EGG-SSRE--9300

DE92 018040

RISK ASSESSMENT HANDBOOK

Frank G. Farmer
James L. Jones
R. Niall Hunt
Marvin L. Roush
Thomas E. Wierman

September 1990

EG&G Idaho, Inc.
Idaho Falls, ID 83415

Prepared for the
U.S. Department of Energy
Idaho Operations Office

Under DOE Contract No. DE-AC07-76IDO1570

RISK ASSESSMENT HANDBOOK

Abstract

The Probabilistic Risk Assessment Unit at EG&G Idaho has developed this handbook to provide guidance to a facility manager exploring the potential benefit to be gained by performance of a risk assessment properly scoped to meet local needs. This document is designed to help the manager control the resources expended commensurate with the risks being managed and to assure that the products can be used programmatically to support future needs in order to derive maximum benefit from the resources expended. We present a logical and functional mapping scheme between several discrete phases of project definition to ensure that a potential customer, working with an analyst, is able to define the areas of interest and that appropriate methods are employed in the analysis. In addition the handbook is written to provide a high-level perspective for the analyst.

Previously, the needed information was either scattered or existed only in the minds of experienced analysts. By compiling this information and exploring the breadth of knowledge which exists within the members of the PRA Unit, the functional relationships between the customers' needs and the product have been established.

TABLE OF CONTENTS

1 INTRODUCTION

Safety in the operation of processes involving hazardous materials is a critical issue. It is important from the perspective of those people at risk of exposure to the products of unplanned or accidental releases of radio-isotopes or other hazardous materials from a facility. It is also important from the perspective of the manager or owner/operator of the facility who accepts the potential liabilities which originate within the process. This latter perspective raises concern for the need not only to evaluate risk from possible accidents but also to examine the issue of inadvertent chronic or acute exposures of staff personnel to potentially damaging levels of hazardous materials during normal facility operation.

A facility manager must commit to: (1) knowing the risk of operating the facility, (2) managing the risks, and (3) operating within some acceptable level of risks. A Probabilistic Risk Assessment (PRA) can be useful to a manager in efforts to manage risk. While the use of PRAs has been particularly prominent relative to nuclear facilities, the techniques which are used to assess the risk from each hazard (not limited to radiation hazards) are similar over the complete range of concerns, and the risk assessment process is generally applicable to any hazards[1-9].

This handbook provides a facility manager the background information and guidance needed to determine what a PRA can and should do for him. PRAs can vary greatly in scope and required resources, and thus should be defined properly in advance to meet the specific needs for the given facility. PRAs can be used in a number of on-going management activities throughout the life of the facility; they must be conducted with those objectives in mind up front, however, if the necessary detail and format are to be available later to make those uses possible. With that need in mind, this handbook provides a discussion of various uses of PRAs so that a manager can plan for a risk assessment of optimal scope. To ensure that the completed risk assessment will actually be capable of meeting the needs of an in-plant decision maker, it is essential that the anticipated applications for the risk assessment be clearly delineated at the time the analytical requirement specification and methods selection[10] are performed. In addition, the handbook is written to provide a high-level perspective for the analyst to ensure that all available tools are considered for each task and that the best are selected to provide the most accurate, cost-effective analysis for the customer.

A probabilistic risk assessment can make a rational program of risk reduction feasible. A policy that all identified risks must be eliminated, or reduced as far as possible, can only lead to excessive costs. [If absolute safety is required, with no acceptance of risk, no operation is possible; all activity involves some risk.] Risk management[11-12] is the optimization of safety programs. It is best accomplished through a formal systems approach to hazards identification, risk quantification, and resource allocation/risk acceptance as opposed to case-by-case decisions.

A manager must face the risks of operating a facility directly. The historical defense of "Acts of God" for low-probability/high-consequence accidents is becoming increasingly untenable in most industries and activities. In addition, many significant or damaging events are seen, in retrospect, as having had precursor events or situations that, while not damaging in themselves, should have triggered a recognition that a damaging event was likely. Acting upon precursor events requires both an understanding of potential accident sequences (that have so far stopped short of catastrophic consequences) and the presence of a management climate in which abnormal events are recognized and studied rather than missed or "swept under the rug". This handbook, then, is viewed as an aid in identifying the proper role of PRAs in an overall program of risk management.

1.1 The Relationships Between Risk and Safety

Risk is defined here as a quantified estimate of the expected damages or consequences which a specific subject (people, property or the environment) will incur from a failure to contain a particular hazard. For all industrial facilities, this risk will involve the potential for economic cost either from loss of the productive capability of the facility or from liabilities incurred. These liabilities arise when failure to completely contain a process hazard results in injuries to people or damage to property either within or beyond the facility boundary.

The risk associated with operation of a complex facility arises from numerous sources. An accident **scenario** details a sequence of events from accident initiation, its propagation to an identified damage state, and the resultant effects on the subjects exposed. The risk arising from a single scenario by which there may be a failure to completely contain a process hazard is given as the product of the probability of the scenario times the consequence of the scenario.

Risk = Probability x Consequence

The total facility risk is then the summation of the risks associated with all of the many contributing scenarios.

While risk is a measure of the expected damage that will be incurred over some period of time (years, mission, etc.), **safety** is an expression of the acceptability of risk. When the level of risk is acceptable, one feels and defines oneself to be "safe".

The following example[13] typifies the subjectivity of thresholds for safety. An attempt to locate a nuclear power plant in a particular community tends to elicit a strong "instinctive" negative response from the general populace. However, evidence shows those persons residing near existing nuclear facilities accept the production of electricity from nuclear power more readily than the general public. The primary reasons for this response are hypothesized to result from individual and group experiential feedback which leads to a perception that:

a) Accidents really are very unlikely;

b) Operation of the facility does not have a major negative impact on the community, a situation commonly reinforced by the utility through their attempts to educate the public, and;

c) Local communities rely heavily on the utility and its facility for economic support.

There is also some evidence to indicate that the local populace may have an altruistic view of their living near the nuclear plant, based upon their conviction that the plant is beneficial to the general public. Within this example we see several possible influences which ultimately have an effect on the level of safety perceived as acceptable by differing segments of the general population, although the direct economic benefit is most likely the driving factor. The other factors tend more toward the role of justification for acceptance.

Since levels of acceptable risk are not absolute, and frequently are related to the perceived benefit from the activity, before a particular activity can be deemed safe, or the safety assessment judged "acceptable", the threshold of acceptability for risks must be defined.

Following this definition, the risk assessment will either demonstrate that the activity meets the established safety criteria or provide the necessary insight and guidance for a designer, manufacturer or program manager to institute hardware and/or administrative changes which reduce the risk to an acceptable level.

1.2 Integrated Safety Assessments[14]

Safety is not absolute, but is represented by a level of risk deemed acceptable. A safety assessment must provide assurance to the public and the facility staff that all the processes involving the manufacture or manipulation of hazardous materials are "adequately safe".

The process described here as an Integrated Safety Assessment (ISA) is presented in Figure 1. It can be seen that the ISA involves the integration of a standard Safety Analysis and a Probabilistic Risk Assessment. It is our objective here to examine the context in which the PRA contributes to the Integrated Safety Assessment. The ISA process can be viewed as composed of four major elements. They are:

a) Assurance that the equipment and procedures in the facility is capable of performing their assigned mission, i.e., preventing the release of hazardous materials in the presence of all credible threats to the boundaries which contain or confine them.

b) Assurance that the same equipment has a high likelihood of being available at the time of the threat and that the probability of a resulting failure of confinement or containment is acceptably low.

c) Consideration of all possible sequences of events and assurance that barriers are maintained or set in place to ensure the mitigation or prevention of consequences for all important accident scenarios.

d) Initiation of a process to maintain the validity of all assumptions made during the capability and risk or reliability assessments, for all phases of facility operation.

The dependency of assessments of "adequate safety" upon quantitative measures implies the need for both probabilistic and deterministic measures of facility performance. This section describes how one can use a combination of capability assessment and risk assessment to provide this requisite information. The next subsections define the terms Capability Assessment and Performance Assessment to bring clarity to discussions of the process of Integrated Safety Assessment; these terms may have different connotations than those commonly associated with them.

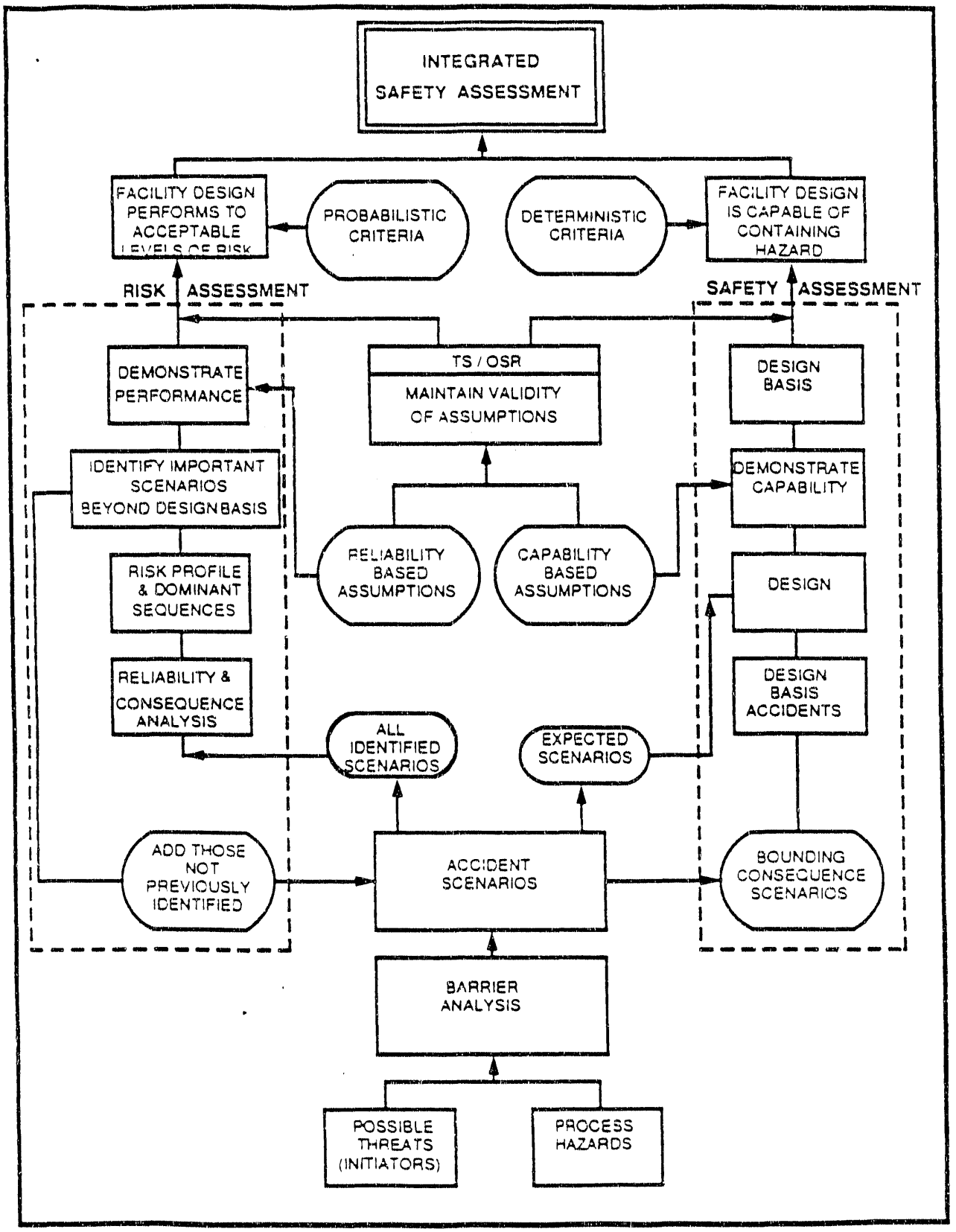

Figure 1 Integrated Safety Assessment

1.2.1 Safety Analyses

A Safety Analysis for a facility is commonly described as a deterministic evaluation of the ability of the facility to respond appropriately to a set of design basis accidents. For clarity, we will use the term Capability Assessment.

Capability Assessment, within the context of this document, represents the process used to verify that the facility is capable of responding to all identified credible or important threats (initiating events) without resulting in a loss of hazard confinement. In other words, Capability Assessment is verification that the design of the facility is capable of preventing or mitigating the source term release for all expected or important accident conditions and scenarios. This verification will often use thermal-hydraulic analyses and simulations, functional testing of hardware, personnel certification, walkthroughs and/or simulations to ensure that the capability exists under the expected conditions.

For example, verification that a pump produces sufficient head and capacity to keep a reactor flooded under accident conditions will be made with design reviews, thermal-hydraulic simulations and functional performance tests. The entire bounding scenario in which the hardware is called upon to perform becomes one of the design basis accidents for the design envelope, and analytical verification of the capability of all elements called upon to respond in the scenario is performed.

1.2.2 Probabilistic Risk Assessments[15-17]

A Risk Assessment, in contrast to a Safety Analysis, is predominantly a Performance Assessment.

Performance Assessment, within the context of this document, presumes capability and seeks to answer the question, "What is the probability that hardware will achieve requisite levels of capability when needed?" In other words, how likely is it that the facility hardware and staff will perform their intended functions to prevent or mitigate a release of the hazard when called upon.

For example, a Performance Assessment could involve the estimation of the likelihood that a pump will start and provide sufficient head and capacity to keep a reactor flooded under accident conditions.

The Risk Assessment combines hazards analysis, initiating event identification and hardware failure information to produce logical descriptions of the possible accident scenarios and their individual frequencies. From this process emerges the risk profile for the facility. This risk profile can be used to ensure that the design basis includes all scenarios which are either expected during operation or are important to risk.

1.2.3 Reliability Assessments

Reliability is defined as the probability that an item will perform as required without failure for a selected period of time (the mission time).

Reliability Assessments of specific systems are required as a part of the overall Risk Assessment of a facility. Reliability Assessments of certain systems may be sufficient for some

limited applications. The reliability analysis of selected systems may be part of an availability improvement program or may be needed to support a parts sparing program.

1.2.4 Achieving and Maintaining Validity of the Analysis

A Performance Assessment and a Capability Assessment are inevitably interdependent since the success criteria (used in the PRA) are established from the hardware capability tests and analyses, and scenarios defining the design basis envelope either originate within, or are confirmed by, the risk/reliability assessment. An Integrated Safety Assessment reflects the combination (or integration) of these two analyses and coordinates the iteration and data transfer between them. Only by integrating probabilistic and deterministic analyses can the risk status of the facility be defined and compared to established limits.

During the performance of these analyses and assessments, the boundary conditions reflect a set of assumptions. To ensure the validity of these assumptions during the operation of the facility, steps must be taken to administratively control them. The estimation of failure rates for the hardware are made under the assumption of a maintenance program that keeps the equipment in good operating condition. Controls which ensure that the plant or facility never moves outside the assumed operating envelope comprise the basis for Technical Specifications, Operating Procedures, and the Training Program.

1.3 References

1. W.S. Durant, C.R. Lux and W.D. Galloway, "Data Bank for Probabilistic Risk Assessment of Nuclear-Fuel Reprocessing Plants," IEEE Transactions on Reliability, vol. 37-2, 1988, pp 138-143.

2. D.F. Paddleford, "Use of Risk Analysis in Support of Decision to Provide Loss Prevention Systems Hardware to the Chemical Process Industry," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 98-99.

3. J.S. Arendt, D.J. Campbell, M.L. Casada and D.K. Lorenzo, "Risk Analysis of a Petroleum Refinery, Chemical Engineering Progress, Aug. 1984, pp 58-64.

4. D.F. Montague and G.A. Holton, "Risk Assessment of Mixed-Waste Sites," IEEE Transactions on Reliability, vol. 37-2, 1988, pp 178-191.

5. M.F. Versteeg, "The Practice of Zoning; How PRAs Can Be Used as a Decision-Making Tool in City and Regional Planning," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 91-97.

6. M.F. Versteeg, "The Seveso Directive in the Netherlands; The Requirement for Chemical Industries to Submit an External Safety Report Including a PRA," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 71-76.

7. M.V. Frank, "Quantitative Risk Analysis of a Space Shuttle Subsystem," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 211-217.

8. P.J. Pelto, "Use of Risk Analysis Methods in the LNG Industry," in Low-Probability High-Consequence Risk Analysis: Issues, Methods, and Case Studies, eds. R.A. Waller and V.T. Covello, Plenum Press, New York, 1984, pp 239-255.

9. R.A. Cox and D.H. Slater, "State-Of-The-Art of Risk Assessment," in Low-Probability High-Consequence Risk Analysis: Issues, Methods, and Case Studies, eds. R.A. Waller and V.T. Covello, Plenum Press, New York, 1984, pp 257-283.

10. R.N.M. Hunt and T.E. Wierman, "RAM Methodology Selection," Proceedings of the 17th Inter-RAM Conference for the Electric Power Industry, Hershey, PA, 1990, pp 136-141.

11. A frequently used risk management process is the Management Oversight and Risk Tree (MORT) process.

R.W. Eicher, N.W. Knox, The MORT User's Manual, DOE 76-45/4, SSDC-4, Revision 2, May 1983.

G.J. Briscoe et al., Applications of MORT to Review of Safety Analyses, DOE 76-45/17, SSDC-17 July 1979.

12. E.L. Zebroski, "Safety Management of Large Operations," in Risk Assessment and Management, ed. L.B. Lave, Plenum Press, New York, 1987, pp 113-126.

13. G.L. Rogers, "Residential Proximity, Perceived and Acceptable Risk," in Low-Probability High-Consequence Risk Analysis: Issues, Methods, and Case Studies, eds. R.A. Waller and V.T. Covello, Plenum Press, New York, 1984, pp 507-520.

14. R.N.M. Hunt and T.E. Wierman, "The Role of Risk Assessment and Safety Analysis in Integrated Safety Assessments," Transactions of the American Nuclear Society, 1990.

15. R.R. Fulwood and R.E. Hall, Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications, Pergamon Press, New York, 1988.

16. J.W. Hickman et al., PRA Procedures Guide, USNRC Report NUREG/CR-2300 vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1983.

17. D.M. Ericson, Jr. et al., Analysis of Core Damage Frequency: Internal Events Methodology, USNRC Report NUREG/CR-4550 vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

2 RISK-BASED MANAGEMENT PROGRAMS

In the management of any facility, we can always ask whether or not the performance of the facility is optimal. If it is not, it is important to know whether implementation of various enhancements proposed to improve its performance will result in a net benefit to the owner/operator. Answers to such questions are based on:

a) the costs of implementation of the enhancements, and

b) the quantified estimates of the expected benefits resulting from the enhancements.

One goal of a facility risk management program is the implementation of all plant enhancements shown to be cost effective. These enhancements may involve modifications of hardware and/or changes of procedures.

Measures of facility performance are usually linked in some way to economics. Typically, in all facilities there are two different kinds of factors which influence its economic performance:

a) production costs that can be reduced by increasing equivalent availability of the facility or by increasing productivity, and

b) liabilities arising from third party damages which originate with either operation of the facility or the product itself.

When these two types of costs are not optimally minimized, the departure from the optimum represents an economic loss.

2.1 Risk Management

A manager who wishes to manage the economic risk for any particular facility must first have an understanding of the meaning of risk, and then be cognizant of the importance of potential individual contributors to that risk for his particular facility.

Risk can be viewed as "the average expected loss rate during some defined period of time". For all industrial facilities, this risk originates with either the potential for economic loss from degraded or total failure of the productive capability of the facility, or from liabilities incurred when injury to people or damage to property beyond the facility boundary results from failure to completely contain a process hazard.

The following provides a list of potential sources of risk to which a facility manager/owner is exposed during the operation of his facility. The first question to be answered within the risk management framework is, which of these contributors are most important, and which should be of secondary concern.

2.1.1 Productivity Risk

"Productivity risk" (typically using economics as the metric) is the expected loss in productive capability of a facility over some period of time. This loss can result from:

- temporary degraded performance because of failure of repairable hardware/human process components,
- permanent degraded performance resulting from either failure of non-repairable human/hardware performance or the imposition of administrative (regulatory) constraints on the process,
- total, and permanent, loss of the facility as a result of a major industrial accident whose economic impact (repair costs) makes abandonment prudent, and
- total, long term, loss of productive capability of the facility as a result of regulatory action.

2.1.2 Risk From Liabilities

"Liability risk" (typically using expected health effects or economics as the metric) is the expected economic loss which will be incurred by a facility owner in making whole any third parties who are damaged by the industrial process. These liabilities can result from:

- chronic damage to on-site personnel as a result of exposure to common industrial hazards such as:
  - falls, bumps, burns
  - low levels of toxic, carcinogenic or mutagenic materials
  - low level radiation,
- acute damage to on-site personnel as a result of exposure to uncommon industrial hazards such as:
  - explosions
  - exposure to concentrated or lethal levels of toxic or carcinogenic materials
  - exposure to high levels of radiation or radioactive materials,
- chronic epidemiological damage to off-site personnel as a result of long term exposure to low levels of chemical or radiological materials released to the environment,
- acute physical or psychological damage to off-site personnel as a result of relatively short term exposure to:
  - hazardous materials (radiological, emitted from the facility)
  - blast or thermal energy
  - events which are perceived to be life-threatening,
- temporary or permanent loss of the use of land and property outside the facility which leads to:
  - clean-up and waste processing costs
  - reimbursement for loss of income to the property holders.

2.2 Risk-Based Management Program

Establishment of an effective risk-based management system for a facility requires that the owner/operator institute the following elements of the program.

a) Develop, or obtain access to, the capability to define the facility "risk profile" which will:
   - identify all discrete sources of risk associated with the operation of the facility, and
   - provide an assessment of both the absolute and relative magnitudes of each individual risk contributor in the facility.

b) The facility manager should have access to an on-site capability which can quickly estimate the effects of all changes to the facility. This is required so that decisions to institute permanent change at the facility are always made following an assessment of its impact on risk. These facility change considerations should include:

- facility design,
- operation or operating configuration, and
- institutional programs or organizational characteristics.

Evaluations of the above should be done "a priori" to ensure that any proposed changes to the facility:

- are not implemented unless a favorable risk/cost ratio is confirmed,
- do not lead to an unanticipated net increase in facility risk, as a result of a failure to adequately consider competing goals or objectives,

or, if net facility risk does increase,

- the increase in risk is accepted openly and in context.

c) To manage risk during routine facility operation, the facility manager should establish a process for quickly assessing the change in risk which results from:

- temporary plant configurational changes required for improved operability, or to allow the performance of maintenance or testing activities, and
- transient effects or operational events incurred or seen during facility operation.

Having the above information allows the facility operations manager to establish effective measures and apply resources to:

- prevent the plant from being placed in a high risk configuration, and
- prevent the recurrence of risk significant failures or events.

2.3 Risk-Based Performance Indicators

One of the prime goals in an effective risk-based management program is to provide the facility manager or oversight organization with a tool that can be used routinely to provide insights into the current facility risk profile, and to identify any trends which are likely to be indicators of degraded "safety" or increased risk. Ideally a "living" facility risk assessment would be useful in providing guidance in how to estimate or monitor the trend in facility risk. The question to be answered is one of how this can be achieved.

A limited set of functional variables exists which relates directly to the risk which a facility presents to its workers, the general public and the environment. If each one can be identified, and the relationship determined between these variables and routine plant information, then the foundation for a risk-based performance indicator program can be established.

In the assessment of facility risk, there are several discrete functional contributors which play a role:

- Frequency of events which can initiate an accident sequence
- Reliability of barriers which are used in the confinement/containment of the hazard
- Expected consequences from a failure to confine the hazard. This latter contribution is a function of:
  - the damage state for the facility following a barrier failure which may affect,
    - the magnitude or concentration of the released hazard
    - the duration of the hazard release

- the likelihood that potential targets can be protected following a failure to confine or contain the hazard.

The goal for a risk based performance indicator program is to identify the set of available operating facility information provides inference of undesirable trends in each of the above functional areas, and utilize the existing risk assessment to either:

- determine, "a priori" the points at which action must be taken to correct undesirable trends, or,
- estimate the significance of identified trends to determine the need for remedial actions.

The potential information which can be used in each area will be described, and from that an attempt will be made to identify specific "performance indicators."

2.3.1 Initiating Event Frequency

Initiating events have a single common characteristic that may represent a de facto definition, namely, that the event leads to a loss of one or more functions which must be maintained to keep the facility in its normal operating mode or state.

The loss of a normal function results from one or both of the following:

- Loss of capability of a success path which is maintaining the required function, resulting in a transition to a new facility operating state. Such a loss normally results from a functional failure of one or more of the process functional elements;

- Loss of integrity of the process system boundaries, which leads either to a loss of success path function or to an immmediate loss of confinement of the process hazard.

Any facility event or changing condition which affects the frequency of occurrence for either of the above must become an immediate candidate for surveillance as a Risk-Based Performance Indicator (RBPI).

Before this information can be used in an RBPI program, relevant and appropriate plant informational parameters must be identified. The following preliminary list is an attempt to provide this identification for each class of initiating events.

a) Process transients

1. In-process transients, or upset conditions which result from the loss of functional capability of a process element and necessitate a change in the facility operating state, are typified by step changes in process throughput, including shutdown which are required to mitigate the effects of functional failure of the normal process.

   In a reactor, these conditions are represented by SCRAMs or sharp reductions in power, which follow the failure of some part of the normal heat generation or heat rejection hardware.

   Note: The cause is not important, and can result from hardware or human induced failures.

2. Events which are external to the process, but which lead to an in-process transient condition, typified by loss of a vital support system, such as a failure to supply external power, cooling or process feedstock.

3. Failures which lead to loss of available support systems which increase the probability of occurrence of either 1 or 2, above.

4. Component functional failure resulting from the inadvertant or improper actuation of protective equipment (individual hardware protective trips).

The performance measure which is appropriate for each of the above can be represented by the RELIABILITY of each of the required NORMAL OPERATING functional elements.

The indicator for the reliability is the number of failures which are experienced per unit time for all normally operating process systems which cause or threaten a loss of a critical process function, i.e., those parts of the system, which if they fail, cause failure of the process. Failure represents the point at which functional capability is reduced to the point that the process fails, and is not necessarily "totally" failed.

b) System or process integrity

Boundary components (pipes, ducts, conveyors, conductors) are required to be functional because they provide the transport function within the process. These components are typically "passive" in nature and failure usually results from a loss of integrity.

Any information which indicates a reduction in the reliability of the components is a candidate for an RBPI.

In summary, potential RBPI's for initiating events are:

- reliability data (number of failures per period, or time between failures) for critical operating components or process elements (a human performing operations within the normal process may become a functional element)
  - failure history from maintenance records
  - reports of human failures (errors)

- evidence for the functional capability of critical operational elements
  - surveillance test data
  - operational parameter trending

- data providing the rate of occurrence for failures which result in spurious actuation of protective systems

- reliability data for passive components (e.g. number of failures of the process boundary), or the collection of data from which a prediction in failure probability can be made.

In each of the cases above, SCRAM or process shutdown data may provide most of the needs, although the goal is to be able to infer the rate of occurrence for initiators. Many events which only increase the potential for a process failure may have an effect on the future likelihood of

process failures, and as a result, information on failures which threaten process failure should be collected.

2.3.2 Barrier Reliability

Barrier reliability depends upon:

- the probability that barrier is in place and available at the time of initiation of the threat

Note: This barrier may be physical, it may be protected by the functionality of other support hardware (energy removal systems, for example) or may represent a distance which is maintained between the hazard and the target. In this latter case, human activities and associated administrative controls can also be considered part of the barrier and must be addressed in terms of their reliability.

- the probability that the barrier will fail at the time of the challenge
- the probability that the barrier will survive the initial challenge but fail before the threat passes

In each case, the systems involved are "safety" systems, and the measures which can be identified which directly affect barrier reliability are:

a) availability of safety systems, and;

b) reliability of safety systems (demand and operating).

Specific Information which provides inference of the actual reliability experienced in an operating facility are:

- test unavailability (hours disabled for test per period)
- maintenance unavailability (hours disabled for maintenance per period)
- contributions to unavailability which result from restoration errors following test or maintenance activities (unavailable hours per period)
- surveillance test failure data (failures per demand)
- operating reliability (failures per period when in an operating state)
- capability verification (operating surveillance test program)
- changes in system configuration represented by a newly discovered dependencies or changing requirements which affect system success criteria.

These factors can be condensed into four continuous inputs for PRA evaluation:

- safety system unavailability;
- safety system capability;
- safety system reliability, and;
- safety system architecture or system logic changes.

For effective monitoring and evaluation, these data should be rolled up to the system segment or sub-system level in the PRA and their importance verified with some form of consistent calculation from the PRA.

There are other less direct measures which may affect the reliability of safety systems, typified by the following:

- outstanding maintenance requests (backlog) for safety systems;
- outstanding modification packages awaiting installation;
- the average time taken to resolve and implement corrective actions which affect safety system availablity, reliability or capability;
- failures in the review and approval process for facility modifications, and;
- failures in human performance or administrative controls which result in human contributions to safety system unreliability.

The difficulty in using these types of indicators (there may be others not listed) is that their importance can only be assessed when they are related in terms of one of the broad indicating variables listed above, and used with the PRA. This may not be possible for all but a few important issues which can be evaluated on an "ad hoc" basis.

Note: the above discussion of barriers includes all of the barriers which play a role in the containment or confine ment of the hazard and reflect the series of barriers which are typically encountered when defense in depth becomes the design philosophy. This means that ventilation and filtering system performance are included in the above.

2.3.3 Expected Consequences

The expected consequences from an accident are affected by the release magnitude and duration, meteorology, population density and mobility of the material released. Factors which may be indicative of changing risk levels, and candidates for monitoring are:

- degraded conditions in the confinement scrubbing or filtering systems which may not affect the probability of release, but will affect its concentration, and
- results from any facility drills or emergency exercises which indicate changes in facility response capability.

There are several typical, measurable occurrences which may be indicative of performance in this area, namely:

- time taken for fire brigade or other emergency response activities, including evacuation drills;
- results from site emergency communications drills and communication system unavailability;
- backlog of unimplemented changes to the emergency response plan;
- time for resolution of emergency response issues;
- filter testing results (may also fall under the barrier reliability section), and;
- local population changes.

The difficulty in the direct use of the above is that the importance of individual trends may be difficult to ascertain. A detected trend without an attendant measure of importance can lead to misallocation of available resources (the squeaky wheel gets the grease).

2.4 Relating a PRA to Risk-Based Management

The generic requirements for the risk-based management program outlined above can be satisfied by a program in which a probabilistic risk assessment is one element. The requirements are:

a) The facility management must have access to risk assessment models which provide a complete description of the plant risk profile..

b) The risk models must be capable of modification to reflect both proposed and actual changes to:
- plant state or operating configuration,
- the performance levels or capabilities of individual systems and components, and
- human interfaces.

c) The modified models must be capable of re-solution to find the new plant risk profile, and that the timeliness of the re-solution is consistent with the needs of the decision making process.

d) Any institutional effects which manifest themselves as increased/decreased effectiveness of the human as he interacts with the hardware can be quantitatively assessed and incorporated into the risk models. These effects are typically measured as:

- change in the error likelihood for humans acting in the role of configuration or systems operations managers, and
- change in the availability/reliability/maintainability of individual components, sub-systems or systems which results from maintainer/maintenance actions.

e) The effects of the calculated or assessed changes in plant risk can be ascribed performance measures or metrics which are consistent with operating/management personnel experience.

The risk assessment models mentioned above are sufficient for facility management to use to establish "the worth of a change" and make technically justified decisions as to the disposition of proposed or needed changes. However, **the PRA does not intimate how the change is to be effected.**

As an example, the PRA may show that if the unavailability of a specific component is reduced by 10%, facility risk will be reduced by a significant amount. The PRA tells management the worth of a 10% change in component unavailability, but does not say how or whether it can be achieved. Achieving a 10% reduction in component unavailability only results when facility staff examine the discrete sources and contributors to component unavailability and institute corrective measures to reduce their effect.

This means that for comprehensive risk-based management, there are always two parts to the program.

a) Identification of areas in which change is needed, and quantitative assessment of the individual worths of all proposed changes.

b) Identification of ways in which the needed change can physically be achieved.

Conventional PRAs achieve only the former, and do so only on the basis of the assumptions made during the analysis regarding:

- component unavailabilities (data and its processing),
- component/system functional requirements and capabilities (event sequences and success criteria), and
- points and degree of human interactions (human reliability assessment and plant behavior).

2.4.1 Limitations of Baseline Risk Assessments

While risk assessment models can be extremely valuable within a risk-based management program, the models normally generated for a baseline risk assessment have some shortcomings. The following discussion is presented to highlight some of those limitations and indicate how they can be avoided.

- A conventional PRA focusses only on the health and property damage risks, and does not look at the probabilities that the process will fail and that the productivity of the facility will be reduced. This means that changes to the plant which are intended solely to improve productivity cannot be evaluated with conventional risk models. If this is an objective, then models should be constructed with the objective in mind.

- During the performance of a conventional PRA, decisions are made to deliberately omit certain plant components, or during the solution of the models certain components are truncated from the analysis on the basis of their negligible likelihood. This explicit or implicit elimination from the models is justified on the basis of assumptions made during the analysis. If these assumptions are erroneous, or a desire arises to change the assumptions, re-solution of the models is frequently necessary.

  Problems can arise when the user of the PRA wishes to modify the results of the PRA to judge the importance of a change in the availability of a particular component (if that component has been truncated from the analysis). Since the component does not appear in any of the results, when an attempt is made to see if an increase in its failure probability is important, the total value of the cut-set probabilities will not change, and the user may erroneously conclude that the resulting risk increase is zero.

  Such problems arise because a typical baseline risk assessment has a level of detail which results in the need for manipulation of literally billions of individual component-failure / failure-mode combinations (cut sets). The need for such extreme levels of detail is perceived to be necessary so that the risk importance of all individual risk contributors can be identified. The methods employed in both the large-event-tree/small-fault-tree and the small-event-tree/large-fault-tree approaches reach such levels of complexity that the analyst must resort to mainframe codes for solution of the plant model. The solution involves the generation of huge numbers of individual fault sets, which are then winnowed down to a managable group which can be ranked on the basis of their expected frequency of occurrence.

  In summary, the conventional baseline risk assessment results for a facility are generated to provide the dominant risk contributors under a particular set of

assumptions. A study of the risk exposure associated with removing a given system from service using the above cut sets may give erroneous results because the question violates the assumptions made in carrying out the previously mentioned truncation process. Therefore, such evaluations of risk exposure must be established as an objective before the PRA is done if valid results are to be obtained.

2.5 Discussion of PRA Applications

The performance of a Probabilistic Risk Assessment involves the development of models of the facility systems, data bases giving component failure rates, and a base-line of dominant risk sequences. These elements can be applied to many other uses. These uses tend to fall into three distinct categories. The first contains those cases where consideration is being given to changes in hardware to improve safety, availability, or process quality. The second includes those cases where consideration is given to changes in normal operations. The third grouping involves those considerations related to off-normal operations. The following sections contain lists which compile a number of Applications which can utilize the results of a Probabilistic Risk Assessment. Although a very limited description is given for the potential applications, references are provided to articles which will give greater detail about the application.

2.5.1 Discussion of Example Applications

"Living PRA Plant Model" Use

A completed PRA is a "snapshot" in time of a plant's characteristics. Maintaining a living PRA requires that all changes be evaluated and, when applicable, incorporated into the PRA, since any change in the plant procedures and/or hardware has the potential to change the plant's characteristics and the PRA results. The living PRA provides a current model which can be used to quickly evaluate the merit of potential changes or alternative operational strategies.

In addition, decisions on scheduling equipment outages can benefit from an examination of the related risk exposure. For example, if Auxiliary Feedwater Pump A is currently "out of service" for repair, the incremental risk associated with taking DC Bus B down for a particular maintenance activity may be unacceptably large and the maintenance consequently should be delayed. In another case of equipment being out of service, it may be valuable to alert the operators to the "dominant risk sequences" associated with the particular outage; their preparation and "alert status" may reduce the associated risk exposure.

A "Risk-Based Inspection and Testing" Program

Inspection and test programs are designed to examine passive components for any signs of deterioration of their capability and to test standby components to ensure their operability. Optimum scheduling of inspection and test intervals should be based upon the risk significance of potential failures of the components and upon the expected time interval between the appearance of early failure symptoms and the time at which the component will fail. Since passive components (such as a specific section of pipe) are often not included explicitly in a PRA, knowledge of this planned activity can result in the appropriate detail being built into the plant model.

2.5.2 Applications Involving Hardware Change Consideration

The availability of models of the plant systems and their relationships to system availability, plant availability, as well as to public health and safety makes it easy and economical to do thorough studies of the implications of any proposed changes to the hardware. Cost/benefit studies can be readily done and decisions based upon rational considerations. As more plant-specific failure-rate data become available, the data base for the plant model can be updated.

Baseline Risk Profile and Vulnerability Assessment[1-3]:

The baseline assessment identifies the "as designed" or "as built" risk levels and provides a ranked list of the individual contributors. This ranked list of contributors becomes the starting point for a comprehensive risk reduction program whether in the design stage or post-construction.

Condition Monitoring Analysis[4-6]:

The process of gathering information "on-line" for operating or standby hardware to provide an inference of internal condition or proper alignment can lead to real time assessments of failure propensities. The net benefit of these systems can be assessed with a risk model so that an estimate of their effectiveness can be established and the decision to install them made on a cost-justified basis.

Integrated Living Schedule (ILS) or Integrated Management System (IMS)[7]:

ILS/IMS is a process by which the implementation schedule for proposed facility changes is optimized on the basis of risk, within the normally present schedule and budgetary constraints.

Life Cycle Costing[8]:

The process of allocating resources for facility improvements on the basis of their impact on lifetime facility costs. The plant models provide a mechanism for simulating the worth of the changes during the expected plant lifetime so that their integrated benefits can be estimated, and compared with the costs of their implementation. For example, the costing of various alternative process temperature control devices should include the liability risks that are associated with potential thermal runaway accidents.

Living PRA Plant Model[9-12]

A completed PRA is a "snapshot" in time of a plant's characteristics. Maintaining a living PRA requires that all changes be evaluated and, when applicable, be incorporated into the PRA, since any change in the plant procedures and/or hardware has the potential to change the plant's characteristics and the PRA results. The living PRA provides a current model which can be used to quickly evaluate the merit of changes or alternative operational strategies.

Man-Machine Interface[13-14]:

The role of the human is critical in the operation of all industrial facilities. A risk model can provide the necessary information on the "worth" of changes to this interface to ensure that resources expended to improve them are optimally expended.

On-line Process Disturbance Analysis and Intelligent Monitoring and Alarming[15-17]:

Monitoring system parameters on-line may identify changes which are precursors to more significant events. A fault is diagnosed and provides forewarning to the operator

so that preventive measures can be taken in time to mitigate an event which may become an "initiator". This type of system can also be used to diagnose system state during an upset so that direct event-specific recovery actions can be implemented by the operating staff, and limit the severity of the event. The cost effectiveness of the system can be established with the risk models.

System Interactions[18-19]:

The safety characteristics of a facility are often dominated by interactions between two or more seemingly independent systems. A risk assessment can identify coupling mechanisms and can provide a quantitative assessment of their importance. The assessment can then be used to evaluate the various proposed countermeasures and allow the identification of the most appropriate response.

2.5.3 Applications Involving Normal Operations

The availability of models of the plant systems and knowledge of how operational procedures and maintenance policies affect system availability, plant availability, and public health and safety makes it easy and economical to do thorough studies of the implications of any proposed changes to the procedures and policies.

Administrative Policies/Practices Evaluation[20]:

Administrative Policies/Practices Evaluation is a process by which the effects of proposed changes to the management and operation of a facility can be measured in terms of their impact on hardware and human performance, and their "worth" established a priori with a risk model.

Availability Improvement Program[21-22]:

An Availability Improvement Program is a structured examination of the productivity characteristics of a facility, in which a ranked list of contributors to unavailability is identified. This list becomes the starting point for an availability improvement process in much the same way as the facility baseline risk profile became the starting point for a risk reduction process.

Performance Analysis[23]:

Performance Analysis is the process by which the individual events which occur in the operation of a facility can be simulated in the risk models to provide a high-level indication of facility performance. Performance indicators can be identified as surrogates for these detailed assessments.

Reliability Centered Maintenance (RCM)[24-27]:

RCM is a structured approach which identifies the important functional failure modes for plant hardware and the specific maintenance activities which can be implemented to prevent their unexpected occurrence. Risk models can provide both the prioritization for the examination of the individual hardware elements and the cost justification for any needed capital or operating expenses which result from the RCM analysis.

Risk-Based Inspection and Testing Programs[28-30]

A probabilistic risk assessment of a plant provides a basis for the prioritization of systems and components in terms of their risk importance. This can provide a rational basis for the scheduling of inspection and testing of those components and systems.

Risk Importance of Operating Events[31-33]:

To ensure that requisite resources are applied in the prevention of events which have risk significance, a risk assessment can provide direct estimates of the actual risk exposure from an experienced event. The magnitude of risk exposure for experienced events can then be used to prioritize the allocation of resources for a Corrective Actions program.

Technical Specification Conformance and Optimization[34-38]:

The technical specifications are designed to maintain the validity of the assumptions made in the facility safety analysis. It is economically important that they be no more restrictive than necessary, so risk assessments can be used to relax the requirements where appropriate. The duration of allowed safety equipment outage times and the frequency of required testings are defined by the technical specifications. These can be optimized with a risk assessment by ensuring that the requirements are modified to maximize the availability of individual hardware systems while maintaining an acceptably low level of risk.

2.5.4 Applications Involving Off-Normal Operations

A facility risk assessment provides a valuable resource — the list of dominant risk contributors. This list of those scenarios or event sequences which contribute most of the facility risk allows one to carry out accident planning in an effective manner so as to ensure that personnel are prepared to deal with the most important classes of off-normal operation.

Accident Management[39]:

Risk assessments provide a clear definition of the dominant facility accident scenarios and can be used to develop strategies for dealing with accidents (planning) and in some cases can be used during an accident to prioritize the operator's recovery and mitigation actions.

Training Program Risk Focus[40-41]:

Having a baseline risk model for a facility allows the training program to both develop effective procedural responses for the important scenarios identified by the risk analysis, and to allow some prioritization within the training program to ensure that the program includes a recognition of all the dominant risk contributors.

2.6 References

1. S. Sancaktar and D.R. Sharp, "Use of Probabilistic Risk Assessment and Economic Risk at the Plant Design Stage: An Application," Nuclear Technology, vol. 84-3, 1989, pp 315-318.

2. T. Arthur et al., "Probabilistic Risk Criteria and Their Application to Nuclear Chemical Plant Design," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 159-167.

3. S.H. Levinson and R.S. Enzinna, "Probabilistic Analysis for Conceptual Design of the Babcock & Wilcox Advanced Light Water Reactor," Nuclear Technology, vol. 91-1, 1990, pp 102-111.

4. C.D. Heising and W.S. Grenzebach, "A Computerized Diagnostic System for Nuclear Plant Control Rooms Based on Statistical Quality Control," Nuclear Technology, vol. 90-1, 1990, pp 7-15.

5. R. Bhatnagar, D.W. Miller, B.K. Hajek and J.E. Stasenko, "An Integrated Operator Advisor System for Plant Monitoring, Procedure Management, and Diagnosis," Nuclear Technology, vol. 89-3, 1990, pp 281-317.

6. J.R. Lewis, "Safety System Status Monitoring," Nuclear Safety, vol. 26-4, 1985, pp 459-467.

7. Delian Corporation, "The Living Schedule" Concept: A White Paper for Industry, prepared for NSAC/EPRI, issued by the Atomic Industrial Forum, August, 1983.

8. A. Lyytikainen, H. Malkki, and J. Holmberg, "Life Cycle Costing and Reliability Centered Maintenance — Practical Applications," Proceedings of the Seventeenth Inter-RAM Conference for the Electric Power Industry, Hershey, PA, 1990, pp 403-414.

9. S. Sancaktar, ""Living PRA" Concept for Risk Management of Nuclear and Chemical Processing Plants," in Risk Assessment and Management, ed. L.B. Lave, Plenum Press, New York, 1987, pp 201-204.

10. S.C. Dinsmore and H.P. Balfanz, "Living PRA Computer Systems," Nuclear Safety, vol. 30-3, 1989, pp 335-343.

11. E. Rumble and B.B. Chu, "An Approach for Integrating Plant Operations and Maintenance Information With Systems Reliability Analysis," Nuclear Technology, vol. 79-1, 1987, pp 7-19.

12. D.L. Batt, P.E. McDonald, M.B. Sattison and W.E. Vesely, Organization of Risk Analysis Codes for Living Evaluations (ORACLE), Report EGG-M-37186 (CONF-870820-12), 1986.

13. A.A. Husseiny, Z.A. Sabri, S.K. Adams and R.J. Rodriguez, "Automation of Nuclear Power Plants," Nuclear Technology, vol. 90-1, 1990, pp 34-48.

14. R.E. Uhrig, "Opportunities for Automation and Control of the Next Generation of Nuclear Power Plants," Nuclear Technology, vol. 88-2, 1989, pp 157-165.

15. A.B. Long, "Computerized Operator Decision Aids," Nuclear Safety, vol. 25-4, 1984, pp 512-524.

16. DASS: A Decision Aid Integrating the Safety Parameter Display System and Emergency Functional Recovery Procedures, Report NP-3595, Electric Power Research Institute, Palo Alto, CA, 1984.

17. D.G. Cain, "Review of Trends in Computerized Systems for Operator Support," Nuclear Safety, vol. 27-4, 1986, pp 488-498.

18. M.D. Muhlheim and G.A. Murphy, "Systems Interaction Analyses: Concepts and Techniques (Part I)," Nuclear Safety, vol. 30-2, 1989, pp 252-265.

19. M.D. Muhlheim and G.A. Murphy, "Systems Interaction Analyses: Concepts and Techniques (Part II)," Nuclear Safety, vol. 30-3, 1989, pp 400-412.

20. N.B. Closky, M.J. Hitchler, J.M. Grigsby and N.J. Liparulo, "The Use of PRA for Operational/Regulatory Issue Resolution," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 1040-1045.

21. R.C. Young, "UNIRAM Modeling of Nuclear Power Plants to Support Availability Improvement," Proceedings of the 13th Inter-RAM Conference for the Electric Power Industry, Syracuse, NY, 1986.

22. D.S. Richards, "Availability Improvement Programs Can Accrue Significant Economic Benefits," Proceedings of the Fourteenth Inter-RAM Conference for the Electric Power Industry, Toronto, 1987, pp 597-604.

23. M.A. Azarm, J.L. Boccio, W.E. Vesely and E. Lofgren, "Risk-Based Performance Indicators," Proceedings of the Fourteenth Water Reactor Safety Information Meeting, USNRC Report NUREG/CP-0082, vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1986, pp 155-161.

24. G.L. Crellin, T.D. Matteson, and A.M. Smith, Use of Reliability-Centered Maintenance for the McGuire Nuclear Station Feedwater System, Report NP-4795, Electric Power Research Institute, Palo Alto, CA, 1986.

25. R. Vasudevan, A.M. Smith, and T.D. Matteson, Application of Reliability-Centered Maintenance to Component Cooling Water System at the Turkey Point Power Plants No. 3 and 4, Report NP-4271, Electric Power Research Institute, Palo Alto, CA, 1985.

26. B.H. Fox, M.G. Snyder, A.M. Smith and R.M. Marshall, "Experience With the Use of RCM at Three Mile Island," Proceedings of the Seventeenth Inter-RAM Conference for the Electric Power Industry, Hershey, PA, 1990, pp 26-32.

27. J.P. Gaertner, C. Edgar and M.E. Rodin, "Large-Scale Demonstration of Reliability Centered Maintenance at Two Nuclear Generating Stations," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 303-307.

28. T.V. Vo, B.F. Gore, E.J. Eschback and F.A. Simonen, "Probabilistic Risk Assessment Based Guidance for Piping In-Service Inspection," Nuclear Technology, vol. 88-1, 1989, pp 13-20.

29. K.M. Campe, J.W. Chung and S.M. Long, "PRA Guidance in Nuclear Regulatory Commission Inspection Efforts," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 153-158.

30. T.V. Vo, M.S. Harris and B.F. Gore, "Probabilistic Risk Assessment Based Inspection Guidance for Arkansas Nuclear One Unit 1," Nuclear Technology, vol. 84-1, 1989, pp 14-22.

31. V.M. Bier and A. Mosleh, "The Analysis of Accident Precursors and Near Misses: Implications for Risk Assessment and Risk Management," Proceedings of the

International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 1125-1130.

32. J.W. Minarick, J.D. Harris, P.N. Austin, J.W. Cletcher and E.W. Hagen, Precursors to Potential Severe Core Damage Accidents: 1985, A Status Report, USNRC Report NUREG/CR-4674, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1986.

33. P. Bacher, J.P. Kus and D. Vignon, "The Use of Operating Experience to Reduce Risk," in Risk Assessment and Management, ed. L.B. Lave, Plenum Press, New York, 1987, pp 127-136.

34. G.R. Andre, N.L. Burns and R.L. Jansen, "Technical Specification Optimization Program — Reactor Protection System," Proceedings of the Fourteenth Inter-RAM Conference for the Electric Power Industry, Toronto, 1987, pp 195-202.

35. D.P. Wagner, L.A. Minton and J.P. Gaertner, "Risk-Based Analysis Methods Applied to Nuclear Power Plant Technical Specifications," Nuclear Technology, vol. 84-3, 1989, pp 233-238.

36. User's Guide for PRISIM — The Plant Risk Status Information Management System, Report JBFA-101-87, JBF Associates, Inc., 1987.

37. G.R. Andre, M.J. Hitchler, N.J. Liparulo and R.K. Rodibaugh, "The Use of Probabilistic Risk Assessment to Obtain LCO and Surveillance Frequency Relaxation," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 427-433.

38. "Risk-Based Analysis Methods Applied to Nuclear Power Plant Technical Specifications," Nuclear Technology, vol. 84-3, 1989, pp 233-238.

39. E.D. Copenhaver, J.H. Sorensen and M.V. Adler, "Organizational Interfaces in Emergency Planning for Nuclear Power Plants," Nuclear Safety, vol. 26-3, 1985, pp 273-285.

40. D.A. Dube, "PSA Support of Nuclear Power Plant Engineering and Operations," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 443-452.

41. S.-K. Cheng, "Seal Loss-Of-Coolant Accident and Recovery Actions Following Loss of Component Cooling Water," Nuclear Technology, vol. 84-3, 1989, pp 305-314.

3 OVERVIEW OF A PROBABILISTIC RISK ASSESSMENT

This section of the handbook is directed more to a discussion of the philosophy and content of a risk assessment than to the details of how to carry out a risk assessment. A list of references[1-6] giving various detailed procedures for the conduct of PRAs is included in Section 3.3.

3.1 A General Approach to Risk Assessment

The risk assessment process is primarily one of scenario development, with the risk contribution from each possible scenario which leads to the outcome or event of interest described in terms of a triplet:

$$\text{Risk}_i = \langle \text{scenario}_i, \text{likelihood}_i, \text{consequences}_i \rangle$$

The sum of the contributions from all unique scenarios represents the overall risk for the facility. Because the risk assessment process focusses on scenarios which lead to undesired events, the general methodology becomes one which allows the identification of all possible scenarios, calculation of their individual likelihoods and a consistent description of the consequences which result from each.

Scenario development:

> Scenario development inevitably leads to a set of descriptions, each of which describes how a barrier confining a hazard is threatened, how the barrier fails and the effects on the subject when it is exposed to the uncontained hazard.

This means that there are several generic elements to the risk assessment process:

a) Identification of hazards

A survey of the facility is initially performed to identify the hazards of concern. These hazards can be:

- ionizing radiation (nuclear),
- non-ionizing radiation (microwave, RF),
- chemical (toxic, reactive),
- thermal (contact, radiative, explosive),
- mechanical (kinetic or potential energy), and
- electrical (potential difference, E&M fields).

Each of these hazards, presumably, will be part of the process and will utilize normal process boundaries as the containment. This means that provided there is no disturbance in the process, the barrier which contains the hazard will be unchallenged.

b) Identification of barriers

Each of the identified hazards is examined in detail to define all the physical barriers which contain it or can intervene to prevent or minimize exposure of the subject to damage. These barriers may physically surround the hazard (walls, pipes, valves, fuel clad), they may use

distance to separate the subject from the hazard to reduce its effects (radiant energy, radioactive materials or location of process in isolation from the subject), or they may provide direct shielding of the subject from the hazard (protective clothing, bunkers, etc).

c) Identification of threats to the barriers

Identification of each of the individual barriers is followed by a concise definition of the requirements for maintaining each one. This can be done by developing an analytical model which has a hierarchical character or by simply identifying what is needed to maintain the integrity of each barrier by answering the following question:

What can cause degradation of the barrier?

- barrier strength degraded because of:
  - reduced thickness (geometrical change, erosion /corrosion),
  - reduced integrity (cracking, pitting, fatigue), and
  - change in material properties (toughness, yield strength - may be affected by local environment, e.g., temperature).
- load on the barrier increased by:
  - internal pressure, and
  - penetration or distortion by external objects/forces.

In many cases protection from the hazard results from maintenance of distance between subject and hazard, or the installation of a protective barrier around the subject. The nature of a barrier which is dependent on administrative controls may appear to be different than those consisting of functionally dependent hardware, but they are actually analogous to those described above.

An administrative barrier (distance) can be degraded as a result of:

- change in barrier thickness as a result of a failure to maintain its configuration (distance reduced between subject and hazard, akin to erosion - familiarity breeds contempt),
- reduced integrity as a result of procedural or administrative controls which are not adequate to cover all situations (cracks in the administrative armor), and
- change in material properties (effectiveness and format of controlling procedures and practices, the caliber, experience and training of the personnel who maintain the barrier, and their willingness to adhere to management directives and policy).

The load on the barrier can also be a factor in maintaining its integrity; how often a person moves within the proximity of a barrier (challenge rate), and productivity or efficiency demands put pressure on personnel to cut corners and challenge a barrier, or actually ignore it (stress on barrier).

Constant interaction between people and a barrier can have an effect on its capability much like fatigue in materials. Constant interaction can act like:

- high cycle fatigue - no apparent effects until one day the barrier fails completely without warning (initiation dominated), and
- low cycle fatigue in which several failures occur, but each is recovered (arrested) before propagation to full failure (propagation dominated).

d) Quantified Estimates of Releases

The risk assessment proceeds by defining those sequences of events in which the barriers protecting the subject may be breached, and then making the best estimate possible of the frequency for each sequence. Those sequences which release similar amounts of hazardous material under similar conditions of dispersal are grouped together and the frequencies of the various release groups determined.

e) Effects on the Subject

The range of effects produced by the release of hazardous material may encompass harm to people, damage to equipment, and the contamination of land or facilities. These effects are evaluated from a knowledge of the toxic behavior of the particular material(s) and the specific outcomes of the accident scenarios considered. In the case of the dispersal of toxic materials, the size of the releases are combined with the potential dispersion mechanisms to calculate the outcomes. The dispersal may depend strongly upon weather conditions and, in such cases, the complete range of conditions observed at that location over a multi-year period should be evaluated along with the likelihood of each.

From the generic nature of the risk analysis, there appears to be a common approach to understanding the way in which a subject is exposed to a hazard. This understanding is key in the development of logical scenario models which can then be solved. Quantitative and qualitative solutions can provide estimates of barrier adequacy and clues to effective enhancement.

Examination of these elements leads us to our first important insight into the process of developing scenarios. Each sequence of events is typically initiated by a disturbance of some kind. If the normal industrial process serves as a barrier which confines the hazard, any upset to the process could initiate a scenario which leads to loss of containment or confinement. If we understand the functions required to maintain normal operation of the process, it becomes apparent that anything which threatens a process function becomes an initiating event. It is also important to recognize that anything which directly causes failure of the primary containment boundary (first line of defense or first barrier) leads to a sequence of events which could lead to release of the hazard. Therefore, two important categories of initiators are:

- disturbance of the process (upset condition), and
- failure of the process boundary.

Note: the use of the term "process" is intended to embrace the broadest possible meaning. All hardware/software/human assemblies which, as a group or system, perform a single definable objective comprise the "process". A single facility may have several processes within it, even though it may have only one mission.

3.2 The Steps in Conducting a Risk Assessment

The following sections provide a discussion of the various parts of a PRA as we walk our way through the steps that must be accomplished.

3.2.1 Methodology Definition and Familiarization

Preparation for a risk assessment begins with a review of the objectives of the customer and assembly of any related analyses previously done on the facility of interest. An inventory of possible techniques for the desired analysis should be developed, and a similar inventory of technical resources. The technical resources available range from available computer codes to available facility experts and analytical experts.

An evaluation should be made of the resources required for each analytical option and a selection made of those which will prove to be most cost effective. The basis of the selection should be documented briefly, and the selection process reviewed with the customer to insure customer concurrence that their needs will be met.

The training needs of the staff must be evaluated and a training program covering the methods to be used should be planned and implemented.

3.2.2 Plant Familiarization

A general knowledge of the physical layout of the facility, the specific facility processes, administrative controls, maintenance and test procedures, and protective systems which function to maintain facility safety is necessary in order to begin the risk assessment process. All systems, locations, and activities expected to play a roll in the initiation, propagation, or arrest of an upset condition must be understood in sufficient detail to construct the models necessary to analyze the facility. Each analyst will have to perform a detailed inspection of the facility (walkdown) in the areas expected to be of interest and importance to their analysis.

To ease the way into the walkdown phase of the plant familiarization, arrange for the facility staff to supply knowledgeable escorts who have an overall understanding (both physical and operational) of the facility. Contact the security department (if necessary) to find out what they can do to make access to the facility easier. The facility contact named for the walkdown may be requested as the primary interface between the facility and the analysts. Prior to going to the facility, collect necessary documents such as the safety analysis report (SAR) and systems descriptions in order to plan the most productive walkdown possible. Interview enough people during the familiarization phase so that the analysts can obtain a sense of the facility's true operating philosophy. Try to identify the discrete operational modes for the facility. Take special note of the spatial relationships between hardware. Note any essential documents not gathered during the walkdown and plan for their collection after returning from the facility (including maintenance history, operating logs, operating procedures, emergency procedures).

3.2.3 Setting The Basis For The Analysis

Work with facility personnel to determine the ground rules for the analysis, the scope of the analysis and the configuration to be analyzed. Be sure to define faults and conditions to be included in or excluded from the analysis, operating modes of concern, and hardware configuration on the design "freeze date". The "freeze date" is an arbitrary date after which no additional facility changes will be modeled without negotiating with facility personnel. This negotiation will usually lead to a change in scope of the analysis; therefore, an agreement must

be made up front about how changes to the frozen design will be handled (out-of-scope negotiation on budget and schedule).

Agreement must also be reached concerning the requirements for future updates of the analysis. Do not overlook the manner in which the approach to be taken when information is not available to the analyst (e.g., operating and maintenance procedural inadequacies, hardware technical manuals not available, testing or surveillance programs not defined) is determined; that is, how will those assumptions be made? Define the events of concern (the undesired consequences which the customer wants to avoid) and the conditions which initiate the sequence which leads to events of concern (internal, external events). Ascertain whether events leading to personnel injuries or other undesired consequences (industrial hazards, maintenance activities) need to be considered for the analysis.

Consideration of all these items will lead to an agreement about the schedule, task breakdown and scope to be accomplished in minimal time and with little or no need for negotiation (except for out-of-scope activities) during the analysis.

3.2.4 Identification of "Initiators" or "Initiating Events"

From the list of identified hazards, select those of concern and develop functional models of the processes in which they are contained. This development leads to a perspective in which the events that can initiate potential accident scenarios can be specified.

Example: If the process contains alpha-emitters, a radiological hazard, and the process is one of reduction of the volume (incineration) of the waste containing the alpha emitters, identify the process functions:

a) Incineration (conditions for ensuring the oxidation reaction)

- combustion
  - fuel (primary fuel, secondary fuel, combustible waste)
  - combustion air (primary and secondary air)
- exhaust of combustion products
  - bottom ash
  - volatile waste, combustion gases and flyash.

b) Control of the process boundary (integrity of the system boundary and control or capture of any hazardous effluents which pass through the boundary)

- treatment and or recovery of hazardous waste materials
  - bottom ash processing
  - flyash removal and processing
  - volatile exhaust gas treatment (removal via adsorption)
  - particulate removal (filters)
- hazard confinement by process boundary
  - structurally intact
  - penetrations controlled (dampers, valves, etc).

A failure of any of the above functions will lead to either a direct failure of the primary means for confinement or the need to stabilize the process by shutting it down. If control of the boundary is successful, confinement is assured. This means that following an upset which

requires a change in process state, the transition must not result in failure of either the treatment of the waste processes or the process boundary, unless the hazard is naturally retained within the process as a result of a passive barrier (plate-out, settling).

The next questions to be resolved are:

What events can occur in operation that can lead to a direct threat to the integrity of the process boundary?

- loss of control of a penetration
  - normally closed, unplanned opening,
  - loss of filter capability to retain hazard,
  - loss of encapsulation of solid waste from the process,
  - flow conditions which overload or bypass filtering or waste product handling systems,
- loss of structural integrity of the process boundary
  - external forces which lead to mechanical degradation as a result of structural overload,
  - internal forces (overpressure, acute or chronic) which lead to failure of the boundary,
  - environmental conditions which lead to an acute or chronic loss of material strength and failure of the boundary (overtemperature leading to creep), and
  - material flaws which initiate and propagate to cause rupture or leakage (corrosion, erosion, cracking or fatigue failure).

What events can occur following a transient condition which leads to process shut-down?

- In addition to those identified above, there is an acute concern for overpressure which can result from conditions which are different from those encountered in normal operation
  - forced convection systems (fans) which overpressurize the system if it is "bottled up", and
  - explosions which result from the accumulation of combustible material which approaches its flash point.

REMEMBER:

Initiators either lead to a direct failure of the primary hazard confinement or cause uncontrolled transient conditions resulting in loss of structural integrity of the boundary.

Initiators can be identified by examining the functional nature of the process — any threat to one of these functions is potentially an initiator, as is anything which leads to a direct breach of the confinement boundary.

3.2.5 Initiating (Operational) Event Study

A facility may have one or more operational processes that occur in order to produce a finished product or products. In each operational process, specific functions are performed which result

in the final product. Each function is directly related to one or more systems which perform the necessary functional actions. The systems, in turn, are composed of components that accomplish the performance of system actions. As long as a system is operating within its design parameters, there is very little chance of challenging system boundaries in such a way that process materials may be released beyond those boundaries. Operation in this mode is called "normal" operation.

Loss of certain functions or systems will cause the process to enter an off-normal condition. Once in this condition, there are two possibilities. First, the state of the process could be such that no other function is required to maintain the process in a safe condition; *safe* refers to a mode where the chance of releasing process materials beyond the process boundaries is incredible. The second possibility is a state wherein other functions or systems are required to prevent release of process materials beyond the system boundaries. For this second possibility, the functional or systemic loss is an initiating event. Since these events are related to the operating process equipment, they are termed Operational Initiating Events.

Operational initiating events can also apply to shutdown and start-up processes. The terminology remains the same since, for a shutdown or start-up procedure, certain equipment must be functioning for the shutdown or start-up process.

For example, an operational initiating event found in the ATR (Advanced Test Reactor) PRA initiator list is Low Primary Coolant System Flow. Flow is required to transfer heat produced in the reactor to heat exchangers and ultimately to the cooling towers and the air. If this coolant flow function is reduced to the point where insufficient heat is transferred, core damage could result. Therefore, another system must operate to remove the heat produced by the reactor. For ATR this other system could be the firewater injection system. By definition, then, Low Primary Coolant System Flow is an operational initiating event.

A method for determining the operational initiating events begins by first drawing a functional diagram of the process. From the functional diagram, produce a goal tree with the top goal being successful completion of the desired process. The goal tree will contain logical combinations of the process functions that lead to the top goal. Each function can then be developed into its systems, and components can be combined in a logical method to represent success of that function. Potential initiating events are then the failures of particular functions, systems, or components; an occurrence which causes the process to fail. These potential initiating events are grouped such that members of a group require similar process system and safety system responses to cope with the initiators. These groupings will be the operational initiator categories. The initiating events can be quantified through specific analyses of the phenomena, actual data collected for a particular initiator, or using a combination of generic data with plant specific data in a Bayesian update.

3.2.6 Initiating (Non-operational) Event Study

Events which cause off-normal operation of the chosen facility process and require other systems to operate to maintain process materials within their process boundaries, but are not directly related to a process system or component, are non-operational initiating events. These events can be determined by using a Master Plant Logic Diagram (MPLD), examining initiating events from similar facilities with similar equipment and processes, examining plant records and maintenance evolutions for initiating events, and reviewing NUREG/CR-3862[7], Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk

Assessments, for PWR and BWR initiating events. All of the above methods are used to obtain the highest feasible level of completeness.

Of these methods, the one which does not involve review of work already done is the MPLD[8]. The MPLD is an analysis in success space to obtain the undesired event for a particular process. The top event might be "Offsite Exposure of the Public to Process Materials". Events that would make the top event happen would be logically connected to the top event. Each supporting event would be logically developed to a level consistent with the analysis being done. Proper development of the supporting events results in both potential operational and non-operational initiating events being listed across the bottom level of the MPLD. Non-operational events include (but are not limited to) internal fires, internal floods, seismic events, vulcanism, loss of coolant accidents (LOCA's), external floods, external fires, high winds, and transportation accidents. Initiating events which are mitigated by similar plant responses are grouped together into initiating event categories. Quantification of the initiating events can be accomplished, just as for operational initiating events, through specific analyses of the phenomena, actual data collected for a particular initiator, or using a combination of generic data with plant specific data in a Bayesian update.

An ATR example of a non-operational initiating event is the Seismic event. Seismic activity is a natural phenomenon and not directly associated with the ATR process. Seismic activity can defeat the function of many ATR process and safety systems; therefore, the seismic event is an initiating event.

3.2.7 Sequence or Scenario Development

The goal for scenario development is to derive a complete set of scenarios which identify all of the potential propagation paths which can lead to loss of confinement of the hazard or exposure of the subject following the occurrence of an initiating event. To describe the cause and effect relationships between initiators and the event progression, it is necessary to identify those functions (critical safety functions) which must be maintained to prevent loss of hazard confinement. The scenarios which describe the functional response of the process or facility to the initiating event are frequently displayed in an inductive or event tree format.

Digression: Why an inductive rather than deductive process?

If a deductive process is employed, there must be a model which describes all of the contributing events which lead to a single outcome. A typical initiating event may lead to one of many possible outcomes, each of which differ in severity and importance. An inductive model allows the display of all intervening event possibilities and their individual tracks to each possible outcome. A complete description of the process is possible.

The second reason for displaying the event scenarios in inductive fashion is that the conditionalities which result from the differing character of the initiating event are apparent, so that any quantification of the conditional probabilities is easily traced.

Another reason for using inductive behavioral models is that the scenarios are apparent — this is not true for a fault (deductive) model since it does not display temporal (time sequence) relationships between constituents of the cut sets.

It is possible to structure a set of deductive models which identify the relationships between all initiating events and the functional response of the facility or process for each defined outcome of interest (damage state). Such an approach, however, requires very precise definition of the conditionalities associated with each basic event, and can be quite difficult to accomplish.

3.2.8 Event Tree (inductive) analysis

Grouping of initiators

After each individual initiator is identified, each resultant process or facility response and outcome (plant damage state) must be described. There will be a two-tiered approach to this development — first the functional response will be identified, and then the corresponding hardware used to achieve each individual function will be included. The result of this activity is the construction of the event tree which displays all of the possible facility or process responses to that individual initiator. Events displayed in the tree are typically in terms of hardware systems.

Problem: there may be many, many initiating events, each of which requires its own event tree. To simplify the analysis, grouping of initiators is frequently performed. Grouping of initiators is possible if the facility response to each one in the group is identical, and the availability of systems responding to the individual group initiators is affected equally.

Question: How to inductively find the proper grouping?

- Find the initiating events which lead to direct confinement breaching.
- Find the initiating events that lead to direct release of process materials from the process boundary.
- Find initiating events which require the same set of actions, safety systems, and process systems to mitigate consequences within approximately the same time frame.
- Find initiating events which disable the process and specific responding systems in the same manner.

Once the initiators are grouped, the proper functional responses are determined for each initiator. Each group member is validated against the functional responses. The functional responses are broken down into systemic responses, and again each group member is validated against the systemic responses. If any group member does not require all the systems determined in the response, then that initiator has to be grouped with another initiating event group which requires its particular system responses.

3.2.9 Fault Tree Development

Event trees commonly involve branch points at which a given system either does work or does not work. The systems are built to be highly reliable, and therefore may not have an adequate record of observed failures to provide a dependable data base of failure rates. In such cases, fault tree analysis can be used to calculate the expected system failure rate. This is done by developing a system model in which the overall system is broken down into basic components or modules for which adequate data exists.

A second reason for performing fault tree analysis of a system is to develop a model of the system dependencies; that model indicates the conditions outside of the system boundary which can lead to system failure. Thus, if successful system performance is dependent upon an air-operated valve which is a part of the system, system failure might result whenever the plant air compressor system fails.

A Fault Tree Analysis of a system starts by specifying a given system failure as the "top event" of the fault tree. The complete fault tree is developed by creating a logic model of all of those conditions which can lead to the undesired top event. The development takes place from the top downward, until the items listed are components or independent subsystems with known failure rates; these items are "basic events."

Different event-tree modeling approaches imply variations in the complexity of the system models that may be required. If only front-line systems or combinations of systems are included as event-tree headings, the fault trees are more complex and must accommodate all dependencies between front-line and support systems within the fault tree. If support systems are explicitly included as event-tree headings, more complex event trees and less complex fault trees result.

3.2.10 Study of Internal Events External to Process

Events that originate within the facility proper are called internal events. Furthermore, we define events which adversely affect the process and which occur outside of the process boundaries but within the facility "internal events external to the process." This definition can be used as a parameter for binning (grouping) the final sequences resulting from the event trees.

Typical internal events external to the process are internal fires, internal floods, and high-energy events within the facility which do not result from the process under study.

3.2.11 External Events Study

The obvious counterpoint to the definition posed in section 3.2.10 is an initiating event that originates outside of the facility proper. This type of event is called an external event. Examples of external events are fires beginning outside the facility, floods beginning outside of the facility, seismic events, transportation events, volcanic events, and high-wind events. Again, this classification can be used in binning the event tree sequences.

3.2.12 Dependent Failure Considerations

To attain the very low levels of risk acceptable to the general public and participants in the nuclear industry and in future space exploration activities, the systems and hardware which comprise the barriers must have very high levels of reliability. This high reliability is typically achieved by using redundant and/or diverse hardware, providing multiple success paths. The problem then becomes one of ensuring the independence of the paths, because there is always some degree of coupling between their failure mechanisms, either through the operating environment (events external to the hardware) or through functional and spatial dependencies. A support system which is needed to power, control, cool, or lubricate physically-redundant trains of hardware is a functional dependency; two trains of fully redundant hardware sharing

a particular location in which cooling or motive fluid could be released by one (causing its failure) and lead to an explosion which fails the other have a spatial dependency. A fault on one electrical bus which is not physically and electrically isolated from another, may lead to a similar consequent failure on the second bus and result in total failure.

Several terms have been used to describe dependent failures, e.g., "common-cause" failures and "propagating" failures. We will use the term dependent failures and emphasize the importance of constantly being alert to possible dependencies.

As the reliability of individual systems and subsystems increases, the contribution from dependent failures becomes more important; at some point dependent failures dominate the overall reliability. Including their effects in the reliability models is difficult and requires that sophisticated fully-integrated models are developed and solved to find those failure combinations which lead to mission failure. It is through this (typically) deductive and integrated modelling process that insidious failure events can be identified. The treatment of dependent failures is not a single step performed during the PRA; it must be considered throughout the analysis.

3.2.13 Data Study

A critical building block in assessing the reliability and availability of systems is data on the performance of systems and equipment. In particular, the best resource for predicting future availability of equipment and plants is past operating histories. Component reliability indices are inputs to system reliability studies, and much of the validity of the results depends on the quality of this input information. It must be recognized, however, that historical data has predictive value only to the extent that (1) the conditions under which the data were generated remain applicable, and (2) constant failure rate data are not projected into the wear-out phase of component life. The determination of the various component failure data consists essentially of the following steps: the collection of generic data, the assessment of generic distributions, the statistical evaluation of plant-specific data, and specialization of the generic distributions using plant-specific data. Two types of events identified during the accident-sequence definition and systems modeling must be quantified for the event trees and fault trees in order to estimate frequencies of occurrence for accident sequences. They are: (1) initiating events, and (2) component failures, or primary events.

The quantification of initiating and primary events involves two separate activities. First the reliability model for each event must be established, and then the parameters of the model must be estimated. The necessary data include component failure rates, repair times, test frequencies and test downtimes, common-cause probabilities, and uncertainty characterizations. The establishment of the data base to be used will generally involve the collection of some equipment- or facility-specific data and integration with broad generic data bases.

The way data are evaluated will be affected by whether it is decided to use a classical or a Bayesian framework for treating uncertainties. The tools selected for use in sequence quantification will also affect the data analysis, in that the data must be in a form compatible with the tools. For example, the data analysis could yield probability distributions for reliability models that cannot be exactly represented by any defined distribution (e.g., a gamma or a lognormal distribution), and yet the quantification tools may require that all inputs be described by a set of predefined distributions.

Instead of collecting and analyzing raw data, it may be sufficient to use data from a previous PRA study. This could save considerable time and cost, but it may diminish confidence in the results.

For Initiating Event Frequencies applicable to light-water nuclear reactors, references 3 and 7 have both tabulations of data and references to many other data sources. References 3 and 9 have tabulations of data and references to other sources for Generic Failure Rate data bases. what about our draft report?

3.2.14 Quantification

Quantification of the fault-tree/event-tree sequences is done to determine the plant-damage frequencies. The approach is somewhat dependent upon the manner in which system dependencies have been handled. We will describe the more complex situation in which the fault trees are not independent of one another and have dependencies upon support systems.

The quantification will use the code SETS or some other fault tree reduction code; we discuss the process here for SETS. The SETS code accepts input in the form of fault trees, Boolean equations, and point values. Starting with fault-tree models for the various plant front-line systems and support systems and probability estimates for each primary event for these fault trees, the data are input to SETS. The fault trees for support systems are merged where needed with the front-line systems and converted into Boolean equation representations, and the equations solved for the minimal cut sets for each of the front-line systems (those identified as headings on the event trees). The minimal cut sets for the front-line systems are then combined appropriately to determine the cut sets for the accident sequences.

If all possible cut sets are retained during this process, an unmanageably large collection of terms will almost certainly result. Truncation (discarding of insignificant members) of the collection of cut sets is performed on the basis of the number of terms in a cut set or upon the probability of the cut set, while obtaining the minimal cut sets for the systems and accident sequences. This is a practical necessity because of the overwhelming number of cut sets that can result from combination of a large number of failures, even though the probability of any one of these combinations may be vanishingly small. The truncation process will not disturb our effort to determine the dominant accident sequences since we are discarding sequences that are each very unlikely.

A valid concern is sometimes voiced that even though the individual discarded cut sets may be at least a thousand times less probable than the average of those retained, the large number of them might represent a significant part of the plant risk. The actual plant risk might thus be considerably larger than the PRA result. Detailed examination of a few PRA studies of nuclear power plants showed that truncation did not have a significant effect upon the total plant risk result in those particular cases.

3.2.15 Report Development

The final report for the PRA should provide a summary compilation of all of the individual tasks, describe the methods and indicate the input data and materials used, and detail the results and insights. The risk contributions associated with each of the initiating events should be prsented. The report should detail the strengths and weaknesses of the facility analyzed, establishing a context in which to view the risk analysis results. The dominant accident sequences should be highlighted with discussion provided about potential risk

reduction opportunities that could be accomplished through changes in hardware, operation or maintenance procedures or policies, or specific training.

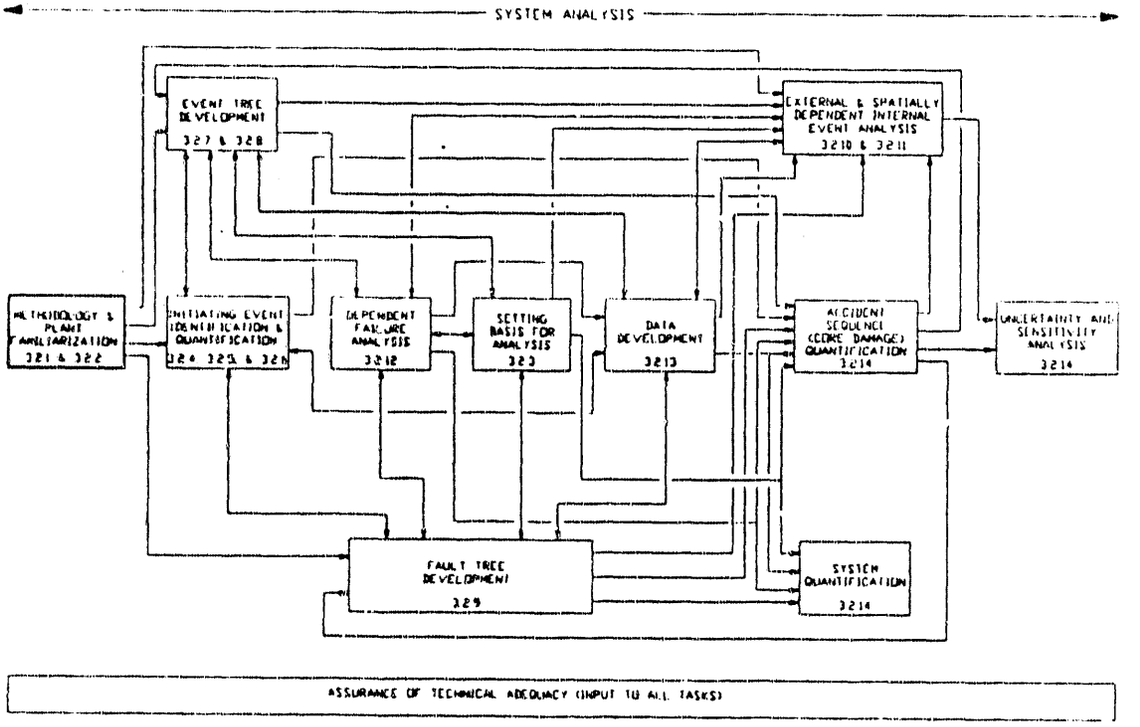

Figure 2 Risk Assessment Flowchart

3.3 References

1. M.P. Bohm and J.A. Lambright, Recommended Procedures for External Event Risk Analyses for NUREG-1150, USNRC Report NUREG/CR-4840, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1989.

2. D.D. Carlson et al., Interim Reliability Evaluation Program Procedures Guide, USNRC Report NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1983.

3. D.M. Ericson, Jr. et al., Analysis of Core Damage Frequency: Internal Events Methodology, USNRC Report NUREG/CR-4550 vol. 1, Rev. 1, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

4. R.R. Fulwood and R.E. Hall, Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications, Pergamon Press, New York, 1988.

5. E. Gorham-Bergeron et al., Evaluation of Severe Accident Risks: Methodology for the Accident Progression, Source Term, Consequence, and Risk Integration and

Uncertainty Analysis, USNRC Report NUREG/CR-4551, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

6. J.W. Hickman et al., PRA Procedures Guide, USNRC Report NUREG/CR-2300 vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1983.

7. D.P. Mackowiak et al., Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments, USNRC Report NUREG/CR-3862, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1985.

8. R.N.M. Hunt and M. Modarres, "Performing a Plant Specific PRA by Hand -- A Practical Reality," Proceedings of the 14th Inter-RAM Conference for the Electric Power Industry, pp 159-163, Toronto, 1987.

9. J.P. Bento, Reliability Data Book for Components in Swedish Nuclear Power Plants, Report No. RSK 85-25, Nuclear Safety Board of the Swedish Utilities for Swedish Nuclear Power Directorate, Sweden.

4 FACILITY CHARACTERIZATION

This chapter addresses the characterization of a facility, identifying those features which complicate the performance of a probabilistic risk assessment. The facility hazards, complexity, approaches to operation, and even its mission, will all affect the detail needed in a risk assessment as well as the analytical tools which will be required.

4.1 Facility Hazards and Potential Subjects

A first step in characterizing a facility for scoping a risk assessment is to identify the various hazards. These hazards may involve radioactive materials, toxic chemicals, biological agents, or high-energy materials (e.g., steam, compressed gases, or explosives). The inventory of each material present is important along with consideration of the speed at which toxic effects become irreversible. Consideration should also be given to the possibility that accident conditions can cause normal process materials to be transformed into toxic compounds.

The various mechanisms for exposure should be considered along with the toxicity/lethality of the hazards. These exposure mechanisms may include diffusion through or transport by the air, direct exposure and possibly the handling of contaminated materials. Dispersion may take place rapidly in the case of energetic releases either because the release is buoyant because of high temperature or because of kinetic energy imparted by the release conditions. Attention should also be given to possible degradation mechanism that will reduce the toxicity of the toxic materials in the normal environment.

The range of potential exposure subjects must be defined. Subjects that might be considered range from the process equipment itself, to the facility employees, the persons in neighboring communities, and the external environment. All barriers that separate the subjects from the hazards should be enumerated. These barriers should include administrative controls as well as physical barriers. The likelihood that a given subject will be exposed to the hazard is dependent upon the reliability of the barriers and also upon factors such as meteorology. Important factors will include the density of population surrounding the facility. The impact of a release upon the surrounding environment will be influenced by whether it contains pristine parkland, fragile ecosystems, or possibly agricultural land. The ease (cost) of immobilization of any residual hazard, or its removal from the environment will have an effect on the potential liability.

The internal events and external events that will be considered in the analysis must be specified. We are interested here in the events that could lead to a loss of hazard confinement. Possible events would include internal events such as flooding from pipe rupture, or internal fires, and external events such as wind, earthquakes, floods or fires.

4.2 Facility Mission

The risks associated with operation of a facility include considerations of the public health and safety as well as potential losses resulting from equipment failure or contamination. The latter issues may vary dramatically depending upon facility mission. A manufacturing facility will be impacted strongly by events that shut down the manufacturing line and thus decrease average availability of the process capability. A research facility might be impacted less by average availability but be sensitive to possible interruptions of very expensive one-time

experiments. A pilot plant, whose mission is to demonstrate the feasibility of a new process, might find a program canceled because of a leak of hazardous material, even though no persons were actually harmed by the release.

4.3 Facility Complexity

The complexity of the facility risk assessment model for is dependent on a number of factors. We will address these major factors below.

Degree of Redundancy — Single-train systems are simple to analyze (but not highly reliable) because system failure can be caused by the failure of many single components. For highly-reliable systems, system failure may not occur unless there is failure of 'm out of n' of the redundant elements in a particular section of the system. The analytical models used in such redundant cases may present a much greater challenge to the computer codes or analytical tools.

Support System Requirements — Operation of the normal process as well as safety systems may be dependent upon support systems which provide utilities such as: compressed air, cooling water, AC and DC power of various voltages, and inerting gases.

Degree of System Inter-Dependence — The dependence of one system upon others adds complexity to the facility model; that adds difficulty to the analytical process and can be important to the risk determination. A classic example of inter-dependence is that of a diesel-powered emergency electrical generator which is dependent upon a cooling-water system; under certain conditions, the cooling-water system, in turn, is dependent upon the emergency electrical generator to drive its pump.

Number of Process Control Variables and Process Sensitivity to the Control Variables — Successful operation of a given process may be sensitive to temperatures at various points, levels of liquids in several tanks, pressures in reaction chambers, flow rates into important volumes, and a large number of other specific variables. These factors increase the complexity of the model to be analyzed directly and in more complex ways when the process is non-linearly dependent on combinations of the variables.

Number of Subsystems or Process Steps — The complexity of the analytical model increases with the number of process steps and the number of subsystems that make up the facility systems.

Frequency and Level of Human Interaction to Control Process — Human involvement enters more than once in our consideration of facility characterization. Here we recognize that a facility may be dependent upon human action to accomplish normal control functions that could alternatively have been realized by hardware. These activities may need to be modeled as an integral part of the process operation.

Different Products and Different Mission Phases — Each of the different products may require a unique set of systems, and the systems needed or requirements to be met by the systems may change in the different mission phases (e.g., startup, test, operation, and shutdown).

4.4 Facility Operational Considerations

The complexity of conducting a risk assessment can also be affected by a number of other factors we will address here.

Maintenance Policies — The accuracy of the analytical model will be dependent upon the existence of defined policies and procedures. In some facilities, equipment is allowed to run until it fails. This policy tends to get maximum use out of a given part (assuming its failure does not damage other parts) at the expense of unexpected interruption of the process. A second approach is that of preventive maintenance in which parts are replaced at specified intervals, ideally shortly before the time at which they would wear out. These approaches can be improved in some situations by using a predictive maintenance approach in which sensors are used to detect early symptoms of wearout. Predictive maintenance then allows maximum use of the part without suffering the costs of forced outages. The failure rate used in modeling systems will be dependent upon the maintenance policy in use.

Degree of Automation — The degree of automation of the facility will determine the amount of human reliability analysis that will be required. The emphasis here is on the analytical tools that will assist in estimating human reliability in performance of the required actions.

Administrative Controls — The use of administrative controls will complement the physical protective barriers, sometimes controlling access to hazardous areas and other times controlling human actions in appropriate manners to enhance safety. These controls are an important part of the overall plant and its operation, and must be evaluated for risk contributions.

Operator Training and Facility Documentation — The quality of the human performance will be affected by the training of the facility staff. It will also be affected by the completeness and currency of the facility documentation. Any incompleteness in facility documentation will make the job of analysis extremely difficult.

Degree to Which Facility and Hardware Design Match Facility Mission — Operations which take place in facilities not designed for that use have the potential to be hazardous and are difficult to evaluate; there are usually greater uncertainties in knowing how the facility will respond to various accident conditions. It is necessary to determine if adequate barriers have been installed to contain the hazards.

5 ANALYTICAL METHODS

A broad range of analytical methods are utilized by different practitioners in the conduct of risk assessments. In addition, there exist other methods used for various forms of systems analysis. The selection of methods to be used for analysis of a given facility depends upon the features of the facility, the specific results needed, and the complete set of applications to be facilitated. It is our objective to provide assistance in selection of methods to be used and to encourage a broad look at available methods during that selection.

Analysts tend to develop great expertise in the use of a few tools (methods), then use these same tools for all analyses, whether those methods are overkill for the facility, appropriate for the job, or incapable of providing the complete results desired. Rather than following that course, we should each expand our consideration of methods to be used and select tools that fit the job at hand.

The difficulty the facility manager faces is that of ensuring that maximum use is made of the resources invested in the analytical process. Section 2 provided some assistance to see that numerous applications are considered before the analysis begins; this section should help to see that the methods proposed for the analysis meet the requirements of each application with minimum expenditure of available resources.

5.1 Linking Application/Facility to a Method

Several applications were presented in Chapter 2; we presume that each of these applications has a set of requirements that can be met adequately by some of the methods to be considered in this chapter. The characteristics of the facility as discussed in Chapter 4 will also have a significant impact upon the selection of the method(s) to be used. It is simply noted here that the analytical methods to be used and the associated documentation to be generated should be adequate to meet all of the requirements of all of the applications desired in the context of the facility of interest.

5.2 Attributes of the Methods

Cost — Some methods will drive the analysis to greater costs than others. The approach in this chapter is to determine the best method to use for a specific situation. This will be the least cost approach that satisfies all of the requirements.

Success / Failure — A success-oriented analysis can be of greater use in applications which relate to plant operations and to training programs. An example would be the development of an operator advisory system to indicate how to achieve success with only some systems functional. Failure-oriented analyses are the approach of choice to identify weak links and thereby highlight hardware that can benefit by redesign or modification.

Quantitative / Qualitative — Qualitative analysis methods are most useful for evaluating design, operations, and maintenance concepts; they are useful in defining hazards and in constructing hazardous event sequences. A list of cut sets for a system can identify undesirable dependencies and single- or double-failure events that the designer may want to design around. The event sequences can then be studied in more detail by quantitative methods. The quantitative methods can be useful in comparative evaluation of alternate design, operations, and maintenance concepts.

Inductive / Deductive — Inductive methods are those which postulate a given event or failure and then determine the possible outcomes; they are exemplified by FMEAs or event trees. Deductive methods are those in which a particular failure or outcome is postulated and the modes of system/component behavior which can contribute to this failure are specified. An example of a deductive method is that of fault tree analysis.

Model Capabilities — The analysis of the facility will involve some modeling of the systems, their behavior, and their interfaces. The size of the model will depend upon the facility itself and on the requirements for the analysis. It is critical that the method selected be appropriate for the size model needed. An additional element of consideration is the complexity of the model. The distinction between size and complexity is that size is increased by repetitive modules while complexity is increased by diversity and by system interactions. The size and complexity of the model are both affected by the degree of inclusion of implicit or explicit detail.

Human Reliability / System Analysis — Passive or highly automated systems may be able to use a systems analysis only. When human intervention can significantly affect the outcome, a human reliability analysis should be an integral part of the analysis.

Solution Speed — It is important to select methods that provide adequate speed of solution of both the original analysis and subsequent resolution with varied parameters. The requirements will vary depending upon the facility being analyzed, whether it is a preliminary or final design for the facility, and upon the number of parametric variations being considered.

Computer Facility Requirements — A feature of the methods being considered is whether they are amenable to hand solution, solution on a PC, or require the use of a mainframe computer.

User Interface — Many of the methods are embodied within computer code packages that provide varying degrees of 'user friendliness'. These interfaces may have graphical displays or may be usable by the non-expert, features that may be of considerable importance. The package may also provide valuable features such as an editor that will handle model variations or modifications.

Special Options — Some computer packages will provide the user with special options that may prove valuable, options such as: the handling of uncertainties, calculations of sensitivity to particular parameters, calculations of the importance of parameters, self-documentation of the models and the calculations, modularization of fault trees, and the possibility of global data base changes.

5.3 List of Analytical Methods

The methods below fall into "keyed" categories where the factors above will dictate one or more of these methods. The mapping may not be exact; in that case, the parameters that do not match should be well understood and must not pose a major fault with the "pick".

Cause-Consequence Analysis[1]

Cause-consequence analysis is a formalized combination of event tree analysis and fault tree analysis. The event trees are used to determine the sequence of events that can lead to the consequences of interest. Event trees are developed for each of the distinct classes of initiating events of interest. The fault trees are then used to model the causes of the failure events

within the sequences. The causes of the event sequence failures can be modeled as either system failures or component failures. If a lack of failure data exists on the system level, the causes would be modeled on the component level where such data are more readily available. The results of a cause-consequence analysis can be either qualitative or quantitative.

Event Tree Analysis[1]

Quantification of the risk associated with a plant requires the delineation of a large number of possible accident sequences. Because of the complexity of a plant, it is not feasible to write down (by inspection) a listing of all important accident sequences. Event Tree Analysis provides a systematic and orderly approach to properly understand and identify the many factors that could influence the course of potential accidents.

Construction of an event tree begins with the identification of initiating events, those events which have some potential to lead to a serious accident if equipment were to fail and/or persons were to act incorrectly. For each initiating event, a list is made of those actions or systems which will stop the accident progression or will reduce the severity of the final outcome. The event tree starts at the left of a diagram and lists headings across the top of the diagram for each of the mitigating actions or systems. The event tree starts with the existence of the selected initiating event and branches to represent the different outcomes (both failure and success) of the actions or systems.

The resulting event tree depicts, both visually and rigorously, the complete set of accident sequences that need to be considered individually.

Fault Tree Analysis[2-4]

Fault tree analysis is an analytical technique in which an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the undesired (top) event. The faults can be events that are associated with component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that can lead to the undesired event — the top event of the fault tree.

Construction of a fault tree begins with a definition of the top event and proceeds to an identification of its causes, which are connected to the top event by conventional logic gates. The procedure is repeated for each of the causes, and the causes of the causes, etc., until all the events have been considered. Fault tree analysis has found application in the aerospace industry for several decades and more recently has been widely used in the nuclear industry. Fault tree analysis is particularly useful in the early design phases of new systems when one can benefit from evaluating selected design alternatives. It is able to use failure rates, down times, repair times, and other dynamic systems functions or measures of these functions.

FMEA[5-8]

A failure modes and effects analysis (FMEA) identifies failure modes for the components of concern and traces their effects on other components, subsystems, and systems. Emphasis is placed on identifying the problems that result from hardware failure.

To prepare for an FMEA, several steps may be useful. The system to be analyzed, including its mission and operation, should be defined, with all interfaces clearly identified. The failure categories and environmental conditions may be specified. The extent to which each of these steps proceeds depends on the complexity of the system. Once the system and its intended use are described and understood, the FMEA can be performed.

The analysis uses a tabular worksheet to document the analysis. Specific entries in the columns typically include: a description of the component, its function, its failure mode, causes of failure, possible effects, and method of failure detection. In addition, columns may be present to indicate: failure probability, criticality (a quantitative measure of the component in the system), mitigation, and general remarks.

The main disadvantage of FMEA is that it considers only one failure at a time, and not multiple or pre-existing failures. There is no limit, in principle, to the number of components that can be considered simultaneously, but the number of combinations becomes prohibitively large with complex systems. The advantages of FMEA are that it is simple to apply and it provides an orderly examination of the hazardous conditions in a system.

GO Method[7-10]

The GO method is a success-oriented system-analysis technique. It uses inductive logic to model system performance, both successes and failures. It has the capability to evaluate system reliability and availability, identify fault sequences, and rank the relative importance of the constituent elements.

A GO model can generally be constructed from engineering drawings by replacing engineering elements (valves, switches, etc.) with one or more GO symbols, which are combined to represent system function and logic. The GO computer code uses the GO model to quantify system performance.

The GO model can be more easily inspected for validity in representing the actual system than can a fault tree, but is more difficult to review in terms of failure modes since it does not explicitly display failure modes. GO is also well suited to the analysis of systems involving great numbers of pieces of hardware or hardware that is physically highly interconnected.

GO-FLOW Method[11-13]

The GO-FLOW reliability analysis methodology has a modeling method and a calculational procedure that are both similar to the GO method. The GO-FLOW methodology can analyze a time-dependent system unavailability by a single chart with one computer run. It can readily analyze a system that has a complex sequence of time-variant states.

Goal Tree Analysis[14-16]

A goal tree is a visual representation of the goals and subgoals which must be satisfied to meet a top goal or "objective". A goal tree analysis is useful because it forces a great deal of thought to be given to all aspects of the problem at hand; it also leads to a clear display of the resulting organized knowledge in a form readily understood by others.

Following the definition of a single objective, development of the goal tree proceeds through the decomposition of this defined top goal into subservient or dependent goals, taking care to adhere rigorously to the hierarchy or dependence between each identified subgoal. To ensure

that the hierarchy is rigorously maintained, rules are applied during tree construction. The test for proper hierarchy indicates that, for any subgoal in the tree, the goal up one level in the tree will indicate **why** the selected subgoal should be achieved, and the subgoals one level below will indicate **how** the selected subgoal will be achieved.

Goal Tree/Success Tree Analysis[17-19]

A goal tree/success tree (GTST) has a tree-like hierarchical structure which can represent the deep-knowledge of complex process systems for problem solving. The upper part of the GTST model consists of a goal tree as described above for goal tree analysis. The lower portion of the tree consists of success tree models of the hardware components and systems which are used to achieve the lowest level goals of the goal tree. Although the GTST model can be used for reliability allocation during the design process, quantification is more difficult than for fault tree modeling. The success orientation is very useful for persons in plant operations, and has a structure that can be very useful in the development of expert systems.

Hazard Analysis[20-21]

Hazard analysis of a system in the development phase of its life cycle is a critical part of a system safety program. A hazard is defined as a potential for doing harm. The harm may take the form of injury, morbidity, or damage to equipment or other property. Hazard analysis encompasses a set of methodologies that first searches for potentials to do harm, which we call hazards. Having found these hazards, hazard analysis attempts to control them to an acceptable level. Control requires some understanding of the causes of the hazards. So hazard analysis not only seeks out hazards judged to be unacceptable, but also endeavors to determine the primary elements or events of the hazard generation process. Having discovered these elements/events, it attempts to modify their logical relationship so that the hazard is reduced to an acceptable level.

A Preliminary Hazard Analysis (PHA) is conducted early in the development stage, so it can aid the early formation of design and procedural safety so requirements for controlling the hazardous conditions, thereby avoiding costly design changes later on.

Human Reliability Analysis[22-23]

The treatment of human action is an important aspect of any Probabilistic Risk Assessment. Given the high degree of hardware reliability and redundant design associated with hazardous plant systems, human interfaces with the system are often significant contributors to system unavailability. The human actions may involve errors ranging from a failure to restore the equipment to operability following test and maintenance tasks to errors in manipulating the equipment in response to accident situations. On the other hand, operators may take action to correct misalignments of equipment or to overcome failures under accident conditions.

Master Plant Logic Diagrams[24-26]

A Master Plant Logic Diagram (MPLD) provides a visual display of the plant reliability structure so that the interrelationships can easily be seen among: (1) the initiating events, (2) the front-line systems, and (3) the support systems. The MPLD is generated by first determining the functional requirements which must be satisfied to prevent a severe accident. The front-line systems are then those systems which are present to satisfy the functional requirements.

The upper part of the MPLD displays the information normally contained in the front-line system event trees. The systems themselves are modeled into trains or subsystems which are logically related by their success criteria. The hierarchy of the model is displayed in the support system matrix. This matrix is developed by performing an interfacing systems FMEA for each front-line system component, and then similarly for the support systems. The last task in development of the MPLD is to identify the effects of initiating events on the availability of both front-line and support systems. A major value of this approach is its openness with analytic assumptions made deliberately and with a clarity provided to the overall analytic process.

Reliability Block Diagrams[27-29]

A reliability block diagram (RBD) is a model of a given system generated by an inductive process; the system is divided into blocks representing distinct portions of the system and the blocks are arranged to represent "system success" pathways. The model generally is used to represent active elements in a system in a manner that allows an exhaustive search for, and the identification of, all pathways for success. The RBD method is commonly used in plant or system reliability predictions or allocations. Numerical calculations of system reliability are made, and sensitivity studies can be performed to allocate desired reliability values and to optimize overall system reliability.

When used in the PRA process, the intent of the RBD is to combine components that are functionally in series in a system train into one supercomponent and then link together parallel supercomponents to form a summary model of the system. The collection of minimal fault sets or cut sets expresses the logical relationship between the system and its components.

Single-Point Failure Analysis[30]

This approach, applicable for relatively small systems, is accomplished by examining the system, element by element. Those discrete elements and/or interfaces whose malfunction or failure taken individually will induce system failure are identified. The technique is equally applicable to hardware systems, software systems, and formalized human operator procedures. Single-point failure analysis is a natural consequence of the application of fault-tree analysis as used to determine cut sets.

Sneak Analysis[31-33]

The technique of sneak circuit analysis is based on the discovery that topological criteria exist which can be used to recognize unplanned operational modes of an electrical circuit. A sneak circuit is a latent path or condition in an electrical system which inhibits a desired condition or initiates an unintended or unwanted action. This condition is not caused by component failures; rather, it has been inadvertently designed into the electrical system. Sneak circuits often exist because subsystem designers lack the overall system visibility required to interface all subsystems properly. When design modifications are implemented, sneak circuits frequently occur because changes are rarely submitted to the rigorous testing that the original design undergoes. Some sneak circuits are evidenced as "glitches" or spurious operational modes and can be manifested in mature, thoroughly tested systems after long use. Sometimes sneaks are the real cause of problems thought to be the result of electromagnetic interference or grounding "bugs".

A software sneak is defined as a logic control path which causes an unwanted operation to occur or which bypasses a desired operation, without regard to failures of the hardware system

to respond as programmed. Software sneak analysis has evolved along lines very similar to electrical sneak circuit analysis. Topological network trees are used with electrical symbology representing the software commands to allow easy cross analysis between hardware and software trees and to allow the use of a single standardized analysis procedure. As hardware and software systems increase in complexity, the use of interface bridging analysis tools such as sneak analysis, becomes imperative to help provide assurance of total system reliability and maintainability.

UNIRAM[34,35]

UNIRAM is an availability assessment methodology developed by ARINC Research Corporation for the Electric Power Research Institute. The method is used to predict the effectiveness of improvement options and to establish improvement goals.

UNIRAM is employed to determine the relationship between component reliability and unit equivalent forced outage rate (EFOR). Because of the different down times and effects on plant output for the components, each component has a discrete curve correlating reliability to unit EFOR. The curve is developed by using UNIRAM to model the system. The model is run repeatedly, using incrementally increasing values of component reliability. The worth curves present the results of complex reliability analyses in a manner that is both precise and easily understood. The curves can be used as a basis for, and in defense of, prudent management of complex facilities.

5.4 References

1. P. Cybulskis et al., Review of Systems Interaction Methodologies, USNRC Report NUREG/CR-1896, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1981.

2. W.E. Vesely et al., Fault Tree Handbook, USNRC Report NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1981.

3. P.K. Andow, "Fault Trees and Failure Analysis: Discrete State Representation Problems," Transactions of the Institute of Chemical Engineers, vol. 59, 1981, pp 125-128.

4. S. Caceres and E.J. Henley, "Process Failure Analysis by Block Diagrams and Fault Trees," Industrial and Engineering Chemistry Fundamentals, vol. 15-2, 1976, pp 128-134.

5. P.D.T. O'Connor, Practical Reliability Engineering, Second Edition, John Wiley & Sons, New York, NY, 1985.

6. US MIL-STD-1629A, Procedures for Performing Failure Mode, Effects and Criticality Analysis, National Technical Information Service, Springfield, VA, 1980.

7. W.V. Gately et al., GO, A Computer Program for Reliability Analysis of Complex Systems, Report KN-67-704(R), Kaman Sciences Corporation, 1968.

8. W.V. Gately and R.L. Williams, GO Methodology — Overview, EPRI Report NP-765, Electric Power Research Institute, Palo Alto, CA, 1978.

9. W.V. Gately and R.L. Williams, GO Methodology — System Reliability Assessment and Computer Code Manual, EPRI Report NP-766, Electric Power Research Institute, Palo Alto, CA, 1978.

10. W.V. Gately and R.L. Williams, GO Methodology — System Reliability Assessment and Computer Code Manual, EPRI Report NP-766, Electric Power Research Institute, Palo Alto, CA, 1978.

11. T. Matsuoka and M. Kobayashi, "GO-FLOW: A New Reliability Analysis Methodology," Nuclear Science and Engineering, vol. 98, 1988, pg 64.

12. T. Matsuoka and M. Kobayashi, "A Phased Mission Analysis by the GO-FLOW Methodology," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 1138-1145.

13. T. Matsuoka, M. Kobayashi and K. Takemura, "The GO-FLOW Methodology: A Reliability Analysis of the Emergency Core Cooling System of a Marine Reactor Under Accident Conditions," Nuclear Technology, vol. 84-3, 1989, pp 285-295.

14. R.N.M. Hunt, M. Modarres and M.L. Roush, "Use of Goal Tree Methodology to Evaluate Institutional Practices and Their Effect on Power Plant Hardware Performance," Proceedings of the Twelfth Inter-RAM Conference for the Electric Power Industry, Baltimore, MD, 1985.

15. M. Modarres, M.L. Roush and R.N.M. Hunt, "Application of Goal Trees in Reliability Allocation for Systems and Components of Nuclear Power Plants," Proceedings of the Twelfth Inter-RAM Conference for the Electric Power Industry, Baltimore, MD, 1985.

16. M.L. Roush, M. Modarres and R.N.M. Hunt, "Application of Goal Trees to Evaluation of the Impact of Information Upon Plant Availability," Proceedings of the ANS/ENS Topical Meeting On Probabilistic Safety Methods and Applications, San Francisco, CA, 1985.

17. M.L. Roush, M. Modarres, R.N.M. Hunt, D. Kreps and R. Pearce, Integrated Approach Methodology: A Handbook for Power Plant Assessment, Report SAND87-7138, Sandia National Laboratories, Albuquerque, NM 87185, 1987.

18. I.S. Kim, and M. Modarres, "Application of Goal Tree-Success Tree Model as the Knowledge-Base of Operator Advisory Systems," Nuclear Engineering and Design, vol. 104, 1987, pp 67-81.

19. H.T. Su, L.W. Chen, M. Modarres, R.N.M. Hunt, and M.A. Danner, "A Knowledge-Based Approach to Root-Cause Failure Analysis," Proceedings of Conference on Expert System Applications for the Electric Power Industry, Orlando, FL, 1989.

20. H.E. Roland and B. Moriarty, System Safety Engineering and Management, John Wiley & Sons, New York, 1983.

21. T.C. McKelvey, "How To Improve the Effectiveness of Hazard and Operability Analysis," IEEE Transactions on Reliability, vol. 37-2, 1988, pp 167-170.

22. A.D. Swain and H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Report NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, 1983.

23. A.D. Swain, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, Report NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, Albuquerque, NM, 1987.

24. R.N.M. Hunt and M. Modarres, "Performing a Plant Specific PRA by Hand — A Practical Reality," Proceedings of the 14th Inter-RAM Conference for the Electric Power Industry, pp 159-163., Toronto, 1987.

25. J. Wang, M. Modarres, and R.N. Hunt, "Probabilistic Risk Assessment: A Look at the Role of Artificial Intelligence," Nuclear Engineering and Design, vol. 106, 1988, pp 375-387.

26. J. Wang and M. Modarres, "REX — An Intelligent Decision and Analysis Aid for Reliability and Risk Studies," Reliability Engineering and System Safety, vol. 30, 1990, pp 195-218.

27. A.E. Green and A.J. Bourne, Reliability Technology, Wiley-Interscience, New York, 1972.

28. M. Shooman, Probabilistic Reliability of Engineering Approach, McGraw-Hill, New York, 1968.

29. "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," ANS/IEEE Standard 352-1987, pp 35-37.

30. J. Hrzina, "Single-Point Failure Analysis in System Safety Engineering," Professional Safety, vol. 25-3, 1980, pg 20.

31. Sneak Circuit Analysis of N Reactor, Report D2-118542-1, (prepared for the Atomic Energy Commission, Richland Operations Office), Boeing Aerospace Company, Houston, TX, 1974.

32. R.C. Clardy, "Sneak Circuit Analysis," in Reliability and Maintainability of Electronic Systems, eds. J.E. Arsenault and J.A. Roberts, Computer Science Press, Rockville, Md, 1980.

33. J.P. Rankin, "Sneak-Circuit Analysis," Nuclear Safety, vol. 14-5, 1973, pp 461-469.

34. R.C. Young, Maintainability Analysis Using the UNIRAM Methodology, Report AP-4580, Electric Power Research Institute, Palo Alto, CA, 1986.

35. R.C. Young, "UNIRAM Modeling of Nuclear Power Plants to Support Availability Improvement," Proceedings of the 13th Inter-RAM Conference for the Electric Power Industry, Syracuse, NY, 1986.

6 COMPUTER CODES

Most of the analytical methods listed in Chapter 5 have been used as the basis for constructing computer code packages. These codes can assist an analyst in building and editing analytical models, assembly and maintenance of a data base, and analytical computations. Some of those computer codes will be briefly discussed here to assist a new team of analysts in familiarizing themselves with the tools that are available.

6.1 Code Selection Factors

Once the analytical requirements are known and the methods to be used have been selected, only a small subset of the codes discussed in this chapter will be satisfactory. Where more than one code will do the job, the following factors are relevant to the selection.

- Compatibility — If system models exist from previous work or if data bases have been developed, which of the codes will be compatible with these materials? Which of the codes will be compatible with the needs for the follow-on applications?
- Availability — Which of the codes is available within the constraints of the task, e.g., resources?
- Experience of the Analysts — For which of the codes do you have experienced personnel? What training will be required to use each of the codes and how will it be provided?
- Additional Resources — Will the code selected require a computer other than those readily available? Will mainframe computer services be required?

6.2 Available Computer Code Packages

This handbook describes a number of computer codes currently available for the qualitative and quantitative evaluation of system or plant logic models. It is difficult to recommend a specific code for use in evaluating plant or system logic models. A great many codes or code packages are available, each having some particular objective toward aiding or improving the solution of complex models. Even for a particular function, it is difficult to reach a consensus on a given code because many different factors — such as available computer facilities, staff expertise, and the specific objectives of the analysis — affect selection of the computer codes. The intent here is to provide a starting point for someone who wants to find out what codes are available. There are numerous codes available in addition to those listed here; some of them are listed in NUREG-2300[1].

6.2.1 Computer Codes for Qualitative Analysis

These codes compute the minimal cut and/or path sets of a fault tree or perform Boolean reduction for the fault trees. Minimal cut sets give all the unique combinations of primary-events that cause system failure; minimal path sets give the smallest group of primary-event successes that guarantee system success. Details about the methods for determining minimal cut sets and minimal path cuts are described in the Fault Tree Handbook[2].

CAFTA+[3,4] — The CAFTA+ code, developed by Science Applications International Corp., is a PC(workstation)-based fault tree package which includes a full-screen fault tree editor, a multi-level reliability data base, a plotting package, a cut set generation routine, and a cut set results editor.

IRRAS[5] — The IRRAS (Integrated Reliability and Risk Analysis System) code, developed by the Idaho National Engineering Laboratory, is a microcomputer-based probabilistic risk assessment model development and analysis tool. IRRAS is an integrated software tool that gives the user the ability to create and analyze fault trees and accident sequences using a microcomputer. This program provides functions that range from graphical fault tree construction to cut set generation and quantification. Also provided in the system is an integrated full-screen editor for use when interfacing with remote mainframe computer systems.

PRA-WORKSTATION[6] — The PRA-WORKSTATION code, developed by EI International, is a microcomputer-based probabilistic risk assessment model development and analysis tool. Operating under the Microsoft WINDOWS environment, an editor is available to use in development of fault trees and to develop the data base for those events present in the fault trees. It also permits merging of fault trees. Following the input of all data for a fault tree, the tree can be graphically displayed. The fault tree can then be converted within the PRA workstation to a SETS format (see SETS section below), ready to be used in a SETS user program. The SETS code can be run directly from the workstation to quantify the fault tree and produce minimal cut sets. The cut sets can be viewed by a full screen viewer. Although fault trees can be directly quantified on the workstation, event tree sequences are quantified external to the workstation. SETS user programs have to be written for event tree sequence quantification external to the work station program. These SETS user programs can then be run from the workstation to quantify and generate minimal cut sets for sequences. In this sense the PRA Workstation is loosely integrated unlike the CAFTA workstation which can quantify trees and sequences essentially automatically due to the integration of the event tree and fault tree modules.

RISK-MAN[7] — The RISK-MAN code, developed by Pickard, Lowe and Garrick, Inc., is a microcomputer-based integrated PRA workstation package. It runs on a PC-AT or 386-based computer.

SETS[8,9] — The SETS (Set Equation Transformation System) code, developed by Sandia National Laboratories, is a general program for the manipulation of Boolean equations to find minimal cut or path sets. It finds cut sets of any length (the maximum length can be specified by the user) for fault trees with AND, OR, NOT, or special gates (specified the corresponding Boolean equation).

SETS is not a user-friendly program; it requires input from a program designed by the user. The user's program must be set up in a manner that the fault tree is evaluated efficiently, and it largely determines the evaluation algorithm. In general, two major algorithms are used. The first substitutes the Boolean equation of each gate from the top to the lowest branches of the tree; the second identifies independent subtrees,

replaces them by a module, and then performs a simple substitution of the Boolean equation from top to bottom. By manipulation of the user's program, these two algorithms can be applied first to intermediate gates and then to higher-order gates, achieving a bottom-up solution of the tree.

SETS has an option of logical merging for fault trees. This is very useful when systems in the event trees (i.e., front-line systems) must be merged with their support systems. Steady-state probability calculations are performed by SETS and make it possible to truncate the Boolean equation by probability or cut-set order. SETS can handle up to 8000 events (gates and primary events); it is capable of handling very large fault trees. Its main disadvantage is that an efficient fault-tree evaluation is highly dependent on a well setup user's program, which requires extensive knowledge and experience on the part of the user. An extensive routine for input-error checking is available.

A fully-functional microcomputer version of SETS is available as SETS/386[10] which is designed to take advantage of the increased speed and memory of the 80386 computers, although it can be run on a 286 machine.

6.2.2 Computer Codes for Quantitative Analysis

A variety of codes have been developed for the quantification of accident sequences. Most of these codes are used to calculate point estimate probabilities, thus providing a single number which can provide some measure of the relative safety of a given configuration of a system from the probability given for the top event. The codes will generally also provide a list of probabilities associated with the dominant minimal cut sets or primary events that contribute to system failure. Other quantitative results that are calculated by these codes are sensitivities and importance measures for primary events, minimal cut sets, and modules of the tree.

CAFTA+/ETA-II — The CAFTA+ code described previously, when combined with ETA, provides the capability to develop and modify large event trees. It can quantify and display sequences for each support state using fault tree results from CAFTA.

GO[11-14] — GO calculates the probabilities of all operating and non-operating states for a system. It uses a set of standardized functional operators to model physical primary events with mathematical entities that are easily identified as primary events. The modeling technique produces the GO chart, which corresponds closely to the physical layout, diagram, or schematic.

In the modeling procedure, 16 GO operators are used. Some of them are similar to fault-tree gates, but in addition to logic functions, time delays and switches can be modeled as well as complementary events and mutually exclusive states. The development of the GO chart consists of selecting the functional operators and connecting them with arrows to represent the flow of information. The GO code performs the logical connections and generates the minimal cut sets.

Required input is the GO chart and probabilities associated with the possible operational modes of each primary event, which is analogous to applying probabilities

for the primary events of a fault tree. The output consists of probabilities for several output events in several operating states. In addition, cut sets of up to order 4 are generated.

The GO code reduces storage requirements by eliminating low-probability paths at an intermediate stage of the processing and at the same time keeps track of the total of the discarded path. Because of the diversity and detail of the GO operators and the need to include all system primary events, the modeling process is quite complex. Furthermore, a change in probabilities often requires a complete rerun. However, the GO chart can be useful for design and system engineering.

IRRAS — The IRRAS code has quantification capabilities. After constructing the system fault tree models, the analyst processes these models within the integrated fault tree analysis package. This package includes the capability to read a fault tree and failure rate data associated with the basic events. The program then generates the minimal cut sets of the fault tree and quantifies the fault tree top event probability using the minimal cut set upper bound. Importance measures for both cut sets and basic events are calculated. The results are documented in various reports generated by the program. The user may truncate cut sets by size and/or probability and specify the gate where reduction is to begin. The user may perform some cut set level analysis by using a cut-set editor to modify the cut sets, saving the new cut sets, and recalculating the minimal cut set upper bound and the new importance measures.

The analyst defines accident sequences in terms of systems. IRRAS has the ability to link fault trees according to the accident-sequence logic to create core damage sequence cut sets. These accident-sequence cut sets are then quantified to determine the accident-sequence frequency. Importance measures are also calculated. Error-checking routines have been added to ensure that the input can be processed when it is time to analyze the fault trees.

In IRRAS, the graphical fault tree logic can be directly generated from alphanumeric input. This allows the user to read mainframe code input files, such as those for SETS, and generate the fault tree graphics. The logic models are then easily modified for re-analysis. IRRAS includes fault-tree, event-tree and cut-set editors to improve the analysis capabilities without requiring complete regeneration and reduction of the fault trees. Basic event or initiating-event frequencies are easily changed. Cut sets are easily modified with the cut-set editor to add recovery actions, or cut sets may be deleted if desired. These changes can be saved in the data base and quantified as desired.

IRRAS is written for an IBM-PC or compatible computer with 640k of main memory, a math coprocessor and a minimum of 7.5 Mb available on a hard disk.

PRA-WORKSTATION — This code provides the capability to graphically develop event trees. It provides the option of event tree sequence reduction as well as a mature RESULTS module which allows general manipulation of the event tree sequence cut sets. The capability is present to do importance and uncertainty analyses using a limited latin hypercube sampling engine. The system also has provision to assist the analyst in doing cost/benefit analyses. The approach to handling of failure rate data allows Bayesian updates on individual component data or on groups or classes of components.

For documentation, complete descriptions of the origins of each data value can be kept with that data value. Other data bases can be cloned and modified from the base case data base without changing the base case data. The development of data can be done on a PC while the system quantification is done on a mainframe.

EVNTRE[23-24] — This FORTRAN code was developed at Sandia National Laboratories for probabilistic risk analysis of severe accident progressions for nuclear power plants. EVNTRE is a generalized event tree processor. It is useful for a large class of applications since many safety and risk assessments involve analyzing the progression of events that lead to a large number of conditions or scenarios. Such progressions can depend upon both continuous and discontinuous processes. The outcomes of particular events can affect subsequent events. Generally, the large uncertainties in the outcomes of specific events can lead to many possible progressions for a given scenario. The analysis's most important goals usually include the identification of important factors. Examples of the factors are the details of the scenario definition and the assumptions regarding individual processes which strongly influence the output of interest and its associated uncertainty.

EVNTRE has the capability to process complex event trees that systematically follow the progression of severe accidents. Although detailed computer programs exist to simulate some aspects of the progression of severe accidents, few mechanistic codes have scope sufficient to describe the full spectrum of possible events. Thus, performance of calculations for all possible variations in scenario and accident progression is impossible. On the other hand, event trees can integrate the results of detailed calculations and provide a generalized context for their interpretation.

A flexible facility in EVNTRE used for processing multiple sets of input allows Monte Carlo sampling for generating an approximate mapping from input to output. By using a post processor (such as PSTEVNT[24]), the output can be sorted or reclassified and summary tables can be generated. The mapping results and statistical analyses of the branches form the basis of the sensitivity analysis t) at identifies the questions, branches, input parameters, or dependencies in the tree which contribute to the outcomes of interest and the associated uncertainty.

The branch split fractions for the questions or events for a particular scenario sometimes depend on the questions or events and system functions from both a current step in the scenario and a previous scenario step. The event tree developer can identify the possible cases for which the branch split fractions in a given question should be different. Boolean expressions involving the branches taken at previous questions in the tree can be developed to characterize each case. Branch split fractions can be supplied for all cases, and EVNTRE will use the particular split fraction assigned to the first case whose Boolean expression is satisfied by the path through the tree.

Many questions may be required to adequately describe the progression of the scenario through all relevant time regimes. However, characterization of the individual paths through the tree in terms of a small number of characteristics or attributes can be much more useful. EVNTRE allows binning of the paths through the tree according to user selected characteristics.

EVNTRE efficiently stores the input information in a format that can be easily adjusted if required. EVNTRE uses the FORTRAN-77 PARAMETER statement to set the dimensions of the various storage arrays in COMMON blocks. The user can adjust the values in the parameter statements to accommodate the size of the event tree. The utility code EVNTSUB is designed to perform a global substitution of these parameters into EVNTRE.

EVNTRE has been successfully run on the following machines:

VAX machines with the VMS operating system,
VAX machines with the UNIX operating system,
MS-DOS machines using Lahey FORTRAN,
PRIME computers with the PIC operating system,
and CRAY machines with the COS operating system.

6.2.3 Computer Codes for Time-Dependent Unavailabilities

FRANTIC[15] — The FRANTIC (Formal Reliability Analysis including Testing Inspection and Checking) code computes the average and time-dependent unavailability of any general system model like a fault tree. It can be used to assess the effects on system unavailability of test downtimes, repair times, test efficiency, test bypass capabilities, test-caused failures, and different test staggering. The events handled by FRANTIC are primary events involving periodically tested, nonrepairable, and monitored components; human-error and dependent-failure contributions can also be modeled.

FRANTIC uses a system equation that represents the general system model much as a fault tree does. The system equation must be formulated by the user before the FRANTIC run. The primary events of the system equation are assigned an exponential distribution to describe hardware failures. At different instants of time the unavailability associated with each primary event is calculated. A Monte Carlo version of FRANTIC can be used to input sampling distributions for primary-event failure rates.

The input to FRANTIC consists of the system equation, primary-event failure rates, and test and repair characteristics; other inputs include the time period for the calculations as well as print and plot options. The output consists of system unavailability at different instants of time and, if requested, Calcomp plots of the time-dependent system unavailability.

A second version of the code, FRANTIC II[16], has been developed to enhance the capability to model the time-dependent unavailability of primary events and systems over their total in-service lifetime. The effects of the initial burn-in period, the time region of normal operation, and finally the wear out period can be modeled (the bathtub curve model). For this FRANTIC uses the Weibull distribution, which has a time-dependent failure rate. In addition, FRANTIC II allows the investigation of discontinuous changes in the failure rate as a function of the number of tests performed. This is essentially a demand-related, rather than a time-related, burn-in and wear out model. FRANTIC II also incorporates the effects of renewal on aging by introducing "good as new" or "good as old" primary events.

The FRANTIC and FRANTIC II codes are very simple to use. There is essentially no limit on the number of primary events in the system equation, but the construction of a system equation for a large system containing a large number of primary events is a nontrivial task. FRANTIC and FRANTIC II are written in Fortran IV for the IBM 360/370.

6.2.4 Computer Codes for Analysis of Dependent Failures

There are a large number of specialized codes that have been developed to incorporate consideration of specific types of dependent failures. Commonalities considered span the range from common support systems, or common human interaction, to spatial common features that could relevant in cases of severe wind, flood, fire, or earthquake. The approaches to incorporating such considerations into the analysis are largely spelled out in NUREG-4780[17].

COMCAN[18-19] — The COMCAN code can be used to identify potential common-cause failures in a system or combination of systems. It searches each cut set of system failures for commonality among all the primary events in that cut set.

A minimal cut set will be identified as a common-cause candidate by one of two criteria. The first criterion is met when all the primary events in a minimal cut set share a special condition that alone can result in the simultaneous failure of all the primary events in the cut set. An example of a common special condition is a common maintenance crew servicing all of the components implied by the primary events in a minimal cut set. The second criterion is met if all the primary events in a minimal cut set are susceptible to the same secondary-failure cause and are located in the same domain with respect to that failure cause. An example is a minimal cut set with primary events that will all occur when the associated components get wet and no water barrier exists between them.

The input must include the secondary-failure susceptibilities and applicable spatial conditions for primary events and domain maps for secondary-failure causes. The output provides the analyst a listing of minimal cut sets that have potential for dependent failures. The number of these common-cause candidates can be limited to those that are probably most important. The method used does not provide partial common-cause dependencies in systems under study.

COMPBRN[20] — The COMPBRN code is a deterministic fire hazards computer program designed to be used in a probabilistic analysis of fire growth in a particular room. Possible output of COMPBRN includes the total heat release rate of the fire, the temperature and thickness of the hot gas layer formed near the compartment ceiling, the mass burning rate for individual fuel elements, the surface temperature of the elements, and the thermal heat flux at user-specified locations.

COMPBRN follows a quasi-static approach to simulate the process of fire growth during the pre-flashover period in an enclosure. Briefly, the compartment is modeled using two zones (or control volumes), which means that the enclosure is divided into two distinct, homogeneous, stably-stratified regions. The hot gases accumulating under the ceiling due to fire plume entrainment and negative buoyancy are defined as

the upper layer (the ceiling hot gas layer). The lower region is assumed to be thermally inert and contains relatively quiescent cool air, which remains at ambient conditions at all times. The hot gas layer can play a significant part in the growth rate of the fire. Heat fluxes from this gas layer preheat non-burning fuel elements, reducing their time to damage. The burning rate of a fuel element is used to determine the heat output rate of that element. This burning rate depends on the physical properties of the fuel and on the compartment ventilation rate. Using standard shape factor analysis and idealizing the flame as a cylinder, the heat transferred to other fuel elements, the walls, and ceiling via radiation is computed.

Correlations are used to determine the convective heat transfer in the buoyant plume of hot gases above the flames. Provisions are also made to simply model the layer of hot gases accumulating near the ceiling as a thermal source. The temperature profile within each "fuel element" (including the compartment walls and ceiling) is computed as a function of its thermal environment. An element is considered ignited (or damaged) if its surface temperature exceeds the user-specified ignition (damage) temperature. Time is incremented, and the process starts over, with newly ignited fuel elements adding their contributions to the total rate of heat release.

The COMPBRN code is written in FORTRAN and usable on IBM, CDC, and Prime computers.

IRRAS — The IRRAS code is not constructed to identify dependencies but can be used with the methodology of NUREG-4780 to change the structure of fault trees to represent the potential for dependent failures and thereby incorporate this aspect of the analysis.

RISK-MAN — The RISK-MAN code assists the analyst in restructuring fault trees to account for potential dependent failures in redundant systems. It utilizes SETS as a part of the code package and thereby has the capability of identifying components sensitive to various dependent failure possibilities as described below.

SETS[21] — The SETS code, described earlier, can also be used for dependent-failure analysis. The analysis is conducted by inputting generic cause susceptibilities for each primary event. A transformation of variables incorporates the dependent-failure susceptibilities into the Boolean equation for the top or any intermediate gate of the fault tree, and a few simple manipulations allow the user to display the cut sets that are dependent-failure candidates. The use of SETS for dependent-failure analysis has an advantage in that SETS can handle very large trees, which other dependent-failure codes are unable to do.

6.2.5 Computer Codes for Uncertainty Analysis

Uncertainty analyses are important parts of PRA studies because of the statistical uncertainty in the failure and event-frequency data. To model statistical uncertainties, first, failure and initiating-event-frequency data distributions are selected. Then, based on the logical relationship (e.g., cut sets) of these distributions, they are combined.

The computer codes developed to deal with uncertainty analysis can be divided into two categories: codes that perform the analysis through Monte Carlo simulation and codes that perform the analysis by mathematically combining the distributions. Most of the uncertainty programs can handle a variety of statistical distributions: normal, lognormal, uniform, and empirical distributions being most commonly used.

CAFTA+/UNCERT — The CAFTA+ code along with UNCERT will determine the uncertainty of system failure probabilities or accident sequence frequencies based on input uncertainties. UNCERT reads CAFTA's cut set and database files, performs Monte Carlo random sampling, and displays the results graphically on the screen as the run progresses. Among other things, the analyst can specify the number of samples and type of graphics display. The analyst can request importance measures be evaluated for selected basic events. The run can be stopped at any time, reports generated, basic event parameters changed and the run restarted or continued. Available uncertainty distributions include uniform, constant, normal, lognormal, and gamma distribution.

MOCARS[22] — MOCARS is a FORTRAN Monte Carlo code for determining the means, the standard deviation, and distribution for fault-tree models. The Monte Carlo simulation used is performed by sampling primary-event values from their input distributions and finding the system-failure probability corresponding to this "trial." MOCARS can use primary-event data with either a normal, lognormal, log-uniform, exponential, Cauchy, Weibull, Pearson type IV, or empirical distribution. Once selected, the same type of distribution is used for all primary events throughout the problem. After all these trials, results are sorted and the accuracy is tested. Finally, median and 90th percentile confidence bounds are calculated by using the sorted results.

Input is a system-unavailability function specified either in FORTRAN statements or in terms of cut sets. The output includes a listing of input data, the median value of the point estimates, as well as the system-failure probability in various increments and distribution confidence limits. The output distribution is presented in terms of estimated empirical probability percentiles from which the estimated median and upper and lower bounds can be easily read. MOCARS has the option of microfilm plotting with the integrated graphics system and the ability to perform a Kolmogorov-Smirnov goodness-of-fit test. This test shows whether the output distribution resembles a normal, lognormal, or exponential function. The probability distribution for the top event of the fault tree can be plotted as an optional output. MOCARS is written in Fortran IV for the CDC-7600 computer.

PRA-WORKSTATION — This package uses the Latin-hypercube sampling approach to generate random vectors representing the events. These vectors are then input into TEMAC (described below) to generate the uncertainty distribution for each accident sequence. The importance can be calculated in any of a number of formats. These include the partial derivative technique, risk reduction technique (modified Fussell-Vesely), and the risk increase technique. The events can be ranked with respect to any one of the techniques.

The partial derivative is determined by summing the frequencies or probabilities of all cut sets containing the event in question, with the probability of the event in question set to unity. Risk reduction is evaluated by subtracting from the total core damage

frequency or system unavailability the sum of all cut sets with the event in question set to zero. This importance measure is identical to the Fussell-Vesely importance measure, except that each result has not been divided by the original core damage frequency or system unavailability. Risk increase is the sum of all core damage or system unavailability cut sets with the probability of the event in question set to 1, minus the original total core damage frequency or system unavailability.

TEMAC[25] — TEMAC, the Top Event Matrix Analysis Code, is a FORTRAN program developed by Sandia National Laboratories to estimating risk and perform uncertainty and sensitivity analyses with a Boolean expression such as produced by the SETS computer program. SETS produces a mathematical representation of a fault tree used to model system unavailability. In the TEMAC terminology, such a mathematical representation is referred to as the top event. Depending on the complexity of the system being analyzed, the Boolean expression (referred to as the top event) can be quite large, involving thousands of terms (referred to as cut sets). In the assessment of system unavailability, higher order terms are usually truncated from expressions since their contribution to the total unavailability is negligible. Even after such truncation, the expression can still be very large. Existing methods of risk analysis have not coped well with top events having a large number of cut sets. Sensitivity and uncertainty analyses associated with top events involve mathematical operations on the corresponding Boolean expression for the top event. In addition, repeated Monte Carlo evaluations of the top event are required. The usual polynomial form of the Boolean expression does not easily lend itself to performing such calculations.

A general matrix approach provides a convenient form for Boolean expressions. Representing Boolean expressions in matrix form is computationally efficient. Furthermore, due to the way that a matrix can be programmed, large problems can be analyzed.

The TEMAC program is written in FORTRAN 77 and is written in a manner to make the code as machine-independent (i.e. portable) as possible within the confines of the ANSI standard for FORTRAN 77. In addition, great effort has been expended towards making TEMAC as user friendly as possible.

6.3 References

1. J.W. Hickman et al., PRA Procedures Guide, USNRC Report NUREG/CR-2300 vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1983.

2. W.E. Vesely et al., Fault Tree Handbook, USNRC Report NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1981.

3. J.M. Koren and J.P. Gaertner, "CAFTA: A Fault Tree Analysis Tool Designed for PSA," presented at the International Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, 1987.

4. The CAFTA+ computer code and related tools are available from: Science Applications International Corporation, 5150 El Camino Real, Suite C-31, Los Altos, CA 94022.

5. K.D. Russell, M.B. Sattison and D.M. Rasmuson, Integrated Reliability and Risk Analysis System (IRRAS) Version 2 User's Guide, USNRC Report NUREG/CR-5111, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

6. The PRA-WORKSTATION computer code is available from: EI International, Inc., 545 Shoup Avenue, Idaho Falls, ID 83401.

7. The RISK-MAN computer code is available from: Pickard, Lowe and Garrick, Inc., 2260 University Drive, Newport Beach, CA 92660.

8. R.P. Worrell and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, Report SAND77-2051, Sandia National Laboratories, Albuquerque, NM, 1978.

9. R.P. Worrell, SETS Reference Manual, USNRC Report NUREG/CR-4213, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1985.

10. The SETS/386 computer code is available from: EI International, Inc., One Energy Drive, PO Box 50736, Idaho Falls, ID 83401.

11. W.V. Gately et al., GO, A Computer Program for Reliability Analysis of Complex Systems, Report KN-67-704(R), Kaman Sciences Corporation, 1968.

12. W.V. Gately and R.L. Williams, GO Methodology — Overview, EPRI Report NP-765, Electric Power Research Institute, Palo Alto, CA, 1978.

13. W.V. Gately and R.L. Williams, GO Methodology — System Reliability Assessment and Computer Code Manual, EPRI Report NP-766, Electric Power Research Institute, Palo Alto, CA, 1978.

14. D. Rees and S. Lainoff, GO Methodology — Modeling Manual, EPRI Report NP-3123 vol. 3, Electric Power Research Institute, Palo Alto, CA, 1985.

15. W.E. Vesely and F.F. Goldberg, FRANTIC — A Computer Code for Time-Dependent Unavailability Analysis, USNRC Report NUREG-0193, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1977.

16. W.E. Vesely et al., FRANTIC II — A Computer Code for Time-Dependent Unavailability Analysis, USNRC Report NUREG/CR-1924, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1981.

17. A. Mosleh et al., Procedures for Treating Common Cause Failures in Safety and Reliability Studies, USNRC Report NUREG/CR-4780 vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1988.

18. G.R. Burdick, H.H. Marshall and J.R. Wilson, COMCAN — A Computer Program for Common Cause Failure Analysis, ERDA Report ANCP-1316, Aerojet Nuclear Company, 1976.

19. D.M. Rasmuson et al., Use of COMCAN III in System Design and Reliability Analysis, Report EGG-2187, EG&G-Idaho, Inc., Idaho Falls, ID 83415, 1982.

20. V. Ho, N. Siu, and G. Apostolakis, COMPBRN III — A Computer Code for Modeling Compartment Fires, USNRC Report NUREG/CR-4566, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1985.

21. R.P. Worrell and D.W. Stack, "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings of the Annual Reliability and Maintainability Symposium, San Francisco, CA, , 1981, pp 363-366.

22. S.D. Matthews, MOCARS: A Monte Carlo Simulation Code for Determining Distribution and Simulation Limits, ERDA Report TREE-1138, EG&G Idaho, Inc., Idaho Falls, ID 83415, 1977.

23. J. M. Griesmeyer and L. N. Smith, A Reference Manual for the Event Progression Analysis Code (EVNTRE), USNRC Report NUREG/CR-5174, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1989.

24. S. J. Higgins, A User's Manual for the Postprocessing Program PSTEVNT, USNRC Report NUREG/CR-5380, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1989.

25. R. L. Iman and M. J. Shortencarier, A User's Guide for the Top Event Matrix Analysis Code, USNRC Report NUREG/CR-5380, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1989.

7 SELECTION OF ANALYTICAL METHODS TO USE

We have listed a number of methods for analysis in Chapter 5 which vary in complexity and in resources required for the assessment of risk associated with operation of a facility. The simplest approaches will identify the principle hazards and are adequate for the analysis of relatively simple processes and systems. The cost will be higher to conduct assessments of more complex facilities, to provide more thorough analyses documented to support an audit associated with some form of regulation, or in which models and data bases are established for on-going applications. This chapter addresses the selection of optimum methods to accomplish the established objectives.

7.1 Factors Affecting Selection of Methods To Use

7.1.1 Some Broad Generalities

Clearly, facility character has an impact on the process of methods selection, since the importance of quantitative decision making increases as hazard level and facility size increase.

For those facilities in which the hazards are not too severe and in which the systems to be analyzed are not overly complex, a simple and straightforward analysis will be adequate. This evaluation can use methods such as FMEA, Hazard Analysis, Reliability Block Diagram Analysis, and Single Point Failure Analysis either singly or in combination to satisfy the given needs.

For facilities requiring analysis of moderate complexity, the methods mentioned in the preceding paragraph may be used in a pre-analysis phase of data gathering, facility familiarization, and scoping of the analysis. This moderately-complex evaluation can generally be accomplished with methods such as: Event Tree Analysis, Fault Tree Analysis, GO Analysis, Goal Tree Analysis, Master Plant Logic Diagram Analysis, and UNIRAM Analysis.

For the most complex analyses, the methods of the previous paragraph are often complemented by the use of linked Event-Tree/ Fault-Trees. For all of these analyses, it is essential to identify the man-machine interfaces which have a potential to affect the confinement of hazards. Modeling and evaluation of the human reliability at these interfaces will be a required part of all analyses.

7.1.2 New Plant Design

The design of a new facility offers a prime opportunity to use reliability assessment techniques to rationalize and optimize the decision making process. The following discussion provides some insight into how that can happen and indicates some of the important attributes for the methods to be selected.

Conceptual Plant Design

Identification of hardware functional objectives and requirements and translation of these requirements into a conceptual facility design are among the first issues of concern in new plant design. These requirements are then reassessed and modified until the fundamental performance objectives are met. These performance objectives relate to either the facility

equivalent availability, or the risks engendered by any process hazard. The designer (decision maker) must have the ability to develop high-level reliability and availability models easily and quickly, change their logic and re-solve them to answer fundamental questions about the needed degree of system-success-path redundancy and diversity. The models should provide direct estimates of facility performance which can be used with a basic cost model to perform the initial trade-off analyses.

Reference Plant Design

The reference plant design represents elaboration of the preliminary design with details of the expected hardware configurations, and the first round of optimization performed to find the best system and success-path configurations which meet the target facility availability or reliability goals.

Since few of the participants in the design process will be reliability specialists, the production models must have a character which makes them easily understood. The models must also be capable of speedy change and re-solution as detail is added and new configurations are examined. As the facility design matures, increased involvement by reliability specialists means that there is less need for the method to provide direct estimates of performance measures (equivalent availability or hazard release frequency); these predictions can be synthesized from the results of individual inter- and intra-system studies. To minimize the likelihood of a loss of hazard confinement, the design of a high hazard facility usually includes multiple barriers, or a "defense in depth" philosophy. This means that the modeling approach used in the reliability assessment must be sufficiently detailed to allow full assessment of the importance of intersystem dependencies, dependent faults and the effects of external influences, yet still allow rapid re-solution of the resultant complicated network whenever changes are proposed. The results of the analyses of both availability and reliability models should provide a ranked list of contributors which can serve as the basis for the next round of optimization.

Final Plant Design

The final design models which are analyzed to confirm that the expected performance characteristics for the facility meet the proposed goals will be extremely detailed, well documented and form an integral part of the facility design basis. The confirmatory analysis must fully document the qualitative and quantitative system and facility reliability and availability characteristics. The documentation must be in a form which is understandable, reviewable and retrievable, so that when the facility moves into its operational phase, the models and analyses can be updated to reflect "as built" conditions and thus maintain the facility design basis. The attributes required of these models include scrutability, high detail, and qualitative and quantitative capability. Speed of solution may not be of paramount importance unless the facility undergoes a significant number of changes which involve dependencies or success criteria.

7.1.3 Plant Operations

In an operating facility, just as in the design phase, justification for proposed changes to administrative programs, processes or hardware is based on a prediction of their worth. This implies that the requisite models must contain enough detail to allow the simulation of all proposed facility or program changes and provide an output in a form which can be directly correlated with expected economic performance. Generally speed of solution is not important,

other than as an economic concern — one can't pay an analyst $1000 to justify a $500 modification. Ideally the models will all be operating in a personal computer environment and will have pre- and post-processors so that the models are transparent to the user, making them directly usable by the decision maker. There are some additional relevant concerns in the operating environment of a high-hazard or high-cost facility which are quite different than those seen during design. These differences result from the need to understand and monitor the importance of functional success path availability during normal and emergency operation, and the need to recognize the need for corrective actions following the occurrence of a risk significant precursor event. The following examples typify the applications for quantitative decision making in an operating facility.

Operational Decision Making

Potential applications for operational decision making support can be subdivided into two general categories or issues. Management of economic risks which result from failures in the production cycle is the first issue, and failure in the systems and processes which result in a loss of confinement of the hazard, with its attendant potential liabilities is the second.

Availability or Equivalent Availability

When a facility manager is proposing a change to the process hardware, the benefits often do not result from increased availability, but rather from an increase in the success probability for an intermediate production state. This means that the benefit from the change can only be assessed if multi-state models with variable success criteria can be solved to generate the equivalent availability curve. The benefit is then calculated from the change in area under the curve. The speed of solution is reasonably important, but quantitative estimates represent the prime need. There is generally no need for qualitative assessments since the models are typically solved on an "ad hoc" basis for prescribed issues, and a process which can find numerical estimates without recourse to qualitative techniques would appear preferable. The model should be scrutable and have a form which is reasonably understandable to a non-analyst user. If the facility is capable of only two states, working at full capability or shutdown, then availability is the measure of performance. The issues for availability models differ from those described above because variable success criteria are no longer an issue.

To allow a facility manager to assess the future impact of observed trends in hardware performance, both the availability and equivalent availability model should be easily modifiable, be amenable to both local and global data changes, and provide an output which can be correlated directly to economics.

Risk Management

In the management of a facility which contains hazards of concern, the manager must understand the absolute levels of risk he is accepting, how the risk changes as a result of operational conditions and occurrences, and the relative magnitudes of each of the contributors; then decisions made to enhance the facility can be both justified and implemented in the most cost effective way. This leads to the need for the following types of decision making support, which are typically more diverse than those encountered during the optimization of the operational capability for the facility.

Engineering Support, in which: The worth of a proposed enhancement is used to establish the justification, the schedule or priority for its implementation, the assessment of the significance and impact of observed hardware performance trends on facility risk, and the need for change.

These items could include time-dependent failure rates which result from aging or wearout, in addition to increasing numbers of human errors.

Operational Safety Program support which includes: The assessment of the significance of operating events (search for important precursors), the management of the operational plant configuration (tagging), and the prioritization and justification of maintenance activities by identifying risk important hardware.

Accident management support which includes: Accident management, in which the reliability models can be updated in (nearly) real time during an event to reflect actual plant state, and solved to find vulnerabilities which reflect the greatest conditional risk and training program support in which the identification of important sequences which should be included in the facility training program, both from the perspective of the operator and the accident manager.

Regulatory Support to include: Justification for changes to technical specifications, by providing estimates of the net benefits which result from changes in surveillance test intervals and allowed outage times and provision of a rationale for licensing relief during interaction with a regulator.

7.2 A Quantitative Selection Process

This handbook has, to this point, discussed the selection of analytical methods from a qualitative point of view. In this section, we present an approach to quantitative provision of a figure-of-merit for the various methods as they apply to a specific set of requirements arising from the set of uses anticipated for a risk assessment of a specific facility.

For the following we will use the word "application" to indicate a specific use of the risk assessment. The premise for the quantitative approach presented is that for a specific facility, a correlation can be made between the desired set of attributes for each anticipated application and the attributes for each modelling approach or "method". The use of this quantitative generation of a figure-of-merit for each method can help a facility manager to meet all of his decision making needs as easily and effectively as possible.

Characteristics of Sample Case

Clearly, facility character has an impact on the process of methods selection, since the importance of quantitative decision making increases as hazard level and facility size increase. For the sample case presented along with the approach, we have made a presumption of the presence of high-level process hazards and of high economic risks. The potential applications for quantitative decision making will be evaluated within this constrained context.

7.2.1 Attributes of Selected Applications

In Table 1, seven general application areas are listed across the top of the chart; these are the seven applications discussed in section 7.1. The table also lists 26 attributes down the left side of the chart. These attributes have been selected to characterize analytical needs in terms of:

- The ease of use of the method, the degree of needed analyst expertise, whether the method is self-documenting and the ease with which the results and approaches can be used and understood by a non-specialist user.

- Whether the approach can quickly provide both quantitative and qualitative results if complete re-solution is required to evaluate a hardware dependency or success criteria change and if the method provides a rank order set of contributing faults, and a description of important scenarios.
- Whether data can easily be changed on a global or local basis to allow assessment of the worth of programmatic changes or changes in the performance of individual hardware elements.

- Whether a non-specialist can identify scope, fidelity or simplification, and understand the limitation of the models when it is used (graphical representations or display format).

Additional generic factors which enter into the method selection process and have a fundamental impact are whether the approach should be inductive, deductive, success or failure oriented and whether the fundamental differences in the character of operating and standby systems (success criteria and data) are sufficient to have a major impact on operating facilities (production or "throughput").

The entries in Table 1 are pairs of numbers. The first is a ranking of the attributes as they relate to the application heading the column of interest, ranging in value from 0 to 10. The second factor is a correlation factor, ranging from -3 for negative correlation through the neutral value of 0 to +3 for highly correlated.

We will refer to the entry in the "ith" row and the "jth" column of the Applications Matrix as A_{ij}. Looking at some specific elements of the matrix we see that for

TABLE 1 **APPLICATIONS**

ATTRIBUTES	Design			Operational Decision Making Support			
	Preliminary	Reference	Final	Availability Improvement	Operational Safety	Engineering Support	Regulatory Support
Inductive	(1,0)	(1,0)	(1,0)	(4,3)	(2,3)	(1,0)	(0,0)
Deductive	(1,0)	(1,0)	(1,0)	(4,-3)	(4,-3)	(1,0)	(1,3)
Success	(2,0)	(2,0)	(2,0)	(4,3)	(2,3)	(1,0)	(1,0)
Failure	(2,0)	(2,0)	(2,0)	(4,-3)	(2,-3)	(1,0)	(1,0)
Quantitative	(7,3)	(8,3)	(8,1)	(10,3)	(10,3)	(9,3)	(9,3)
Qualitative	(7,1)	(8,3)	(8,1)	(10,-3)	(10,-3)	(9,-3)	(9,3)
Model Capabilities							
- Complexity	(6,1)	(8,2)	(8,3)	(7,0)	(10,3)	(8,3)	(8,3)
- Size	(6,1)	(8,2)	(8,3)	(7,1)	(8,-2)	(8,3)	(8,3)
- Implicit Detail	(6,3)	(8,0)	(9,0)	(7,0)	(10,3)	(8,3)	(8,0)
- Explicit Detail	(6,-2)	(8,2)	(9,3)	(7,3)	(10,0)	(8,3)	(8,3)
Solution							
- Speed	(10,3)	(7,2)	(6,1)	(8,0)	(10,3)	(6,0)	(6,0)
- Re-Solution	(10,3)	(6,1)	(5,1)	(8,0)	(10,3)	(6,2)	(6,0)
Solution Options							
- Hand Solution	(2,3)	(1,0)	(1,0)	(1,0)	(8,0)	(2,0)	(1,0)
- PC Capable	(9,3)	(7,3)	(6,0)	(9,3)	(10,3)	(7,0)	(8,2)
- Mainframe	(6,-3)	(7,2)	(7,2)	(6,0)	(2,0)	(8,0)	(6,0)
Calculations							
- Availability	(9,3)	(9,3)	(9,3)	(10,3)	(2,-3)	(8,3)	(1,-3)
- Reliability	(10,3)	(10,3)	(10,3)	(4,-3)	(9,3)	(10,3)	(10,3)
Options							
- Sensitivity	(8,3)	(9,3)	(9,3)	(10,3)	(9,-3)	(8,3)	(9,3)
- Importance	(4,-2)	(7,3)	(9,3)	(3,-3)	(1,-3)	(4,0)	(9,3)
- Uncertainty	(4,0)	(8,3)	(9,3)	(5,0)	(3,-3)	(6,0)	(8,3)
- Global Data Change	(9,3)	(6,3)	(4,3)	(6,3)	(2,-3)	(3,0)	(2,0)
- Modularization	(5,3)	(4,-3)	(3,-3)	(2,3)	(4,1)	(4,1)	(3,-3)
- Self Documenting	(5,0)	(7,3)	(5,3)	(4,3)	(7,0)	(7,3)	(5,3)
User Interface							
- Graphical	(10,3)	(7,0)	(5,0)	(8,0)	(7,3)	(7,0)	(7,0)
- Non-Analyst	(9,3)	(7,0)	(5,-3)	(8,3)	(8,3)	(7,3)	(8,3)
- Model Change	(8,3)	(8,0)	(6,-3)	(8,3)	(10,3)	(7,3)	(7,3)

preliminary design application (column 1) the attribute of being able to use a personal computer for the analysis (PC Capable — row 14) is ranked highly (9) [$A_{14,1}$ = 9,3]. The second factor in the entry (+3) indicates a strong positive correlation. This fits with the needs during the preliminary design phase to have quick turnaround on analyses of fairly simple high-level views of the systems.

For contrast, consider the next lower element which relates to the attribute of needing to use a mainframe computer for the analysis (Mainframe — row 15). This issue is considered to be slightly less highly ranked (6) [$A_{15,1}$ = 6,-3]. The second factor in the entry (-3) indicates a strong negative correlation. This fits with our understanding that when one needs quick turnaround, requiring the use of a mainframe computer to do the analysis could be a hindrance.

7.2.2 Attributes of Selected Methods

In Table 2, seven specific analytical methods are listed as titles of columns across the top of the chart. These are a selected set of those methods discussed in Chapter 5. The same 26 attributes used in Table 1 are listed down the left side of this chart. The entries in this table are correlation factors that indicate how well each attribute correlates with the particular method.

We will refer to the entry in the "ith" row and the "jth" column of the Methods Matrix as $M_{i,j}$. Looking at the lower left portion of the table, the fault tree (column 1) is seen to be a poor

TABLE 2 **METHODS**

ATTRIBUTES	Failure				Reliability		
	Fault Tree	Event Tree	FMEA	MPLD	UNIRAM	GO	RBD
Inductive	-3	3	3	3	-3	3	0
Deductive	3	-3	-3	-3	3	-3	0
Success	-3	3	-3	3	-3	3	0
Failure	3	-3	3	-3	3	-3	0
Qualitative	3	3	3	3	3	3	3
Quantitative	3	3	-3	3	-3	3	-3
Model Capabilities							
- Complexity	3	3	-3	3	0	3	1
- Size	3	3	1	3	3	-1	2
- Explicit Detail	3	3	3	0	2	3	3
- Implicit Detail	3	3	3	3	3	3	3
Solution							
- Speed	0	3	-3	3	3	2	1
- Re-Solution	-2	0	0	3	3	3	0
Solution Options							
- Hand Solution	-3	2	3	3	-3	-3	3
- PC Capable	3	3	-3	0	3	3	0
- Mainframe Reqd	0	0	-3	0	0	0	0
Calculations							
- Availability	-3	-3	-3	-3	3	3	3
- Reliability	3	3	-3	3	3	3	3
Options							
- Sensitivity	3	3	-3	3	3	3	3
- Importance	3	3	-3	-3	3	3	-3
- Uncertainty	3	3	-3	0	3	3	-3
- Global Data Change	3	3	-3	-3	3	3	-3
- Modularization	3	3	-3	3	3	3	3
- Self Documenting	0	0	3	3	3	3	3
Interface							
- Graphical	3	3	-3	3	-3	3	3
- Non-Analyst	-3	3	3	3	0	3	3
- Model Change	-1	3	1	3	3	3	0

representation for the non-analyst (row 25) [$M_{25,1}$ = -3]. This can be contrasted with event trees (column 2) which are easily understood by the non-specialist (row 25) [$M_{25,2}$ = 3].

7.2.3 Figure-of-Merit Calculations

Our objective in this section is to provide a specific process leading to a resulting figure-of-merit for each of a number of methods; these methods being evaluated in the context of a specific facility coupled with requirements for use in certain applications. We will choose here to evaluate each method for each application. The figure-of-merit for method 'k' in terms of its use for application 'j' is given by the following:

$$\textit{Figure-of-Merit} = FM_{j,k} = \sum_{i=1}^{n} [\, A_{i,j} * M_{i,k} \,]$$

In this computation, the product of the two numbers stored in location $A_{i,j}$ is used as the value of $A_{i,j}$. For our sample case being displayed, the summation goes over all 26 attributes.

Consider evaluating the Event Tree method (k = 2) for use in Regulatory Support applications (j = 7). The calculation of the figure-of-merit then proceeds as follows:

$$FM_{7,2} = \sum_{i=1}^{26} [\, A_{i,7} * M_{i,2} \,]$$

$$= A_{1,7} * M_{1,2} + A_{2,7} * M_{2,2} + \ldots + A_{26,7} * M_{26,2}$$

$$= (0 * 0) * 3 + (1 * 3) * (-3) + (1 * 0) * 3 + \ldots + (7 * 3) * 3$$

$$= 885$$

Table 3 displays a summary of this computation of figures-of-merit. For each application, the method with the highest figure-of-merit was identified and the corresponding location in the table is shown with a black stripe. Those methods that had figures-of-merit only slightly smaller are shown with a patterned grey stripe. This sample display of the process was for an assumption of a high-hazard, high-economic-risk facility. The evaluation was done by interrogating a single analyst on his evaluations of importance of the various attributes for the applications considered.

TABLE 3 **SAMPLE RESULTS**

APPLICATIONS	METHODS						
	Fault Tree	Event Tree	FMEA	MPLD	UNIRAM	GO	RBD
Preliminary Design							
Reference Design							
Final Design							
Availability Improvement							
Operational Safety							
Engineering Support							
Regulatory Support							

Ends very abruptly

8 APPENDIX A

DETAILED OUTLINE OF A PROBABILISTIC RISK ASSESSMENT

This Appendix is composed of a topical outline structured approach to defining the complete content of a risk assessment analysis. The outline topics are generally such that they could be viewed as separate tasks in a breakdown of the overall project. Each topic in the outline is then addressed in turn in a rigorous way to define:

A. What is the process under consideration?
B. What is the scope of the process?
C. What are the outputs that will be generated by this activity?
D. Who are the customers for this output?
E. What are the requirements for the output produced?
F. What are the inputs needed for this activity?
G. Who are the suppliers of the needed input?
H. What are the requirements upon the needed input?

This material provides a great amount of detail to guide a PRA Team in preparing for and in conducting a Probabilistic Risk Assessment.

8.1 Project Management

A. **Process**

1. Administer the Level 1 and 2 PRA.

B. **Scope**

1. To administer the project to meet the customer's requirements and to keep the project within budget and on schedule.

C. **What is the output?**

1. Tasks for the PRA Team members.
2. Level 1 and Level 2 PRA.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Meet customer requirements for Level 1 and Level 2 PRA.
2. Maintain the project within budget and on schedule.
3. Assign tasks to the most appropriate team members and also to help further develop team members capabilities.
4. Monitor tasks assigned to keep them on schedule.
5. Monitor tasks for time spent for budget.
6. Liaison between team members and Customer.
7. Keep customer informed of progress.

F. **What are the inputs?**

1. Negotiated budget and schedule.
2. Negotiated requirements.

G. **Who are the suppliers**

1. PRA Team (F.1,2).
2. Customer (F.1,2).

H. **What are the input requirements?**

1. QPP Plan.
2. Process flow sheets or equivalent.
3. Sufficient personnel to complete project within budget and on schedule.
4. Project management software.
5. Sufficient calendar time to complete the project on the negotiated end date.

8.2 Level 1 PRA

8.2.1 Methodology Definition and Familiarization

A. **Process**

1. Use available resources to define the feasible analytical options which will meet the product requirements and the requirements of the applications proposed for the completed product.
2. Assess the expected expenditure of resources for each option and select the most cost effective.
3. Document the selection (briefly) and develop a description of the methodology to be implemented.
4. Implement training for the staff in the application of the selected methodology.

B. **Scope**

1. Use results (if any) from existing Reliability, PRA, and FMEA efforts.
2. Requirements as documented from the Customer.
3. Delineation from the Customer of the proposed applications of the completed product.
4. Methodology training must be sufficient to allow each PRA Team member to perform any part of the technical tasks.

C. **What is the Output?**

1. Technically competent analysts in the chosen methodology.
2. Informed customers on the chosen methodology.
3. Presentation (1 hour) to the Customer's staff on the proposed approach.
4. Methodology description (documented, to be included in the Final Report).

D. **Who is the customer?**

1. PRA Team(C.1)
2. Customer(C.2,3,4)

E. **Output Requirements?**

1. PRA Team members comfortable in using the chosen methodology.
2. Expertise on call to assist in methodology problem resolution.
3. Customer's staff agrees with the methodology.

F. **What are the Inputs?**

1. Documentation of methodology.
2. Proper software.
3. Hardware capable of running IRRAS and/or any other PRA calculation code.
4. Inventory of available techniques for the analysis.
5. Inventory of related products developed to date for Customer.
6. Inventory of available technical resources (i.e. tools, computer codes, analyst availability, and expertise).
7. Performance criteria for the completed product (i.e. speed of resolution and depth of model detail [application dependent]).
8. Modelling philosophy (i.e. functionally based, failure oriented, and inductive/deductive.
9. Trainer for the selected methodology.

G. **Who are the suppliers?**

1. Experts on the selected methodology-(instructors)(F.1,9)
2. Customer (F.4,5,6,7).
3. PRA Team (F.2,3,4,6,8)

H. **What are the input requirements?**

1. Dedicated trainer for the training period (F.9).
2. Documentation to be clear and understandable (F.1).
3. Training held at most economical location (F.9).
4. Inventories be available for decisions to be made on methodologies (F.4,5,6).
5. Software be documented and supported (F.2).
6. Performance criteria available at the beginning of the project (F.7).
7. Modelling philosophy be defensible (F.8).

8.2.2 Plant Familiarization

A. **Process**

1. Familiarize all PRA Team members with the Customer facility, process, and documentation.

B. **Scope**

1. All systems, locations, and activities expected to play a roll in the initiation, arrest, or propagation of an upset condition in the facility.

C. **What is the Output?**

1. Each analyst will have performed a detailed inspection of the facility in the areas expected to be of interest and importance to the analysis and will become familiar with the following:
   a. Operating philosophy and administrative controls.
   b. Discrete operational modes for the facility.
   c. The overall process functional characteristics.
   d. The functional and spatial relationships between hardware.
   e. The general maintenance philosophy for the facility.
   f. The locations for all available sources of information which describe the facility design and its bases.
   g. The locations of all sources of information which describe any operational history or experience for the facility.
   h. The names of people who will provide access to all the needed information to be used in the analysis.

D. **Who is the Customer?**

1. PRA Team.

E. **What are the Output Requirements?**

1. All analysts are able to fully understand the role which all Customer hardware and human actions play during each expected operating mode.

F. **What are the Inputs?**

1. Escort.
2. PRA Team members.
3. Unescorted access capabilities.

G. **Who are the suppliers?**

1. Customer personnel (F.1,3).
2. PRA Team (F.2).

H. **What are the input requirements?**

1. Escorts knowledgeable of the facility layout and the process and maintenance activities (G.1).
2. Access to the Customer's facility (G.1).
3. Contact security at EG&G to make any security arrangements that have to be made to be able to access the Customer facility (G.2).
4. Access to the facility, its operating and maintenance staff, and procedures. Efficiency would dictate that presentations by the Customer staff be used to brief all analysts at one time (G.1).
5. Access to Customer design basis documentation — drawings, technical manuals, administrative controls, etc. (G.1).
6. Identification of the Customer staff members with whom analysts can interface directly (a single point contact may be designated by Customer) (G.1).
7. Access to facility operating and maintenance history (G.1).

8.2.3 Setting the Basis for the Analysis

A. **Process**

1. Determine the ground rules for the analysis, the scope of the analysis and the configuration to be analyzed.

B. **Scope**

1. Faults and conditions to be included/excluded from the analysis.
2. Operating modes of concern.
3. Hardware configuration on the design "freeze date".
4. Approach to be taken (assumptions) when information is not available to the analyst. i.e., operating and maintenance procedural inadequacies, hardware technical manuals not available, testing or surveillance programs not defined.
5. Definition of events of concern (the undesired consequences which the Customer wants to avoid).
6. Conditions which initiate the sequence which leads to events of concern (internal, external events).
7. Events leading to personnel injuries or other undesired consequences (industrial hazards, maintenance activities, etc.).

C. **What is the Output?**

1. An agreement upon schedule, task breakdown and scope which can be accomplished in minimal time and with little or no need for negotiation (except for out of scope activities) during the analysis.

D. **Who are the customers?**

1. The PRA Team.
2. The Customer.

E. **What are the Output Requirements?**

1. Customer and supplier agree upon outputs.

F. **What are the Inputs?**

1. Analytical ground rules and analytical scope.
2. Definition of the expected applications for the analysis.
3. All requisite facility information including defined and scoped design on the "freeze day".
4. Actions to be taken by analysts to complete analysis when information is not available (assumptions).
5. How changes to the frozen design will be handled (out-of-scope negotiation on budget and schedule).
6. Requirements for future updates of the analysis.

G. **Who are the suppliers?**

1. Customer (F.1,2,3,4,5,6).
2. PRA Team (F.1,4,5,6).

H. **What are the input requirements?**

1. Analytical ground rules developed jointly with the Customer (F.1).
2. Definitions set by the Customer since they will affect the format and content of the delivered product (F.2).
3. Facility information including defined and scoped design on the "freeze day" provided by the Customer (F.3).
4. The Customer and the PRA Team agree on the actions to be taken (F.4).
5. The Customer and the PRA Team agreement (F.5).
6. Developed by the Customer and the PRA Team.

8.2.4 Initiating (Operational) Event Study

A. **Process**

1. Determine events which cause departure from normal operation (all phases).

B. **Scope**

1. Events which could lead to the undesired consequence(s).
2. Internal events (for example fire and flood) which could lead to the undesired consequence(s).
3. All modes of operation for induced sequences.
4. All modes of facility operation and attendant activities for examination of non-process induced consequences(industrial hazards, etc.).

C. **What is the output?**

1. List of all initiating events which lead to the undesired consequence(s) that are scrutable and well justified.
2. Initiating event frequencies.
3. Report identifying each initiating event which is germane to the assessment of the undesired consequence(s) from the Customer process, or initiates any sequence of events which lead to a facility damage state or consequence of concern.
4. A grouping of the initiating events into categories which represent a commonality in facility response.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report in EDF format.
2. Output files on disk.
3. Functional description of the facility and identification of the required functions to sustain each mode of facility operation. The events which threaten these functions will be the "initiators".

F. **What are the inputs?**

1. Plant operational data — satisfactory operating data and abnormal event data.
2. Facility familiarization.
3. Data base manager.
4. Process experts.
5. Wordperfect EDF form.
6. NUREG 3862.
7. Facility operation/abnormal event data from similar facilities.

G. **Who are the suppliers**

1. Customer personnel (F.1,2,4).
2. PRA Team (F.3,5,6,7).

H. **What are the input requirements?**

1. Access to process experts (F.4).
2. Timely Provision of data (F.1).
3. Relational data base (F.3).
4. Wordperfect 5.1 (F.5).
5. Access to NUREG 3862 (F.6).
6. Have access to similar facility information and data (F.7).
7. Completed to the point of defining initiating events (F.2).

8.2.5 Initiating (Non-operational) Event Study

A. **Process**

1. Evaluate the non-operational initiating events.

B. **Scope**

1. Events which could lead to the undesired consequence(s) which occur when the facility is non-operational.
2. Internal events (for example fire and flood) which could lead to the undesired consequence(s) when the facility is not operating.
3. All modes of facility maintenance activities and test activities when the facility is not operating that lead to the undesired consequence(s).

C. **What is the output?**

1. List of all initiating events when the facility is not operating which lead to the undesired consequence(s) that is scrutable and well justified.
2. Initiating event frequencies.
3. Report identifying each initiating event which is germane to the assessment of the undesired consequence(s) from the Customer activities when the facility is not operating, or initiates any sequence of events which lead to a facility damage state or consequence of concern.
4. A grouping of the initiating events into categories which represent a commonality in facility response for events when the facility is not operating.

D. **Who are the customers?**

1. The Customer.
2. The PRA Team.

E. **What are the output requirements?**

1. Report in EDF format.
2. Output files on disk.
3. Functional description of the non-operational initiating events.

F. **What are the inputs?**

1. Any Customer studies or data for non-operational events.
2. Facility familiarization for the non-operational mode.
3. Data base manager.
4. Non-operational activities experts.
5. Word Perfect EDF form.
6. NUREG 3862.
7. Facility non-operational/abnormal event data from similar facilities.
8. Human Error event analysts.
9. Non-operational maintenance procedures.

G. **Who are the suppliers**

1. Customer personnel (F.1,4,6,9).
2. PRA Team (F.2,3,5,6,7).
3. Human Reliability Group (F.8).

H. **What are the input requirements?**

1. Access to non-operational activities experts (F.4).
2. Timely provision of non-operational studies, data, or procedures as to allow enough time to complete the analysis and to incorporate into the Level 1 analysis and report (F.1,9).
3. Relational data base (F.3).
4. Word Perfect 5.1 (F.5).
5. Events defined adequately for the Human Reliability Group to analyze (F.8).
6. Familiarization complete to the point of being used for this analysis (F.2).
7. Access to NUREG 3862 (F.6).
8. Access to similar facility non-operational events (F.7).

8.2.6 Event Tree Development

A. **Process**

1. Event tree development through a process of functional block diagrams, followed by a success tree for not having the consequence take place, and finally, production of the event trees from the success trees.

B. **Scope**

1. Event trees are developed to the level dictated by the methodology chosen for all modes of operation for internal initiators.

C. **What is the output?**

1. Event tree files.
2. Binned event tree state definitions.
3. Description of the set of event trees which define the facility response to each of the identified initiator categories, and the resultant damage state for each of the sequences.

D. **Who are the customers?**

1. The Customer.
2. The PRA Team.

E. **What are the output requirements?**

1. Event trees developed to the level for the methodology chosen.
2. Event tree states binned according to the commonality of failure.
3. Identification of all hardware and human systems which provide success paths which achieve individual functions.
4. Development of a systemic event tree which includes only hardware or human actions.
5. A nomenclature scheme which provides consistent unambiguous definition of events which is consistent with (or the same as) any existing facility or analytical systems. Customer staff should be able to interpret the scheme with little difficulty.
6. A nomenclature system which includes "locators" so that the physical location of systems and components can be identified from their descriptor.

F. **What are the inputs?**

1. Outputs from the plant familiarization.
2. Outputs from the methodology familiarization.
3. Outputs from the initiating event study.
4. IRRAS or other applicable event tree code- Event tree drawings.

G. **Who are the suppliers**

1. PRA Team.
2. Special Applications Unit for IRRAS or other applicable source for other software.

H. **What are the input requirements?**

1. Sections complete to the point of being useable for event tree development (F.1,2,3).
2. Bug-free version with documentation (F.4).
3. Design freeze on facility drawings and documentation (F.1,2,3).
4. Understanding of the functional response of the facility to an abnormal condition triggered by an event which threatens a needed facility function (F.1,2,3,4).

8.2.7 Fault Tree Development

A. **Process**

1. Develop fault trees using NUREG 0492 as a guide.

B. **Scope**

1. Develop trees required by the initiating event study and event tree study.
2. All systems (hardware and human) which are shown to be relevant as initiation sites of events which influence the likelihood of achieving any undesired facility damage.

C. **What is the output?**

1. Fault tree files.
2. The set of fault trees which describe the relationships between hardware and human faults and events which are either initiating events or events described on the event trees.
3. A set of computer models which are capable of solution to provide both qualitative (cut-sets) and quantitative insights (probabilities and importance, when failure probabilities are known).

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Full description of the hardware systems and their inter-relationships (dependencies) (functional diagrams).
2. Identification of dependencies and relevant hardware faults and documentation of exclusions (i.e. interfacing system FMEA).
3. Fault tree code with graphical interface.
4. Fault trees developed to the level to quantify the top events of trees.
5. Fully documented and reviewable product.
6. Model of sufficient detail to meet future applications and be solved in the required time (performance criteria).
7. Model compatible with the event tree solution process.

F. **What are the inputs?**

1. Outputs from the plant familiarization.
2. Outputs from the methodology familiarization.
3. Outputs from the initiating event study.
4. Outputs from the event tree analysis
5. IRRAS or other applicable fault tree code.
6. Facility drawings.
7. Customer process expert.
8. Basic event naming scheme.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4,).
2. Special Applications Unit for IRRAS and the applicable source if another code is used (F.5).
3. Customer (F.6,7).

H. **What are the input requirements?**

1. Outputs complete to the point of being useable for fault tree development (F.1,2,3,4).
2. Bug-free versio with documentation (F.5).
3. Drawings legible and on paper (F.6).
4. Expert who is knowledgeable of the Customer facility and the process.
5. NUREG-4550 Naming Scheme Adaptation.

8.2.8 Internal Events Study of Events External To The Process

A. Process

1. Perform a scoping study to identify all internal events external to the process that may initiate an unwanted occurrence in the process and compromise safety systems (these events usually include internal floods and fires).
2. From the list generated in the scoping study, pick the events that cause the greatest effect and have the highest probability of occurrence as determined by the project imposed cutoff limit.
3. Analyze the resulting events in greater detail to determine their means of mitigation and the way they affect process equipment and the process itself.

B. Scope

1. Examine events for all facility areas in which process hazards exist, or in which there is support equipment which plays a roll in the facility response to an initiating event or creates an initiating event.
2. Screen out events external to the process whose plant damage frequency is less than 0.1% of the internal event frequency.

C. What is the output?

1. A documented and scrutable report detailing the description of the analytical process, the results of the analysis and an interpretation of the results.
2. A set of documented models which can be used in the future to support the decision making process at the Customer facility.
3. A solvable model which provides a realistic assessment of the effects of the selected internal non-process events, which is understandable and useable by the Customer staff.

D. Who are the customers?

1. Customer.
2. PRA Team.

E. What are the output requirements?

1. Report in EDF format.
2. Data files produced are on disk.
3. A full description of the expected objectives for the analysis.
4. A full description of the analytical groundrules and basic assumptions and methodology description.
5. Plant description, specifically to the functional characteristics of the facility which are important to the analysis, and the systems which achieve the requisite functions (Master Logic Diagram, Functional Diagrams and System Descriptions).
6. A full description of the scoping rationale and excluded facility hardware.
7. A full description of the initiating event analysis and identification.
8. A full description of event trees which provide the description of the plant functional response to each group of initiators.

9. A full description of the fault trees which correspond to the functional diagrams and FMEA Dependency analysis.
10. A full description of the data base used to develop the failure probabilities for each event, and the process used.
11. A full description of the solution process, including parameters used for truncation, etc.

F. **What are the inputs?**

1. Facility walkdown.
2. Customer's facility drawings.
3. Basic event naming scheme.
4. IRRAS or other appropriate PRA codes.
5. Customer process expert.

G. **Who are the suppliers**

1. PRA Team (F.1,3).
2. Special Applications Unit for IRRAS or the applicable organization for other codes (F.4).
3. Customer (F.2,5).

H. **What are the input requirements?**

1. Walkdown complete to the point of being useable for Internal non-process event analysis (F.1).
2. Bug-free version with documentation (F.4).
3. Drawings legible and on paper (F.2).
4. Expert knowledgeable of the Customer facility and the process (F.5).
5. Identification of all equipment which is involved in the initiation of events or their mitigation (F.1).
6. Identification of the location of each piece of equipment (F.1).
7. Identification of the expected origins for the non-process events, their anticipated or possible propagation paths and their associated probabilities (F.1).
8. Identification of dependencies between hardware which has the same location and will be subjected to simultaneous effects of the non-process events, and assessment of their common-failure probabilities (F.1,2).
9. Models which explicitly relate dependent components (F.1,2).
10. Tools and techniques which allow the solution of the models (F.4).
11. Knowledge of the capabilities and the role of the human in the course of the fire and flood events (F.5).
12. NUREG-4550 — Naming Scheme Adaptation (F.3).

8.2.9 External Events Study

A. **Process**

1. Perform a scoping study to identify all external events that may initiate an unwanted occurrence in the process and compromise safety systems (these events usually include external floods, external fires, seismic events, high winds, tornadoes, plane accidents, vehicle accidents, lightning strikes, etc.).
2. From the list generated in the scoping study pick the events that cause the greatest effect and have the highest probability of occurrence as determined by the project-imposed cutoff limit.
3. Analyze the resulting events in greater detail to determine their means of mitigation and the way they affect process equipment and the process itself.

B. **Scope**

1. Examine events for all facility areas in which process hazards exist, or in which there is support equipment which plays a roll in the facility response to an initiating event or creates an initiating event.
2. Screen out external events whose plant damage frequency is less than 0.1% of the internal event frequency.

C. **What is the output?**

1. A documented and scrutable report detailing the description of the analytical process, the results of the analysis and an interpretation of the results.
2. A set of documented models which can be used in the future to support the decision making process at Customer.
3. A solvable model which provides a realistic assessment of the effects of the selected internal non-process events, which is understandable and useable by the Customer staff.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report in EDF format.
2. Data files produced are on disk.
3. A full description of the expected objectives for the analysis.
4. A full description of the analytical groundrules and basic assumptions and methodology description.
5. Plant description, specifically to the functional characteristics of the facility which are important to the analysis, and the systems which achieve the requisite functions (Master Logic Diagram, Functional Diagrams and System Descriptions).
6. A full description of the scoping rationale and excluded facility hardware.
7. A full description of the initiating event analysis and identification.
8. A full description of event trees which provide the description of the plant functional response to each group of initiators.

9. A full description of the fault trees which correspond to the functional diagrams and FMEA dependency analysis.
10. A full description of the data base used to develop the failure probabilities for each event, and the process used.
11. A full description of the solution process, including parameters used for truncation, etc.

F. **What are the inputs?**

1. Facility walkdown.
2. Customer's facility drawings.
3. Basic event naming scheme.
4. IRRAS or other appropriate PRA codes.
5. Customer process expert.

G. **Who are the suppliers**

1. PRA Team (F.1,3).
2. Special Applications Unit for IRRAS or the applicable organization for other codes (F.4).
3. Customer (F.2,5).

H. **What are the input requirements?**

1. Walkdown complete to the point of being useable for external event analysis (F.1).
2 Bug-free version with documentation (F.4).
3. Drawings legible and on paper (F.2).
4. Expert knowledgeable of the Customer facility and the process (F.5).
5. Identification of all equipment which is involved in the initiation of events or their mitigation (F.1).
6. Identification of the location of each piece of equipment (F.1).
7. Identification of the expected origins for the external events, their anticipated or possible propagation paths and their associated probabilities (F.1).
8. Identification of dependencies between hardware which has the same location and will be subjected to simultaneous effects of the non-process events, and assessment of their common failure probabilities (F.1,2).
9. Models which explicitly relate dependent components (F.1,2).
10. Tools and techniques which allow the solution of the models (F.4).
11. Knowledge of the capabilities and the role of the human in the course of the fire and flood events (F.5).
12. NUREG-4550 - Naming Scheme Adaptation (F.3).

8.2.10 Data Study

A. **Process**

1. Supply hardware and human-error failure rates for basic events in the event trees and fault trees.

B. **Scope**

1. All events which are included in the event tree and fault tree models.

C. **What is the output?**

1. Data frequency files.
2. A set of failure probabilities which reflect best estimates of hardware and human performance and which have known uncertainty bands.
3. A report detailing a set of fully-documented and scrutable quantitative estimates which will allow the quantitative solution of the fault trees and event trees and provide the frequency of occurrence for each of the initiating event categories.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report in EDF format.
2. Data files suitable to the methodology used.
3. Data sources documented.

F. **What are the inputs?**

1. Plant operational Data — satisfactory operating data, and abnormal event data.
2. Data base manager.
3. Industry PRA failure rate data as applicable (ex. Seabrook PRA).
4. NPRDS Data Base.
5. Military Handbook 217.
6. Commercial Data Bases as applicable.
7. Wordperfect EDF form.
8. Human-error events from fault trees and event trees.
9. Basic events from event trees and fault trees.
10. Basic event naming scheme.

G. **Who are the suppliers**

1. PRA Team (F.2,7,9).
2. Customer (F.1).
3. Technical Library (F.3,4,5,6).
4. EG&G Human Factors Group (F.8).

H. **What are the input requirements?**

1. Timely provision of data (F.1).
2. Relational Data Base (F.2).
3. Wordperfect 5.1 (F.7).
4. Adequate procedure definitions to allow human error analysis (F.8).
5. NUREG-4550 Naming Scheme Adaptation (F.10).
6. Adequate information to quantify basic events (F.9).
7. Data bases current (F.3,4,5,6).

8.2.11 Quantification

A. **Process**

1. To quantify all fault trees using IRRAS or another appropriate fault tree reduction code, and all event trees using the appropriate methodology.

B. **Scope**

1. To determine the plant damage frequencies for the internal operational event sequences which will lead to the desired consequence(s) to the Customer's process . Also, to determine the frequency of the desired consequence(s) as a result of internal non-operational event sequences. Finally, to integrate the results of the internal and external Non-process event studies with those from the internal process events.

C. **What is the output?**

1. Plant damage frequencies in files.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Data files on disk.

F. **What are the inputs?**

1. Output from the initiating event study.
2. Output from event tree development.
3. Output from the fault tree development.
4. Output from the data study.
5. Output from the internal non-process event study.
6. Output from the external event study.
7. IRRAS or other appropriate fault tree reduction code for fault tree quantification.
8. Appropriate methodology for event tree quantification.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4,5,6,8).
2. Customer (F.8).
3. Special Applications Unit or appropriate organization (F.7).

H. **What are the input requirements?**

1. Outputs are complete to the point of being used for quantification (F.1,2,3,4,5,6).
2. Bug-free version with documentation (F.7).
3. Method capable of reducing event trees and supplying sequence frequencies (F.8).
4. Support available to correct any bugs uncovered (F.7,8).
5. Software able to run on project computers (F.7,8).

8.2.12 Report Development

A. **Process**

1. Compile the results of the initiating event study, internal non-process event study, external event study, event tree study, fault tree study, data study and quantification results into a report.

B. **Scope**

1. In addition to describing methodologies , results, problems, sources of information, and systems, the report will also try to detail strengths and weaknesses of the Customer's facility and operations.

C. **What is the output?**

1. Report on Level-1 PRA.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report is in EDF format detailing highlights and conclusions of the Level-1 effort.
2. Report is well documented and contains all applicable references.

F. **What are the inputs?**

1. Initiating event reports.
2. Internal non-process event report.
3. External event report.
4. Results from the event tree development.
5. Results from the fault tree development.
6. Data study report.
7. Quantification results and conclusions.
8. EDF format.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4,5,6,7,8).

H. **What are the input requirements?**

1. Level-1 work is complete (F.1,2,3,4,5,6,7).
2. Wordperfect 5.1.

8.3 Level-2 PRA

8.3.1 Walkdown for Confinement Analysis

A. **Process**

1. Examination of all Customer facility rooms and areas where hazardous source terms could originate or propagate in a manner that affects Customer's personnel or offsite/onsite personnel.

B. **Scope**

1. Examine all areas to compile a list of ingress and egress paths as well as physical dimensions, ventilation conduits, and leakage areas around paths of ingress and egress.

C. **What is the output?**

1. PRA Team members sufficiently familiar with the Customer's physical configuration to aid in the performance of the confinement analysis.

D. **Who are the customers?**

1. PRA Team.

E. **What are the output requirements?**

1. PRA Team members capable of aiding in the performance of the confinement analysis.

F. **What are the inputs?**

1. Customer PRA Level-1 results.
2. Customer escort.
3. PRA Team members.
4. Unescorted access capabilities at Customer.

G. **Who are the suppliers**

1. PRA Team (F.1,3).
2. Customer (F.2,4).

H. **What are the input requirements?**

1. Customer Level-1 PRA complete to the point necessary for the walkdown (F.1).
2. Knowledgeable escort (Process and Plant) (F.2).
3. Appropriate security and badge paraphernalia for the Customer's facility (F.4).
4. Contact EG&G security, if necessary, to have PRA Team personnel able to access the Customer's facility (F.3).

8.3.2 Confinement Analysis

A. **Process**

1. Determine the integrity of the specified rooms detailing areas of ngress and egress and areas where there is communication from one compartment to another using information from the walkdown and other applicable references.

B. **Scope**

1. Perform the process for all rooms where a source term could originate or propagate.

C. **What is the output?**

1. A report detailing the findings of confinement analysis.
2. Detailed enumeration of the compartment penetrations and dimensions.

D. **Who are the customers?**

1. PRA Team.
2. Customer.

E. **What are the output requirements?**

1. Report in EDF format.
2. Comprehensive evaluation of compartments so that the results can be used in the confinement quantification.

F. **What are the inputs?**

1. Confinement walkdown.
2. Detailed facility drawings.
3. External events confinement analysis.
4. Wordperfect 5.1.

G. **Who are the suppliers**

1. PRA Team (F.1,3,4).
2. Customer (F.2).

H. **What are the input requirements?**

1. Walkdown completed to the stage necessary for the confinement analysis (F.1).
2. Drawings legible and on paper (F.2).
3. Customer external events confinement analysis available (F.3).
4. Wordperfect available (F.4).

8.3.3 Confinement Event Tree Analysis

A. **Process**

1. Event tree development through a process of functional block diagrams, followed by a success tree representing the conditions necessary for the facility being normally isolated,and finally production of the event trees from the success trees.

B. **Scope**

1. Event trees are developed to the level dictated by the methodology chosen for all confinement modes.

C. **What is the output?**

1. Confinement event tree files.
2. Binned event tree state definitions.
3. Description of the set of event trees which define the facility response to each of the identified initiator categories, and the resultant confinement state for each of the sequences.

D. **Who are the customers?**

1. Reactor Safety Group.
2. PRA Team.

E. **What are the output requirements?**

1. Event trees developed to the level for the methodology chosen.
2. Event tree states binned according to the similar confinement states.
3. Identification of all hardware and human systems which provide success paths which achieve individual functions.
4. Development of a systemic event tree which includes only hardware or human actions.
5. A nomenclature scheme which provides consistent unambiguous definition of events which is consistent with (or the same as) any existing facility or analytical systems. Customer staff should be able to interpret the scheme with little difficulty.

F. **What are the inputs?**

1. Facility walkdown.
2. Confinement analysis report.
3. External events report.
4. Output from the confinement source-term analysis.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4).
2. Reactor Safety Group (F.3).

H. **What are the input requirements?**

1. Sections complete to the point of being useable for event tree development (F.2,4).
2. Understanding of the functional response of the facility to an abnormal condition triggered by different confinement states (F.2).
3. Walkdown to be completed (F.1).
4. Access to the external events analysis report (F.3).

8.3.4 Source Term Calculations

A. **Process**

1. From the binned Level-1 event tree states, calculate the release to a particular location for that bin by summing the releases for each Level-1 damage state in that bin. The same type of process applies to the bin probabilities.

B. **Scope**

1. All Level-1 event tree bins.

C. **What is the output?**

1. Source terms for each Level-1 PRA event tree bin.
2. Probabilities of source terms for each bin.

D. **Who are the customers?**

1. Reactor Safety Group.
2. PRA Team.

E. **What are the output requirements?**

1. Source terms in a data base.

F. **What are the inputs?**

1. Event tree analysis — Level 1.
2. Sequence Quantification — Level 1.
3. Source term calculational method.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3).

H. **What are the input requirements?**

1. Level-1 event tree analysis and Quantification complete (F.1,2).
2. Calculational method is defensible and procedurally documented (F.3).

8.3.5 Containement Data Study

A. **Process**

1. Supply hardware, human-error failure rates for basic events,and portal opening frequencies in the event trees and fault trees.

B. **Scope**

1. All events which are included in the event tree and fault tree models for the Level II effort.

C. **What is the output?**

1. Data frequency files.
2. A set of failure probabilities which reflect best estimates of hardware and human performance and which have known uncertainty bands.
3. A report detailing a set of fully-documented and scrutable quantitative estimates which will allow the quantitative solution of the fault trees and event trees.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report in EDF format.
2. Data files suitable to the methodology used.
3. Data sources documented.

F. **What are the inputs?**

1. Plant operational data — satisfactory operating data, and abnormal event data.
2. Data base manager.
3. Industry PRA failure rate data as applicable (ex. Seabrook PRA).
4. NPRDS data base.
5. Military Handbook 217.
6. Applicable commercial data bases.
7. Wordperfect EDF form.
8. Human error events from fault trees and event trees.
9. Basic events from event trees and fault trees.
10. Basic event naming scheme.

G. **Who are the suppliers**

1. PRA Team (F.2,7,9).
2. Customer (F.1).
3. Technical Library (F.3,4,5,6).
4. EG&G Human Factors Group (F.8).

H. **What are the input requirements?**

1. Timely provision of data (F.1).
2. Relational data base (F.2).
3. Wordperfect 5.1 (F.7).
4. Adequate procedure definitions to allow human-error analysis (F.8).
5. NUREG-4550 Naming Scheme Adaptation (F.10).
6. Adequate information to quantify basic events (F.9).
7. Data bases current (F.3,4,5,6).

8.3.6 Confinement Fault Tree Development

A. **Process**

1. Develop fault trees using NUREG 0492 as a guide.

B. **Scope**

1. Develop trees required by the top events in the event trees.
2. All systems (hardware and human) which are shown to be relevant to supporting the confinement analysis.

C. **What is the output?**

1. Fault tree files.
2. The set of fault trees which describe the relationships between hardware and human faults and events which are events described on the event trees.
3. A set of computer models which are capable of solution to provide both qualitative (cut-sets) and quantitative insights (probabilities and importance, when failure probabilities are known).

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Full description of the hardware systems and their inter-relationships (dependencies) (functional diagrams).
2. Identification of dependencies and relevant hardware faults and documentation of exclusions (i.e. interfacing system FMEA).
3. Fault tree code with graphical interface.
4. Fault trees developed to the level to quantify the top events of trees.
5. Fully-documented and reviewable product.
6. Model of sufficient detail to meet future applications and be solved in the required time (performance criteria).
7. Model compatible with the event tree solution process.

F. **What are the inputs?**

1. Confinement event trees.
2. IRRAS or other applicable PRA code.
3. Facility drawings.
4. Customer process expert.
5. Basic event naming scheme.

G. **Who are the suppliers**

1. PRA Team (F.1,4,5).
2. Special Applications Unit for IRRAS or other applicable organization (F.2).
3. Customer (F.3).

H. **What are the input requirements?**

1. Confinement analysis complete to the point of being useable for fault tree development (F.1).
2. Bug-free version with documentation (F.2).
3. Drawings legible and on paper (F.3).
4. Expert knowledgeable of the Customer's facility and the process (F.4).
5. NUREG-4550 Naming Scheme Adaptation (F.5).

8.3.7 Confinement Quantification

A. **Process**

1. To quantify all fault trees using IRRAS or another appropriate fault tree reduction code and all event trees using the appropriate methodology.

B. **Scope**

1. To determine the confinement release state frequencies for the confinement states and bin similar states.

C. **What is the output?**

1. Probability, quantity and location of external and internal releases in a data file.

D. **Who are the customers?**

1. PRA Team.

E. **What are the output requirements?**

1. Data files on disk.

F. **What are the inputs?**

1. Output from the confinement event tree analysis.
2. Output from the confinement fault tree analysis.
3. Output from source term analysis.
4. Output from the confinement data study.
5. IRRAS or other appropriate fault tree reduction code for fault tree quantification.
6. Appropriate methodology for event tree quantification.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4,6).
2. Customer (F.6).
3. Special Applications Unit or other applicable organization (F.5).

H. **What are the input requirements?**

1. Outputs are complete to the point of being used for quantification (F.1,2,3,4).
2. Bug-free version (relatively) with documentation (F.5).
3. Method capable of reducing event trees and supplying sequence frequencies (F.6).
4. Support available to correct bugs (F.5,6).
5. Software able to run on project computers (F.6).

8.3.8 Report Development

A. **Process**

1. Compile the results of the confinement analysis, source term calculations, confinement data study, confinement fault tree analysis, confinement event tree analysis, and the confinement quantification into a report.

B. **Scope**

1. In addition to describing methodologies, results, problems, sources of information, and systems, the report will also try to detail strengths and weaknesses of the Customer's facility and operations.

C. **What is the output?**

1. Level-2 report.

D. **Who are the customers?**

1. Customer.
2. PRA Team.

E. **What are the output requirements?**

1. Report is in EDF format detailing highlights and conclusions of the Level-2 effort.
2. Report is well-documented and contains all applicable references.

F. **What are the inputs?**

1. Confinement analysis report.
2. Source term calculations.
3. Results from the confinement event tree analysis.
4. Results from the confinement fault tree analysis.
5. Confinement data study report.
6. Confinement quantification results and conclusions.
7. EDF format.

G. **Who are the suppliers**

1. PRA Team (F.1,2,3,4,5,6,7).

H. **What are the input requirements?**

1. Level-2 work is complete (1,2,3,4,5,6,7).
2. Wordperfect 5.1.

8.4 Customer Final Report

A. Process

1. Combine the Level-1 PRA Report and the Level-2 PRA Report into a Final PRA report.

B. Scope

1. In addition to describing methodologies, results, problems, sources of information, and systems, the report will also try to detail strengths and weaknesses of the Customer's facility and operations, and lessons learned.

C. What is the output?

1. Final Customer PRA Report.

D. Who are the customers?

1. Customer.

E. What are the output requirements?

1. Report is in internal report format.
2. Report is well-documented and contains all applicable references.
3. Report is auditable.

F. What are the inputs?

1. Level-1 PRA results.
2. Level-2 PRA results.

G. Who are the suppliers

1. PRA Team.

H. What are the input requirements?

1. Level-1 PRA work is complete.
2. Level-2 PRA work is complete.

END

DATE FILMED

9/22/92