiating events and other internal-plant-fault initiating events.

iv) If the CCDP due to the configuration compromise identified in the LER is below about 1.0×10^{-6}, the LER is screened out. If this criterion is exceeded, proceed to the next stage, the "final-analysis" stage (6B).

6B) If necessary, perform the final analysis. This consists of the following sub-elements:

i) Perform a complete fire PRA modeling for each fire scenario. This will allow the development of a more realistic likelihood for fire-caused failure than the pessimistic assumption of 100% likelihood that was used in the intermediate-screening in (6A). In doing this modeling, the analyst should apply the procedures employed in a standard fire PRA, with the goal of producing a realistic quantification of the impact of the configuration compromise. Manual and automatic suppression, fire brigade actions, and so on should be included. For fire scenarios that were originally modeled, the analyst must perform the appropriate modifications to reflect the configuration compromise. For fire scenarios that were not originally modeled, a full model must be developed.

ii) Using the model(s) from above, re-run the plant-specific fire analysis for each fire scenario.

iii) Work out the conditional core damage probability according to the usual ASP methods and using the appropriate assumptions for the plant-specific PRA under consideration. In this analysis, use the full spectrum of fire initiating events and other internal-plant-fault initiating events. If more than one fire scenario is involved, sum up the various scenario contributions for the purposes of CCDP analysis.

iv) If the CCDP due to the configuration compromise identified in the LER is below about 1.0×10^{-6}, the LER is screened out. If this criterion is exceeded, the LER is screened in and documented according to the ASP methodology.

4.5. An actual fire reported in an LER

Here is considered an LER that reports an actual fire. The evaluation described below will consider not only the location and size of the fire, but also the damage that it caused or that it might have caused. The evaluation will also consider the automatic response or the or fire-brigade response, if any, to the fire. A block-form flow diagram for analyzing these LERs is shown in Figure 4.5.1.

In the screening and analysis, the methodology will concentrate principally on the fire-related events reported in the LER. Sometimes, an LER which reports an actual fire will also report about various internal faults not related to the fire, perhaps involving a plant trip or what is called a full "accident sequence initiating event" in the PRA literature.

4.5.1. Step-1. Screening Criterion and Guidance

For an actual fire reported in an LER, the step-1 screening criterion takes the following form:

4.5.1.1. Step 1-A.

The LER is screened in and passed on for step-2 analysis if the LER reports any one of the following (see Section 4.7.3 for a discussion of the rationale for these four criteria). Otherwise, move to step 1-B.

1) If the LER reports a plant trip.

2) If the LER reports any one of the usual list of PRA accident-sequence initiators (LOCA, LOFW, loss of offsite power, turbine trip, etc.) used in the internal-faults ASP analysis methodology.

3) If the LER reports damage to more than a single train of a multi-train front-line safety system or function.

4) If the LER reports damage to the functioning of more than one train of a support system (cooling water, instrument air, electrical power, instrumentation and control, etc.) supporting a safety-relevant front-line system or function.

4.5.1.2. Step 1-B

Compare the individual fire's location and size with the generic fires data base. Expert judgment is necessary to accomplish this comparison. If this comparison reveals that fires in this type of location and of this size are absent or rare in the data base, then the event is screened in and the analyst should go to step 2 (the opposite is when the fire is common in the fires data base). Otherwise, go to step 1-C.

4.5.1.3. Step 1-C

Evaluate the actual plant response to the fire, either the automatic response or the fire-brigade response. Expert judgment is necessary to accomplish this evaluation. If the evaluation reveals something out-of-the-ordinary about the response, then the event is screened in and the analyst should go to step 2. Otherwise, go to step 1-D.

4.5.1.4. Step 1-D

If the fire actually spread beyond a single fire zone, or if in the analyst's expert judgment the fire had a reasonable likelihood of having spread beyond a single fire zone, then the event is screened in and the analyst should go to step 2. Otherwise, go to step 1-E.

4.5.1.5. Step 1-E

Postulate that everything in the entire fire zone (or zones) in which the fire occurred is destroyed by the fire. Evaluate the damage to safety-related equipment that would be caused by such a fire. The LER can be screened out if all of the following four criteria are met (see Section 4.7.3 for a discussion of the rationale for these four criteria). Otherwise, the LER is screened in and the analyst should go to Step 2:

1) if the fire damage would not have caused a plant trip;

2) if the fire damage would not have caused one of the usual list of PRA accident-sequence initiators (LOCA, LOFW, loss of offsite power, turbine trip, etc.) used in the internal-faults ASP analysis methodology;

3) if the fire damage would be limited to the net effect of compromising at most only a single train of a multi-train front-line safety system or function;

4) if the fire damage would not have compromised the functioning of any one train of a support system (cooling water, instrument air, electrical power, instrumentation and control, etc.) supporting a safety-relevant front-line system or function.

4.5.2. Step-2. Preliminary-Analysis Criterion and Guidance

This is the preliminary-analysis step, whose objective is to screen out through preliminary analysis those LERs that do not meet certain criteria, so that only a small fraction of the LERs get passed on to step 3 for detailed analysis.

4.5.2.1. Previous classification

Before beginning the step-2 analysis, it is necessary to differentiate three different classes of fire LERs that include an actual fire:

<u>Class A</u>: The LER reports neither a plant trip nor an "accident sequence initiating event" as usually defined in the PRA literature.

<u>Class B</u>: The LER reports a plant trip or a PRA "initiating event", and reports that the fire caused or was involved in the trip or initiating event.

<u>Class C</u>: The LER reports a plant trip or a PRA "initiating event", but reports that the fire did not cause and was not otherwise involved in the trip or initiating event.

Class C will be dispensed with first, after which Classes A and B will be dealt with in much greater detail. Therefore, for Classes A and B the analyst should proceed to the rest of step 2 below.

<u>For Class C:</u>

LERs that report a plant trip or a PRA initiating event but report that the fire did not cause and was not otherwise involved in it (see Section 4.7.8 for a more extensive discussion of Class C LERs). For these LERs, because the plant trip/initiating event is unrelated to the fire, the LER should usually be returned for internal-events ASP analysis. However, before returning it, the fire ASP analyst should evaluate the effects of the fire. This evaluation will require considerable expert judgment. There are two qualitatively different cases here:

1) In the first case, the fire did not induce any damage to safety equipment and/or did not have the potential to do so, in which case the internal-events ASP analyst can proceed without accounting for the fire in the ASP model, although there may be some lessons learned about what happened, from which recommendations can be developed.

   It will require considerable expert judgment to conclude, one way or the other, whether or not the fire had the potential to damage any safety equipment. Specifically, in situation (i) the ASP analyst must evaluate all of the characteristics of the fire, concentrating on its potential for inducing other damage beyond what actually occurred; and should attempt to quantify, if possible, an approximate contingent probability that other fire-induced damage [that did not actually occur] might have occurred. If this probability is truly negligible then the analyst can safely categorize the event into this subclass.

These LERs should be analyzed by the internal-events ASP methodology, not the fire ASP methodology. However, before returning them to the internal-events ASP, these LERs should be passed through steps 2-B, 2-C, and 2-D (below), and any insights gained there should be documented.

2) In the second case, the fire in the LER did damage some safety equipment, or had an important potential to have done so. In this case, the analyst should carry the LER forward to the ASP fire analysis (continue with the full step 2 below).

The main Step-2 analysis guidance begins here. LERs that have reached this stage in the methodology will be passed on to the step-2 sub-step(s), depending on which sub-step(s) in Step 1 caused the LER to be screened in. That is, if step 1-A (or step 2-C) caused the LER to be passed to step 2, then begin with step 2-A (step 2-C) and continue from step 2-B to 2-E (step 2-D to 2-E).

4.5.2.2. Step 2-A

The fire caused a trip, an initiator, or damage (real or potential) that is judged to be potentially important as defined in Step 1. After evaluation, the analyst should document any "lessons-learned" concerning this fire as a safety insight. This requires considerable expert judgment. Following this evaluation, the event should then be passed back through the rest of the step-1 screening: either it is passed on to the rest of step 2 based on other criteria, or it is screened out so that it need not be subjected to further analysis. In performing this evaluation, the analyst should consider the following points:

- The analyst should consider, if there has been a plant trip or an initiating event, the degree of participation of the fire in the incident (for example, whether the fire induced the initiating event, or the initiating event was due to other causes.)
- The analyst should determine the degree of participation of the fire in the reported events (for example, whether all of the failures reported in the LER were a result of the fire, or only some of them, and why.)
- The analyst should list and consider the human errors in the event and whether any of them were induced by the fire. Also, the analyst should consider various postulated sequences related to the actual sequence of events in the LER, and the impact of the fire on operator performance.
- If fire suppression was successful in limiting the fire, the analyst should evaluate the extent of potential damage that could have occurred had there been no or inadequate fire suppression.
- The analyst should identify the ignition source, the cause or mode of ignition, all damaged components (especially including cables), and other aspects that deserve attention.

4.5.2.3. Step 2-B. Fire location/size not common in the fires data base

After evaluation, the analyst should document any "lessons-learned" concerning this fire as a safety insight. This requires considerable expert judgment. The event should then be passed back through the rest of the step-1 screening: either it is passed on to the rest of step 2 based on other criteria, or it is screened out so that it need not be subjected to further analysis. In performing this evaluation, the analyst should consider the following points:

- Reference to this type of fire in the data base
- Whether the plant has or has not considered this particular type of fire as an ignition source.

- Whether this fire ignited due to a violation of procedures regarding storage of potential fuel.
- Whether the fire occurred in a manned location
- Whether the fire occurred where separation criteria were not effective
- Whether materials ignited whose resistance to ignition was less than expected
- Whether the fire occurred in a location where ignition sources were expected to be absent
- Whether the fire location had been screened out as unimportant in the earlier fire analysis, and if so why
- If considered, how the fire location was considered: in which scenarios, and for which accident sequences.

4.5.2.4. Step 2-C. Out-of-the-ordinary fire-brigade or automatic response

After evaluation, the analyst should document any "lessons-learned" from the plant-response aspect of this fire as a safety insight. This requires considerable expert judgment. The event should then be passed back through the rest of the step-1 screening: either it is passed on to the rest of step 2 based on other criteria, or it is screened out so that it need not be subjected to further analysis. In performing this evaluation, the analyst should consider the following points:

1) Detection

- Problems with actuation of detection devices
- Problems in performance of detection systems, either automatic or human such as a roving firewatch
- Timing of actuation
- External actuation for suppression; procedures
- Degradation of other plant functions for the benefit of the fire brigade

- Problems with the availability and/or the effectiveness of suppression materials
- Lack of clarity in procedures or responsibilities
- Duration required for fire suppression: comparison with "expected" time as used in safety basis for the plant

2) Automatic suppression

- Problems with actuation of automatic devices
- Inadequate automatic-suppression devices in the location of the fire
- Properties of involved materials different than expected
- Problems with the elements considered in the fire safety system, as set down in the Safety Analysis Report.

4.5.2.5. Step 2-D. Fire-spread beyond a single fire zone

After evaluation, the analyst should document any "lessons learned" from the fire-spread aspect of this fire as a safety insight. This requires considerable expert judgment. The event should then be passed back through the rest of the step-1 screening: either it is passed on to the rest of step 2 based on other criteria, or it is screened out so that it need not be subjected to further analysis. In performing this evaluation, the analyst should consider the following points:

- Whether the zone(s) in the fire were considered in the plant's safety-basis fire analysis
- Whether the fire spread to multiple trains or functions beyond the separation criteria used in the plant's safety basis
- Existence of redundant trains without appropriate separation criteria, or without the proper materials (given that the normal separation criteria may not have been feasible for that location)
- Whether the fire spread to other fire areas or zones

- Whether any problems were observed regarding the resistance of fire barriers (walls, doors, seals, etc.)

4.5.2.6. Step 2-E. LER arriving at Step 2 because it has failed one or more of the systems-damage criteria.

The guidance for this key part of the Step-2 analysis is as follows:

1) The analyst should continue with the postulate that everything in the entire fire zone in which the fire occurred has been destroyed by the fire. If fire-spread beyond the host zone is a factor for this LER, then the analyst should postulate that all equipment in all involved zones has been destroyed.

2) Assume no fire suppression.

3) Determine whether the damage assumed in (1) would cause a plant trip (unless a fire-induced trip has already been reported in the LER itself).

4) If either a plant trip or one of the standard list of PRA initiating events was reported in the LER or would have been induced by the damage assumed in have occurred at the fire's location, use the event tree corresponding to that initiating event. Otherwise, conservatively assume that a manual plant trip would be produced by the fire, and use the event tree that captures the events that follow this manual trip (see Section 4.7.9 for a discussion of the rationale for assuming a manual trip).

5) Work out the conditional core damage probability as per the normal ASP analysis methodology, using the accident-sequence initiator from (4) and assuming the fire damage from (1). Use all of the appropriate assumptions for the plant-specific PRA under consideration.

6) If the ASP CCDP criterion of 1.0×10^{-6} is not exceeded, the event is screened out. If this criterion is exceeded, the event is screened in and passed on to step-3 (Detailed Analysis) for further evaluation.

4.5.3. Step-3. Detailed-analysis criterion and guidance

In this step, the analyst will perform either full or partial, but detailed, probabilistic fire modeling of the event. This involves evaluating the events, failures and human errors reported in the LER, in two separate phases.

Phase I is designed to evaluate quantitatively the actual damage induced by the fire reported in the LER. Phase II is designed to evaluate the LER quantitatively in terms of the potential damage that the reported fire might have induced (but did not induce) in safety-related equipment in the involved locations.

In order to perform the detailed analysis, the analyst must make extensive use of all prior plant-specific documentation covering earlier fire analyses that examined the relevant locations and the relevant ignition sources as reported in the LER. In addition, the analyst will require the information that can support developing either a partial or a complete fire model for each relevant fire scenario.

4.5.3.1. Phase I. Analysis of actual fire damage

In this phase the analyst should evaluate the LER, based on the actual damage induced to safety-related equipment, including direct fire damage itself; human errors that occurred as a consequence of the fire; non-fire-induced human errors; and internal or non-fire-induced failures. For this actual-damage analysis, the evaluation should be limited to mapping the actual reported events onto the logic model and quantifying that model to obtain a conditional core damage probability.

In order to do the required evaluation, the analyst must perform a detailed analysis of the LER, to determine all of the actual failures and human errors that occurred as reported in the LER.

1) <u>Sub-Task I-A. Definition of actual damage</u>

In this sub-task, the analyst should perform a detailed analysis of the LER, in order to list all of the failures to safety-related equipment as reported in the LER, along with the human errors that occurred. The failures and human errors need to be expressed in terms of the basic events considered in the logic models, event trees, and fault trees, that have been structured for analyzing sequences and system failures (see next sub-task}. If a plant-specific fire-PRA model exists, it should be used as the basis for this work. Otherwise, it is likely that the analyst will need to rely in a major way on the plant-specific internal-events PRA model.

2) Sub-Task I-B. Definition of the logic model

The sequence is completely defined by the logic model along with the failures and human errors reported in the LER. In this sub-task, the analyst should define the logic model that will be used for calculating the conditional core damage probability.

If the sequence corresponding to the ignition source reported in the LER has been modeled by the plant in its earlier fire analyses, then the logic model should be that earlier model, using the same initiating event that was reported in the LER. If the LER reports that no initiating event occurred as a consequence of the events being reported, the analyst must estimate the most likely one that might have been produced. In many cases, this will be a manual trip, but might be a more serious initiator, depending on the circumstances.

If the sequence corresponding to the ignition source reported in the LER has not been modeled by the plant, then the analyst should use the event tree from the internal-events PRA, corresponding to the initiating event reported in the LER. If the LER reports that no initiating event occurred as a consequence of the events being reported, the analyst must estimate the most likely one that might have been produced. In many cases, this will be a manual trip, but might be a more serious initiator, depending on the circumstances.

3) Sub-Task I-C. Quantification

In this sub-task, the analyst should calculate the conditional core damage probability corresponding to the actual events reported in the LER, based on the model developed in sub-task I-B. For each reported failure or human error, the basic-event failure probability should be set to 1.0 and mapped onto the logic model. If a safety-related equipment failure or human error has not been included directly as a basic event in the logic model, the failure should be reflected by modifying those basic events that are impacted by the failure or human error.

The CCDP analyzed here will be used below when it is compared to the CCDP for the potential-fire-damage case.

4.5.3.2. Phase II. Analysis of potential fire damage

In this second phase, the analyst should evaluate the LER, based on both the actual damage and the potential damage that might have been induced to safety-related equipment as a consequence of the reported fire. For this potential-damage analysis, the difficult part of the evaluation will involve **(i)** the determination of the potential losses to safety-related equipment, followed by **(ii)** the estimation of the probability that such losses might have occurred, given the information from the LER as well as other available information. Based on that analysis, an ASP quantification will be performed, making use of the logic model defined above as part of the Phase-I actual-damage analysis.

In order to screen out some LERs before performing a detailed fire modeling analysis, an intermediate quantitative screening step is recommended (see below), to eliminate those scenarios found to have negligible risk significance.

1) <u>Sub-Task II-A. Assessment of potential damage</u>

In this sub-task the analyst should assess all safety-related equipment that had the potential for being affected by the fire. This involves **(i)** definition of one or more fire scenarios, **(ii)** an intermediate-screening evaluation, and then, if necessary, **(iii)** a full fire-modeling analysis.

a) Sub-Task II-A.1. Scenario definition

In this sub-task, the analyst should define all safety-related equipment with the potential for being affected by the fire.

If the sequence corresponding to the ignition source reported in the LER has been modeled in the plant's earlier analyses, the safety-related equipment with the potential to be affected by the fire will already be defined from the scenario corresponding to the sequence.

If the sequence corresponding to the ignition source reported in the LER has not already been modeled by the plant, the equipment with the potential to be affected by the fire must be defined from the scenario corresponding to the ignition source reported, based on the physical information and the plant documents regarding the relevant location.

b) Sub-Task II-A.2. Intermediate screening of each scenario

This sub-task is performed separately for each scenario. In this sub-task, the analyst should:

i) Assume that all of the safety-related equipment defined in Sub-Task II-A.1 has been destroyed; this corresponds to setting the failure probabilities for each impacted basic event to 1.0.

ii) Map the real damage and the potential damage already defined, onto the logic model defined in Sub-Task I-B.1.

For each scenario, quantify the logic model. If the resulting conditional core damage probability exceeds the screening value of 1.0×10^{-6}, the scenario should be passed on to sub-task II-A.3 for detailed fire modeling, so that a less conservative calculation of the probability of damage can be performed for each safety-related equipment item. Otherwise, the scenario can be screened out. If all scenarios are screened out, then the entire LER can be screened cut.

c) Sub-Task II-A.3. Fire modeling assessment for each scenario

This sub-task is performed separately for each scenario. In this key sub-task, the analyst should perform a complete fire modeling for all of the safety-related equipment identified as the target(s) for the ignition source reported in the LER, in order to define fully those that had a potential for actual damage.

The analyst must develop or obtain information regarding the time-to-damage for the safety-related equipment corresponding to the scenario, making use of a probabilistic fire model.

If the sequence corresponding to the scenario associated with the reported ignition source has already been modeled by the plant, then the information can be obtained from that existing modeling process.

If the sequence corresponding to the scenario has not been modeled previously by the plant, the analyst must perform a full fire modeling assessment of the scenario, using as the ignition source the actual fire reported in the LER, and using the target developed in sub-task II-A.1.

For each scenario, the product of the fire modeling assessment should be expressed as an estimate of the equipment damage resulting from the thermal effects of the fire (conductive, convective and radiative), in terms of a probabilistic curve of time-to-damage for each safety-related piece of equipment.

d) Sub-Task II-A.4. Estimation of failure probabilities for each scenario

This sub-task is performed separately for each scenario. In this sub-task, the analyst should estimate the probability that each item of safety-related equipment would have been lost due to the thermal effects from the ignition source reported in the LER. This estimation will require considerable expert judgment. The analyst should base his estimate for each safety-related piece of equipment on the following factors:

- A probabilistic distribution of the time-to-damage
- Information from the LER concerning the characteristics of the fire and the occurrence of events related to the induced damage.
- Information in the LER concerning the time involved in the suppression of the actual fire, accounting for the actuation of the various suppression systems (both automatic and manual).

- Information provided by the plant, regarding the characteristics of the suppression systems and the procedures established for the actuation of the fire brigade in cases like that reported in the LER.
- The analyst's own experience and judgment for the particular situation.
- Opinions of fire experts, from inside and/or outside the plant.

2) Sub-Task II.B. Final Quantification

In this sub-task, the analyst should calculate the conditional core damage probability corresponding to both **(i)** the actual failures and human errors reported in the LER and **(ii)** those estimated to have the potential for having damaged safety-related equipment during the occurrence of the events reported in the LER.

For each actual failure or human error, the basic event probability should be set to 1.0. For each potential failure the basic event probability should be set to the value estimated in sub-task II-A.4.

Finally, such failures should be mapped onto the logic model determined in sub-task I-B.1. If a damaged or failed component has not been included as a basic event in the logic model, the failure will be reflected by modifying the basic event (s) impacted by the failures or human errors.

If the resulting total conditional core damage probability exceeds the screening value of 1.0×10^{-6}, the LER should be reported and documented as an Accident Sequence Precursor. Otherwise, the LER should be screened out.

3) Sub-Task II.C. Evaluation of CCDPs

In this sub-task, the analyst should compare the CCDP determined in Phase I for the actual damage in the LER, with the CCDP determined in Phase II for the analysis of the actual damage plus the potential damage. Safety insights from this comparison should be documented.

4.6. Non-fire failures affecting fire-initiated accident sequences

For these LERs, there is no multi-level-screening followed by analysis. The evaluation is all done in one step, as the guidance below will indicate. However, the guidance is different for plants that have performed a fire-PRA analysis (Group 1) than for those that have not performed such an analysis (Group 2). A flow diagram in block form for analyzing these LERs is in Figure 4.6.1.

Here it is considered an LER involving a so-called "random" failure (see Section 4.7.4 for a more extensive discussion of the rationale for the guidance below). To select all such LERs for this analysis, however, could be very costly, so a criterion has been developed for selecting those few LERs likely to have most safety significance.

4.6.1. Proposed criterion for selecting LERs for non-fire-failure analysis

The difficulty addressed here is as follows: if every LER reporting a non-fire problem or failure, which would be over 99% of the LERs, were to be examined for its potential to affect fire-initiated accident sequences, the ASP analysis task would be enormous. Requiring every LER to be subjected to analysis of this kind would be very costly and undoubtedly not worth the effort in a cost-benefit sense. Therefore, some selection criterion is needed, so that only a small fraction of the LERs are subjected to this analysis.

It is recommended here that the starting point for selecting LERs for this type of analysis should be the group of LERs that have already been analyzed by the internal-events ASP process, and have not been eliminated during its initial screening process, but have survived that initial screening and are subjected to detailed ASP analysis (there are a few dozen of these LERs each year, only a fraction of which end up with CCDP $> 1.0 \times 10^{-6}$ so that they are designated as accident sequence precursors). The set of safety issues raised in these LERs defines a group of events that clearly should be considered relevant in terms of safety significance.

It is recommended that the non-fire failures in each such LER be subjected to the ASP analysis here. The rationale is that the various internal-plant-fault failures and unavailabilities that have survived the screening of the internal-events ASP process are a useful target group with the potential to affect the risk from fire-initiated sequences.

1) Guidelines for selection

The following four factors should constitute the guidelines for the analyst in the selection of LERs to be examined in the fire ASP analysis for non-fire failures:

a) Select those LERs containing events or issues that have not been screened out in the initial phase of the internal-events ASP review. This is because the issues in these LERs have been identified as being the most significant in terms of risk among the whole family of LERs.

b) Include only those LERs involving failures or unavailabilities considered in the fire-initiated sequences developed by the plant. The information to perform this selection should be taken from the plant-specific fire PRA, if available, or otherwise from whatever other system model exists. This will narrow down the LER list selected in (a) above.

c) Consider as a basic criterion the duration of the non-fire failure or unavailability reported in the LER. Those safety issues or events for which the failure or the unavailability lasts for a "long" duration, as reported in the LER, should be selected preferentially. The phrase "long" should be interpreted, using expert judgment, by comparing the duration to the initiating event recurrence intervals (which are the inverse of the initiating-event frequencies) for the sequences at issue.

d) Finally, an LER that reports only an initiating event should be eliminated from this aspect of the ASP analysis, because the interest here is in potential accident sequences that have their own (fire) initiating event. For every LER being considered, the ASP analyst should calculate the probability that a relevant fire would occur in the reported duration of the failure or unavailability.

4.6.2. Methodological Guidance

4.6.2.1. Group 1: plants with a fire-PRA model

1) Re-run the plant-specific fire-PRA model with the additional random failure inserted into the model (this is essentially identical to how the ASP program evaluates random failures today in its internal-faults precursor studies).

2) If the CDP for the relevant accident sequence exceeds the CCDP criterion of 1.0×10^{-6}, the sequence should be retained, studied, and documented. Otherwise, it is screened out.

4.6.2.2. Group 2: nuclear plants that do not have a fire-PRA model.

For these plants, the absence of a fire-PRA model makes it impossible to analyze the safety significance of a random failure for fire sequences. The only guidance to offer is to admonish the ASP analyst to apply expert judgment to ascertain whether an important safety issue seems to emerge. The important issues for the ASP program have been defined [Minarick, 1990; NRC, 1994a] and should constitute the guidelines on the development of questions for application of expert judgment. While this is far short of an analysis, it can sometimes produce useful insights.

An example would be as follows: suppose that a particular random failure, as reported in an LER, had compromised the operation of one entire train of a two-train safety system for a very long period of time (for example, for an entire year) before it was discovered. One can postulate a fire at a location that would compromise the entire other train, thereby disabling the entire two-train system. Expert judgment can be used to ascertain whether this situation is likely enough and/or serious enough to merit ASP-type analysis.

Such analysis would then require either adapting a generic fire-PRA model to the particular plant, or adapting the plant-specific internal-faults PRA to the fire situation. Neither task is easy or unambiguous except with much effort.

4.7. Rationales applied on the development of the methodology.

4.7.1. Three-step screening/analysis process

Careful thought was given to why a three-step screening/analysis process is best. The rationale is as follows:

The initial step (step 1) in the screening for fires has been structured so that it does not involve any analysis: rather, it involves only checking the information in the LER against a short list of easily determined facts. As such, it is intended to be quick, easy, and uncomplicated. Most LERs that involve fire issues will be screened out at this stage.

Because a full analysis of each remaining LER would be costly and complicated, it is not feasible to recommend such analysis before doing an intermediate step (step 2, preliminary analysis), which involves a certain amount of conservative analysis but does not involve nearly the expense nor the specialized expertise that the full analysis would entail. The decision has therefore been made to perform preliminary step-2 analysis, which it is expected will not only **(i)** screen out a significant fraction of the LERs that survive after step 1, but will also **(ii)** provide some technical insights that can guide the ASP analyst to use resources for the step-3 analysis better.

4.7.2. Existing Models: Use of existing PRA fire models.

The fire ASP methodology guidance here assumes that plant-specific fire PRA analyses or their equivalent exist for every plant. This assumption is based on the observation that all U.S. plants should complete an

IPEEE fire review by the middle of 1997. It is assumed that these models, or their equivalent, are available to the ASP analyst. In the guidance herein, it is explicitly assumed that these PRA-type models, and the data bases that were used to support them in the IPEEE reviews, can be employed by the ASP analyst himself/herself, that they can be used directly, that certain of their inputs and structures can be altered/manipulated, and that sensitivity studies can be performed to obtain the ASP insights sought herein.

Especially for plants that did not perform a full-scope PRA, for example, plants that used a FIVE approach for reviewing fires, the availability of the plant-specific models and their full supporting documentation is essential. Because the FIVE approach is essentially a screening method, the documentation as to what was screened out, and why, is central to their applicability for ASP-type reviews as discussed herein.

4.7.3. Systems screening criteria for step-1 screening

The step-1 system screening for fire LERs uses four criteria. The rationale for choosing these four is that they are essentially the same criteria as are used by the traditional ASP methodology [Minarick, 1990; NRC, 1994a] in the initial screening of LERs that report internal plant faults.

It is recognized that perhaps an LER containing a fire issue might have a CCDP above the 1.0×10^{-6} cut-off and still be screened out by these criteria. While this cannot be ruled out it is judged to be very unlikely.

4.7.4. Non-fire failures

Plants with a fire PRA: For plants with a fire PRA, the appropriate way to examine non-fire failures reported in an LER would be to re-run the plant-specific fire PRA with these failures included. Such an analysis would be in agreement to how the current ASP program evaluates such failures in the context of internally-initiated accident sequences. This is therefore the appropriate guidance.

One problem with this guidance is that most LERs that report safety-equipment problems involve what are called here "non-fire" failures, namely failure modes or other problems with ordinary equipment. Thus, the analysis of all of these LERs using the fire PRA models would pose a very large resource burden on the ASP program. While this is true, it is also worth recognizing that a reasonable fraction of all the plants with full-scope PRAs have cut-sets involving fire and non-fire failures, among the important cut sets. To ignore the potential contribution of such cut sets would not be correct. Therefore, their analysis is included here.

Plants without a fire-PRA model: For these plants, as the text indicates in section 4.6.2, there is no feasible way to do an analysis of the significance of a non-fire failure as it might interact with sequences involving a real fire.

4.7.5. Plant-trip vs. non-trip issue and rationale for initiating-event frequencies.

The case under discussion involves an LER with a fire-related configuration compromise, that has not been screened out using the step-1 system criteria. The Step-2 analysis begins by postulating that everything in the entire co-located fire zone(s) has been destroyed by a fire. The guidance is that one should re-run the plant-specific internal-events PRA model, but with all of this equipment lost. The issue under discussion here is what to use for the initiating-event (s), and with what frequency.

There are two cases, depending on whether the postulated loss of all of this co-located equipment would or would not cause a plant trip. For cases where no plant trip would occur, the guidance is to assume a manual trip as the initiating event (see Section 4.7.9 for a detailed discussion of this point); for cases where a plant trip would occur, the analyst should use that automatic trip as the initiating event. Either way, the guidance is to use the data-base frequency of fires in the zone under consideration as the frequency of the initiating event for purposes of the step-2 analysis.

The rationale for this guidance on the frequency is as follows: the sequence of events being postulated is that a fire occurs in the zone, causing total damage in that zone. Clearly, the best indicator of fire frequency in that specific zone ought to be that zone's data-base fire frequency, taken from either the plant-specific fire-initiator data base or, if necessary, from a generic data base. This is what the guidance calls for.

There may be reasons why the data-base frequency is not appropriate such as when the configuration compromise under review would seriously affect the data-base frequency. However, that type of consideration is too detailed for step-2 preliminary analysis, and it is left for consideration if the LER survives to undergo detailed review under step 3 (detailed analysis). Substep (5) under step 3 for configuration-compromise LERs is where this review is to be done, and Subsection 4.7.7 contains a more detailed discussion of the data-base-frequency issue.

4.7.6. Rationale for starting with the internal-events PRA

The internal-events PRA involves a very wide range of equipment, some of which will have been screened out of the fire analysis because fire scenarios involving its loss in a fire would normally not be of much safety significance. If the fire scenario under review (based on what the LER reports to have been compromised by a fire-configuration problem) is in this category, then that scenario will not be found in the fire model. However, the fire problem identified in the LER may still be important, even if not modeled earlier. If so, if there is any safety role for the scenario involving this equipment, it will be found in the internal-events PRA model, either in certain of the event trees or in some of the numerous fault trees that support them. Therefore, the appropriate procedure is **(i)** to start with the internal-events PRA model; **(ii)** to identify therein the equipment that the LER reports to be potentially compromised, thereby understanding the safety role of this equipment in various accident situations; and then **(iii)** to go to the fire model and adapt into that model the fire scenario, including the insights from (ii).

4.7.7. Fire-initiation data base modifications

In step 3 for fire-configuration LERs, the fifth analysis task is to assess whether the fire configuration compromise would affect any of the fire initiation frequencies used in the base-case fire analysis, and if so, to modify the relevant frequencies. In order to accomplish this step, it is necessary to obtain the plant-specific fire-initiation frequencies, and to determine how the LER information might affect them. To do this, considerable expert judgment is needed.

Most fire LERs probably would not have a configuration compromise that would affect the fire-initiation frequency for the fire zone at issue, but it could happen, for example, if the initiation frequency depends on the amount of transient fuel, and the LER reports a very different amount of transient fuel than assumed in the data base. Another example is if the base-case fire-initiation frequency assumes certain spatial separations that are entirely different as reported in the LER.

The starting point for this reassessment could be either the plant-specific data base used in the plant's PRA, or one or another of the generic data bases currently available, including perhaps that developed under NRC support [NRC, 1986], or the EPRI data base [EPRI, 1993].

4.7.8. Class-C fire LERs

An actual example of this type of LER is the Plant-A actual-fire LER that is discussed in more detail in the case study elsewhere in this report (section 5.2), in which the actual fire was only ancillary to the main safety issues in the event. The guidance here is that if the fire did not induce any damage to safety equipment and/or did not have the potential to do so (ascertaining this latter potential requires considerable expert judgment), such LERs should be returned for ASP internal-events analysis. The reason for this is that in these cases there is no apparent basis for further fire-related accident analysis. The fire is, as in the Plant-A LER (section 5.2), simply and entirely a side issue of little safety significance.

However, it is helpful to the internal-events ASP analyst to develop certain information here, and some qualitative guidance is provided on this subject. The guidance in the main text is self-explanatory; its rationale is that the fire-ASP analyst is in a better position than the internal-events ASP analyst to develop this information.

4.7.9. Manual trip assumption

This case is that of an LER reporting an actual fire is being subjected to step-2-E analysis (sub-task 4), or a configuration-compromise LER is being subjected to Step-2 analysis (subtask 3A). In either case, the analysis has reached a stage where the analyst finds that **(i)** for a real-fire LER, a plant trip did not occur, and the analysts have determined that one would not have occurred assuming that everything in the entire fire zone in which the actual fire occurred were destroyed; or **(ii)** for a configuration-compromise LER, a plant trip would not have occurred under the postulated total damage in the affected-zone conditions.

The guidance is to assume a manual plant trip, and then to proceed with the ASP analysis of CCDP for that plant trip. The rationale for this manual-trip assumption is that given the damage by fire of everything in the zone, and given that, with the assumption of this damage, the LER was not screened out using the step-1.

Figure 4.4.1. Sheet 1 of 4. Fire configuration LER

Methodology of analysis for a fire configuration LER.

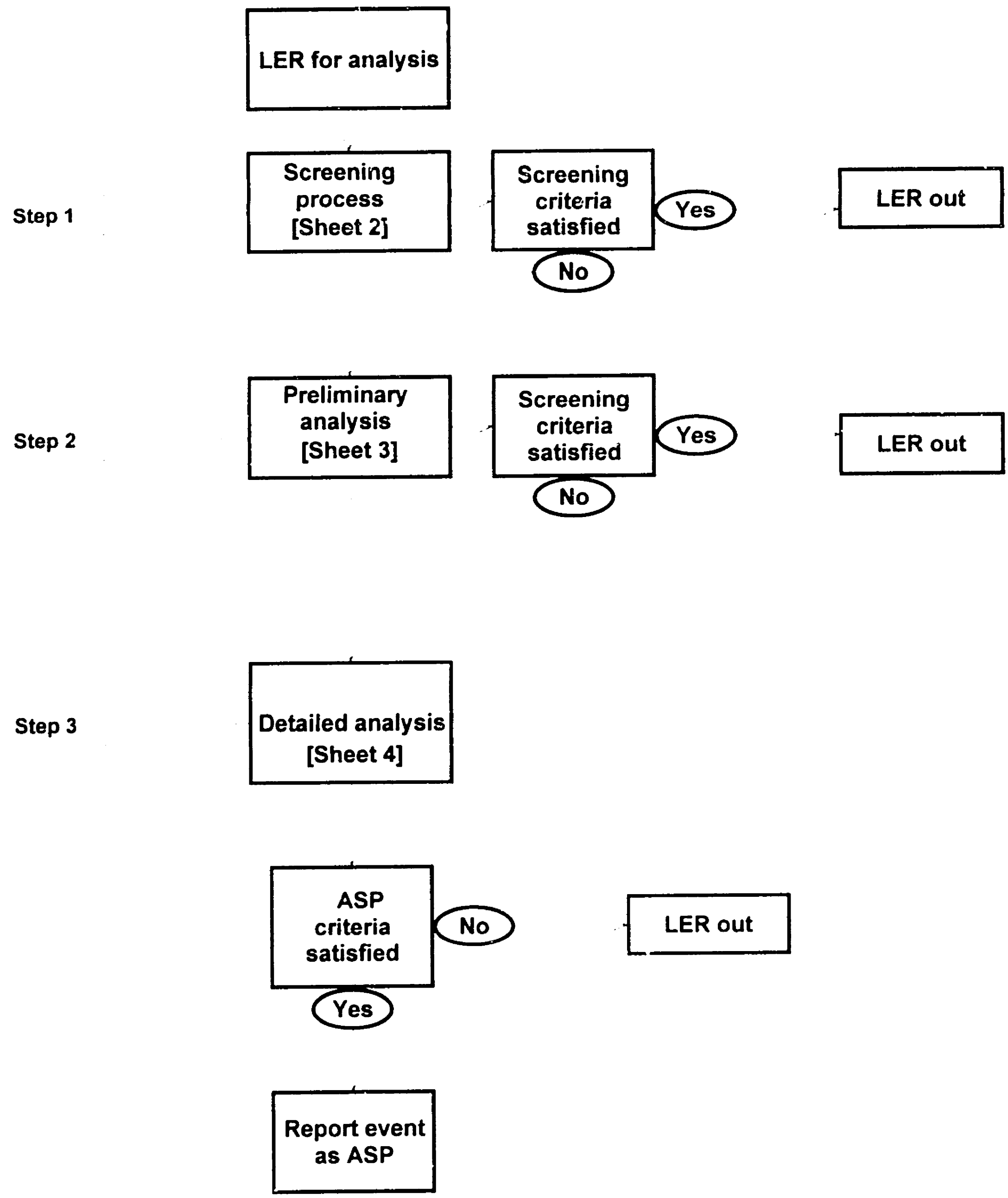


Figure 4.4.1. Sheet 2 of 4 . Fire configuration LER

STEP 1. Screening process for a fire configuration LER

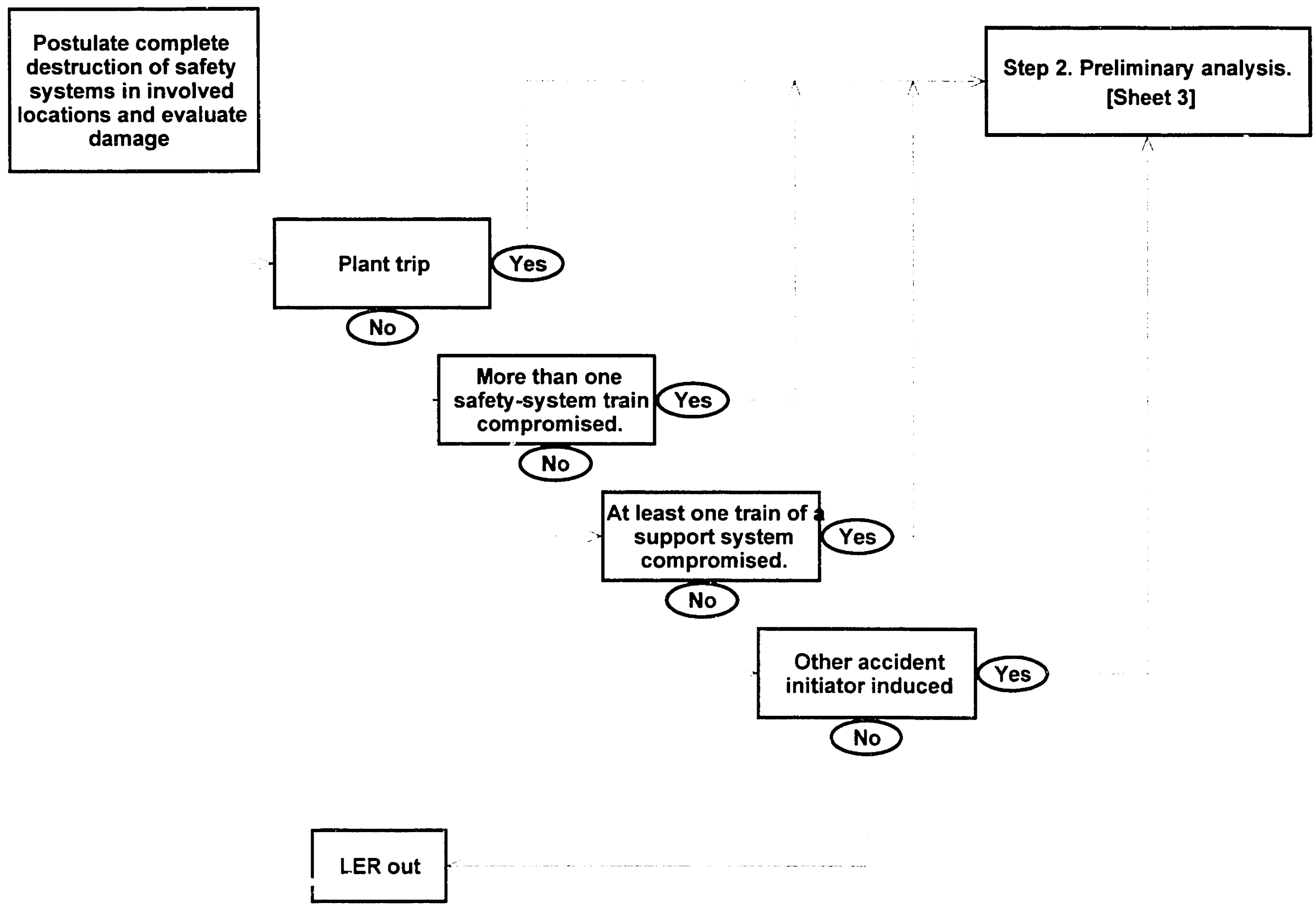


Figure 4.4.1. Sheet 3 of 4. Fire configuration LER

STEP 2. Preliminary analysis for a fire configuration LER

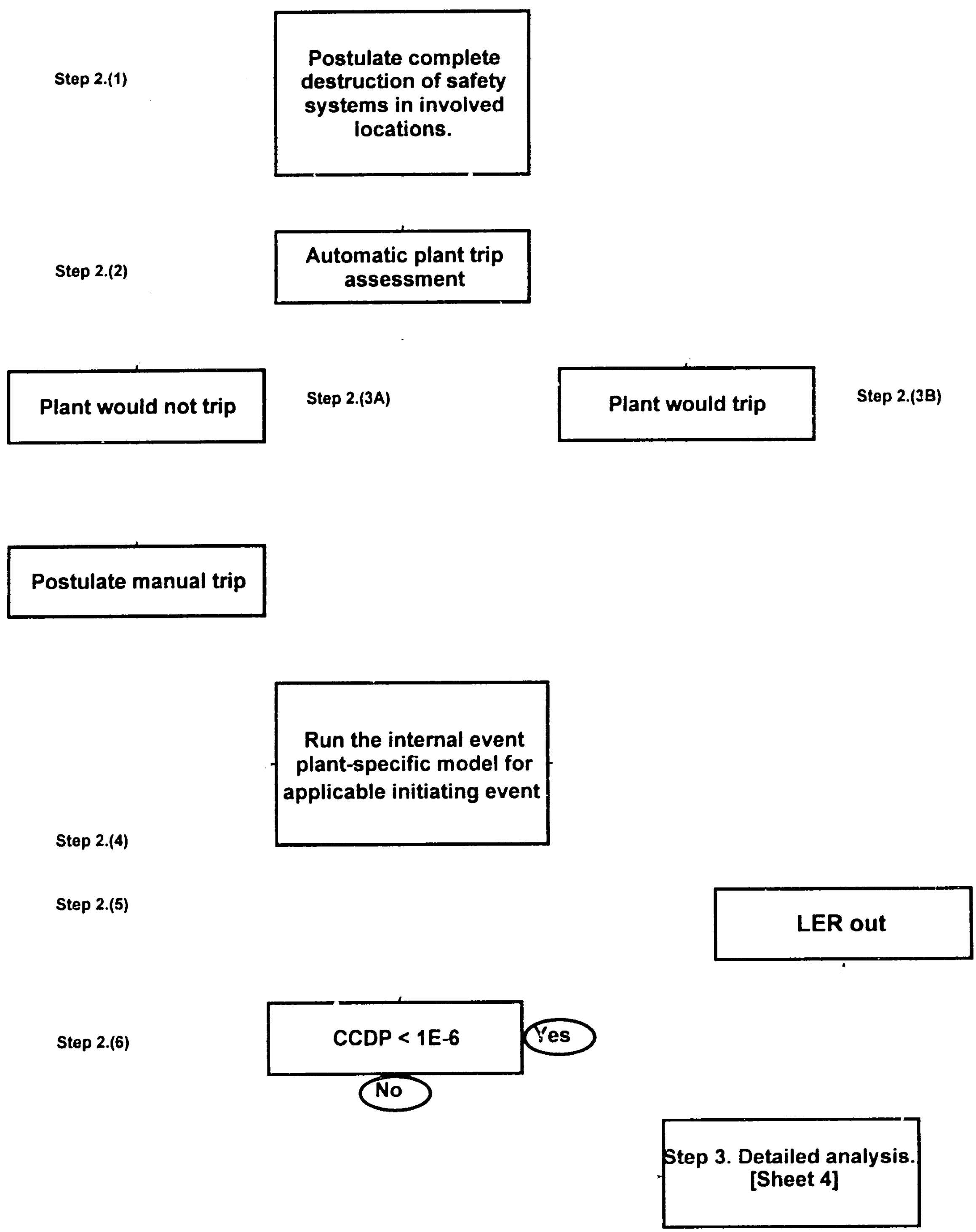


Figure 4.4.1. Sheet 4 of 4. Fire configuration LER

STEP 3. Detailed analysis for a fire configuration LER

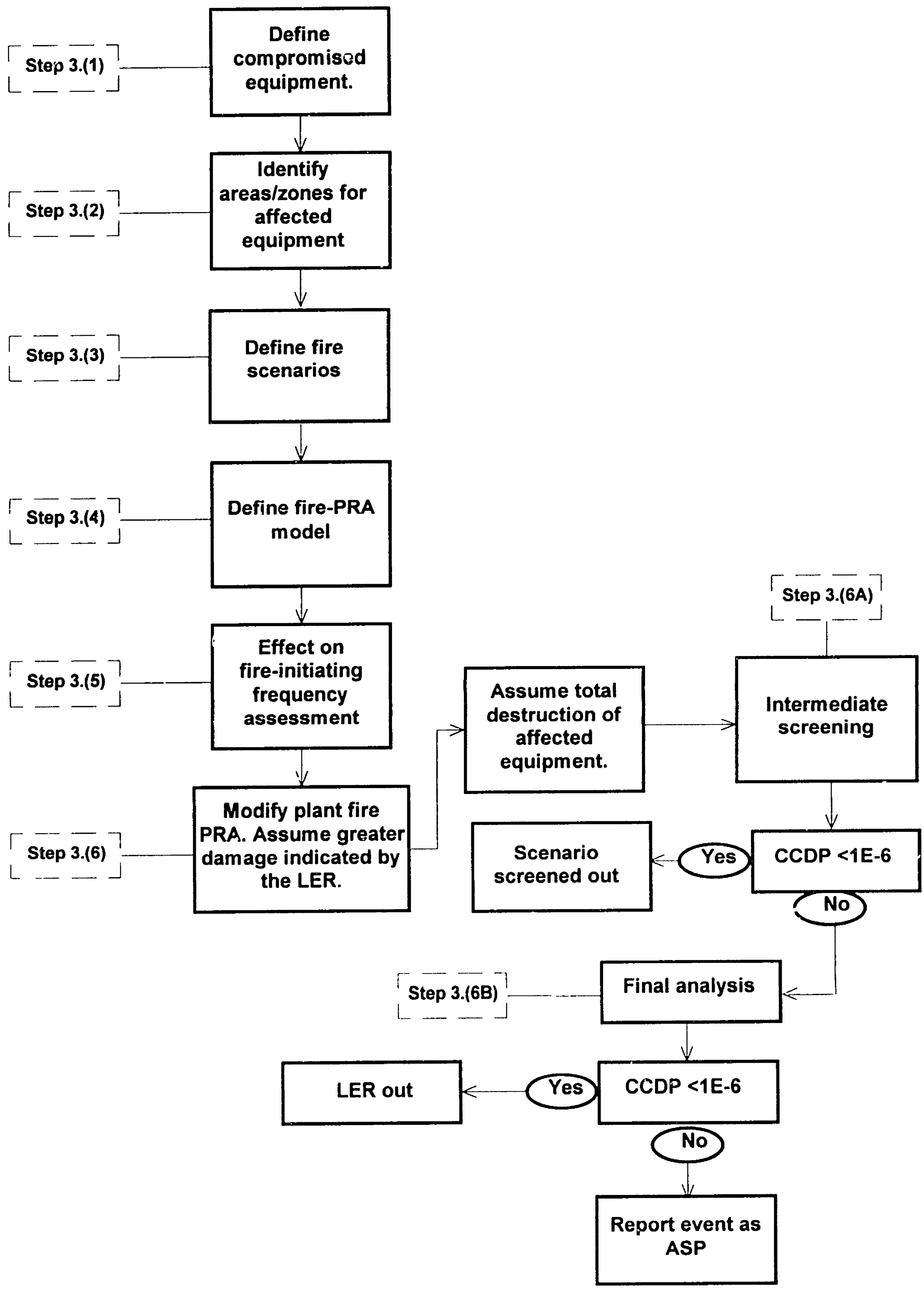


Figure 4.5.1. Sheet 1 of 6 . Actual fire LER

Methodology of analysis for a fire reported in an LER.

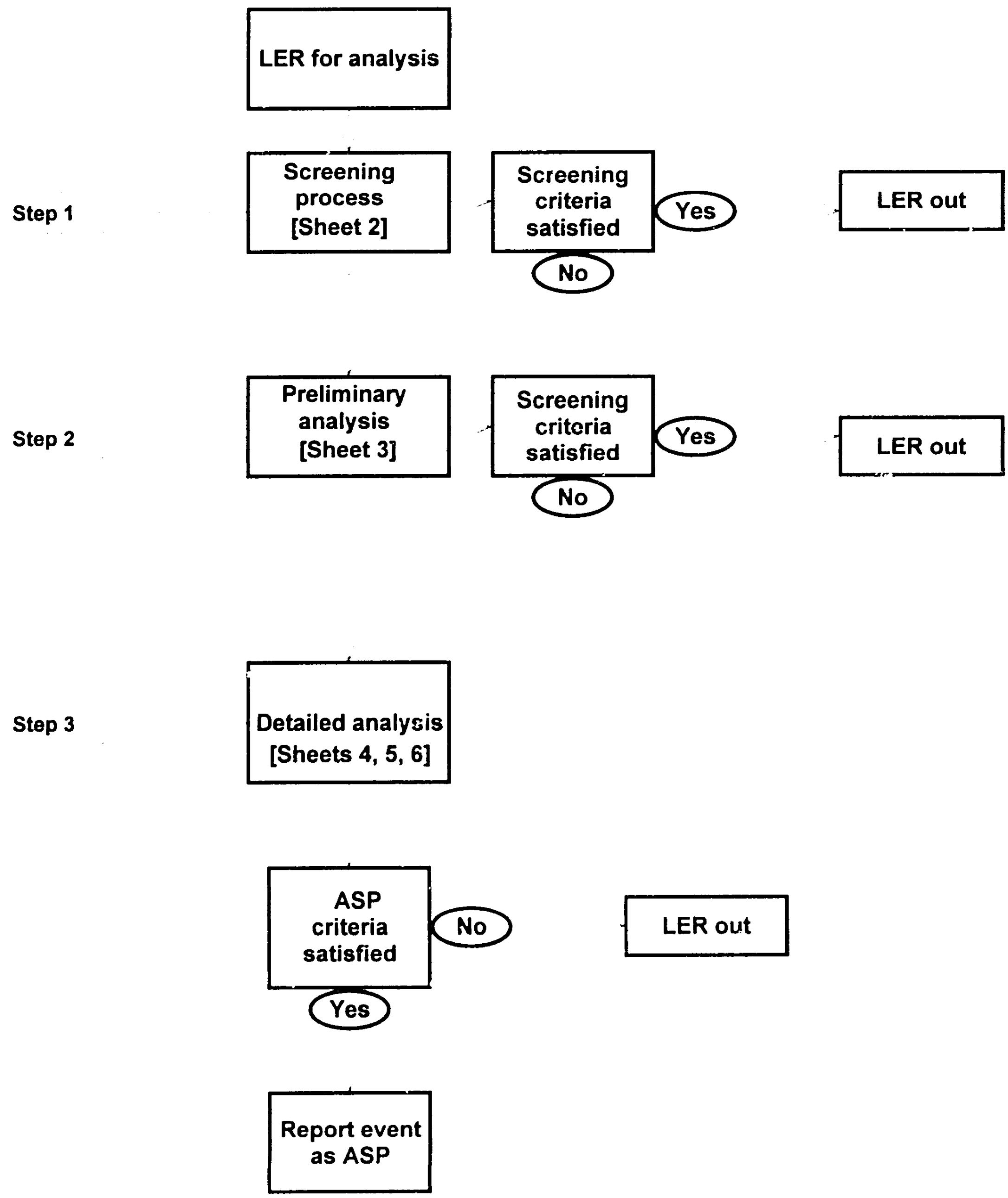


Figure 4.5.1. Sheet 2 of 6 . Actual fire LER

STEP 1. Screening process for a fire reported in an LER.

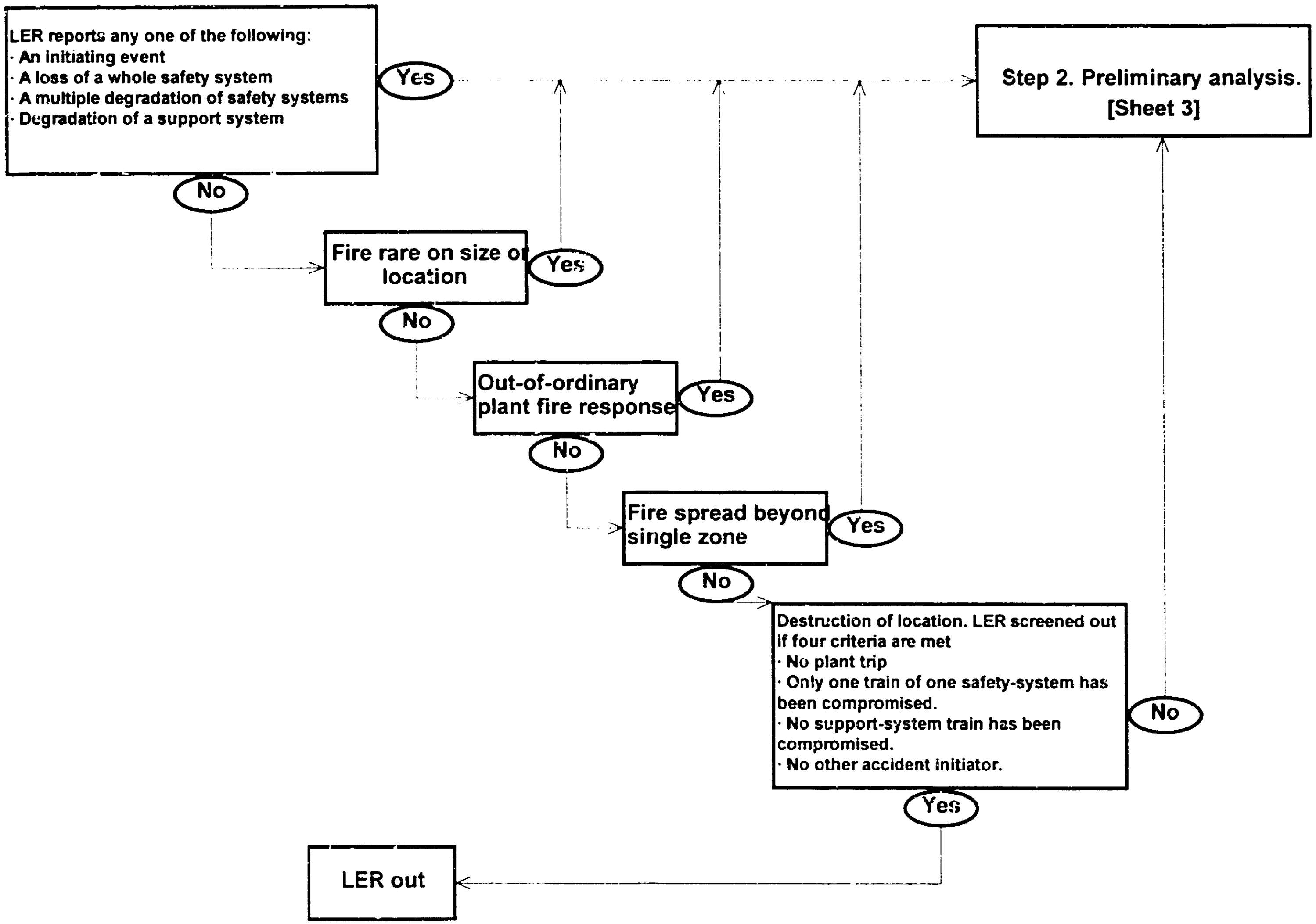


Figure 4.5.1. Sheet 3 of 6. Actual fire LER

STEP 2. Preliminary analysis for a fire reported in an LER.

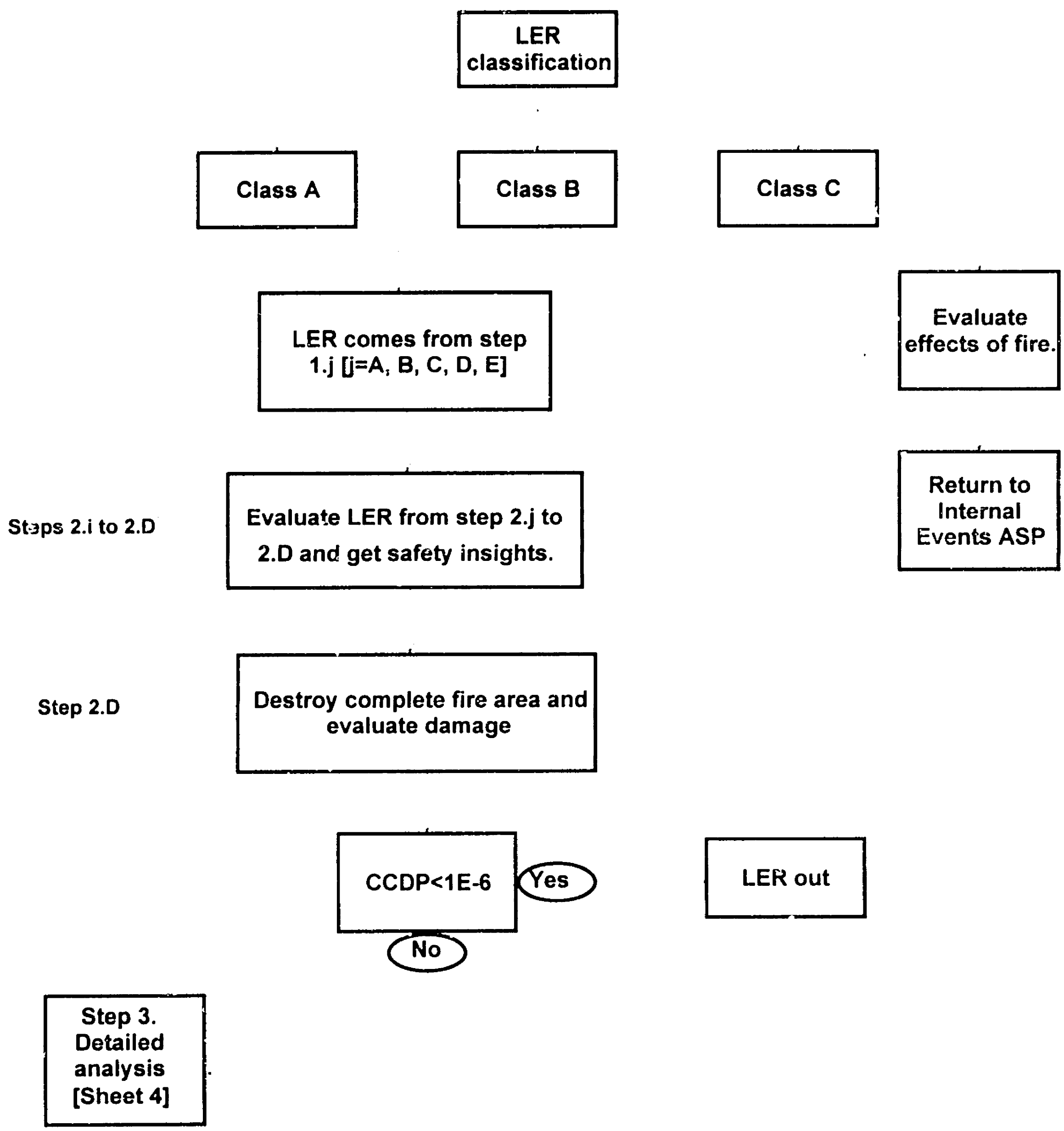


Figure 4.5.1. Sheet 4 of 6. Actual fire LER

STEP 3. Detailed analysis for a fire reported in an LER.

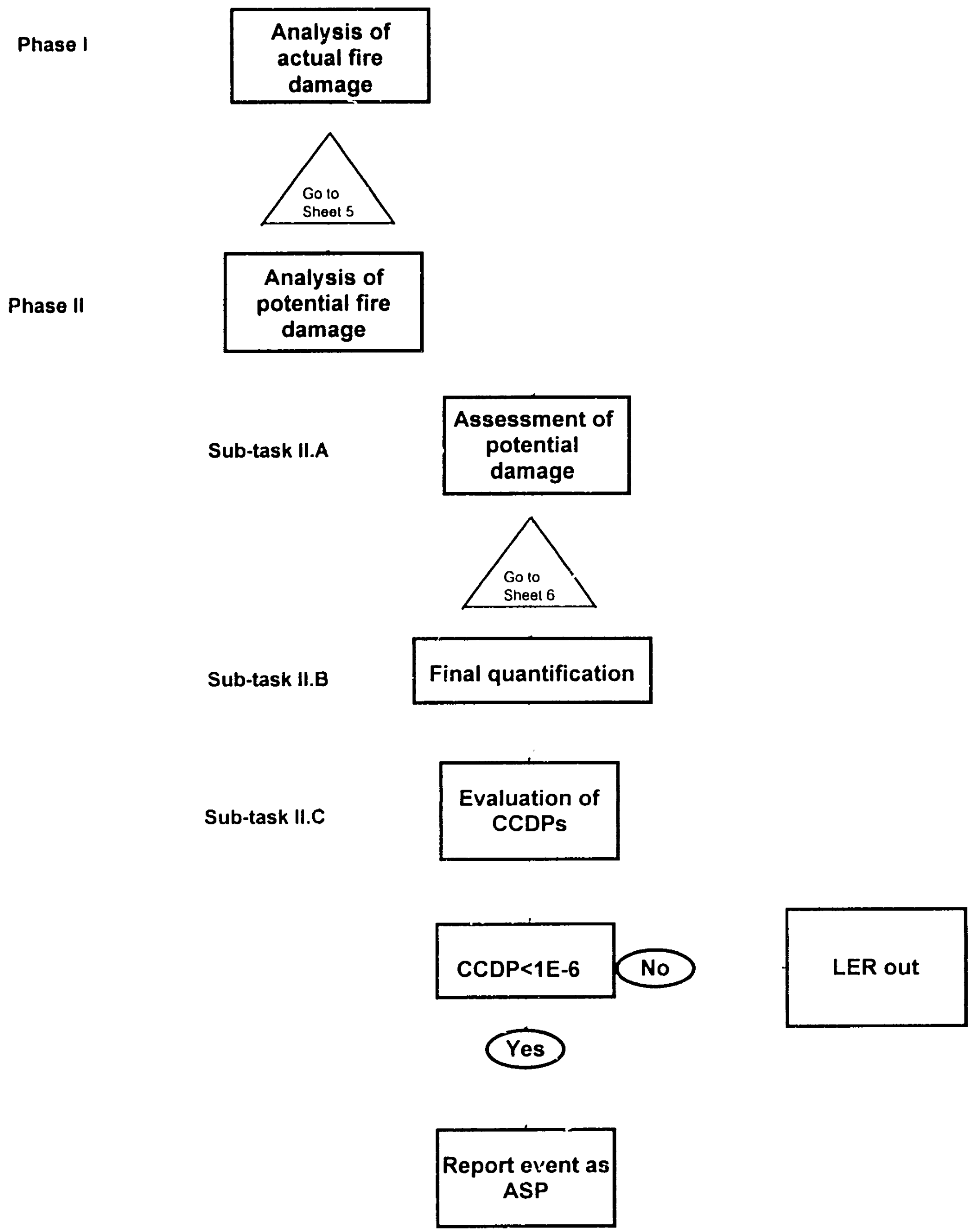


Figure 4.5.1. Sheet 5 of 6. Actual fire LER

STEP 3. Phase I. Analysis of actual fire damage.

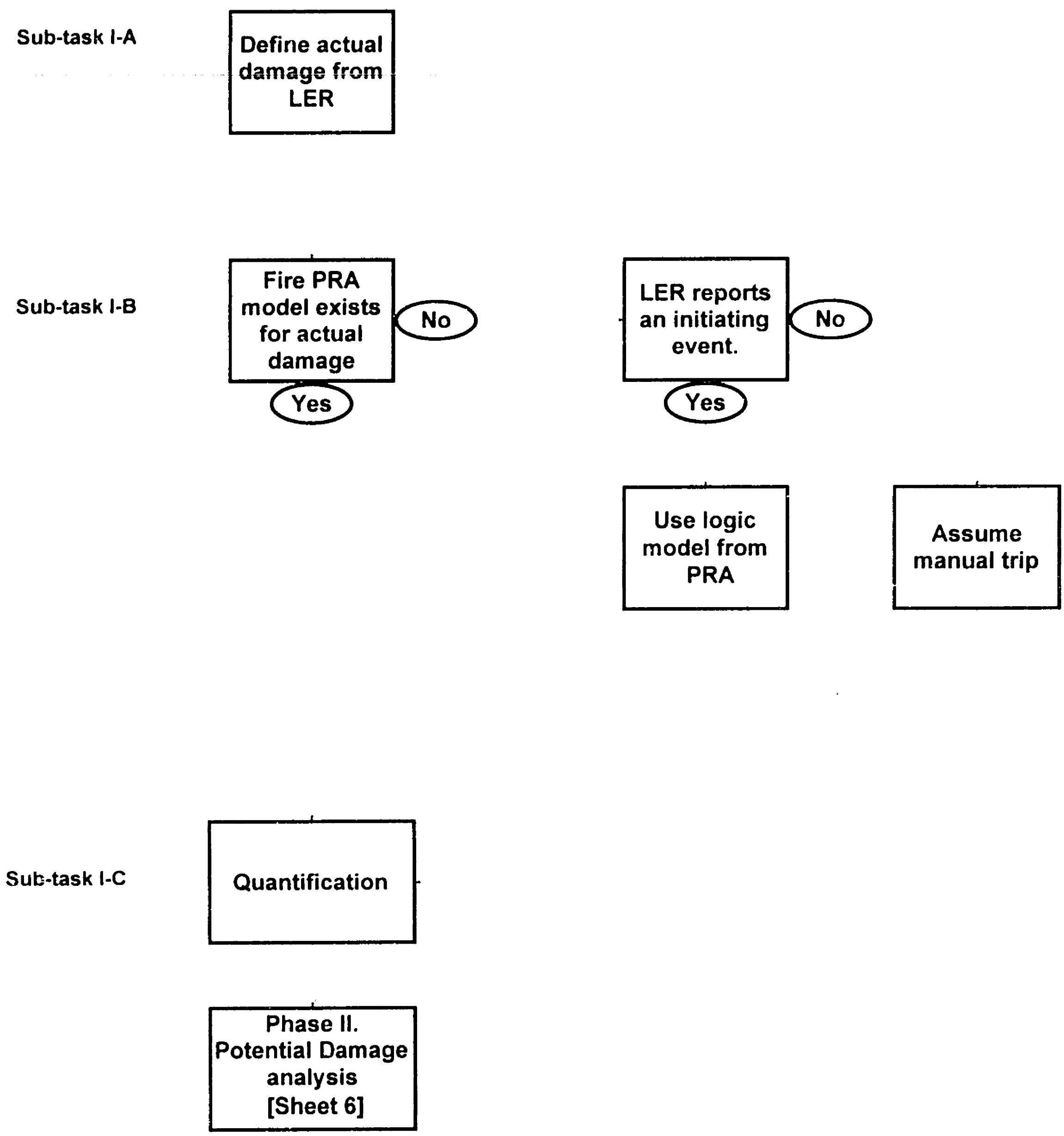


Figure 4.5.1. Sheet 6 of 6. Actual fire LER

STEP 3. Phase II. Sub-task II.A. Assessment of potential fire damage.

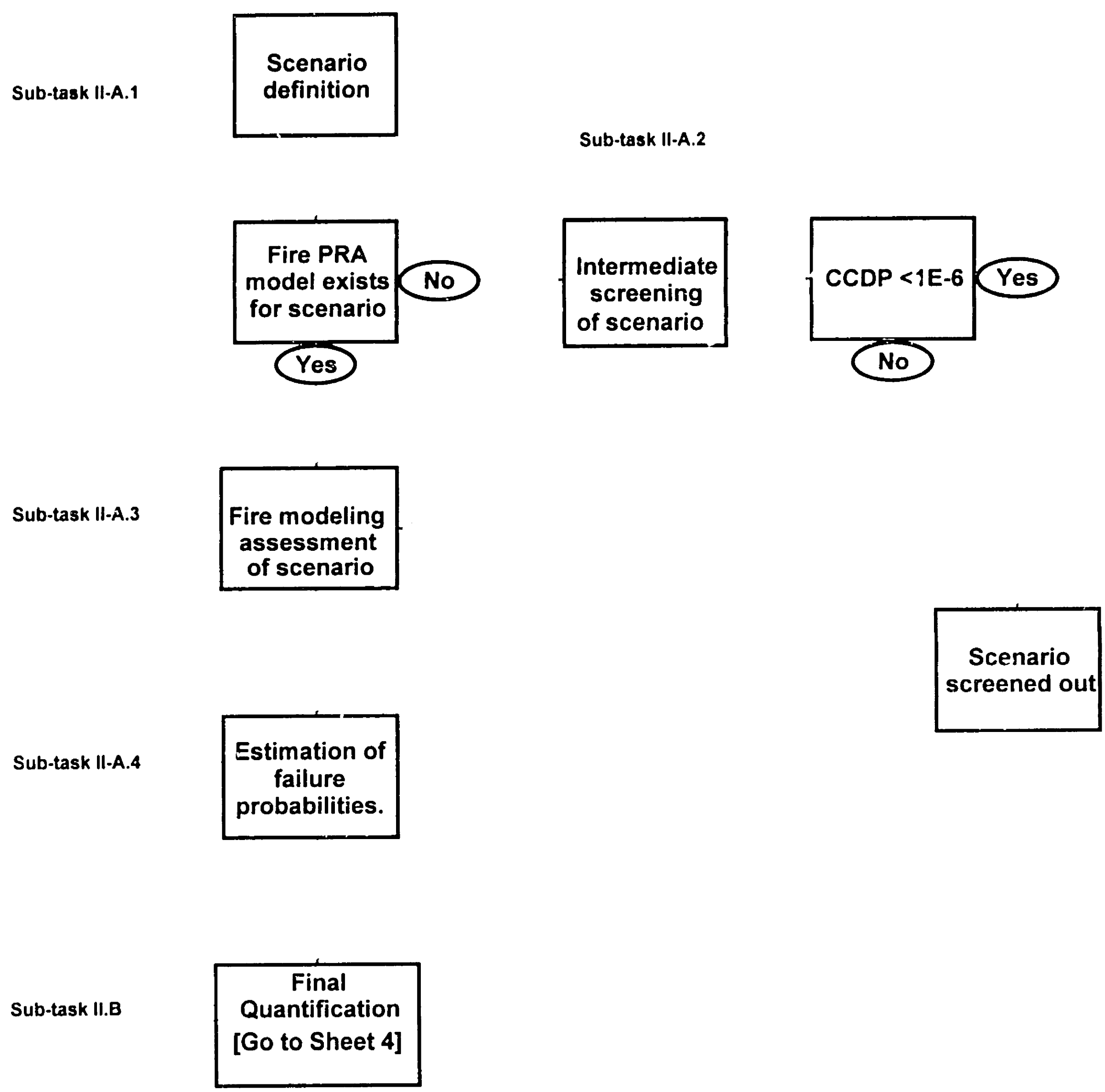
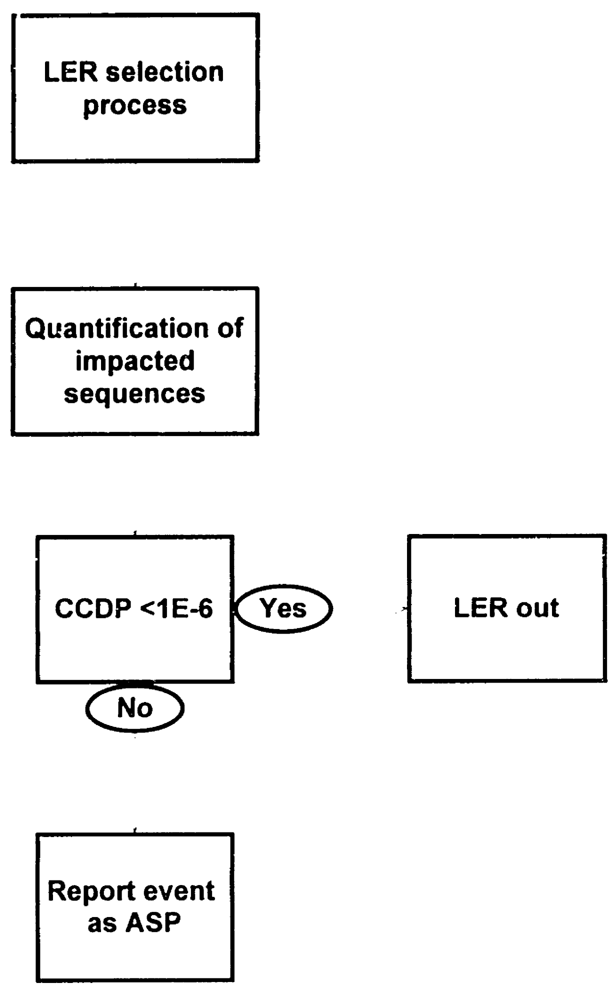


Figure 4.6.1. Sheet 1 of 1. Non-fire failure LER

Methodology of analysis for non-fire failures.



Chapter 5. Case studies

5.1. Introduction

This chapter will introduce and then discuss three "case studies" to illuminate how precursors to fire-initiated accidents, as reported in an LER, can be analyzed using the ASP methodology presented in Chapter 4 of this thesis.

The three case studies cover different aspects of the ASP fire-precursor methodology, and are keyed to the three separate discussions of fire-LER guidance in sections 4.4.1 (guidance for a fire-configuration-compromise LER), 4.4.2 (guidance for a real-fire LER), and 4.4.3 (guidance for a non-fire-failure LER).

The case study involving a real fire is taken from a 1995 LER reported by a Pressurized Water Reactor [PWR] (see Section 5.2 below), in which a fire was caused by a defective automatic fast power transfer.

The case study involving a fire configuration compromise is taken from a 1989 LER reported by a Boiling Water Reactor [BWR] (see Section 5.3 below), involving a potential for a fire in the cable-spreading room to produce a spurious opening of certain valves leading to possible overpressurization of the low-pressure piping.

The case study involving a non-fire failure is taken from a 1994 LER reported by a BWR (see Section 5.4 below), involving the long-term unavailability of the High Pressure Coolant Injection system [HPCI], whose unavailability could make the plant more susceptible to fire-initiated accidents than would otherwise be the case.

It is important to recognize up-front that the actual safety issues reported in these LERs have long since been resolved: no safety issues exist today. These LERs were chosen because they provide useful tutorial examples for the case-study purposes here. The selection of these LERs was done solely to fulfill this tutorial objective.

Note that, in order to keep the focus of the case studies on the methodological guidance, it has been chosen to keep the actual nuclear-plant names anonymous. In the case studies four plants are involved, which are called Plants A, B, C, and D.

5.2. Case study: A fire as a real incident

5.2.1. Summary

Plant A is a Westinghouse PWR with a large dry containment. In late 1995, there was an electrical grid transient in a switchyard near the Plant A nuclear power plant. The actuation of an oversensitive relay resulted in a generator lockout and an automatic fast transfer of power from the main generator to offsite power

The transfer was deficient and caused a reactor trip and a fire. A fire resulted due to large currents on bus 3A2 that was fed simultaneously by the main generator and offsite power. These power sources were out of phase. Under normal conditions the unjustified signal of transfer should not have caused an incident. The root of the problem was a deficiency in the fast transfer.

Given that the LER reports an initiating event (a trip), the LER was screened in during the initial screening process and was selected for further analysis. In the preliminary analysis, it was concluded that the fire reported in the LER neither induced damage nor had the potential to affect safety-related equipment in the location involved. Therefore, the LER was finally screened out from further evaluation. However, given that the LER reports several out-of-the-ordinary situations regarding the suppression activities and the presence of smoke, this analysis evaluated the event anyway from the fire point-of-view and some recommendations were developed as part of the application of the methodology.

5.2.2. Event Description

5.2.2.1. The transfer from onsite to offsite power

The expected action for the transfer is the following: each Unit Auxiliary Transformer [UAT] feeder breaker opens and simultaneously the corresponding Startup Transformer [SUT] feeder breaker closes, transferring power from onsite to offsite.

According to the simplified AC system scheme shown in Figure 5.2.1, the following transfers were expected:

- Train A: From UAT 3A to SUT 3A for buses 3A1 and 3A2.
- Train B: From UAT 3B to SUT 3B for buses 3B1 and 3B2.

The transfer was deficient for the A train, for both buses.

a) Bus 3A1: In the 3A1 bus [6.9 kV], the UAT feeder breaker (henceforth UA1) opened as expected and the SUT feeder breaker (henceforth SA1) failed to close, due to a random failure. As a result, bus 3A1 was lost, with the subsequent loss of the Reactor Coolant Pumps [RCPs] 1A and 1B, leading to a reactor trip due to RCP low flow. In addition, losses of the condensate pumps A and C and circulating pumps A and C occurred. Also, an auxiliary-relay random failure resulted in a false indication, preventing the operating staff from knowing about the loss of the 3A1 bus.

b) Bus 3A2: In the 3A2 bus [4.16 kV], the UAT feeder breaker (henceforth UA2) opened too slowly, while the SUT feeder breaker (henceforth SA2) closed as expected. During a fraction of a second (0.3 sec.) both feeder breakers remained closed, in overcurrent condition. As a consequence of the overcurrent, the breaker UA2 was destroyed and the breaker SA2 was open. The ultimate consequence was the loss of the 3A2 bus, a partial loss of offsite power and the start and run of the electrical diesel generator [EDG] A. The destruction of the breaker UA2 produced a fire and subsequent smoke in the Turbine Generator Building [TGB] Switchgear Room.

5.2.2.2. Chronological description of fire.

- t=0 . Lighting arrester electrical fault on nearby 230-Kv/345-Kv substation. Reactor trip.
- t=1. Fire and smoke are automatically detected by a group of system detectors located in the TGB switchgear room.
- t=8. Smoke coming from the TGB switchgear is reported by a TGB operator. Two auxiliary operators are sent to verify the problem.
- t=37. Fire is reported as occurring above the 3A2 switchgear and declared.
- t=37. Suppression activities are initiated by the plant fire brigade.
- t=47. An unusual event is declared because the fire was not extinguished within 10 minutes.
- t=60. Local fire brigade arrives on site. Portable dry chemical extinguishers are not effective in combating the fire.
- t=84. Following water application with a nozzle, the fire is apparently extinguished. A forced entry into the interior of the affected switchgear is initiated. A reflash occurs, requiring additional water application.
- t=135. The fire is officially extinguished. The time from detection to total suppression was about 134 min., i.e., about eleven times longer than 12 minutes estimated by the plant in its fire analysis.

5.2.2.3. Other relevant operational events.

1. Detection of fire/smoke

The control room operators received a notification of fire/smoke at t=1 from the automatic detection system. Simultaneously, alarms for the scram were received. In addition, a verbal notification about smoke was given at t=8 and a phone notification occurred at the same time, from different personnel.

2. Fire declaration delay

In spite of the alarm notifications for fire/smoke and the reports of smoke, the control-room operators did not declare a fire until the visualization of flames. The firefighting procedures and station policies did not specify when a fire should be declared. Therefore, the fire declaration was left to the judgment of the control-room supervisor. Based on a previous experience, the operators estimated that a fire resulting from an electrical fault would rapidly burn out and produce the smoke being observed.

3. Delay in entering to EOP "Loss-of-offsite-power recovery" after the verification of electrical bus status.

At t=0, due to the scram, the operators entered emergency operating procedure OP-902-000, "Emergency Entry Procedure", consisting of some immediate steps and some diagnostic steps. One of the immediate steps is the verification of safety-related buses (3A3-S, 3B3-S, 3AB3-S) and one of the diagnostic steps is the verification of non-safety-related buses (3A1, 3A2, 3B1, 3B2).

Regarding the verification of the status of the electrical bus, the immediate steps were completed. During the diagnostic steps, the verification of the 3A1 bus loss, source of the trip, was not correctly performed and the deenergization status of the bus was not detected. Given the failure of the auxiliary relay on the 3A1 bus, described earlier, the indications for the loads of the bus, RCPs 1A and 2A, condensate pumps A and C and circulating pumps A and C remained lighted. During that step the following errors were committed with the results that the status of the 3A1 bus and the subsequently decreased coolant flow were not detected:

- The "open" indication light for SUT 3A1 feeder breaker was missed.
- The backup indications for RCP status (loop differential pressure and RCP amperage) were not used. These would have allowed the operating crew to

acknowledge the status of some RCPs and to relate it to the loss of the 3A1 bus.

4. Failure to complete an immediate step of the EOP

The closure of the Moisture Separator Reheater [MSH] control valves to a required post-trip position is one of the immediate steps in the EOP. The operator in charge of the step was directed to the TGB switchgear room, to investigate the smoke. The operator judged that it was unnecessary to notify the control room that the step had not been completed. On the other hand, the control room personnel judged the investigation of the fire to be a high priority and did not send another operator to complete this immediate step. In this case, the out-of-position valves had no effect on reactor operation.

5.2.3. Additional information regarding the incident

5.2.3.1. Effects of the fire.

The fire damage was limited mainly to the UAT feeder breaker supplying the 3A2 non-safety-related bus and the adjoining meter cabinet. The root cause of the fire in the 3A2 switchgear was the improper automatic bus transfer from the UAT to the SUT.

Two switchgear cabinets were heavily damaged by the fire. The insulation on the bus duct from the UAT to bus 3A2 was completely consumed by fire over the approximately 10-feet vertical run where the cables entered the switchgear cabinet. Damage to the horizontal run of the cables appeared to be confined to the plume: that is, there did not seem to be any horizontal propagation.

The cable bus duct for the SUT feed to bus 3A2 [the offsite power feed] is stacked above the UAT to 3A2 bus duct. Damage to the SUT to 3A2 cables was limited to external heat damage to the insulation. Subsequent testing of these cables verified that continuity and insulation were intact. No other significant damage was found. Therefore, the fire damage was limited to the UAT to 3A2 feeder breaker (fire source) and the surrounding cables. The UAT to 3A2 feeder breaker had already been destroyed by the overcurrent, and the fire did not cause damage which could compromise other component or cables.

5.2.3.2. Effects of the smoke

In general, smoke may have two effects: a physical and a psychological one. The physical effect is preventing some action from being performed in the affected location. This refers to situations when smoke obscures some location, affecting actions involving components or elements. The psychological effect is the inducing of human errors or actions no related to smoke-affected locations. This refers, for example, to changes in priorities that could allow or force a procedure to be delayed, dismissed or not completed.

The following are the conclusions about the effects of smoke on the incident, after the reactor trip and partial loss of offsite power were produced, that is, on the significant events identified.

1. Fire declaration delay.

It is judged that the delay of fire declaration should not be attributed to the smoke, even though it hid the presence of flames. The operators had the fire notification from the automatic detection system and even though the policies of the plant regarding a fire declaration did not provide adequate guidelines, the human error was the predominant factor on the delay. Basing the non-declaration on past experience was, in this case, an incorrect decision.

2. Delay on entering EOP "Loss of offsite power [LOOP] recovery".

According to the description of the event given earlier, the crew did not verify correctly the electrical bus status and did not make use of the backup indicators for the loss of RCPs. The delay in that diagnostic step (verification of non safety electrical buses) is judged not to be related to the presence of smoke.

3. Failure to complete an immediate step of the EOP "emergency entry procedure".

This event, according to the plant A event report, was the consequence of the change of priorities made by the control-room personnel due to the presence of smoke. Therefore, it is judged that the smoke played a psychological role in this event. However, the fact that an operator was sent to perform this immediate step but did not complete it is judged to be a human error.

5.2.4. ASP fire review of the case study.

5.2.4.1. Step 1. Screening process.

The LER should be initially screened in, because it reports an initiating event (reactor trip) among the events involved during the operational event. Therefore, step 1-A indicates that the LER should be passed on to step 2, preliminary analysis, specifically to step 2-A.

5.2.4.2. Step 2. Preliminary analysis

1. Step 2-A. LER screened in, because it reports an initiating event.

Given the availability of more detailed information from the plant and the events reported in the LER, the ASP analyst should evaluate the role of the fire in the whole situation, considering the possibility that the fire could have been incidental to the simultaneous occurrence of the other events and also the fire's potential to induce damage in safety-related equipment. If the analyst were to demonstrate that the fire was, in fact, incidental and did not have the potential to affect safety-related equipment, the LER may be screened out in this step.

If it were screened out, the LER should, nevertheless, be passed back through the rest of the steps of the screening process and the analyst should evaluate the events from a fire-analysis point of view and document the lessons learned.

a) Analysis of the LOOP

During the time that the UA2 and the SA2 feeder breakers were closed, the overcurrent caused the former to fail and the latter to open. Once the UA2 feeder breaker was destroyed, the fire was initiated. According to the evaluation of damage in the TGB switchgear room, the fire did not affect the SA2 feeder breaker or cables. For this reason, it is concluded that the partial LOOP was caused by the destruction of the UA2 feeder breaker and not by the resulting fire.

b) Analysis of the trip.

The cause of the trip was the loss of the 6.9 kV Bus 3A1. The loss of this bus causes reactor trip on low RCP speed. Since safety related equipment is powered by a separate 4.16 kV line, the failure of the bus 3A1 does not affect other safety related equipment. The low RCP speed, caused by RCP speed sensed at less than 96.5 % of rated flow, induces a signal of Departure from Nucleate Boiling Ratio [DNBR], which trips the reactor. In the present case, 2 out of 4 RCP pumps were lost.

From the analysis performed, it is apparent that the fire was incidental to the other reported events. That is, the reactor trip as the initiating event and the partial LOOP were not related to the existence of the fire in the plant. Both the initiating event and the partial LOOP are internally-induced events and therefore they should be evaluated accordingly. The fire was a consequence of these events and did not either induce damage or have the potential to induce damage that could have increased the risk from the loss of safety-related equipment.

However, given that the LER also reported problems related to fire detection and suppression and also given the presence of smoke, and considering that such out-of-ordinary situations should be considered for further, the LER should be analyzed in order to obtain safety insights and recommendations from the point of view of fire analysis.

5.2.5. Analysis of problems related to fire.

5.2.5.1. Detection: Declaration of fire incident.

Suppression activities depend strongly on adequate detection. In the present incident, the automatic detection system worked as expected, but the human response was inadequate, so that the fire detection was ignored. Even though the volume of the sound alarms was decreased by the presence of a tape layer over some alarm annunciators, a light signal for fire was available in the control room and was not used by the operators.

The non-declaration of a fire incident, in spite of alarm actuations, a report of smoke from the TGB operator and a phone report of smoke from the Generation Service Building is considered a human error. The personnel in charge based their decision on previous experience. The operator placed inappropriate emphasis on the visual observation of flames. This turned out to be incorrect.

5.2.5.2. Suppression

One of the most important deviations from the plant's IPEEE fire analysis is the effective duration time of the fire. As discussed above, the suppression activities took almost eleven times as long as the time considered by the IPEEE (134 minutes compared to 12 minutes).

Even though this particular event demonstrated that the extensive time did not cause damage to other components or cables beyond the immediate area of the source, it is judged that the assumed 12 min. may not be realistic and it should be revisited.

According to the analysis of the report, there was evidence of the following fire-brigade-training problems during the incident:

- Lack of adequate training on what to do before the leader arrives, which complicated the tasks of ventilation.
- Insufficient training or lack of training for fighting fires in areas such as a run of cables where it was difficult to apply the extinguishing agent and the residual heat was concentrated.

5.2.6. Results

The fire was not a cause but a consequence of the events at plant A and did not have any relationship to the loss of offsite power. The damage from the fire was limited to the already failed UAT to 3A2 feeder breaker and associated cables to 3A2 bus. No other damage was induced.

The presence of smoke in the plant made the incident more confusing to the crew and caused it to change priorities and act erroneously. However, all of the problems caused by the fire (fire-declaration delay, delay in entering the EOP and failure to complete one step) depended strongly on human error, but not on the presence of smoke and apparently none of these had important consequences.

The unexpectedly slow response of the fire brigade probably contributed to more extensive switchgear damage that would have otherwise occurred. However, the damage was limited to the 3A2 UAT and surrounding cables, and other already-failed components (3A2 UAT feeder breaker).

It is judged that in this incident, the fire did not contribute significantly to the sequence of events. First, the fire did not cause any direct impact on the safety of the plant during the development of the incident. The problem reported is completely attributable to other non-fire events. However, the event demonstrated the problems associated with fire detection and fire-fighting procedures and the negative effects of smoke on the operators.

The present LER should be interesting from the point of view of internal events ASP, because the following situations occurred during the incident:

- A new type of initiating event, a reactor trip due to loss of the 3A1 bus, was produced. This initiator had no been previously considered by the plant among the possible initiating events.
- Problems occurred in the transfer from onsite to offsite power, due to an internal failure of an oversensitive relay, thus initiating the incident.

This event should be returned to the internal event ASP for analysis. The internal events ASP analyst should consider the fact that the effect of the smoke on various human actions may lead to higher values of human error probabilities.

5.3. Case Study: a fire configuration compromise

5.3.1. Summary

Plant B is a General Electric boiling water reactor in a Mark II containment. One day in 1989, personnel at Plant C determined that a fire in the Cable Spreading Room [CSR] could result in the spurious opening of two high/low pressure interface shutdown cooling valves, which could result in a possible overpressurization of the low pressure piping. The root cause of this condition was determined to be the lack of detailed procedures used in performing the original safe-shutdown analysis. The reported condition was classified as a configuration compromise and analyzed in detail. The Conditional Core Damage Probability [CCDP] associated with the condition is calculated to be 5.5×10^{-6}. Therefore, the detected condition meets the criteria to be designated as an "Accident Sequence Precursor."

5.3.2. Event description

As a result of a safe shutdown analysis, Plant B personnel determined that a fire in the CSR could result in the spurious opening of the high/low pressure interface Residual Heat Removal [RHR] shutdown cooling valves (designated HV-51-1F008 and HV-51-1F009), which could result in the possible overpressurization of the low pressure piping. As a result, if both of the valves in the RHR system were to open due to fire damage, a Loss of Coolant Accident [LOCA] could occur due to the ruptured piping. Figure 5.3.1 shows a simplified diagram of the RHR system containing the interfacing system valves involved.

The reported condition was present for a long time, four years and nine months, from late 1984 to mid-1989.

As a compensatory measure, some corrective actions were implemented by the plant. The power supply breaker for the RHR shutdown cooling section, outboard containment isolation valve HV-51-1F008 was to be locked open, de-energizing the valve in the closed position whenever the reactor coolant pressure was greater than 75 psig., so that a fire in any one fire area could not cause both the inboard and outboard containment isolation valves to open spuriously and result in overpressurizing the low pressure piping.

5.3.3. Analysis

5.3.3.1. Logic model for quantification

In the compilation of accident sequences developed by Plant B through their Individual Plant Examination [IPE], the frequency of an interfacing-system [ISLOCA] was found to be far below the dominant core-damage-frequency contributors. Therefore, based on the low probability of occurrence of the sequence, an event tree was not developed originally. Given that the LER has been screened in for further analysis, the development of the logic model for quantification will be required.

1. Interfacing-system LOCA event tree development

The interfacing-system LOCA event tree is based on the mitigation features of the plant for a large LOCA and the approach for analyzing interfacing-system LOCAs for PWRs in WASH 1400 [NRC, 1975]. The ISLOCA event tree that was developed is shown in Figure 5.3.2.

The systems available at plants like Plant B to mitigate the consequences of a LOCA are [NRC, 1993]:

- High pressure coolant injection [HPCI].
- Low pressure core spray [CS].
- Low pressure coolant injection/residual heat removal mode [LPCI].
- Reactor core isolation cooling [RCI].
- Automatic depressurization system [ADS].
- Control rod drive [CRD].

<u>Assumptions</u>

The following are the assumptions made in the definition of the event tree with an ISLOCA as the initiating event:

a) It is possible to mitigate an ISLOCA. That is, it is assumed that an ISLOCA does not lead directly to core damage.

b) It is possible to close the path from the high pressure to the low pressure systems before core damage. That is, there is enough time between the ISLOCA initiator and core damage, so that an operator corrective action is possible. The path from the high-pressure side to the low-pressure side can be closed when a certain level of depressurization is reached, by isolating the damaged piping by closing at least one of the compromised RHR shutdown cooling valves.

c) The emergency coolant systems are capable of providing coolant makeup to prevent core damage. That is, it is possible to maintain the core covered before the closing of the path. If this assumption is not correct, then the LOCA leads to core damage immediately. For large LOCAs, the low-pressure systems are designed to provide enough coolant makeup and they will be used for this LOCA model.

d) The event tree for an ISLOCA, under the conditions mentioned, can be based on a large-LOCA event tree, assumed for this case to be the worst condition, considering that for this condition the volume of lost coolant is maximal.

e) It is judged that the most likely action to be performed by the operators would be the manual closing of at least one of the reported valves [Parry, 1996]. A calculation was performed based on expert judgment to work out the "likelihood of failure to close the path opened by the rupture of the low pressure piping". A conservative value of 0.1 will be used as the failure probability to close the path before water depletion.

The following factors were considered in the above estimate:

(i) Assumptions in analyses of similar plants [NRC, 1993] that this type of sequence would lead directly to core damage.

(ii) The fact that it has been assumed that the probability of closing [F-CLOSE] the path exists.

(iii) By performing a sensitivity analysis for that probability, it is found that a value equal to or less than 0.1 causes the reported condition to be screened out as being less than the ASP screening value for the CCDP of 1.0 x 10^{-6}. A more exact calculation may be performed, but the result will not significantly affect the value. A simplified sensitivity analysis for the "failure probability to CLOSE" vs. CCDP is shown in Figure 5.3.3.

5.3.3.2. ISLOCA event tree definition

The interfacing-system-LOCA event tree (Figure 5.3.2) uses the following definitions:

1. Initiating event: Interfacing system LOCA [ISLOCA]

The initiating event is the opening of the upstream and downstream RHR shutdown cooling valves in the CSR, creating a path from the reactor vessel to the reactor enclosure.

2. Reactor Protection System [RPS]

This system performs the subcriticality function. A sufficient number of control rods must be inserted to terminate power production.

3. Low pressure coolant injection [LCI, LCS]

Given the assumption that the large loss of coolant through the valves and the damaged low pressure pipes causes depressurization, the SRV are not used and there is a need for coolant makeup from the low pressure systems, i.e., the Core Spray system [CS] and the Low Pressure Coolant Injection system [LCI], an operating mode of the RHR system. Coolant makeup is provided by the low-pressure systems by using the water located in the Condensate Storage Tank [CST], the suppression pool and the RHR service water [RHRSW].

Even with the low-pressure systems operable, it is still necessary to keep the core covered during the time that the coolant is escaping through the open path. The low-pressure systems may be able to provide the necessary flow rate to keep the core covered, but it is still necessary to close the path before the water sources deplete.

4. Close path before water depletion. [CLOSE]

This function consists of the necessary steps for closing at least one of the valves, assuming that it is possible to isolate the reactor vessel. It is assumed that the most likely action would be performed by plant operators, i.e., manually closing one of the valves. If it is assumed that the path is closed before core damage, then the following functions are designed to remove the residual heat from the core and the containment:

5. Containment heat removal [CHR]

This function preserves primary containment integrity and transfers fission-product decay heat to the environment. It is performed by the RHR and the RHRSW systems.

6. Containment venting [CV]

For LOCAs [large, medium or small], the function "venting success" is included, considering the fact that coolant has been blown down into the containment and therefore the containment pressure has increased. Thus, containment venting is necessary when the containment heat removal fails.

7. Injection systems available

The event "injection systems available" is considered in the event tree because a failure to vent the containment may produce a failure in those systems for this plant. The systems considered are: Control Rod Drive [CRD] and RHRSW injection.

The factors that contribute to the consideration of this branch are:

Failure of the containment heat removal:

Without decay-heat removal from the containment, the suppression pool will eventually heat up and steam will be generated in the condenser. Pressure in the containment will continue to increase. The failure of the containment would lead to two potential phenomena that would compromise the ability to keep the core covered:

(i) The suppression pool may have a substantial portion of the inventory flash to steam, leading to:

- Possible cavitation causing damage to the pumps during the postulated containment blowdown phase.
- Potential piping or valve damage due to the large steam generation rate during the blowdown of the containment.
- Venting of steam into the reactor enclosure, adversely affecting the switchgear, motor control centers or instrumentation for the injection systems located in the reactor enclosure.

(ii) The failure of the containment may also lead to failure of the coolant-injection piping supplying water to the vessel from the hotwell, the condensate storage tank and the suppression pool due to structural damage in the reactor enclosure.

5.3.3.3. Scenario involving reported cables as targets for a fire ignition source

1. Assumptions

For the development of the present case study, not all the required information about the location (CSR) and the physical scenario containing the reported cables was available. For pedagogical purposes, that information was assumed known, based on the use of limited sources from the plant and other alternatives; of course, in a real case the analyst will have or must obtain the necessary information to develop the correct analysis of the reported event. Alternatively, information from generic databases and that from similar plants can be used.

In this case study, the following information was assumed known:

(i) The contents of the physical scenario in the CSR, containing the reported cables for the interfacing system valves, along with other safety-related cables, all of them potentially affected by a postulated fire.

(ii) Characteristics of the involved location. That is, components and cables of safety-related equipment in the CSR, including their spatial distribution, physical properties and parameters of fuel, materials and room required for fire modeling. Table 5.3.1 lists the input data for the scenario in the CSR.

(iii) Necessary information for definition of parameters concerning the fire initiating frequency and the geometric, severity and non-suppression factors, developed according to standard fire-PRA procedures.

2. Cable Spreading Room scenario modeling

According to the available information from the plant, the CSR contains cables that are associated with shutdown methods A, B, C and D of the plant. In addition, the CSR does not contain cabinets and the self-ignition of cables is considered very unlikely. If a potential fire is to be considered, the most likely possibility would be from a transient ignition source.

As a result, for the scenario involving the reported interfacing system valve cables, the existence of a transient source was postulated, with the potential to affect the trays containing the cables involved with power/control for the following safety-related systems:

(i) Tray LHI

- Train B of the residual heat removal service water system.

(ii) Tray LMI

- Train A of the control rod drive.
- Residual heat removal shutdown cooling valve HV-51-1F008, components of RHR train A.

(iii) Tray LLO

- Train B of the low pressure coolant system.

(iv) Tray RHI

- Train A of the high pressure coolant injection system.
- Residual heat removal shutdown cooling valve HV-51-1F009, components of RHR train A.

5.3.3.4. Quantification procedure

According to standard fire-PRA procedures [Apostolakis, 1993], the expression to be used for quantification is the following product:

$$\mathbf{CDF} = \lambda_f \times f_g \times f_s \times f_{ns} \times Q \qquad [5.1]$$

where:

CDF	:	Core Damage Frequency [year^{-1}]
λ_f	:	Initiating event frequency.[Fires/year]
f_g	:	Geometric factor.
f_s	:	Severity factor.
f_{ns}	:	Non suppression factor.
Q	:	Value of the logic model, involving fire-induced failures and random failures.

The quantification process was performed by using the IRRAS computer code [NRC, 1995] and the ASP electronic files for the plant, containing the fault trees for all the safety-related systems included in the event tree corresponding to the ISLOCA as the initiating event. In each case where a quantification was performed, either in the preliminary analysis, the intermediate screening or the final quantification, the procedure was the following:

1. Identify the basic events in the fault trees affected by the reported condition (in this case, the trains or components affected by fire damage). Set the failure probability of identified basic events equal to 1.0. In addition, assume a value of 1.0 for the initiating event for the event tree.

2. The unimpacted basic events maintain their failure probabilities equal to the random failure values established in the fault tree models, from generic and/or plant-specific data.

3. With the information from 1 and 2, quantify the integrated event tree to get the value of **Q**.

4. Estimate, as required, the parameters involved in the fire initiating frequency and its modifying factors, the geometric factor, the severity factor, the non-suppression factor and any other applicable factor, by using standard fire-PRA procedures.

5. The probability, **P**, that a fire-induced initiating event could occur during the period of the failure or unavailability is calculated by multiplying the value of the modified fire initiating-event frequency by the duration of that period.

6. Finally, the conditional core damage probability is calculated by multiplying the value of **Q** by the value of **P**.

7. In addition, the importance measure is determined by calculating the value of the Core Damage Probability [CDP] for the period of the unavailability or failure, with all the failure probabilities for the basic events in the quantification model equal to their random failure values. The importance measure is then the value that results from the subtraction of the CDP from the CCDP determined above, for the same period.

5.3.4. ASP Fire Review

5.3.4.1. Step 1. Initial screening

It is deemed that the reported condition represents a potentially important safety issue and therefore it is of interest to the present ASP methodology, because it involves a potential interfacing system LOCA as the initiating event. Therefore, if the involved location is destroyed, at least one of the consequences would be an ISLOCA. As a result, the LER is screened in and passed on to Step 2, "preliminary analysis", for further analysis.

5.3.4.2. Step 2. Preliminary analysis

For the preliminary analysis, it is assumed **(i)** that the entire zone in which the configuration compromise has been detected is destroyed by fire; and **(ii)** that no fire suppression is available or performed. For every basic event contained in the plant-specific internal-event model that is affected by the destruction of components or cables in the CSR, the failure probability is set to 1.0.

Running the internal-event plant-specific model for the interfacing system LOCA as the initiating event, the LER is screened in for the following reason:

The value of the CCDP, even considering only the scenario containing the reported cables for the interfacing system valves, is 1.0×10^{-4} ,which significantly exceeds the screening value of 1.0×10^{-6}. That is the necessary and sufficient condition for the LER to be passed on to Step 3 for detailed analysis. Definition and failure probabilities for basic events used in this quantification are presented in Table 5.3.2.

5.3.4.3. Step 3. Detailed analysis

1. Substeps (1) and (2)

The equipment items affected by the inadequate configuration were identified and listed earlier in the cable spreading room scenario.

2. Substep (3)

The scenario corresponding to the configuration compromise was defined earlier according to the items in Substeps (1) and (2), with a postulated transient ignition source in the cable spreading room.

3. Substep (4)

In the present case, the consequence of the reported condition (a configuration compromise) has been explicitly defined in the LER as the possibility of an interfacing system LOCA as the initiating event for a fire-initiated sequence.

Analyzing the information from the plant, it has been concluded that no fire PRA model exists for the scenario containing the interfacing system valve cables (for BWRs). Therefore, the condition corresponds to substep (4A), Case A, "not included". Thus, in order to evaluate the risk significance of the reported condition, a PRA model must be created and the LER will be passed on to substep (5) and then to substep (6). However, to reduce unnecessary effort for fire modeling, an intermediate quantitative screening analysis must be performed. Therefore, the reported condition will be passed on to Step (6A) for intermediate screening.

4. Substep (6A). Intermediate screening

To perform this analysis, the parameters associated with the fire initiating frequency, geometric factor and severity factor corresponding to the defined scenario were estimated using standard fire-PRA procedures.

All of the safety-related equipment involved in the scenario containing the interfacing system valve cables was assumed lost. The failure probabilities for the impacted basic events associated with each loss were set to 1.0. Then, the interfacing system LOCA event-tree model was quantified for the period that the detected condition lasted, assuming no fire suppression.

The CCDP resulting from the quantification process is 1.4×10^{-4}. Consequently, the intermediate screening value has been exceeded and the reported condition is passed on to Step (6B) for "final analysis". Definitions and failure probabilities for basic events used in the intermediate screening are presented in Table 5.3.2. Table 5.3.3 summarizes the values for the parameters indicated above and shows the results. According to (6B.i), a fire model must be developed, so that a less conservative calculation of the probability of damage for each safety-related equipment can be performed.

5. Substeps (6B.i) and (6B.ii). Fire model.

In order to determine more realistically the consequences of a postulated fire in the Cable Spreading Room for the reported valves and the safety-related systems, the COMPBRN IIIe [Ho, Chien, and Apostolakis, 1990] fire growth code was used to calculate fire propagation and equipment damage. The code calculates the time to equipment damage given that a fire has started. Input parameters were obtained from the COMPBRN IIIe database and generic case studies [Apostolakis, 1993], as detailed in Table 5.3.1. The description of the scenario is presented in Figure 5.3.4. According to the requirements of COMPBRN IIIe for the development of the model, each tray was subdivided into three parts (for example, for tray LHI, parts LHI1, LHI2 and LHI3 were created).

In addition to providing the time to damage for each target involved in the scenario, COMPBRN IIIe has the capability of performing uncertainty analysis, using simulation techniques, based on the probability distribution of the parameters involved in the model for fuel, targets and room. The uncertainty analysis performed by the code was complemented by the use of an analytic risk-analysis software program, in order to get a probabilistic distribution for the time-to-damage for each component involved in the modeled scenario. The results from the uncertainty analysis for two of the targets are presented in Figures 5.3.5a and 5.3.5b, based on data from COMPBRN IIIe in Tables 5.3.4a and 5.3.4b. The following are the mean values for the time-to-damage for the involved targets:

- Tray LHI. Cable 2-LHI, Train B of the Residual Heat Removal Service Water system is damaged in 8 minutes.
- Tray LMI. Cable 2-LMI, Train A of the Control Rod Drive and Residual Heat Removal shutdown cooling valve HV-51-1F008 are damaged in 7 minutes.
- Tray LOL. Cable 2-LLO, Train B of the Low Pressure Coolant System. is damaged in 7 minutes.

- Tray RHI. Cable 2-RHI, Train A of the High Pressure Coolant Injection System and Residual Heat Removal shutdown cooling valve HV-51-1F009 are damaged in 7 min.

According to standard fire-PRA procedures, the damage time is then used in conjunction with plant specific information regarding fire suppression, to obtain the probability that the fire will cause equipment damage before being suppressed. The reported condition is now passed on to Step 3-C for final quantification.

6. Substeps (6B.iii) and (6B.iv). Final quantification

All of the safety-related equipment involved in the scenario containing the interfacing-system-valve cables is assumed lost, according to the results from fire modeling. The failure probabilities for the impacted basic events associated with each loss were set to 1.0 and the interfacing-system-LOCA event-tree model quantified according to quantification procedures established in Section 5.3.3 ("Analysis").

Definitions and failure probabilities for the basic events used on the final quantification are presented in Table 5.3.2. Table 5.3.5 summarizes the values for the parameters indicated above and shows the results.

5.3.5. Results

Table 5.3.6 shows the values of **Q** for the quantification of the core-damage sequences of the interfacing system LOCA event tree, assuming the loss of the cable trays and associated failures to interfacing-system valves and safety-related systems. Dominant sequences are sequence 12 and sequence 9. Table 5.3.7 shows the sequence logic for dominant sequences identified for the LER.

Dominant cut sets and associated basic events for higher probability sequences are shown in Table 5.3.8.

Finally, Table 5.3.9 shows the final results for the evaluation of the reported condition, in terms of the conditional core damage probability and the importance measure.

The conditional core damage probability for the detected condition is 5.47×10^{-6}. The importance measure for the period of four years and nine months is 5.47×10^{-6}. Based on the CCDP value, the risk significance of the LER exceeds the established ASP screening value and therefore the detected condition should be reported as an "Accident Sequence Precursor."

5.4. Case study: a non-fire-related-failure LER

5.4.1 Summary

This case study involves an LER that was reported in 1994 by a General Electric boiling water reactor with a Mark I containment. This plant will be called "Plant C". However, because some of the systems information from Plant C was not available, this case study has used the system information from another BWR plant, which will be called "Plant D", for parts of this case study. Because this case study is being written for tutorial purposes, it is not considered important that the events described in the analysis are not fully realistic (that is, faithful in detail) compared to the actual events described in the LER.

The LER reported that with the plant at 99% power, the high-pressure-coolant-injection turbine tripped due to high exhaust pressure during a monthly surveillance test. The LER was analyzed by the internal events ASP and modeled as a long-term unavailability of the HPCI system. The period of unavailability was established to be one month (720 hours). The conditional core damage probability estimated for that event was 3.1×10^{-6} and therefore it was reported as an "Accident Sequence Precursor".

According to the requirements established for setting up the fire ASP methodology, the plant has defined the most important fire-initiated sequences. One of the insights is that a fire with enough severity, produced in location A of the

Essential Switchgear Room [ESR], would induce an Inadvertent Opening of a Safety Relief Valve [IORV] and the unavailability of the Main Feedwater [MFW] system.

An accident sequence initiated by an IORV transient was considered by the plant as one of the most risk-important. The HPCI system is one of the important ways to mitigate such events.

The LER was analyzed and the conditional core damage probability related to fires was estimated at 2.7×10^{-7}. Therefore, the relevant accident sequence does not exceed the CCDP criterion of 1.0×10^{-6} and, as a result, the LER was screened out from a fire-ASP point of view.

5.4.2 Event description

5.4.2.1. Internal event description

With Plant C plant at 99% power, the HPCI turbine tripped due to high exhaust pressure during a monthly surveillance test. The cause of the exhaust pressure was determined to be a failed check valve. The failure mechanism indicated that, in the period since the last monthly surveillance test, the HPCI turbine would have tripped shortly after starting if the HPCI system had been called upon to perform its safety function.

The event was modeled as a long-term unavailability of the HPCI system. The difficulty encountered in identifying the root case of the pump failure indicates that the failure would not have been recovered easily during an actual demand. Therefore, the failure was modeled as unrecoverable. The HPCI was considered unavailable for one period of surveillance (one month, or 720 hours). It was assumed that any demand for the HPCI turbine, subsequent to the last successful monthly surveillance, would have resulted in several minutes of high pressure injection followed by a HPCI turbine trip.

The event was modeled as a failed HPCI train (Basic event HCI-TDP-FC-TRAIN set to TRUE) and considered as unrecoverable (Basic event HCI-XHE-XE-NOREC set to TRUE).

The event in the LER was analyzed by the internal-events ASP methodology and reported as an "Accident Sequence Precursor", with an associated Conditional Core Damage Probability of 3.1×10^{-6}.

5.4.2.2. Fire-initiated sequences impacted

The HPCI has been considered in the plant's fire analysis as a mitigating system in a transient sequence initiated by the inadvertent opening of a safety relief valve [IORV]. Therefore, the unavailability of this system to perform its safety function in a situation in which a fire occurred would degrade the response of the plant.

1. Characteristics of the scenario linked to impacted sequence

If a fire with enough severity were to occur in location A of the essential switchgear room, it would cause the following consequences in safety-related equipment associated with the location:

a) A fire-induced spurious opening of a safety relief valve, producing an IORV initiating event.

b) Unavailability of the main feedwater system due to damage to control circuits in the location and a subsequent common-cause failure.

2. Description of sequences

The sequence impacted by the unavailability of the HPCI system is composed of the following events. Figure 5.4.1 shows the impacted sequence from the IORV event tree.

a) IORV. Initiating event

Inadvertent opening of a safety relief valve, an initiating event arising from a spurious signal due to a fire in location A of the essential switchgear room fire area.

b) S1. Reactor trip

There may be no trip signal generated by the reactor protection system during the initial stages of an IORV event sequence. The operator will be alerted to an IORV by observing generator load reduction, the SRV position indicators, the SRV tailpipe temperatures, the annunciators associated with open SRVs or the suppression pool temperature.

Failure to trip [S1] implies failure of the operator to scram the reactor prior to the suppression pool reaching a temperature requiring prompt RHR system operation.

c) RPS. Mechanical portion of the reactor protection system

The reactor protection system performs the subcriticality function. A sufficient number of control rods must be inserted to terminate power production.

d) MFW. Main Feedwater System available for injection

According to operating experience, the IORV event is not expected to cause a Main Steam Isolation Valve closure. Therefore, the MFW system is available to perform its function with the Power Conversion System [PCS] and it is considered as a mitigating system.

e) HPCI. High Pressure Coolant Injection system available

In case of a MFW system failure, the coolant-makeup function can be provided by the HPCI system.

f) ADS. Automatic depressurization system

In case of unavailability of the HPCI system, the coolant makeup can be provided by the low-pressure systems. To operate any of these, it is necessary to depressurize the reactor, which is performed by the ADS. Failure to depressurize would lead to core damage.

5.4.3. ASP fire review

5.4.3.1. Step 1-C. Quantification

In the logic model corresponding to the IORV-initiated sequence developed by the plant, failure probabilities for each basic event impacted by the postulated fire in the indicated location were set equal to unity. The failure probability for the HPCI system was also set equal to 1.0 and an unavailability period of 720 hours was assumed. Basic events that were unimpacted were assigned the corresponding random-failure values. The fire-PRA model corresponding to the sequence was quantified using the data from above. A conditional core damage probability of 2.7×10^{-7} was obtained.

Definitions and failure probabilities for the basic events used in the final quantification are presented in Table 5.4.1.

5.4.4. Results

Table 5.4.2 shows the higher-probability cut sets for the impacted sequence. Table 5.4.3 presents the quantification results, in terms of the CCDP estimated for the period of the HPCI unavailability, 720 hours. Data for the quantification were taken from the IORV-initiated sequence analysis developed by the plant, considering the fire initiating frequency, the geometric factor, the severity factor and the non-suppression factor.

Given that the conditional core damage probability value does not exceed the established criterion of 1.0×10^{-6}, the LER, from the fire ASP point of view, is screened out.

5.5. Overall results from the case studies

Three stylized cases have been presented and the developed fire-ASP methodology has been applied. It is important to recognize that the actual safety issues reported in these LERs have long since been resolved. A complete database of fire-related events occurred in nuclear power plants has been revised and those cases were chosen to fulfill the tutorial objective established here for the application of the methodology.

The fire-ASP methodology has been tested and proved to be adequate for the analysis of real cases, taken from plants of different design and characteristics.

Many of the safety issues recognized during the study of these cases, along with the experience gained from other cases in the database have been incorporated in the development of the methodology, so that the final process reflects what real experience has been.

The application of the methodology has allowed for the review of the documentation of the plants where the reported safety issues have occurred. Moreover, a review of the fire-related methodologies that the plants have used for safety analyses has been conducted. From that process, direct consequences on what the fire-ASP program will be, when implemented. are recognized and analyzed. Main issues are further discussed in Chapter 6.

The main issues that have arisen from the application of the methodology in the case studies can be summarized as follows.

- Even though a case may be important for internal events ASP, it may not be important in terms of fire ASP. Though a safety issue is in any case to be analyzed and reported, the threshold value of 1.0×10^{-6} established for the ASP program constitutes the central figure for deciding the importance of an event.
- The possibility that an LER reports a fire-related event and that event can be incidental to the occurrence of the incident as a whole is a key aspect to be

considered. That reflects the need that the cases be treated in a coordinated effort by the internal events ASP and the fire-ASP analysts.

- One important characteristic of a fire-related event is the potential for inducing damage. Thus, the analyst should evaluate a case on the hypothetical condition that the suppression efforts had not been completely successful in time, so that several scenarios can emerge for the reported event. That consideration will allow the extension of a single and plant-specific case and thus gaining a more comprehensive operational experience.
- One of the most important consequences of working with the case studies was related to the experience gained regarding the status and use of the documentation of the plant. The main documents used in the study of the cases were the IPE and the IPEEE. From these, it was evidenced the need for the analyst to have access to more detailed information, which contains the description of the physical characteristics of locations, presence and distribution of equipment related to safety systems and the factors related to the effects of fires, such as parameters for fire modeling, from both targets and sources. From the experience acquired during the analysis of the case studies, a list of recommendations about the documentation that should be provided to the ASP analyst have been made and further discussed in Chapter 6.

Figure 5.2.1. Schematic AC electrical distribution system of Plant A Nuclear Power Plant.

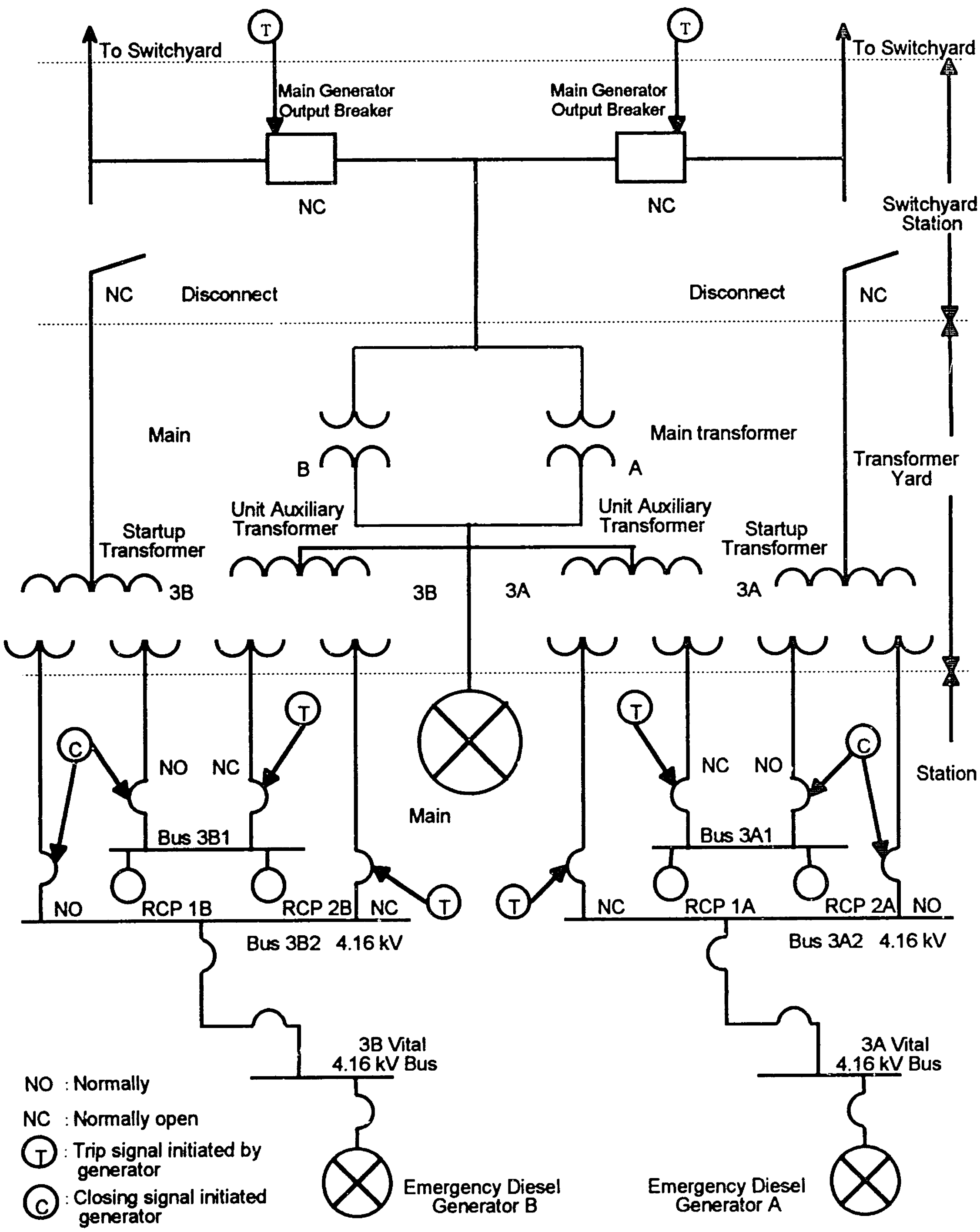


Figure 5.3.1. Simplified P & ID of the Residual Heat Removal System containing the involved interfacing system valves.

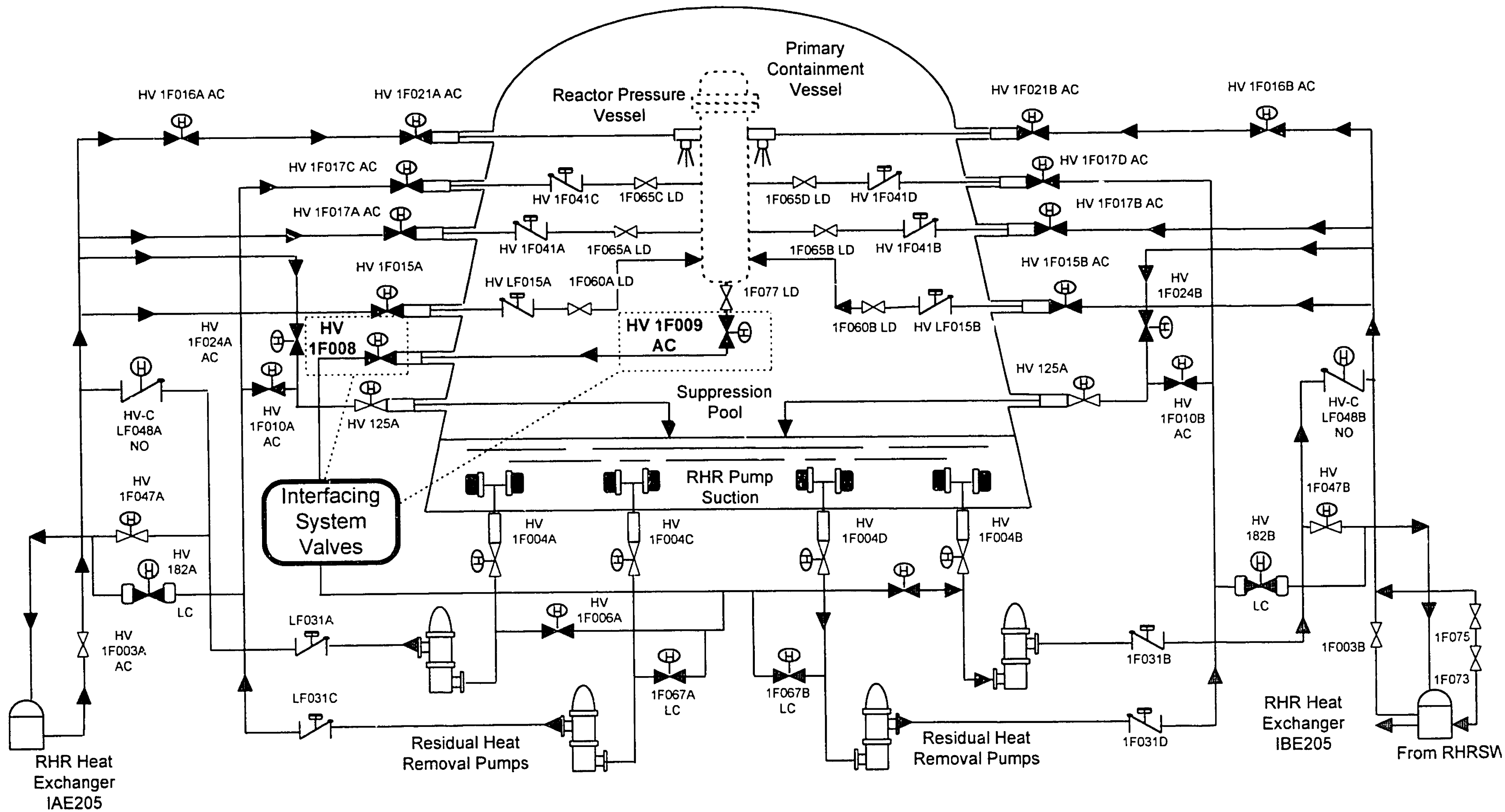


Figure 5.3.2. Interfacing System Loss of Coolant Accident event tree developed.

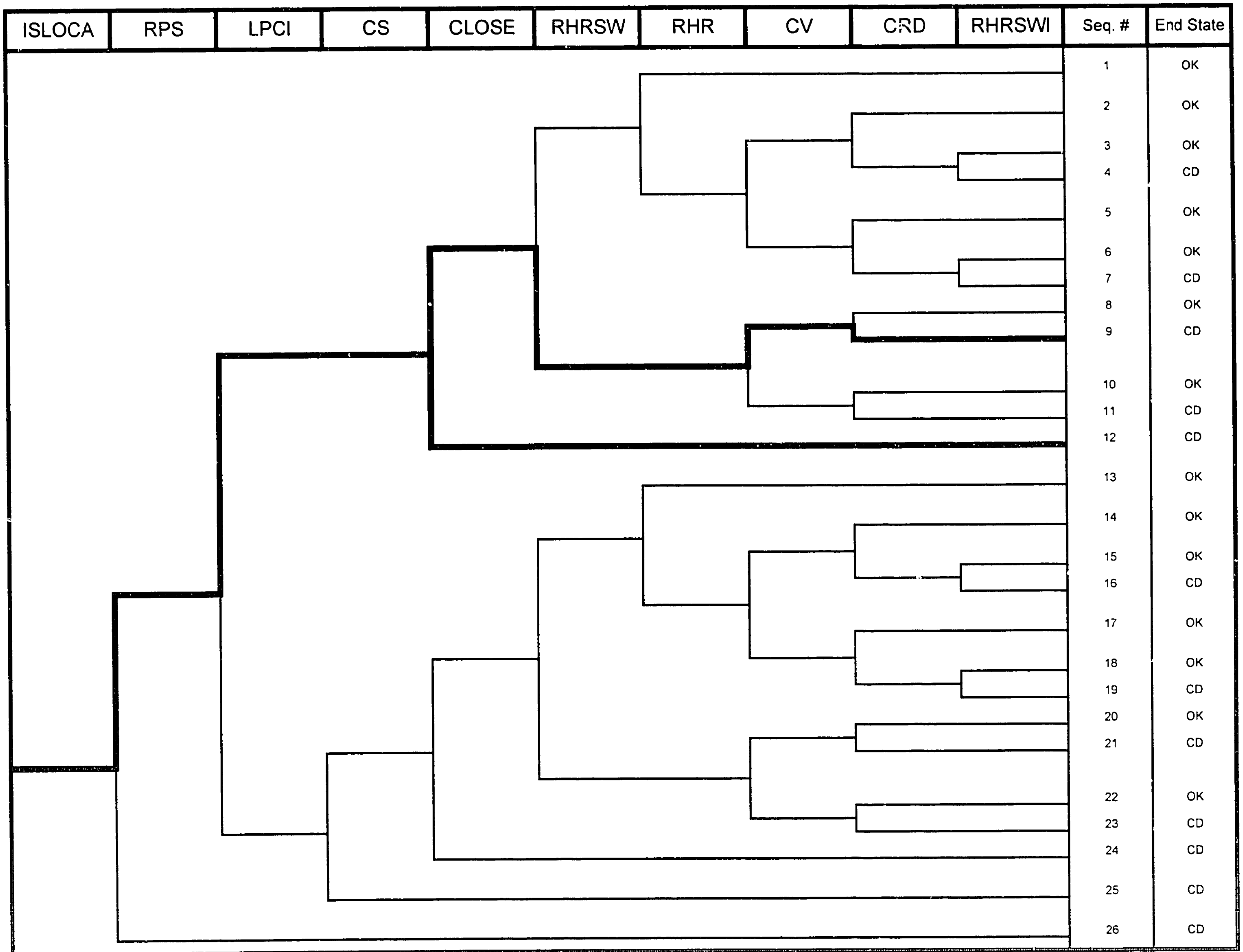


Figure 5.3.3. Simplified sensitivity analysis for the failure probability for CLOSE vs. CCDP.

CLOSE failure probability	Q total	CCDP	ASP Criterion
1.00E-01	1.00E-01	5.47E-06	LER In
1.00E-02	1.00E-02	5.47E-07	LER Out
1.00E-03	1.40E-03	7.66E-08	LER Out
1.00E-04	5.50E-04	3.01E-08	LER Out
1.00E-05	4.60E-04	2.52E-08	LER Out
1.00E-06	4.50E-04	2.46E-08	LER Out
1.00E-07	4.50E-04	2.46E-08	LER Out

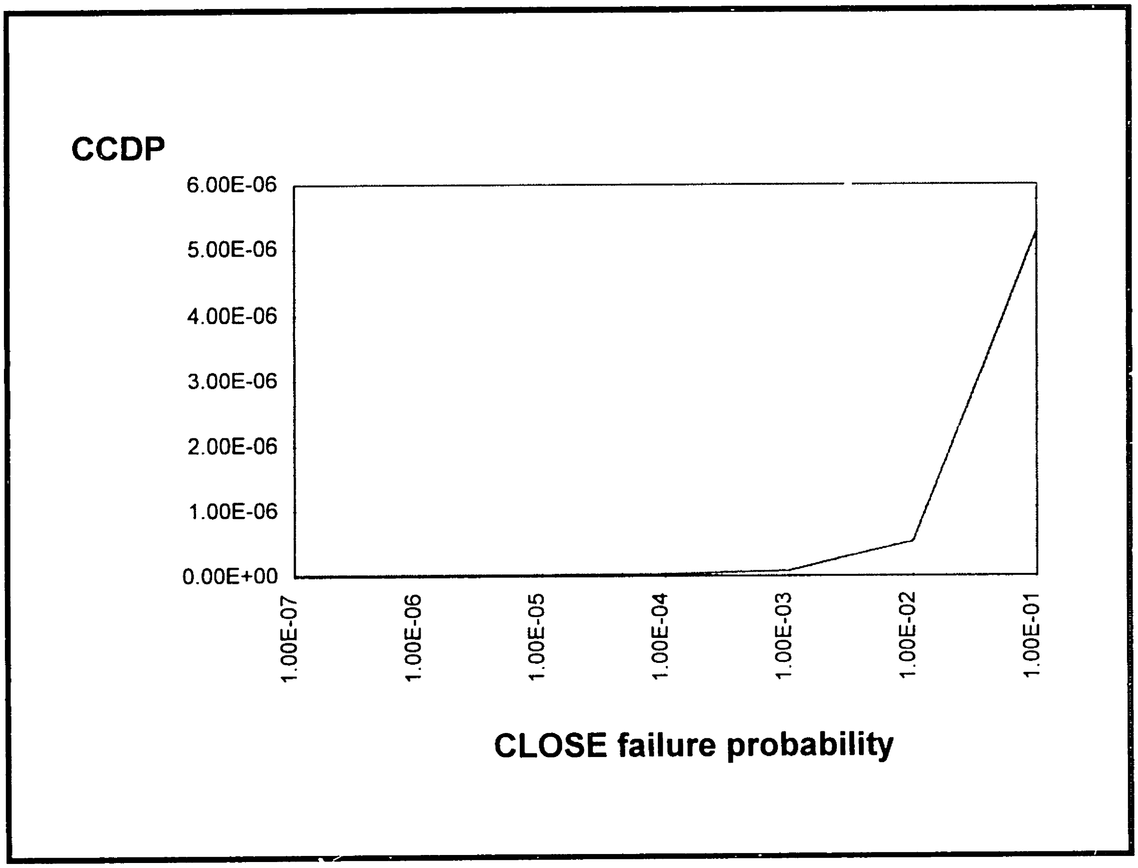


Figure 5.3.4. Schematic description of the postulated scenario in the Cable Spreading Room.

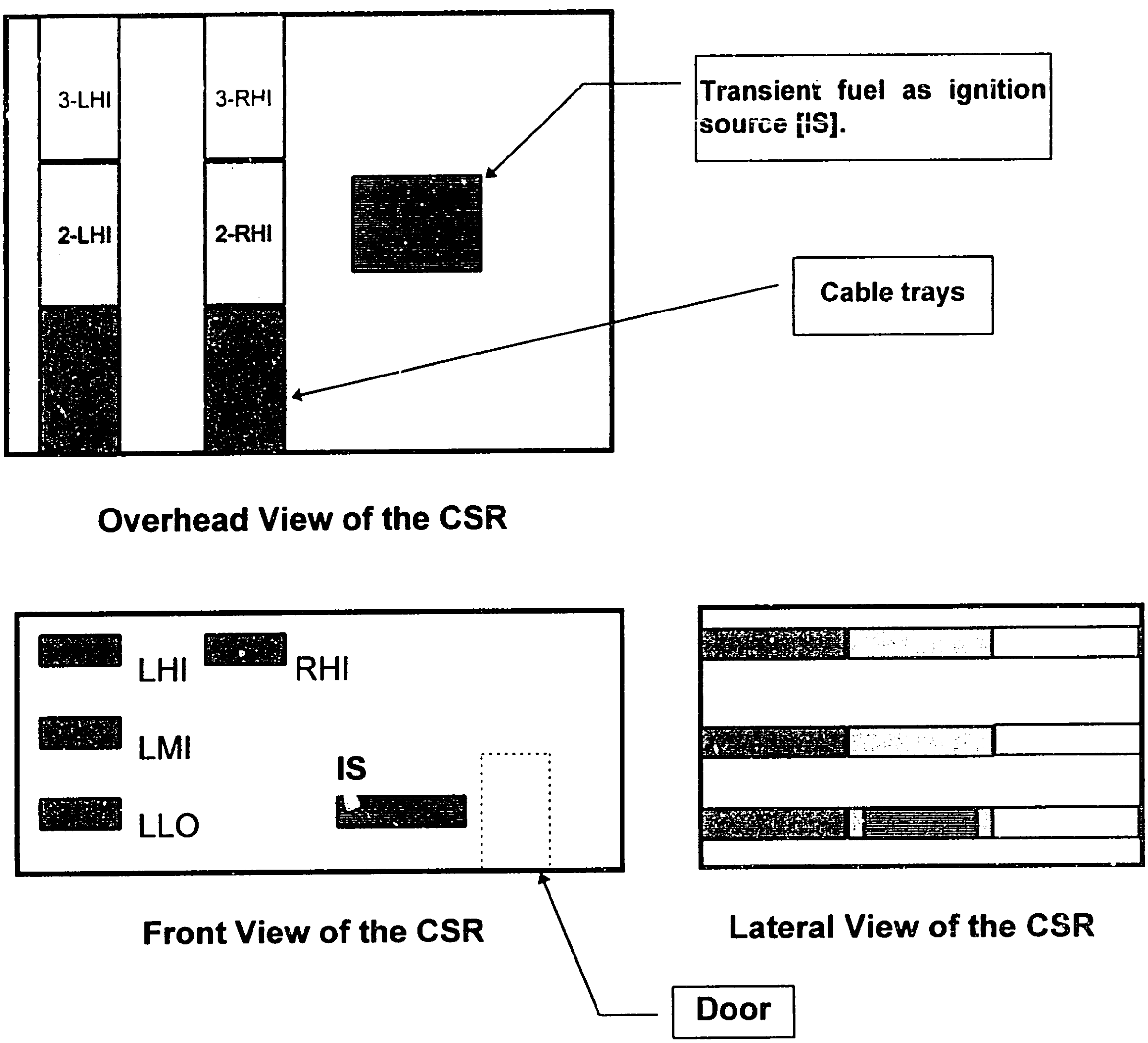


Figure 5.3.5a. **Results from uncertainty analysis for target 2-LHI in the Cable Spreading Room.**

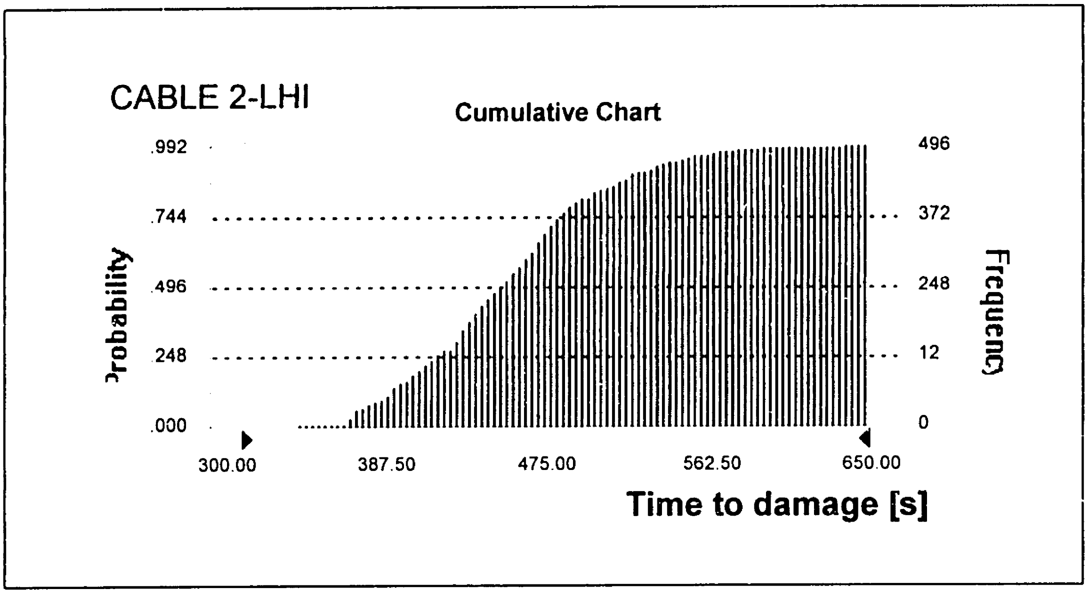


Figure 5.3.5b. **Results from uncertainty analysis for target 2-LMI in the Cable Spreading Room.**

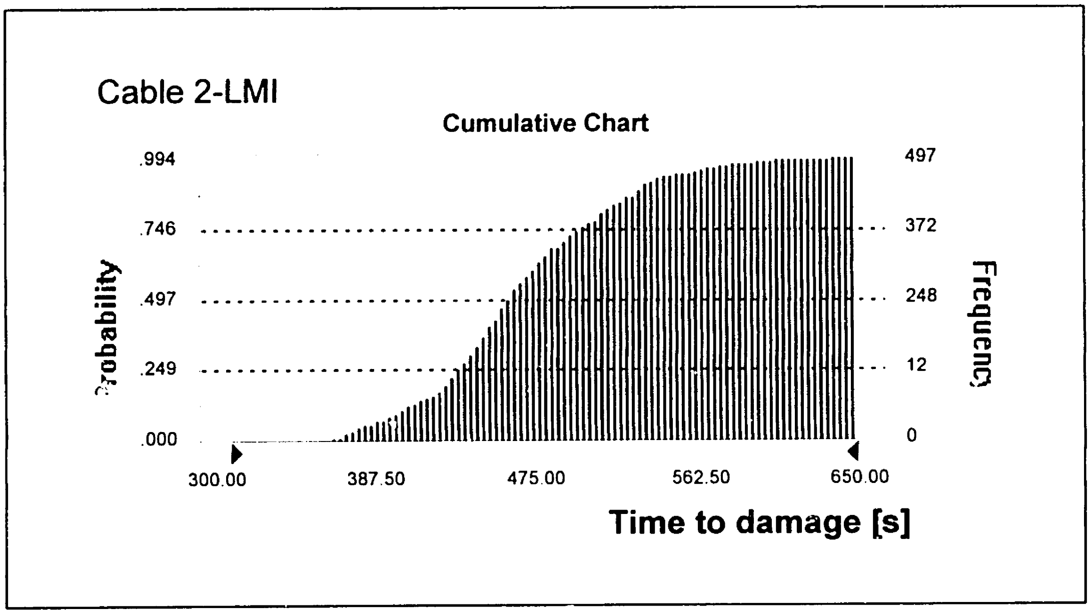


Figure 5.4.1.Impacted sequence in the Inadvertent Opening of a Safety Relief Valve [IORV] event tree.

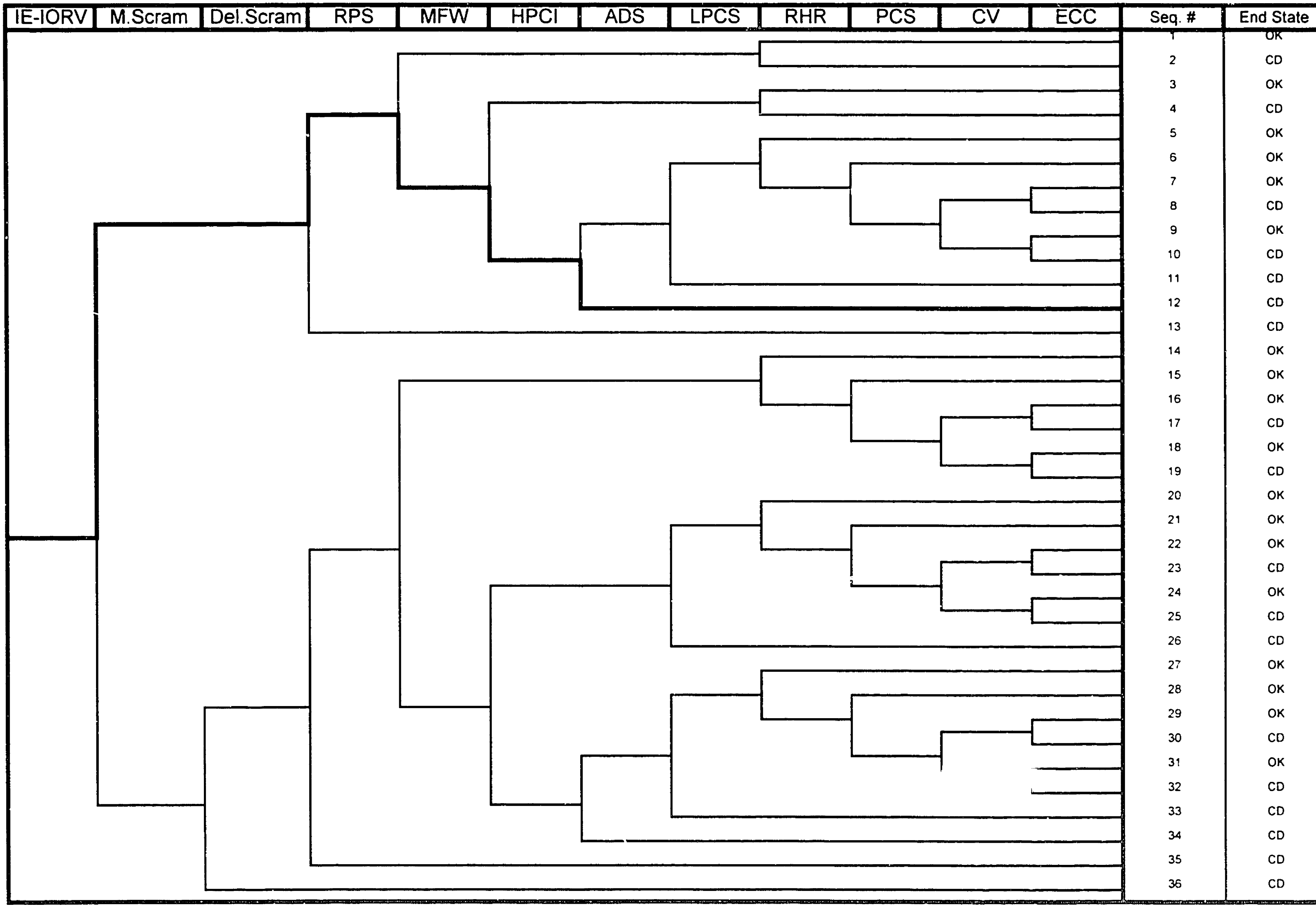


Table 5.3.1. Input data for fire modeling of postulated scenario in the Cable Spreading Room

I. OVERALL JOB PARAMETERS

Time increment:	60.0 seconds
Number of time steps:	60
Total time of simulation:	60.0 minutes

II. VARIABILITY FACTORS FOR FIRE MODELS

Ventilation controlled burning rate	1.00
Fuel-surface controlled burning rate	1.00
Flame height for horizontal fuel	1.00
Flame height for vertical fuel	1.00
Radiative heat flux interchange	1.00
Buoyant plume temperature	1.00
Convective heat transfer coefficient for vertical objects in plume	1.00
Convective heat transfer coefficient for horizontal objects in plume	1.00
Gas layer local temperature	1.00
Heat transfer to self for vertical fuel	1.00
Heat transfer to adjacent fuel	1.00
Heat flux from ceiling hot gas layer	1.00
Heat flux from reflections off walls and barriers	1.00
Mass burnout fraction	1.00

III. PHYSICAL FUEL PARAMETERS

NUMBER OF FUEL TYPES INCLUDED: 4

1. CEILING
2. WALL
3. CABLE
4. SOLVENT

FUEL TYPE No. 1 - CEILING

Parameter	Distribution	Point value	Low value	High value
Thermal conductivity [W/mK]	Normal	1.06	.4200	1.700
Thermal diffusivity [m^2/s]	Point value	0.537E-06		
Reflectivity [dimensionless]	Lognormal	0.950E-01	.5000E-01	.3500

FUEL TYPE No. 2 - WALL

Parameter	Distribution	Point value	Low value	High value
Thermal conductivity [W/mK]	Normal	1.06	.4200	1.700
Thermal diffusivity [m2/s]	Point value	0.537E-06		
Reflectivity [dimensionless]	Lognormal	0.920E-01	.5000E-01	.3500

FUEL TYPE No. 3 - CABLE

Parameter	Distribution	Point value	Low value	High value
Density [kg/m3]:	Uniform	950.	900.0	1000.
Specific heat [j/kgk]	Neg-log	0.225E+04	1823.	2350.
Thermal conductivity [W/mK]	Lognormal	0.100	.8000E-01	.4200
Heating value [J/kg]	Point value	0.231E+08	.7100E+07	.3500E+08
Pilot ignition temperature [K]	Point value	800.	576.0	1029.
Spontaneous ignition temp. [K]	Point value	840	750	850.0
Damage temperature [K]	Shift-log	573	400	700.0
Vent. control burning rate constant [dimensionless]	Point value	0.110	1.000	1.000
Specific burning rate constant [kg/m^2s]	Point value	0.187E-01	.1060E-01	.3300E-01
Surface control burning rate constant [kg/J]	Point value	0.360E-06	.9500E-07	.1020E-05
Combustion efficiency [dimensionless]	Point value	0.265	.2000	.3500
Fraction of flame heat released as radiation [dimensionless]	Point value	0.450	.2700E-01	.7000
Absorption coefficient for flame gases [m^{-1}]	Point value	1.40	1.000	1.000
Reflectivity [dimensionless]	Lognormal	0.120	.8000E-01	.3000

FUEL TYPE No. 4 - SOLVENT

Parameter	Distribution	Point value	Low value	High value
Density [kg/m3]:	Point value	679	679.5	888.2
Specific heat [j/kgk]	Point value	0.224E+04	1880	2364.
Thermal conductivity [W/mK]	Point value	0.128	.1280	.1780
Heating value [J/kg]	Point value	0.467E+08	.4330E+08	.5000E+09
Pilot ignition temperature [K]	Point value	269	228.0	494.0
Spontaneous ignition temp. [K]	Point value	486.	477.0	644.0
Damage temperature [K]	Point value	1.00	1.000	1.000
Ventilation control burning rate constant [dimensionless]	Point value	0.110	1.000	1.000
Specific burning rate constant [kg/m^2s]	Normal	0.610E-01	.5500E-01	.7500E-01
Surface control burning rate constant [kg/J]	Point value	0.200E-06	1.000	1.000
Combustion efficiency [dimensionless]	Uniform	0.925	.8500	.9500
Fraction of flame heat released as radiation [dimensionless]	Point value	0.507	.4000	.5000
Absorption coefficient for flame gases [m^{-1}]	Point value	1.40	1.000	1.000
Reflectivity [dimensionless]	Point value	0.100	.8000E-01	.3500

IV. COMPARTMENT OBJECT DEFINITION

NUMBER OF OBJECTS DEFINED: 18

1. CEILING	3. F-WALL	5. R. WALL	7. C.1LHI	9. C. 3LHI	11. C. 2LMI	13. C.1LLO	15. C.-3LLO	17. C.-2RHI
2. L. WALL	4. B. WALL	6. Solvent	8. C. 2LHI	10. C.-1LMI	12. C.-3LMI	14. C.-2LLO	16. C.-1RHI	18.C.-3RHI

OBJECT 1 - CEILING

Parameter			
Object midpoint coordinates [X-Y-Z]:	8.54	7.32	4.27
Dimensions [length,width,depth] [m]:	17.1	14.6	1.00
Number of subdivided elements:	1		
First element midpoint coordinates [X-Y-Z]:	8.54	7.32	4.27
Direction of logitudinal and normal axes:	X	Z	
Total mass [kg]:	0.100E+04		
Mass per element [kg]:	0.100E+04		
Porosity factor [dimensionless]	1.00		

OBJECT 2 - LEFT-WALL

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.000E+00	7.32	2.13
Dimensions [length,width,depth] [m]:	14.6	4.27	1.00
Number of subdivided elements:	3		
First element midpoint coordinates [X-Y-Z]:	0.000E+00	2.45	2.13
Direction of logitudinal and normal axes:	Y	X	
Total mass [kg]:	0.100E+04		
Mass per element [kg]:	333.		
Porosity factor [dimensionless]	1.00		

OBJECT 3 - FRONT-WALL

Parameter			
Object midpoint coordinates [X-Y-Z]:	8.34	0.000E+00	2.09
Dimensions [length,width,depth] [m]:	17.0	4.24	1.00
Number of subdivided elements:	4		
First element midpoint coordinates [X-Y-Z]:	1.97	0.000E+00	2.09
Direction of logitudinal and normal axes:	X	Y	
Total mass [kg]:	0.100E+04		
Mass per element [kg]:	250.		
Porosity factor [dimensionless]	1.00		

OBJECT 4 - BACK-WALL

Parameter			
Object midpoint coordinates [X-Y-Z]:	8.54	7.32	2.13
Dimensions [length,width,depth] [m]:	17.1	4.27	1.00
Number of subdivided elements:	4		
First element midpoint coordinates [X-Y-Z]:	2.13	7.32	2.13
Direction of logitudinal and normal axes:	X	Y	
Total mass [kg]:	0.100E+04		
Mass per element [kg]:			
Porosity factor [dimensionless]	1.00		

OBJECT 5 - RIGHT-WALL

Parameter			
Object midpoint coordinates [X-Y-Z]:	17.1	7.32	2.13
Dimensions [length,width,depth] [m]:	14.6	4.27	1.00
Number of subdivided elements:	3		
First element midpoint coordinates [X-Y-Z]:	17.1	2.45	2.13
Direction of logitudinal and normal axes:	Y	X	
Total mass [kg]:	0.100E+04		
Mass per element [kg]:	333.		
Porosity factor [dimensionless]	1.00		

OBJECT 6 - HEPTANE-POOL

Parameter			
Object midpoint coordinates [X-Y-Z]:	2.20	7.32	0.153
Dimensions [length,width,depth] [m]:	0.610	0.305	0.305
Number of subdivided elements:	1		
First element midpoint coordinates [X-Y-Z]:	2.20	7.32	0.153
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	37.5		
Mass per element [kg]:	37.5		
Porosity factor [dimensionless]	1.00		

OBJECT 7 - CABLE-1LHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	2.44	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	0.244	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 8 - CABLE-2LHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	7.32	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	5.12	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 9 - CABLE-3LHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	12.2	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	10.0	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 10 - CABLE-1LMI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	2.44	2.30
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	0.244	2.30
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 11 - CABLE-2LMI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	7.32	2.30
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	5.12	2.30
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 12 - CABLE-3LMI

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	12.2	2.30
Dimensions [length,width,depth] [m]:	4.88	0.473	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	10.0	2.30
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 13 - CABLE-1LLO

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	2.44	0.686
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	0		
First element midpoint coordinates [X-Y-Z]:	0.473	0.244	0.686
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 14 - CABLE-2LLO

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	7.32	0.686
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	5.12	0.686
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 15 - CABLE-3LLO

Parameter			
Object midpoint coordinates [X-Y-Z]:	0.473	12.2	0.686
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	0.473	10.0	0.686
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 16 - CABLE-1RHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	1.85	2.44	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	1.85	0.244	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 17 - CABLE-2RHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	1.85	7.32	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	1.85	5.12	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

OBJECT 18 - CABLE-3RHI

Parameter			
Object midpoint coordinates [X-Y-Z]:	1.85	12.2	3.92
Dimensions [length,width,depth] [m]:	4.88	0.458	0.915E-01
Number of subdivided elements:	10		
First element midpoint coordinates [X-Y-Z]:	1.85	10.0	3.92
Direction of logitudinal and normal axes:	Y	Z	
Total mass [kg]:	2.57		
Mass per element [kg]:	0.257		
Porosity factor [dimensionless]	3.14		

V. PILOT-FIRE PARAMETERS:

Parameter	
LOCATION OF PILOT FIRE [OBJECT, ELEMENT]:	6, 1
FUEL TYPE:	SOLVENT [No. 4]
PILOT MASS [KG]:	1.00

VI. ROOM DATA AND MISCELLANEOUS PARAMETERS

Parameter			
Room temperature [k]:	298.		
Calorimeter temperature [K]:	298.		
Flame heat transfer coef. W/m^2K	23.0		
Conv. Heat tran. Coef. Outside	10.0		
Ceiling length, width, height [m]:	17.1	14.6	4.27
Forced ventilation constants [fh and fc]:	1.00	1.00	
Door height, width [m]:	2.13	1.22	
Door inflow coefficient	0.600		
Door outflow coefficient	0.700		
Hot gas absorption coefficient	1.30		
Ceil. Heat transfer coef. W/m^2K	10.0		
Plume entrainment coefficient	1.50		

Values for uncertainty analysis

Parameter	Distribution	Point value	Low value	High value
Flame heat transfer coef. W/m^2K	Shift-log	23.00	15.00	50.00
Conv. Heat tran. Coef. Outside hot gas layer W/m^2K	Normal	10.00	5.000	15.00

Table 5.3.2. Definition and failure probabilities for basic events used in the quantification of the LER.

Event name	Description	Base probability	Current Probability	Type	Modified for this event
ILOCA	Interfacing System LOCA initiator	1.00E-05	1.00E+01	TRUE	Y
CR1-XHE-XE-ERROR	Operator fails to align CRD (After venting)	5.00E-02	5.00E-02		N
CR1-XHE-XE-NOREC	Operator fails to recover CRD	1.00E+01	1.00E+01		N
CDS-TNK-HW-CST	Condensate storage tank fails	1.00E-04	1.00E-04		N
CRD-AOV-CC-FCTRL	CRD flow control station valves fail to open fully	1.00E-02	1.00E-02		N
CRD-CKV-CC-INJEC	CRD injection check valve fails	1.00E-03	1.00E-03		N
CRD-MDP-CF-PUMPS	CRD pumps fail from CC.	7.20E-04	7.20E-04		N
CRD-MOV-CC-MV20	Flow control valve fails to open fully	3.00E-02	3.00E-02		N
CRD-XVM-CC-FILTR	CRD suction filter valve fails to open	5.00E-03	5.00E-03		N
CRD-MDP-FC-TRNA	Train A failures	7.20E-03	1.00E+01	TRUE	Y
CRD-MDP-FC-TRNB	Train B failures	4.70E-02	4.70E-02		N
ACP-BAC-LP-DI	Division I AC power buses fail	9.00E-04	9.00E-04		N
ACP-BAC-LP-DII	Division II AC power buses fail	9.00E-04	9.00E-04		N
SSW-XHE-XE-ERROR	Operator fails to recover RHRSW	5.00E-02	5.00E-02		N
SSW-XHE-XE-NOREC	Operator fails to align RHRSW	1.00E+01	1.00E+01		N

Table 5.3.2. Definition and failure probabilities for basic events used in the quantification of the LER. (Cont.)

Event name	Description	Base probability	Current Probability	Type	Modified for this event
SSW-MDP-CF-MDPS	Common cause failure of RHRSW pumps.	3.70E-03	3.70E-03		N
SSW-MOV-CC-FLOOD	Valves fail to open	6.10E-02	6.10E-02		N
SSW-MDP-FC-TRNB	Train D component failures	3.80E-02	1.00E+01	TRUE	Y
SSW-MDP-FC-TRND	Train B component failures	3.80E-02	3.80E-02		N
CLOSE	Close open path	1.00E-07	1.00E+00	TRUE	N
IE-LOOP	Loss of offsite power initiator	1.70E-04	0.00E+00	IGNORE	y
IE-SLOCA	Small LOCA initiator	4.80E-06	0.00E+00	IGNORE	y
IE-TRAN	Transient initiator	1.10E-02	0.00E+00	IGNORE	y

Table 5.3.3. Fire-related parameters used and results obtained in step 3(6A), Intermediate Screening.

Factor		Value
Initiating event frequency [yr^{-1}]	λ_f	6.48E-03
Geometric factor	f_a	1.50E-01
Severity factor	f_s	3.00E-01
Non suppression factor	n/a	
Logic model value	Q	1.04E-01
Time of duration detected condition [Yr.]	t	4.75
Probability of a fire in t, $P(t) = \lambda_f x f_a x f_s x f_{ns} x t$	P	1.39E-03
Conditional Core Damage Probability= **PQ**	CCDP	1.45E-04

(*) Value from Table 4.3.6

Table 5.3.4a. Results from Montecarlo simulation using output data from COMPBRN for Cable tray 2-LHI.

STATISTICS	VALUE
Trials	500
Mean	451.19
Median (approx.)	447.34
Mode (approx.)	427.88
Standard Deviation	58.67
Variance	3,442.05
Skewness	1.01
Kurtosis	6.37
Coeff. of Variability	0.13
Range Minimum	313.70
Range Maximum	821.18
Range Width	507.48
Mean Std. Error	2.62

PERCENTILE	TIME TO DAMAGE [s]
0%	313.70
10%	380.35
20%	400.82
30%	422.38
40%	432.49
50%	447.34
60%	461.08
70%	473.43
80%	490.89
90%	525.15
100%	821.18

Table 5.3.4b. Results from Montecarlo simulation using output data from COMPBRN for Cable tray 2-LMI.

STATISTICS	VALUE
Trials	500
Mean	464.69
Median (approx.)	457.46
Mode (approx.)	439.92
Standard Deviation	56.06
Variance	3,143.05
Skewness	0.55
Kurtosis	4.16
Coeff. of Variability	0.12
Range Minimum	300.88
Range Maximum	728.69
Range Width	427.81
Mean Std. Error	2.51

PERCENTILE	TIME TO DAMAGE [s]
0%	300.88
10%	396.90
20%	423.34
30%	436.35
40%	446.95
50%	457.46
60%	471.53
70%	488.76
80%	510.10
90%	534.39
100%	728.69

Table 5.3.5. Fire-related parameters used and results obtained in Step 3-C, Final Quantification.

Factor	Distribution	Best estimate	Lower bound	Upper bound
λ_f [yr^{-1}]	Gamma	6.48E-03	1E-08	0.027
f_a	Maximum Entropy	0.15	0.03	0.75
f_s	Maximum Entropy	0.3	0.19	0.67
f_{ns}	Maximum Entropy	0.038	6E-03	0.047
Q	Point value (*)	1.04E-01		

Time of duration detected condition [Yr.]	**t**	4.75
Probability of a fire in t, $P(t) = \lambda_f \times f_a \times f_s \times f_{ns} \times t$	**P**	5.26E-05
Conditional Core Damage Probability= **PQ**	**CCDP**	5.47E-06

(*) Value from Table 5.3.6

Table 5.3.6. Quantification results for sequences of the Interfacing System LOCA event tree.

Impacted sequence #	Q for sequence	% Contribution to total Q
4	3.69E-08	3.55E-05
7	3.73E-10	3.58E-07
9	4.01E-03	**3.85**
11	4.05E-05	3.91E-02
12	1.00E-01	**96.10**
16	4.60E-12	4.42E-09
19	4.64E-14	4.46E-11
21	4.99E-07	4.80E-04
23	5.04E-09	4.84E-06
24	1.25E-05	1.20E-02
25	4.97E-07	4.78E-04
Q total	**1.04E-1**	

Table 5.3.7. Sequence logic for dominant sequences identified for the LER.

Event tree name	Sequence name	Logic
ILOCA	9	/RPS, /LCI, /CLOSE, RHRSW, /CVS, CR1
ILOCA	12	/RPS, /LCI, CLOSE

Table 5.3.8. Conditional cut sets for higher probability sequences

Cut set #	% Contribution	Frequency	Cut sets
Sequence # 12			
1	100	1.0E-1	CLOSE
Total (all cut sets)		**1.0E-1**	
Sequence # 9			
1	77.3	2.5E-3	SSW-XHE-XE-ERROR, CR1-XHE-XE-ERROR
3	7.3	2.4E-4	SSW-XHE-XE-ERROR, CR1-XHE-XE-NOREC, CRD-MDP-FC-TRNB, **CRD-MDP-FC-TRNA**
5	4.6	1.5E-4	SSW-XHE-XE-ERROR, CR1-XHE-XE-NOREC, CRD-MOV-CC-MV20
2	1.9	6.1E-5	SSW-XHE-XE-NOREC, SSW-MOV-CC-FLOOD, CR1-XHE-XE-ERROR
7	1.6	5.0E-5	CR1-XHE-XE-NOREC, CRD-AOV-CC-FCTRL, SSW-XHE-XE-ERROR
Total (all cut sets)		**4.0 E-3**	

Table 5.3.9. Dominant sequence conditional probabilities and importance measure for the LER.

Event tree name	Sequence name	CCDP	CDP	Importance (CCDP-CDP)	% Contribution
ILOCA	9	2.09E-07	1.97E-12	2.09E-07	3.7
ILOCA	12	5.26E-06	5.26E-11	5.26E-06	96.2
Total (All sequences)		**5.47E-06**	**5.47E-11**	**5.47E-06**	

Table 5.4.1. Definition and failure probabilities for basic events used on the quantification for the LER.

Event name	**Description**	**Base probability**	**Current Probability**	**Type**	**Modified for this event**
IE-IORV	Inadvertent SRV opening.	7.00E-03	1.00E+01	TRUE	Y
RPS-SYS-FC-MECH	Mechanical failure of the RPS	1.00E-05	1.00E-05		N
MFW-XHE-XE-NOREC	Operator fails to recover Condensate.	1.00E+00	1.00E+00		N
MFW-TDP-CF-PUMPS	Feedwater pump fail from common cause.	8.60E-04	1.00E+00	TRUE	Y
HCI-XHE-XE-NOREC	Operator fails to recover HCI.	7.00E-01	1.00E+00	TRUE	Y
HCI-TDP-FC-TRAIN	HCI train level failures.	3.80E-02	1.00E+00	TRUE	Y
ADS-XHE-XE-ERROR	Operator fails to depressurize (ADS)	1.00E-02	1.00E-02		N
ADS-XHE-XE-NOREC	Operator fails to recover ADS.	7.10E-01	7.10E-01		N
ADS-SYS-CF-VALVS	Common cause failure of 3/5 ADS system components	7.20E-05	7.20E-05		N
ADS-XHE-XE-MDEPR	Operator fails to depressurize the reactor.	1.00E-02	1.00E-02		N
ADS-SRV-CC-VALVS	ADS valves fail to open.	3.70E-03	3.70E-03		N

Table 5.4.2. Higher probability cut sets for impacted sequence.

Cut set #	% Contribution	Frequency	Cut sets
1	88.3	6.80E-03	IE-IORV, MFW-XHE-XE-NOREC,MFW-TDP-CF-PUMPS, HCI-XHE-XE-NOREC,HCI-TDP-FC-TRAIN, (ADS-XHE-XE-ERROR or ADS-XHE-XE-MDEPR)
3	11.7	9.01E-04	IE-IORV, MFW-XHE-XE-NOREC,MFW-TDP-CF-MPS,HCI-XHE-XE-NOREC,HCI-TDP-FC-TRAIN, (ADS-XHE-XE-ERROR or ADS-SRV-CC-VALVS, ADS-XHE-XE-NOREC)
Total (all cut sets)		7.72E-03	

Table 5.4.3. Data for fire-induced sequences for the LER.

Factor	Distribution	Best estimate	Lower bound	Upper bound
λ_f [yr^{-1}]	Gamma	7.97E-03	7.37E-06	0.084
f_a	Maximum Entropy	0.18	0.036	0.90
f_s	Maximum Entropy	0.3	0.19	0.67
f_{ns}	Maximum Entropy	0.98	0.42	1.0
Q (*)	Point value	7.72E-03		

Time of duration detected condition [Yr.]	t	1/12
Probability of a fire in **t** = $\lambda_f \times f_a \times f_s \times f_{ns} \times t$	P	3.51E-05
Conditional Core Damage Probability= **PQ**	CCDP	2.71E-07

(*) Value from Table 5.4.2

Chapter 6. Discussion and conclusions

6.1. Discussion

6.1.1. Introduction

Three relevant aspects related to the methodology will be discussed in this chapter. The first one is related to the documentation that, according to the author's judgment and the experience gained during the analysis of the case studies, should be provided to the ASP analyst to carry out his job. The second, the necessary revision of the consequences that for the developed fire ASP methodology may have the use of different methodologies for evaluating fire risk, used in different nuclear power plants. Finally, the presentation of future tasks that, under the opinion of the author, should be performed for a complete implementation of the presented fire ASP methodology.

6.1.2. Information to be provided to the ASP analyst

The analysis of fire-related failures is strongly dependent on information about the physical characteristics of locations, presence and distribution of equipment related to safety systems and the factors related to the effects of fires, such as parameters for fire modeling, from both targets and sources.

During the development of the case studies, the analysis was basically supported by both the Individual Plant Examination [IPE] and the fire-section of the Individual Plant Examination for External Events [IPEEE]. Being those documents a product of a complex and elaborated process, the detailed information regarding assumptions, data, considerations and basis for the results is not contained in them. However, it is that kind of information what the analyst needs to carry out the study and evaluation process. From the experience acquired during the analysis of the case studies, it was evident that the fire-ASP analyst should have access to the following documentation:

1) **Concerning basic documentation and fire-related studies.**

- The IPE, as the fundamental tool describing the logic models for different initiating events, accident sequences and systems and actions involved in those sequences.
- Fire-related section of the IPEEE.
- Enumeration of the initiating events in the plant and information associated with failures in plant systems.
- Fire modeling for locations and scenarios involved in the License Event Report [LER]. Sequences and cut sets for fire-initiated events.
- Detailed description of methodology and results for screened scenarios/locations from the fire PRA or similar. Original plant-specific fire location screening analysis database.
- Fire brigade training procedures and related activities.
- Transient combustible control procedures.
- P&ID for the Fire Protection System.
- Fire preparedness information, including Emergency Operating Procedures [EOP].
- Description of human-system interactions.
- Detailed description of the methodology used for defining factors used in the fire risk evaluation, especially if the plant has used marginal methodologies [FIVE or FIVE-standard PRA combination].

2) **Concerning locations.**

- General arrangement drawings
- Definition of both fire areas and fire zones.
- Definition of fire compartments.

- General layout of locations involved in the LER.
- Equipment/cable location database (Appendix R). Cable tray/conduit routing maps.
- List and detailed description the logic of systems and components whose failures may induce an initiating event.
- Plant fire barrier information, including fire rated barriers, cable wraps.
- Database about system diversity/redundancy in other locations.
- Description of contents of the Remote Shutdown Panel [RSP].

3) **Concerning scenarios involved in the LER.**

- Ignition sources and targets for scenarios considered in the location(s) involved in the LER.
- Spatial distribution of contents in locations and parameters for materials and components considered or to be considered in fire modeling.
- Values of parameters needed for fire modeling or physical characteristics of materials involved.
- Sequences involving the scenario and location.
- Consequences of damage to equipment/cables in the scenario/location, for those sequences leading to core damage.

4) **Concerning systems and components**

- Fault trees for systems involved in applicable sequences related to the LER.
- Detailed description of systems, at component level.
- Applicable data (failure probability) for every component of the fault trees

6.1.3. Study of consistency of different fire methodologies.

As it was established in Chapter 2, background, licensees submitted an IPEEE fire risk analysis by using three types of methodologies: FIVE [EPRI, 1993], standard fire PRA [NRC, 1983] and an aggregate of FIVE and PRA. The majority of licensees took some advantage of various features of the FIVE methodology.

According to the experience gained during the analysis and evaluation of the case studies, performed with the use of both the IPEs and IPEEEs from several nuclear power plants, it has been evidenced that the application of different methodologies in the ASP analysis process may give results that sometimes can be non comparable or, at least, should be analyzed very carefully.

The key aspect that deserves to be considered is referred to the models used by these two methodologies. The use of different fire models for evaluating the fire risk runs from a realistic approach by the standard fire PRA to a very conservative approach in the case of the FIVE methodology. Fire models have a direct effect on the Conditional core damage probability, central figure of the ASP analysis. Presumably, these methodologies work with different databases, initiating event frequencies, failure probabilities, human error probabilities, etc. Those differences may be significant when a ranking process for operational events designed as precursors is required. It is the opinion of the author that it is necessary to obtain the necessary consistency and coherency for evaluation of the same class of operational events.

The computer code COMPBRN-IIIe [Ho, Chien and Apostolakis, 1990] for probabilistic fire growth model calculates the fire growth time (or damage time) from a deterministic reference model and an uncertainty factor. It constitutes the central part of the traditional or standard fire PRA evaluation.

On the other side, FIVE methodology uses conservative estimates of fire parameters to provide conservative estimates of fire hazard conditions. In the fire modeling of FIVE, fires are conservatively assumed to achieve their peak heat release rate instantly and burn at this rate until the fuel is consumed. While this is reasonable for oil fire, for electrical cabinets the heat release rate gradually increases to the peak and then falls as combustible materials are consumed. Figure 8.1 is a representation of this behavior. The area under each of the curves in the figure is the total heat release, which controls the size and temperature of the hot gas layer. To make the FIVE fire model represent a realistic fire, the duration of the fire must be set to give a total heat release equal to that of the realistic fire.

Other conservatisms can be summarized [EPRI, 1993] as:

- Targets respond instantly to environmental temperature changes
- Only 70 percent of energy released is lost to boundaries
- Heat loss by convection in ventilated room fires is neglected
- Plume and hot gas layer temperature effects are superimposed

The major conservatism in the FIVE method concerns the frequencies of fires (fire initiator frequencies) and the damage associated with these fires. In FIVE, fire initiator frequencies are calculated from generic industry fire data, the EPRI Fire Events Database [FEDB]. This method additionally makes assumptions about the severity of these fires. From examination of the industry fire data in the FEDB, however, it is clear that very low fires have been as severe as assumed in the FIVE fire method.

Thus, the FIVE methodology allows the use of look-up tables for ease in quantifying the potential fire exposure to targets in a compartment. However, this method utilizes more conservative assumptions to reduce the complexity and number of variables required for calculation. Moreover, the fire modeling from FIVE does not consider uncertainty analysis and thus it can be considered as a bounding, very conservative methodology. It is judged that COMPBRN-IIIe code will have better realistic results than the use of look-up tables.

It is judged that some evaluation, as a task beyond this thesis, should be conducted to get an overall understanding of the impact that on the ASP methodology can have the fact of working with rather dissimilar methodologies. Fires models and databases should constitute the central part of that evaluation.

6.1.4. Tasks recommended beyond this thesis.

It is judged that the basic methodology has been implemented as required. However, in order to complement the ASP effort for external events, in general, and specifically for internal fires, it is judged that the following tasks should be implemented in the near future.

1) Plant-specific Fire-Risk Analysis compilation for ASP

It consists of compiling the IPEEE-fire-PRA system models for each plant in a consistent manner. It is complementary to the work done to compile the internal-events system models for each plant to support plant-specific ASP analysis for internal events. Having the plant-specific models would allow for a further task, which would be the formation of plant-class models, similar to what is actually done in internal events ASP. That would give expedition to the analyst and will give comparable results for different plants. One of the most important benefits would be that the experience would be easily and directly transferable to the rest of the same-class plant.

2) Fire initiating- event database for ASP

It consists of the adaptation of one or more existing fire initiating event databases such as the Electrical Power Research Institute [EPRI] database that was used to support the IPEEE/FIVE methodology, or the Sandia database that was supported by the Nuclear Regulatory Commission [NRC]. The usefulness of the fire initiating-event data can be greatly enhanced by linking a fire initiating-event to the fire location database. By cataloguing the fire events as they occur along with mapping of the locations where they occur, a consistent and convenient method for evaluating the fire-frequency distributions can be developed.

3) Fire accident sequence database for ASP

It consists of compiling in a consistent manner the principal fire-initiated accident sequences from either the IPEEE-fire-PRA or IPEEE-FIVE analysis for each plant. For the plants that have used the FIVE approach, it consists of developing the sequences based on both the vulnerability findings from the FIVE analysis and also the IPE system model. This database, developed for each plant, would help to determine whether a non-fire failure has significant implications as a fire accident sequence precursor.

4) Fire location database with safety mapping for ASP.

It consists of compiling in a consistent manner, from either the IPEEE-fire-PRA or IPEEE-FIVE analysis for each plant, the fire-location/safety-function mapping information necessary to support the fire-ASP analysis. A fire-location database is to be used as a screening device and a functional tool. Incorpcrating the corresponding mapping of safe-shutdown equipment, will allow for quick determination of whether or not a fire location is of consequence, and whether a PRA model exists or need to be developed or altered. It will also provide a basis for a real-time fire-initiating-event-frequency database.

6.2. Conclusions

A methodology for analyzing operational events from those reported by nuclear power plants has been developed and presented. This methodology focuses on the following aspects:

1. Development of a screening criterion for ASP fire analysis

2. Development of a standardized methodology for ASP fire analysis
3. Development of fire-associated-sequence benchmark cases for use in ASP analysis.

This methodology has been developed in such a way that it is consistent with the present approach currently used by the ASP program in the analysis of internal events. In some parts of the methodology it is applied the widely accepted use of judgment which, in many cases, is the most adequate tool to resolve a situation. Perhaps that is a difficult part to accept, but it is used in many aspects where the answers are not purely technical and experience is necessary. It is judged that those professionals involved in the fire ASP program should have the capabilities to apply expert judgment and apply for answers on those cases.

Some recommendations have been presented and discussed. They concern to **a)** the documentation that the analyst requires to perform his job, **b)** the required effort that should be carried out to evaluate the consistency between the methodologies applied for fire risk analysis and **c)** a list of future tasks that, under the judgment of the author, should be performed in the near future. All these recommendations would improve the applicability of the developed methodology and could contribute to make the work of the ASP analyst more efficient and realistic, so that the safety insights from operational experience could be readily available.

Finally, there must be stressed the benefits of the implementation of this methodology, described extensively in Chapter 1, which can be listed as follows:

- Insights about initiating events
- Insights about important components and systems
- Insights about human errors

- Insights about common cause failures
- Insights about regulatory requirements
- Insights about new research topics

Chapter 7. References

Apostolakis, 1993: G. E. Apostolakis, "Fire Risk Assessment and Management in Nuclear Power Plants", Fire Science and Technology, Vol. 13, Suppl. Pp. 12-39.

ASP Plan, 1994: U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data, "Integrated Accident Sequence Precursor Program Plan", draft dated March 2, 1994, included as Enclosure 1 to NRC SECY-94-076, "Status Report on Accident Sequence Precursor Program and Related Initiatives", March 22. Washington D.C.

CFR 50, 1993: Appendix R to 10 CFR 50, "Fire Protection Program for Nuclear Power Facilities Operation Prior to January 1, 1979," Revised as of January 1, 1993, U.S. Government Printing Office. Washington D.C.

EPRI, 1993: Electric Power Research Institute "Fire Vulnerability Evaluation Methodology (FIVE), Plant Screening Guide". Research Project 3000-41. Palo Alto, California.

Ho, Chien, and Apostolakis, 1990: V. Ho, S. Chien and G. Apostolakis, "COMPBRN IIIe: An interactive computer code for fire risk analysis", University of California at Los Angeles, College of Engineering, Report UCLA-ENG-9016. Los Angeles, California.

Hoertner, Kafka and Reichart, 1990: H. Hoertner, P. Kafka and G. Reichart, "The German Precursor Study: Methodology and Insights", Reliability Engineering and System Safety, Vol. 27. Pp. 53-76.

Kazarians, Siu and Apostolakis, 1985: M. Kazarians, N. Siu, and G. Apostolakis, "Fire Risk Analysis for Nuclear Power Plants: Methodological Developments and Application", Risk Analysis, Vol. 5. Pp. 33-51.

Minarick, 1990: J. W. Minarick, "The US NRC Accident Sequence Precursor Program: Present Methods and Findings", Reliability Engineering and Systems Safety, Vol. 27. Pp. 23-51.

NRC, 1975: U.S. Nuclear Regulatory Commission, "Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", Report WASH-1400. Washington D.C.

NRC, 1983: U.S. Nuclear Regulatory Commission, "PRA Procedures Guide", Report NUREG/CR-2300. Washington D.C.

NRC, 1986: W. T. Wheelis, "Users' Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base", NUREG/CR-4586, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC, 1988: U.S. Nuclear Regulatory Commission, Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities". This Generic

Letter is supplemented with additional guidance in Report NUREG-1335, "Individual Plant Examination: Submittal Guidance". Washington D.C.

NRC, 1991: U.S. Nuclear Regulatory Commission, Generic Letter 88-20, Supplement 4, "Individual Plant Examination for Severe Accident Vulnerabilities Due to External Events". This Generic Letter is supplemented with additional guidance in Report NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events [IPEEE] for Severe Accident Vulnerabilities". Washington D.C.

NRC, 1992: U.S. Nuclear Regulatory Commission, "Proceedings of an NRC Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data", NUREG/CP-0124. Washington D.C.

NRC, 1993: Sandia National Laboratories, "Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program [RMIEP], Internal Fire Analysis", for the U.S. Nuclear Regulatory Commission, Report NUREG/CR-4832, Washington D.C.

NRC, 1994a: L. Vanden Heuvel et al., "Precursors to Potential Core Damage Accidents: 1993, A Status Report", NUREG/CR-4674, Vol. 19. Washington D.C.

NRC, 1994b: U.S. Nuclear Regulatory Commission, "Event Reporting Guidelines, 10 CFR 50.72 and 50.73", Report NUREG-1022, Revision 1, Second Draft. Washington D.C.

NRC, 1995: Idaho National Engineering Laboratory, "Systems Analysis Programs For Hands-On Integrated Reliability Evaluations [SAPHIRE] Version 5.0, IRRAS", for the U.S. Nuclear Regulatory Commission, Report NUREG/CR-6116. Washington D.C.

NRC-CFP, 1994: U.S. Nuclear Regulatory Commission, "USNRC Regulatory Information Conference: Fire Protection," pp. 70~96, May 3-4. Washington D.C.

Siu and Apostolakis, 1985: N. Siu and G. Apostolakis, "Models for the Detection and Suppression of Fires in Nuclear Power Plants", Proceedings of the American Nuclear Society Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, February 24 - March 1. La Graye Park, Illinois.

Siu and Apostolakis, 1986: N. Siu and G. Apostolakis, "Models for the Detection Rates of Fires in Nuclear Power Plants: Development and Application of a Methodology for Treating Imprecise Evidence", Risk Analysis, Vol. 6. Pp. 43-59.

Siu and Apostolakis, 1988: N. Siu and G. Apostolakis, "Uncertain Data and Expert Opinions in the Assessment of the Unavailability of Suppression Systems", Fire Technology, Vol. 24. Pp. 138-162.