

**FINAL DRAFT**

**THE ROLE OF FAULT TREES AND EVENT TREES IN DEPICTING  
FAILURE OF A HIGH-LEVEL RADIOACTIVE WASTE PACKAGE IN  
A BASALT REPOSITORY**

**August 1984**

**Prepared for**

**Office of Nuclear Material Safety and Safeguards  
U.S. NUCLEAR REGULATORY COMMISSION  
Washington, D.C.**

**Prepared by**

**Eastern Technical Division  
THE AEROSPACE CORPORATION  
Washington, D.C.**

**8409050067 840817  
PDR WMREB EECAER08  
A-4165 PDR**

**FINAL DRAFT**

**THE ROLE OF FAULT TREES AND EVENT TREES IN DEPICTING  
FAILURE OF A HIGH-LEVEL RADIOACTIVE WASTE PACKAGE IN  
A BASALT REPOSITORY**

**K.W. Stephens, Program Manager**

**Contributors**

**L.P. Boesch  
A.B. Crane  
R.L. Johnson  
R.B. Moler  
S.M. Smith  
K.W. Stephens**

**August 1984**

**Prepared for**

**Office of Nuclear Material Safety and Safeguards  
U.S. NUCLEAR REGULATORY COMMISSION  
Washington, D.C.**

**Prepared by**

**Eastern Technical Division  
THE AEROSPACE CORPORATION  
Washington, D.C.**

## PREFACE

The Nuclear Regulatory Commission (NRC) must pass independent judgment on the adequacy of high-level radioactive waste package designs developed by the Department of Energy. To determine whether the packages meet the requirements of 10 CFR 60, NRC must be able to estimate the lifetime of the package and to quantify the rate of radionuclide release should a package failure occur. The program to develop this capability consists of research projects to (1) develop an understanding of the failure modes and material processes and (2) develop the analytical methodology needed to make independent assessments of waste package performance in support of licensing decisions that ultimately must be made.

The Aerospace Corporation "Preparation of Engineering Analysis for High-Level Waste Packages in Geologic Repositories" project is one of several that collectively will achieve these objectives. The project has four main tasks: (1) evaluation of the methodology for assessing long-term performance of high-level waste packages, (2) construction of fault trees and event trees depicting package failure and transport of radionuclides from the package, (3) assessment of the performance of the Department of Energy waste package designs, and (4) general technical assistance associated with waste package assessments. Task 2 and the initial phase of Task 1 have been completed. During FY 1985, Task 1 will continue, and Task 3 will be initiated. This report presents the results of the work performed under Task 2.

## EXECUTIVE SUMMARY

### BACKGROUND

The work described in this report is part of an overall project that will culminate in an assessment of Department of Energy waste package designs in terms of package lifetime and radionuclide release rates. Activities are now oriented toward examining of methods for waste package performance assessment. Fault trees and event trees have been used since 1961 to analyze a variety of complex systems, including ballistic missiles and nuclear power plants. Thus, it is logical to consider whether fault tree and event tree methods can contribute to performance analysis of radioactive waste packages.

The report presents general information related to fault trees and event trees and then describes the trees developed for the basalt waste packages (included as appendixes). Mathematical considerations associated with quantification of the trees to analyze waste package lifetime and radionuclide releases are discussed. Conclusions are presented and a recommendation is made.

### WASTE PACKAGE DESIGNS

The fault and event trees described in this report use the reference waste package conceptual designs released from the Basalt Waste Isolation Project (BWIP) project office.\* The designs consist of a thick-walled steel container overpack encasing either a steel-canistered glass waste form in the commercial high-level waste (CHLW) design or spent fuel rods in the spent fuel (SF) design. The waste container, surrounded by a packing mixture of bentonite clay and crushed basalt, will be emplaced in either long or short horizontal boreholes in basalt.

---

\*Westinghouse Electric Corporation, 1982, "Waste Package Conceptual Design for a Nuclear Repository in Basalt," RHO-BW-CR-136P/AESD-TME-3142.

The waste package designs are in the conceptual stage with numerous design alternatives and placement options under serious consideration. Adjustments will be made during the performance assessment analysis, to reflect changes to the designs as they are upgraded.

## FAULT TREES

Fault trees depicting failure of the high-level radioactive waste packages in basalt are presented in Appendix A. Radionuclide releases from the package are the top fault or failure event. The trees proceed downward to display the possible failure modes and causes in a formal fault-tree diagram. Events flow downward through intermediate events to primary failure events.

An important observation regarding the fault tree structure is that the trees do not depict (from the bottom up) the exact order in which events occur. Rather, the fault trees show the events that must have transpired for higher level events to occur. The structured form of the trees thus displays the failure mechanisms that are considered potentially significant, but without preference given to any particular failure mode. Included are the expected slow degradation failure modes of corrosion (e.g., uniform, pitting, crevice, stress, hydrogen, etc.) as well as the lesser understood or nonexpected failures such as missed quality control errors, earthquakes, or human intrusion faults.

## EVENT TREES

The event trees presented in Appendix B begin with those actions considered that could initiate a failure and eventually lead to radionuclide release. Eleven possible failure initiating events have been diagrammed and discussed as event trees with simple fail/no fail branches for both the CHLW and SF waste package conceptual designs in basalt. Corrosion mechanisms are generally believed to be the most likely cause of package failure and presence of groundwater is the most likely initiator of corrosion. On the other extreme, less probable events were also included such as corrosion followed by criticality, missed quality control errors, and post-closure human intrusion initiators.

Not all of the events in the sequences leading to system failure are independent, many are interactive and vary greatly in their time to fail (e.g., corrosion is considered slow failure (years) whereas earthquakes loads could cause instant partial failure; furthermore, the earthquake event can interact at any time with the corroding canister).

## MATHEMATICAL CONSIDERATIONS

Boolean algebra is the mathematical technique usually applied to fault and event trees to combine the individual event probabilities and thereby calculate a system failure expectancy. This technique, however, requires the presence of some rather specific relationships among individual events that are not necessarily present in the waste package phenomenology. The three main issues affecting the use of the fault and event tree quantification method:

- Nonindependence of primary event,
- Representation of standby system as parallel systems, and
- Representation of continuous processes by discrete events.

An additional less significant issue is that of combined effects of internal and external degradation.

Many of the events leading to package degradation and failure are interrelated and are affected by common environmental conditions and, therefore, are not statistically independent. This invalidates the rules of Boolean algebra commonly applied to the quantification of the trees.

Another difficulty, for fault trees in particular, is the representation of the sequential failure of the concentric waste package barriers using AND and OR logic gates. The protection afforded by an outer barrier produces a time-lag in the onset of destruction of the inner barriers, and time lags are not readily representable in fault tree logic gates.

For this case, an estimate was made of the comparative magnitude of the time-lag effect on the waste package system reliability. Calculations (Table 3)

were made for the standard fault tree method (parallel system) and a method that accounts for the time-delayed degradation provided by the nested barriers. Results for the first 500 years, for example, show that the fault tree analytic method generated failure probabilities approximately an order-of-magnitude higher than predicted by the time-delayed method. This latter method provides a more realistic representation of waste package physical degradation than does the parallel (fault tree) method.

A third difficulty, which pertains to both fault and event trees, is the representation of continuous degradation processes (e.g., corrosion) by discrete branchings. The complex physical and chemical processes that lead to barrier degradation are best modeled by continuous variables. Multiple tree branchings provide approximations, but because many variables are usually required, the multiple branching approach quickly becomes unwieldy.

The limitations of the fault and event tree method discussed above do not imply that waste package failure probability is not quantifiable. Several other analytical methods are being investigated and are showing promise.

## CONCLUSIONS AND RECOMMENDATION

On the basis of the work to date, it was concluded that:

- Fault trees and event trees can be valuable qualitative tools to display failure modes and event sequences.
- The general methods used to quantify the trees cannot be used in the waste package context because they do not provide a realistic representation of the waste package degradation.

It is therefore recommended that:

- Methods other than fault trees and event trees should be explored for quantitative analysis of waste package performance.

## CONTENTS

	<u>Page</u>
PREFACE	iii
EXECUTIVE SUMMARY	v
I. INTRODUCTION	1
II. REFERENCE WASTE PACKAGE DESIGNS	3
III. GENERAL FAULT TREE/EVENT TREE MODELS	7
A. Fault Trees	7
B. Event Trees	8
C. Fault Trees and Event Trees for Waste Packages	8
IV. FAULT TREES FOR BASALT WASTE PACKAGES	11
A. Approach	11
B. Terminology	12
C. Structure of Fault Trees	15
D. Fault Tree Discussions	16
1. Glass Waste Form	17
2. Spent Fuel Waste Form	19
3. Canister	21
4. Overpack	23
5. Packing	25
V. EVENT TREES FOR BASALT WASTE PACKAGES	29
A. Approach	29
B. Structure of Event Trees	29
C. Event Tree Discussions	31
1. CHLW Package Failure--Corrosion	31
2. CHLW Package Failure--Hole in Overpack Weld and Corrosion	32
3. CHLW Package Failure--Ceiling Collapse and Corrosion	33
4. CHLW Package Failure--Corrosion Followed by Loading from Ceiling Collapse	34
5. CHLW Package Failure--Drilling into Repository Area	35
6. CHLW Package Failure--Drilling into Waste Package	36
7. CHLW Package Failure--Mechanical Failure of Waste Form and Internal Corrosion	38

## CONTENTS (continued)

	<u>Page</u>
Event Tree Discussion (continued)	
8. SF Waste Package Failure--Corrosion	39
9. SF Waste Package Failure--Corrosion Followed by Criticality	40
10. SF Waste Package Failure--Handling/Quality Control and Corrosion	41
11. SF Waste Package Failure--Earthquake and Corrosion	41
VI. MATHEMATICAL CONSIDERATIONS	43
A. Fault Tree Analysis	43
1. Nonindependence of Primary Events	44
2. Representation of Standby Systems as Parallel Systems	45
3. Representation of Continuous Processes by Discrete Events	53
4. Combined Effects of Internal and External Degradation	53
5. Alternative Methods for Quantification of Failure and Risk	54
B. Event Tree Analysis	55
1. Discrete versus Continuous State Variables	56
2. Time-Dependent Probabilities	56
3. Completeness and Overlap of Scenarios	57
VII. CONCLUSIONS AND RECOMMENDATION	59
REFERENCES	61
APPENDIX A. CHLW Fault Trees	A-1
APPENDIX B. SF Fault Trees	B-1
APPENDIX C. Event Trees	C-1

## 1. INTRODUCTION

This report presents a set of fault trees and event trees for failure of an individual high-level radioactive waste package in a basalt repository. This work is part of the overall project described in the Aerospace Program Plan (1983). The complete project will include an examination of other methods for analyzing waste package reliability (Aerospace, 1984) and quantitative assessment of Department of Energy waste package designs. The output of the assessment will include waste package failure probabilities and radionuclide release rates expressed as functions of time. Because fault trees and event trees have been used to analyze the reliability and performance of such complex systems as missiles and nuclear power plants, the tree techniques were examined to determine whether they could serve as tools for waste package performance assessment. This report discusses the effectiveness and suitability of fault tree and event tree techniques in this context.

The reference engineering conceptual designs for commercial high-level waste (CHLW) and spent fuel (SF) waste packages for basalt (Westinghouse, 1982) were used as the basis for the fault and event trees. The main barriers to radionuclide release afforded by the CHLW (waste form, canister, overpack, and packing) and SF (waste form, overpack, and packing) designs were used to structure the trees.

The fault trees for failure of CHLW and SF waste packages are presented in Appendixes A and B, respectively. This analysis is unique in that it considers the value of the barriers provided by the waste package. Other fault tree analyses conducted to date have primarily considered the radionuclide barrier provided by the geologic formation (d'Alessandro and Bonne, 1980). Eleven possible event trees resulting in failure of CHLW and SF waste packages are presented in Appendix C. Discussions regarding the development of the trees and the sources of information are provided.

Based on the experience gained during the development and evaluation of the fault trees and event trees, it is believed that the techniques can be effective tools in the qualitative analysis of waste package performance. The trees, discussed in Sections III, IV, and V of this report, are useful for displaying the scenarios, failure modes, and relationships associated with waste packages and provide a medium for discussion. However, there are difficulties that rule out use of fault tree and event tree techniques for quantitative analysis of waste package reliability. Mathematical considerations and example calculations, presented in Section VI, substantiate this finding.

## II. REFERENCE WASTE PACKAGE DESIGNS

For use with the fault trees and event trees, the reference engineering conceptual designs for CHLW and SF waste packages for basalt are shown schematically in Figures 1 and 2, respectively. The schematics define the components of the engineering packages and were taken from the reference designs presented by Westinghouse (1982). The Westinghouse report includes considerable summary conceptual design information (e.g., dimensions and masses) and performance features (e.g., temperature and corrosion estimates) on both the reference waste package designs and alternatives. The CHLW form resembles the borosilicate glass form developed for fuel reprocessing at Barnwell, South Carolina, and is used for waste resulting from reprocessing spent fuel that originally contained only uranium oxide. The CHLW form is poured, while molten, into a stainless steel canister. The canister, filled to about 85 percent capacity, facilitates handling and interim storage. A steel overpack will be used and will be surrounded by a packing mixture of bentonite clay and crushed basalt (25/75 percent by weight), sized to be suitable for emplacement in reference horizontal boreholes. Therefore, the CHLW package provides four engineered barriers to radionuclide release to the basalt (waste form, canister, overpack, and packing).

The spent fuel form consists of fuel rods (fuel pellets encased in Zircaloy cladding) removed from intact assemblies and consolidated into a closely packed array. In the reference conceptual design, the numbers of rods per waste package is 792 pressurized water reactor rods (3 assemblies) or 441 boiling water reactor rods (7 assemblies). The steel container used as the overpack for the consolidated rods will be designed for a 1000-year containment. A pressurized water reactor fuel rod schematic (Figure 3) (Woodley, 1983) shows the components in a typical configuration for use with the spent fuel fault and event trees. Note that a canister is not used for the SF form as in the CHLW. Thus, the SF waste package only provides three barriers to radionuclide release (cladding, overpack, and packing).

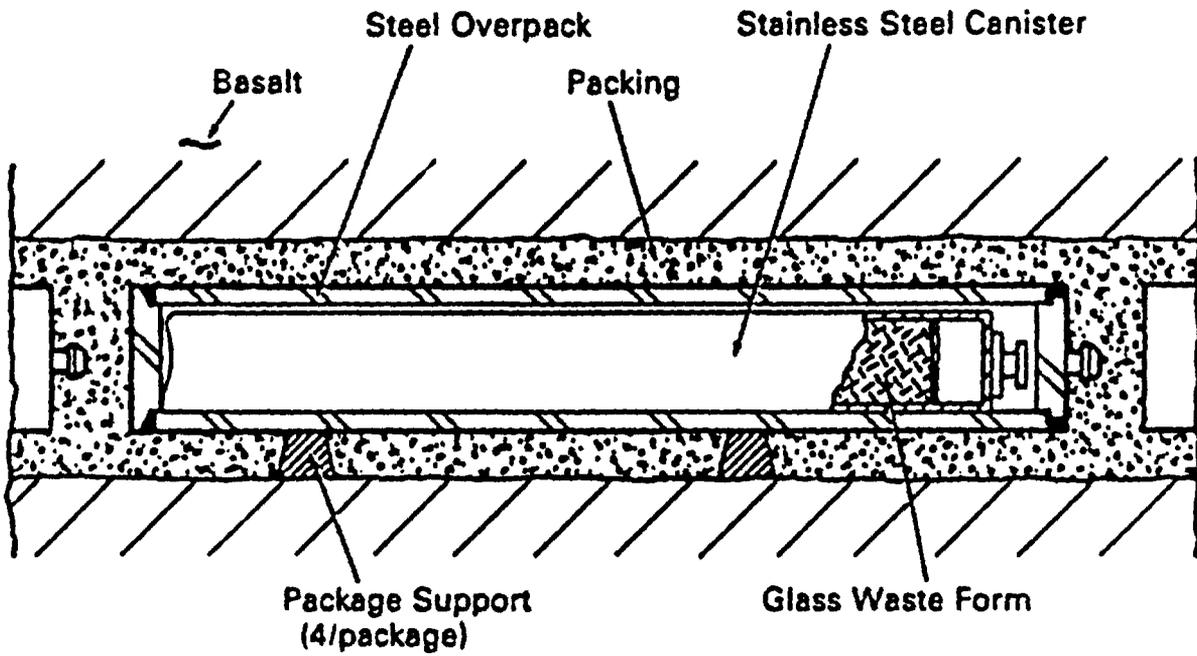


Figure 1. Reference Waste Package Conceptual Design for Commercial High Level Waste in Basalt (Westinghouse, 1982)

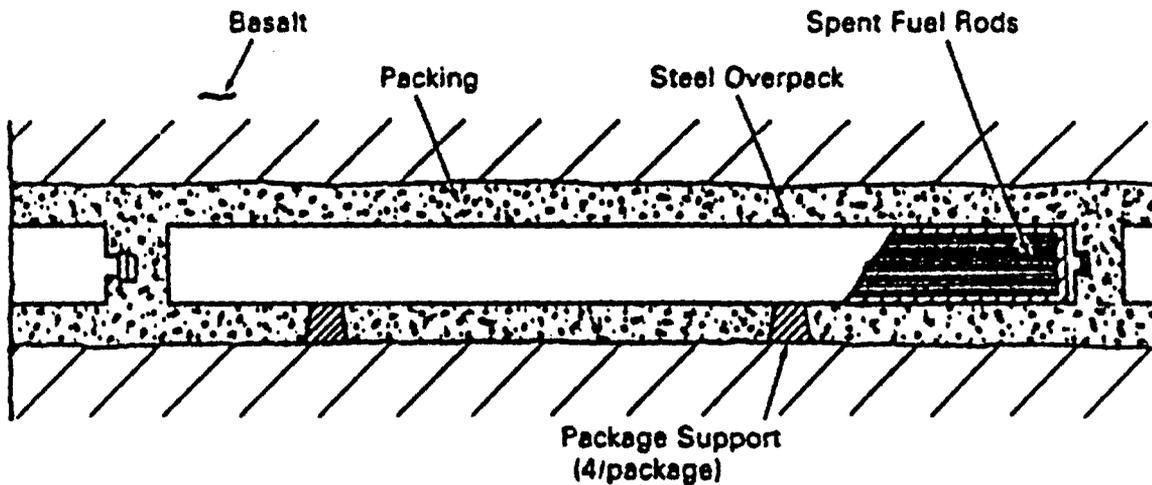


Figure 2. Reference Waste Package Conceptual Design for Spent Fuel in Basalt (Westinghouse, 1982)

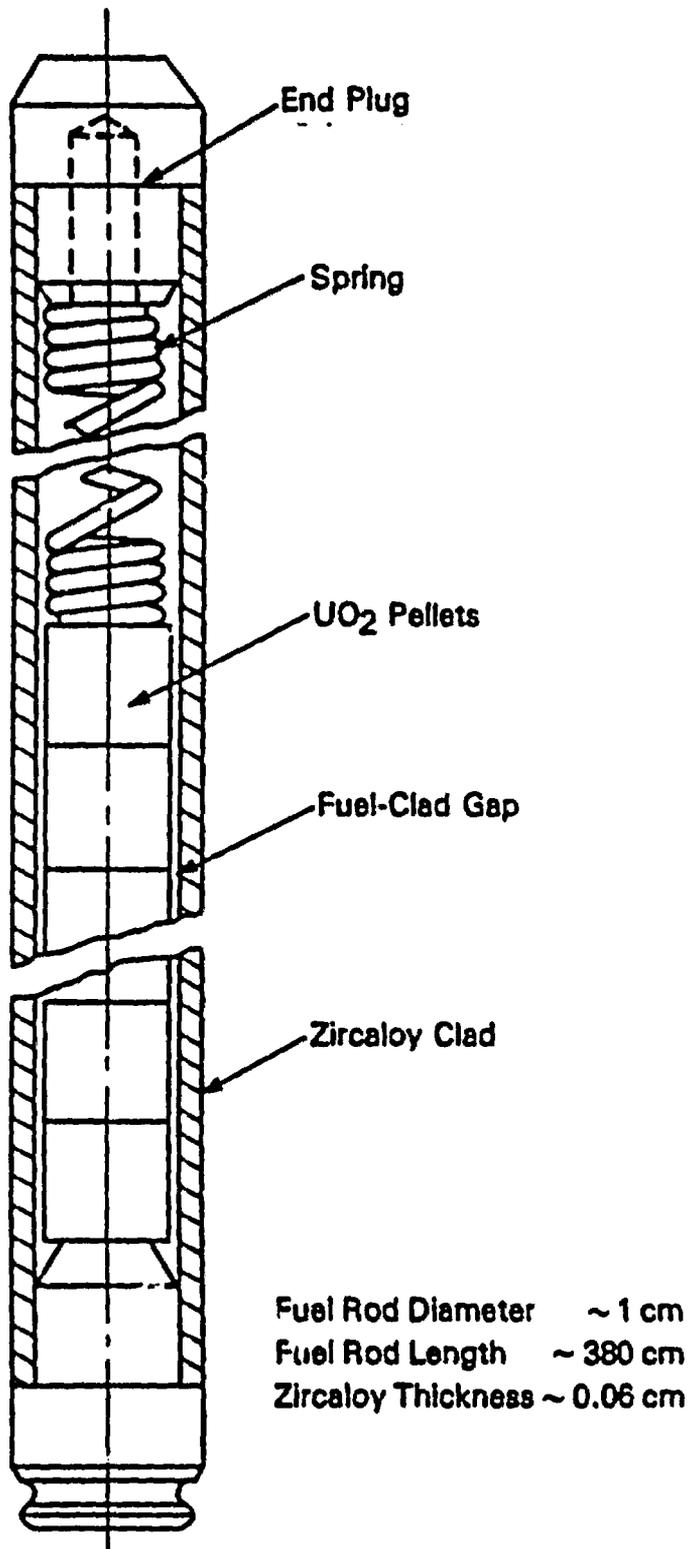


Figure 3. Typical Pressurized Water Reactor Individual Spent Fuel Rod (Woodley, 1983)

The waste package designs for basalt are in the conceptual stage with numerous backup alternatives and placement options still under serious consideration. For example, options under consideration include placement of multiple inline waste packages in long (200-meter) horizontal boreholes versus a single waste package in short horizontal end-drift boreholes. Therefore, whatever performance assessment methodology is selected, adjustments will need to be made as the designs proceed into the preliminary and detailed stages. However, as discussed later in this report, it should be recognized that the current structure of the waste package, using nested barriers that are interrelated in terms of time of failure, is one of the key determinants in the selection of a performance assessment methodology.

### III. GENERAL FAULT TREE AND EVENT TREE MODELS

#### A. FAULT TREES

Fault tree analysis was introduced in 1961 to perform safety evaluations of the Minuteman missile program and has been used since then for a variety of complex systems analyses, the best known of which is the Reactor Safety Study (NRC, 1975). The technique is widely used today as a major tool for probabilistic risk assessment of nuclear power plants and is a proven tool for systems analysis in a wide range of other applications. In fault tree analysis, an undesired state of the system is specified. This state is usually one that is critical from a safety standpoint. The system is then analyzed in the context of its environment and operation to find the ways in which this 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 predefined undesired event. The faults can be events associated with component failures, human errors, or any other pertinent event that can lead to the undesired event. The fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, which is the top event in the tree. For the purpose of this project, the top event is any release of radionuclides outside the engineered waste package (waste form, canister, overpack, and packing material).

As discussed in the NRC "Fault Tree Handbook" (NRC, 1981), it is important to realize that a fault tree is not a model of all possible system failures or all possible causes. A fault tree includes only those faults that contribute to the top event. Therefore, a fault tree includes only the faults assessed by the analyst as being pertinent. Additionally, a fault tree is not in itself a quantitative model. Rather, it is a qualitative model that is often evaluated quantitatively using Boolean algebra to analyze the probability of the outcome. Irrespective of whether the trees are quantitatively evaluated, they offer a means of showing the relationships among the system components and may suggest relationships

not previously considered (i.e., the trees can serve as a "roadmap" to the problem). Persons desiring background information on fault tree analysis in general should consult references such as McCormick, 1981; Reilly, 1978; and Larsen, 1974. They describe the technique and how to apply it.

## B. EVENT TREES

An event tree is a logic method for identifying possible outcomes of a given event. Event trees have been used in decision analysis and have been applied to reactor safety studies (NRC, 1975). Unlike fault trees, event trees begin with a defined initiating event and then examine the consequences of the event, the factors influencing mitigation of its effects, and the results of the sequence of events. The convention followed by event trees is to divide the branches at each junction in the tree into a "success" (top branch) and a "failure" (bottom branch). Figure 4 depicts a sample event tree with an initiating event and two safety systems, the successful operation of which will mitigate the effects of the initial event. The operation of the safety systems is described as either a success or a failure. The resulting accident sequence is thus identified by the possible paths that can be taken. For a situation in which the safety system can fail partially, but not necessarily totally, the success and failure states can have more branches, with each representing a specifically defined type of failure (McCormick, 1981). However, in this report, the event trees have been restricted to the typical binary (success/failure) form. Like fault trees, event trees provide an easily understood way to display particular failure sequences and generally are quantitatively evaluated using Boolean algebra.

## C. FAULT TREES AND EVENT TREES FOR WASTE PACKAGES

Fault tree analysis is not known to have ever before been applied to the problem of high-level radioactive waste packages. Several studies have applied fault tree methods to analyze the geologic formation as a barrier to the release of radionuclides (d'Alessandro and Bonne, 1980; Bertozzi et al., 1977; Logan and Berbano, 1977; Lee et al., 1978; Bhaskaran and McCleery, 1979). Although these studies applied to geologic formations that could act as barriers to the release

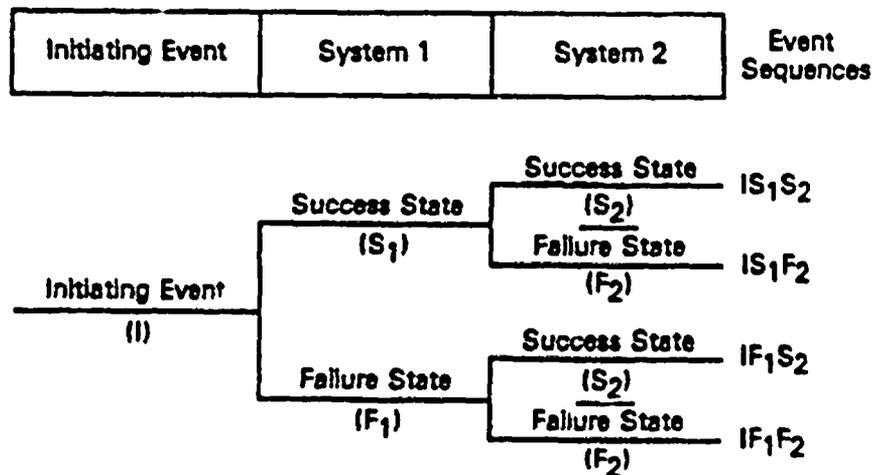


Figure 4. Sample Event Tree (NRC, 1975)

of radionuclides, they did not incorporate an analysis of the waste package. In each study, the same basic approach was used—define the events, prepare the trees, and make whatever assumptions and simplifications are necessary to complete the analysis. Sandia National Laboratories (SNL) (Hunter, 1983) has used logic (or event) trees to construct and screen possible waste release scenarios in the development of a methodology for assessing repository sites. However, SNL's trees have not included the waste package portion of the repository design.

In the waste package, most of the events are affected by common environmental conditions and are also time-dependent due to the multiple barrier system. Neither of these types of dependence can be analyzed by standard fault tree or event tree techniques. Additionally, the waste package is characterized by continuously varying processes. These processes are difficult to model using a fault tree approach that treats continuously interactive processes as singular discrete events.

## IV. FAULT TREES FOR BASALT WASTE PACKAGES

### A. APPROACH

This section of the report presents fault trees prepared to depict waste package failure. These fault trees serve the function of providing a qualitative representation of the possible waste package failures. Discussions regarding how the trees were developed and the sources of information that serve as their basis are provided.

Because 10 CFR 60 is oriented toward preventing any radionuclide release during the specified containment period (300 to 1000 years), fault tree representation was considered as one of the methods to possibly depict waste package failure, where failure is defined as any release of radionuclides by the waste package to the basalt media (very near field). The fault trees have been structured to show the significant items that will affect the likelihood of package failure following permanent repository closure. Some repository pre-closure activities that affect post-closure failure are included as appropriate, such as a breach created in the CHLW canister (which is inside the overpack) due to handling before the package was emplaced in the repository. Other failure modes are also included in the trees to make visible many modes that might not be given due consideration during design or because they have not been evaluated sufficiently to be excluded from further consideration at this time.

The fault trees are developed to present "release of radionuclides," as the top event. To this end, it is considered important to determine whether the radionuclides will be transported from barrier to barrier and, ultimately, to the basalt host rock. The radionuclides can be in gaseous, liquid, solid, or colloidal states. If the radionuclide movement is by water or steam, this transport mechanism is referred to as aqueous transport. If water and steam do not

participate in the transport of the radionuclides, then the transport mechanism is referred to as nonaqueous transport (e.g., granulated glass trickling or falling through a breach in the lower side of the canister).

The transport mechanism is not necessarily dependent on the mechanism that causes package failure. A waste package barrier may be breached or failed due to a wet or dry atmosphere in contact with that barrier, but by the time the radionuclides are in a condition to be transported, the atmosphere may have changed from dry to wet or vice versa. For example, the canister may be breached under dry conditions, but the radionuclides might not be mobilized (transported) until water enters the canister interior.

The packing is considered to be dry if the water content of the packing by volume is equal to or less than the water content at the time of packing emplacement. The canister and overpack are considered to be in a dry state when manufactured. Wet is defined as the state when the moisture level is greater than that defined for dry.

## B. TERMINOLOGY

The NRC "Fault Tree Handbook" (1981) was used as a guide in developing the fault trees presented in this report. A fault tree is a qualitative model of the events resulting in system failure. The trees diagram the logic of the failure path by using a hierarchy of gates and events. The gates permit or inhibit the passage of fault logic up the tree and show the relationships of events needed for the occurrence of higher events. An "upper" event is the output of the gate; "lower" events are the input to the gate.

A set of symbols (Table 1) is used in the fault trees to graphically represent the types of relationships between input and output events. There are four categories of symbols generally used in fault tree analysis: primary event, intermediate event, gate, and transfer.

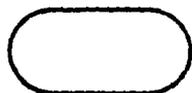
Table 1. Fault Tree Symbols (NRC, 1981)

Primary Event Symbols



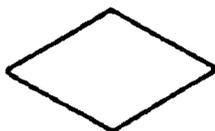
BASIC

A basic initiating fault requiring no further development



CONDITIONING

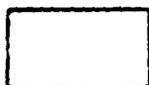
Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)



UNDEVELOPED

An event that is not further developed either because it is of insufficient consequence or because information is unavailable

Intermediate Event Symbols



INTERMEDIATE

A fault event that occurs because of one or more antecedent causes acting through logic gates

Gate Symbols



AND

Output fault occurs if all of the input faults occur



OR

Output fault occurs if at least one of the input faults occurs



INHIBIT

Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING event drawn to the right of the gate)

Transfer Symbols



IN

Indicates that the tree is developed further at the occurrence of the corresponding transfer OUT (e.g., on another page)



OUT

Indicates that this portion of the tree must be attached at the corresponding transfer IN

Primary events are those that have not been developed further and that would have probabilities of occurrence assigned if the tree were quantified. The primary events used most frequently in Appendixes A and B, CHLW and SF waste package fault trees, respectively, are the BASIC (circle) and UNDEVELOPED (diamond) events. A BASIC event is one that requires no further development; thus, a circle represents the lowest level to which a failure can be taken in the fault tree analysis. UNDEVELOPED events have not been developed further either because the event is considered insignificant or because sufficient information is not available to describe the basic input events. In time, the intent would be to remove the diamonds, either by adding more detail or by developing a consensus that the event does not merit further attention. A CONDITIONING event attaches specific conditions or restrictions that apply to any logic gate, but is used in this report only with the INHIBIT gate defined below.

INTERMEDIATE events, represented by rectangles, represent fault events that occur because of one or more preceding (lower) events. Logic gate symbols are used to identify the relationships between the antecedent and intermediate events. The two basic types of logic gates are the OR and the AND gates. OR gates are used to show that the output events occur only if one or more of the input events occur. An AND gate shows that the output event occurs only when all of the input events exist. Another logic gate, the INHIBIT gate, indicates that an output fault occurs if an input fault occurs in the presence of an enabling condition (as represented by a CONDITIONING event). In this report, the INHIBIT gate is also intended to convey the option that a probability can be increased or decreased based on the lapsed time after repository closure or the lapsed time after an event occurred. This INHIBIT gate is being used to account for some of the dependencies among events.

Transfer IN and OUT symbols can be used to avoid duplication in the figures; they are indicative of system interfaces. Additionally, it is frequently not feasible to show an entire fault tree on a single sheet of paper, so transfer symbols are used to divide system trees into subtrees. A numbering convention, using a five-character code identifier placed inside the transfer symbols, has

been implemented in this report. This numbering system enables the user to maintain a record of transfers and is represented by the following format:

<u>Z</u>	<u>XXXX</u>
alphabetic character represents system	four numeric characters identify the subtree

Table 2 identifies the alphabetic characters used to identify the systems where each system is representative of a single package barrier. The numeric characters used to identify the subtrees start at 1000 and are incremented by one for each additional subtree.

Table 2. System Identification Code

Code	System
A	Glass Waste Form
B	Stainless Steel Canister
C	Steel Overpack
D	Packing (bentonite/basalt)
E	Spent Fuel Waste Form

### C. STRUCTURE OF FAULT TREES

Because the ultimate purpose of the fault trees presented in this report is to represent means of releasing radionuclides to the basalt repository wall surrounding the waste package, the overall structure of the fault tree has two parts: one set of trees for a release from the CHLW package (Appendix A) and a separate set of trees for a release from the SF waste package (Appendix B). These two packages are the bases for the top events shown in Figures A-1 and B-1. Within each of the sets of trees, the basic structure centers on the main barriers (waste form, overpack, etc.) provided by the reference package designs.

The barriers formed for the CHLW package are the glass waste form, the stainless steel canister, the steel overpack, and the bentonite/basalt packing. The barriers for the SF package are the spent fuel pellets/zircaloy cladding, steel overpack, and the packing. These barriers are shown as second-level events in Figures A-2 and B-2, respectively.

As the various trees were developed, it was noted that certain events and sequences are common to both types of waste packages. Specifically, some parts of the trees for the overpack and the packing were common to both the CHLW and SF packages, so SF fault tree parts common to the CHLW fault tree parts were combined and presented in appropriate Appendix A figures. Appendix B clearly references those figures presented in common in Appendix A.

The next level of detail in the trees (topped by the triangular transfer symbols) deals with the mechanisms for releasing radionuclides that travel through a breach. Finally, the level of detail is carried down to the point at which the very basic events (depicted by circles) are identified or to the point at which the analysis is stopped at an event that is not further developed here (depicted by diamonds). However, it should be recognized that the lower an event is on the tree, the less is its overall impact. An exception would be an event that occurs in several places in the lower parts of the tree (e.g., presence of water).

One important observation regarding the fault tree structure is that the trees do not depict (from the bottom up) the exact order in which events occur. (That would not be practical, because some events cycle or occur repeatedly.) Rather, the fault trees show the events that must have transpired for higher level events to occur.

#### D. FAULT TREE DISCUSSIONS

The detailed lower events of the CHLW package and SF waste package are described in this section. The parts of the CHLW and SF fault trees that are unique to themselves include the CHLW form, the SF waste form, and the

canister parts and are discussed separately; those parts held in common are discussed together and include the overpack and the packing.

The fault tree diagrams for the CHLW form and the canister are in Appendix A, and those for the SF waste form are in Appendix B. Diagrams for each of the two overpacks are different and thus are presented in Appendixes A and B, respectively, with common parts consolidated in Appendix A. The packing trees are identical for the degree of detail presented for both trees and are therefore consolidated in Appendix A.

### 1. Glass Waste Form

The glass waste form is associated only with the CHLW package. There are no items in the glass waste form section of the fault tree that are common to SF waste form section of the SF fault tree.

Figures A-3 and A-4 of the tree focus on the aqueous transport of radionuclides from the glass waste form to the canister. The release of radionuclides from the glass with water or steam present is generally considered to occur through dissolution and leaching. The radionuclides can be released as colloids that are controlled by thermal, pH, and radiolysis conditions. The concept of radionuclides transported as precipitates suspended in water/steam is shown as an undeveloped event, but this too is controlled by temperature, pH, and radiolysis, because it is solubility-controlled for the most part. Radionuclides could conceivably be released to water by any of several catastrophic events, including earthquakes, volcanos, meteorite impacts. Figure A-5 addresses the concept of nonaqueous methods of mobilizing the radionuclides from the glass to the canister. For this figure, it is assumed that gaseous radionuclides will flow through appropriate breaches, whereas liquid and solid radionuclides will require gravity to allow them to fall or trickle through breaches.

In reference to Figures A-4 and A-5, the information on the events contributing to dissolution and leaching, and hence the failure of the glass to

completely contain the radionuclides, was provided by Oak Ridge National Laboratory (Claiborne et al., 1984) and Battelle Columbus Laboratory (Stahl and Miller, 1983). The influence of pH has been shown to affect dissolution and leaching, as have temperature and radiation. This is illustrated by the INHIBIT gate.

For dissolution and leaching of the glass matrix, the groundwater must be in contact with the waste form, and the physical and chemical conditions necessary for removal must be present. The radionuclides will either be soluble in water, form colloids, or be released as solids (particles or granules that will be spalled from the glass matrix). The required physical and chemical conditions are not presented in the diagrams.

The characteristics of glass also influence its performance as a barrier to radionuclide release. Increases in the surface-area-to-volume ratio result in higher dissolution and leach rates of the radionuclides or other constituents of the glass until the solvent becomes saturated. Changes in the chemical composition of the glass, as the chemical and physical environment changes, may also contribute to dissolution and leaching. Devitrification, hydration, and radiation-induced microfracturing have been identified as processes that contribute to increased surface area. Of these, devitrification is considered the most significant (Claiborne et al., 1984). Devitrification is primarily temperature-dependent with recrystallization limited to temperatures below 500°C (Claiborne et al., 1984). The amount and identity of the crystals also depend on the original composition of the glass (Claiborne et al., 1984). When the volume fraction of crystals formed by devitrification "... approaches approximately 10 percent, additional cracking of the monolithic waste form may occur" (Stahl and Miller, 1983). The formation of crystals will also provide grain boundaries to act as additional surfaces for dissolution and leaching.

As shown in Figure A-5, the radionuclides can be released when the glass devitrifies or cracks by mechanical means. When the glass devitrifies, radionuclides may be released in the gaseous, liquid, or solid states.

## 2. Spent Fuel Waste Form

Historically in waste repository studies, spent fuel has not been credited as a barrier against radionuclide release. However, there is reason to believe that, at least to some degree, the Zircaloy cladding and perhaps the fuel matrix itself will prevent or retard release. The fault tree addresses the degradation of the Zircaloy cladding and  $UO_2$  pellets under wet and dry conditions. Figures B-3 and B-6 present radionuclide transport from the spent fuel to the overpack in water/steam (aqueous) and dry (nonaqueous) atmospheres, respectively. Figures B-4 and B-5 support Figures B-3 and B-6.

Breach of the cladding could occur either prior to emplacement (from reactor operation or from handling) or through a degradation process after emplacement. As shown in the fault tree, pre-emplacment clad defects might be discovered by inspection. This could be important if the assumption of few or no defects is essential to the credit claimed for the cladding as a barrier. In recent years, the failure rate of fuel rods has been quite low. One study performed for the basalt repository effort (Claiborne et al., 1984) cited failure rates in recent years as less than 0.01 percent. Earlier rods failed at higher rates. The possibility of failure of the cladding by mechanical means, such as might result from loads exceeding the design loads, has also been incorporated in the tree.

Cladding degradation after emplacement in the repository has also been examined (Claiborne et al., 1984). As shown in Figure B-3, two degradation mechanisms that occur under wet conditions are hydrogen embrittlement and stress corrosion cracking. Hydrogen embrittlement can occur as a hydride phase forms following to saturation with hydrogen at high temperatures. Stress corrosion cracking of the cladding can occur if chloride solutions are present and the free corrosion potential is exceeded.

Figure B-3 also indicates the possibility that the  $UO_2$  fuel pellets could go critical. This criticality issue has been addressed several times, with the latest assessment (Weren et al., 1983) from Westinghouse Electric Corporation

for the Lawrence Livermore National Laboratory concluding that a canister fully loaded with fuel rods enriched to 4.5 weight percent  $^{235}\text{U}$  could go critical, but it is not likely that fresh fuel rods would be stored in a repository. No spent fuel configuration presented with  $^{235}\text{U}$  enrichment less than 1.6 weight percent had a  $K_{\text{eff}}$  greater than 0.95. (At  $K_{\text{eff}}=1$ , the mass goes critical. Using  $K_{\text{eff}} = 0.95$  as an upper bound provides a margin of safety). In any case, the cladding around the fuel pellets would have to breach, the fuel pellets would have to disintegrate to powder, and the fissionable materials would have to concentrate to a critical mass. Typically, new fuel pellets have an equivalent  $^{235}\text{U}$  enrichment of 3 weight percent for pressurized water reactors and boiling water reactors in the United States. Only the Westinghouse pressurized water reactor uses the 4.5 weight percent fuel in the United States. Criticality remains a possible failure mode.

As shown in Figure B-4, if the fuel has reached a temperature in the reactor greater than approximately  $1000^{\circ}\text{C}$ , fission products can migrate to the gap between the fuel pellets and the cladding. If the cladding is breached in such fuel rods by either wet or dry means, radionuclides could be directly released. There are, however, ways of identifying such fuel, either by the recorded operating history or by testing. If detected, the fuel could be treated as a special case and, therefore, would not appear in the tree. This high-temperature release phenomenon is discussed by Woodley (1983), who concludes is that the majority of fuel rods will not have been operated at this high temperature.

There is the possibility that the matrix could be disrupted, perhaps over time, by either extensive oxidation or dissolution of the matrix (leaching). These items are discussed by Woodley (1983) and Claiborne et al. (1984). Information indicates that, at least in principle, the applicant for a repository license may be able to justify the fuel matrix as either a partial barrier or a delayed release mechanism. On the other hand, work such as the Canadian leaching study cited in Claiborne et al. (1984) indicates that under certain conditions, leaching of some radionuclides may be relatively rapid (e.g., 4 percent of the cesium was known to leach in a few days).

Within Figure B-3, there are two events that would be strongly affected by certain thermal, pH, and radiolysis conditions: releases of radionuclides as solids and as colloids. INHIBIT gates and CONDITIONING events represent the increase or decrease in the probability of failure as the conditions change. Figure B-5 incorporates the thermal, pH, and radiolysis conditions as well as a condition for an increased cracking rate of the pellets.

### 3. Canister

The canister is the barrier that contacts and encloses the glass waste form and, in turn, is enclosed within the overpack in the CHLW package. As described by Westinghouse (1982), the canister currently is Type 304L stainless steel. The canister serves as a barrier to prevent groundwater and other chemicals from reaching the glass waste form and to prevent transport of radionuclides to the overpack. The canister also reduces the radiation intensity to the overpack and packing used in the CHLW package. Canisters are used only with the CHLW package, not with the SF package.

Two important events must occur before radionuclides flow through the canister wall: (1) a breach must exist in the canister wall and (2) the radionuclides must be in a position and state to flow through the breach as seen in subtrees B1000 and B2000, Figures A-6 and A-11, respectively. The various mechanisms by which the canister can be sufficiently breached such that radionuclides flow through the canister wall are shown. These include a path for breaching by (1) crushing the canister with the overpack; (2) degradation of the canister with water/steam or without water; or (3) a catastrophic event (volcano, earthquake, intrusion, etc.), such as discussed for the overpack. As indicated in both figures, thermal conditions can enhance the radionuclide transport from the canister to the overpack.

Failure of the canister can occur in the presence of water/steam that has entered the overpack and consequently has contacted the canister as shown in Figure A-6, or the canister can deteriorate when water/steam is not present as indicated in Figures A-6 and A-11. When a breach occurs in the canister, the

concern focuses on whether water is present or not. Aqueous transport of the radionuclides (Figure A-6) is believed to be the most probable means of radionuclide transport from inside the canister to inside the overpack in the CHLW case. Nonaqueous transport of radionuclides (Figure A-11) is the other mode of radionuclide movement from the interior of the canister to the interior of the CHLW overpack (i.e., transport of radionuclides without the presence of water, as sand trickles through an hourglass).

Many of the branches of the fault tree for the canister were developed based on the failure mechanisms cited in Westinghouse (1982), Brookhaven National Laboratory, BNL (1983b), Stahl and Miller (1983), Ahn and Soo (1982), Claiborne et al. (1984), and Siskind et al. (1983).

In both the aqueous and nonaqueous transport cases, the canister breach mechanism by mechanical, chemical, and other modes was investigated. The mechanisms for degradation and breach cited in the ORNL and BNL references are shown as bottom events in Figures A-7 through A-13. These events may be developed further to show detailed interactions.

It was postulated that the radionuclides could be in a gaseous, liquid, or solid state and available to flow through a breach. If gaseous radionuclides are available, it is assumed that they can flow through any adequate breach to which they can gain access. Because of the limitation created by gravity, liquefied, colloidal, or solid/granular radionuclides would require the breach to occur at a canister level below the upper surface of the radionuclides in order for radionuclides to fall or trickle through a breach in a nonaqueous situation (Figure A-11). In a situation in which water/steam floods (aqueous situation) the canister to the breach level, there are many additional mechanisms for transporting the radionuclides through the breach (Figure A-6).

In situations where water is able to transport radionuclides, it is suggested that the radionuclides could be freed from the glass matrix in a form that would allow their transport either (1) prior to a canister breach (and then further mobilized by water/steam after a canister breach) or (2) after a canister breach

(through the action of water/steam releasing the radionuclides from the glass matrix). Once radionuclides are transported through the canister, the problem is considered as one relating to the overpack, whether or not the overpack was previously breached.

#### 4. Overpack

The overpack is a steel barrier used for encapsulating either (1) a canister with its glass matrix waste form CHLW or (2) a packet of spent fuel rods. Consideration was given only to the reference waste package design for the CHLW and SF overpacks and not to other design alternatives. The overpack forms a barrier that should prevent penetration of groundwater and other chemicals to the canister zone in the CHLW overpack, as illustrated in Figures A-14 through A-21, or to the spent fuel (Zircaloy cladding and fuel pellets) in the SF overpack, as shown in Figures B-7, B-8, A-15 through A-18, A-20, and A-21. The overpack should also prevent the transport of radionuclides to the packing. The overpack must resist being breached by corrosion, mechanical mechanisms, and radiation.

Failure of the overpack can occur in either wet (aqueous) or dry (nonaqueous) packing conditions. These situations are represented in Figure A-2 for the CHLW package and in Figure B-2 for the SF package. It is recognized that the packing (bentonite and basalt) around the overpack may never be completely dry, so some moisture, whether in the liquid or gaseous (steam) state, would be expected to surround the outer surface of the overpack.

The wet condition of the packing also affects the mode of transport of radionuclides through an overpack breach to the packing. If a CHLW overpack is in a wet packing situation, water/steam would enter the breached CHLW overpack and assist available radionuclides (those that had escaped the canister) inside the overpack to migrate or diffuse through the breach. The water/steam also could corrode and eventually breach the canister and reach radionuclides. In the dry packing situation, water/steam is less likely to flow into a breached overpack, so the flow of radionuclides out of the overpack and corrosion of the canister are considered to be less probable than for the wet situation.

For an SF overpack in the wet packing situation, water/steam would enter the SF overpack and attack the Zircaloy-clad spent fuel, eventually allowing radionuclides to flow out of the overpack. In the dry packing situation, water is less likely to enter a breached overpack; consequently, the flow of radionuclides to the packing is less probable than in the wet situation.

Before radionuclides can flow through the overpack wall, two important events must occur: (1) a breach must exist in the overpack wall and (2) radionuclides must be in a position to flow through the wall as indicated in Figures A-14 and A-19 for CHLW and Figures B-7 and B-12 for spent fuel. These figures note mechanisms by which the overpack can be sufficiently breached in order to allow radionuclides to flow through the overpack wall. The rate of radionuclide transport can be thermally enhanced as indicated on these figures. Mechanisms for breaching the overpack include (1) placing hydrostatic or lithostatic forces on the overpack, (2) degrading the overpack in either a wet or dry packing situation, or (3) subjecting the overpack to a catastrophic event such as a volcanic eruption or a meteorite penetrating the package. An earthquake scenario has also been included as a mechanism for loading and failing the overpack. Catastrophic mechanisms will be expanded in future analyses only to the degree warranted relative to other fault event probabilities.

Both the C1000 (Figure A-14) and C2000 (Figure A-19) fault tree branches of the CHLW fault tree and the C3000 (Figure B-7) and C4000 (Figure B-12) branches of the SF fault tree, covering aqueous and nonaqueous conditions, include overpack breach mechanisms by mechanical, chemical, and other means. The degradation and breach mechanisms cited in the BNL and ORNL references (BNL, 1983b; Ahn and Soo, 1982; Siskind et al., 1983; Claiborne et al., 1984) are among the lower events shown in Figures A-15 through A-21 (except A-19) for CHLW and Figures B-8 through B-14 (except B-12) for spent fuel. The interaction of degradation mechanisms, such as pitting corrosion, ductile rupture, and thermal enhancement, could be developed further, if necessary, in future iterations of the fault tree. Thermal interactions with corrosion have been incorporated into the tree.

After repository closure, the overpack can also be breached due to undetected fabrication deficiencies or handling abuses. These mechanisms could be further developed, if desired. Underground explosions, oil and water drilling, tunneling, and other human activities can damage packages in the repository after closure. All these events are considered to be part of the event categorized as "Human Intrusion after Closure."

Another branch in CHLW subtree C1000 (Figure A-14) considers how the radionuclides would be available to flow through a breach. For CHLW subtree C2000 (Figure A-19), there are likewise corresponding breach and radionuclide flow branches. Subtrees C3000 (Figure B-7) and C4000 (Figure B-12) of the SF are similar to C1000 and C2000, respectively. It was postulated that the radionuclides could be in gaseous, liquid, or solid states and could also be available to flow through a breach. It is assumed that if gaseous radionuclides are available, they can flow through any adequate breach to which they gain access. Radionuclides in the liquid or solid/granular state in a nonaqueous situation could flow through a breach only in certain geometric configurations, as presented in Figures A-19 and B-12. If water intrudes to the interior of the overpack, then radionuclides possibly can be released by several mechanisms, including transport of radionuclides already released from the canister or breaching of the canister (or Zircaloy cladding) followed by release of radionuclides.

When radionuclides are in a solid or liquid state, water can either suspend the radionuclides in a mixture and transport the radionuclides through convection of the water and thermal gradients, or the radionuclides could be dissolved by the water and the ions then transported through the overpack breach.

## 5. Packing

After radionuclides are transported through the overpack, the packing acts as the final barrier to radionuclide transport to the basalt. The conceptual design for the waste packages uses a 25 percent bentonite/75 percent crushed basalt (by weight) packing mixture to provide an additional barrier between the

waste form and basalt host rock. The packing primarily serves to (1) control the groundwater flow both to and from the waste form and (2) retard the migration of radionuclides (BNL, 1983b). The packing is also designed to chemically modify or buffer the groundwater and provide a mechanical stress barrier between the overpack and the host rock. Failure of the packing to provide these functions may result from the alteration of the physical, chemical, and mechanical properties of the packing and therefore can affect its ability to control groundwater flow and radionuclide release.

Figures A-22 through A-25, as well as A-2 and B-2, consider radionuclide transport through the packing for both CHLW and SF package configurations. Information on the mechanisms contributing to the failure of the packing to meet its major objectives was provided by ORNL (Claiborne et al., 1984) and supplemented by the work of BNL (BNL, 1983a, 1983b, 1983c; Davis and Schweitzer, 1982; Bida and Eastwood, 1983). The portion of the fault tree that depicts the aqueous transport of radionuclides through the packing is given in Figures A-22 through A-24. The diamond "Rupture [of packing] by Catastrophic Events" incorporates meteorite impact, volcanic eruption, tunnel collapse, and tectonic activity as shown in Figure A-23. The concept of catastrophic events could also be incorporated in the undeveloped events (diamonds) nonaqueous transport tree for packing (Figure A-25).

The cited references focused on the movement of dissolved radionuclides in the groundwater. Therefore, processes that fail to control this method of transport provide the primary structure for the packing portion of the tree. The possible transport of radionuclides as insoluble, fine particulates and as gases was also identified.

For groundwater transport of radionuclides to occur, it was assumed that the packing is wet and the radionuclides are dissolved in the water or are in colloidal form. Failure of the packing to retain the radionuclides by sorption contributes to their presence in the groundwater away from the waste package. The events or processes resulting in reduced sorption capabilities by chemical poisoning, mineral alteration, and selective dissolution and leaching have been

diagramed (Figure A-22). These events are a function of the chemical and physical conditions present in the repository (i.e., temperature, water chemistry, pressure, and radiation). The relationships between the conditions and effects are not well understood. The fault trees were not further developed for these conditions, except to incorporate the thermal condition as an INHIBIT gate for each type of event. Research efforts are under way, and additional work is needed to define the sorptive properties of the basalt and bentonite to identify the interrelationships among the environmental conditions (BNL, 1983b).

The packing is designed to act as a water controlling barrier that limits movement to diffusion of the dissolved species (Westinghouse, 1982). Darcy's law for one-dimensional flow in a homogeneous, isotropic medium has been used as a basis for identifying the factors to be considered (BNL, 1983c):

$$Q = -K A (dh/dl)$$

where    Q       = flow rate, m<sup>3</sup>/s;  
           K       = hydraulic conductivity, m/s;  
           dh/dl = hydraulic gradient, dimensionless; and  
           A       = cross-sectional area, m<sup>2</sup>.

For diffusion to be the principal mechanism of transport through the clay mixture, the water movement must be controlled by the hydraulic conductivity of the packing and the hydraulic gradient. A hydraulic conductivity of 10<sup>-7</sup> m/s and regional hydraulic gradient of 10<sup>-3</sup> have been used together as the basis for the reference waste design (Westinghouse, 1982). Events resulting in changes to the hydraulic gradient and conductivity were considered when the failure of the packing to act as a barrier was described (Figures A-23 and A-24).

Alteration of the packing can influence its ability to act as a filtering medium and barrier to water movement. Because porosity is affected by the degree of cementation and compaction of the packing materials, and the presence of solution openings, joints, or fractures, these factors must also be considered. The fault tree includes such things as wet/dry cycling, hydrologic

erosion, leaching, dehydration, and mineral alteration on the characteristics of the packing. The physical and chemical conditions influencing the packing and fluid characteristics (i.e., pH, Eh, temperature) and interactions have not been detailed.

## V. EVENT TREES FOR BASALT WASTE PACKAGES

### A. APPROACH

Each event tree sequence presents a scenario of possible events that could lead to waste package breach and subsequent releases of radionuclides to the basalt host rock. Some trees show more than one event sequence that results in radionuclide release, but none of the trees show all possible sequences. It would be reasonable to take either a part or all of one sequence and combine it with another sequence and show multiple paths that lead to failure. The event tree sequences are intended to provide a qualitative representation of possible waste package failures, but are not intended to be used to provide quantitative values using conventional event tree computational techniques. These techniques cannot be applied properly to the waste packages, as explained in "Mathematical Considerations," Section VI.

One of the intents in presenting event trees was to provide the reviewers of the waste package designs with several plausible scenarios for waste package failure, but not all possible scenarios. Because event trees illustrate particular scenarios, there is almost no limit to the number of event trees that could be generated. Accordingly, the event trees included here are examples of scenarios that may be important to consider. Analysts will ultimately have to put together models that simulate waste package failure and transport of the radionuclides to the basalt, based on failure scenarios. Current computer codes attempt to predict time of failure of the waste package and subsequent radionuclide release rates and have incorporated models for several failure mechanisms.

### B. STRUCTURE OF EVENT TREES

The event trees were developed as follows. First, the events that could initiate a sequence of occurrences leading to radionuclide release were

considered. Corrosion mechanisms are generally believed to be the most likely causes of package failure, and presence of groundwater is the most probable initiator of corrosion. Thus, for the CHLW and SF waste package designs, a base case was established using presence of water and corrosion to breach the package, with waterborne radionuclide flow as a release mechanism. Because of design differences, separate base case event trees (presented in Figures C-1 and C-8) were developed for each package design.

To illustrate the effect of quality control on package reliability, scenarios were developed for each design to include this type of failure. For the CHLW package, a hole through the overpack was assumed to have occurred as a manufacturing defect (Figure C-2), and for the SF package, the Zircaloy cladding was assumed to have been breached in handling (Figure C-10). In each case, the presumption was that the defect was undetected.

In addition, scenarios were selected to represent combinations of events (e.g., loading from tunnel collapse in combination with corrosion). Also, some scenarios that may not be highly probable were included. These include human intrusion into the repository (drilling), corrosion from within the package without water being the main contributor, fuel mass reaching criticality ( $K_{eff} > 0.95$ ), and catastrophic events, such as an earthquake.

Not all the events are independent--many are interactive. A typical example of this occurs in the interaction between lithostatic loading and corrosion of the overpack. Corrosion could begin before loading occurs, but in time, the loading could increase (either steadily or due to an abrupt catastrophic occurrence), thus hastening the time and probability of failure. Alternatively, loading could occur first; then at a latter time, corrosion could begin as groundwater contacted the overpack.

These changes in sequences may provide significant differences in waste package times to failure.

## C. EVENT TREE DISCUSSIONS

Of the many event trees considered, 11 have been developed for this document to illustrate the scenarios. The following event trees are discussed, and the figures are in Appendix C.

### 1. CHLW Package Failure--Corrosion (Figure C-1)

Failure of a commercial high-level waste package due to the presence of water (or steam) and the related corrosion mechanisms is diagrammed as the base case in Figure C-1. Water/steam drives the mechanisms in the depicted scenario and therefore is used as the initiating event. This assumes that water/steam is available to the waste package as a result of resaturation of the repository after waste package emplacement. For radionuclide release to occur, four barriers (packing, overpack, canister, and glass waste form) must fail. The event tree shows the events required for water/steam to flow to the waste form and for the movement of radionuclides through the breached barriers to the basalt interface. A separate event is given for the penetration of each barrier. Additionally, the movement of water through each barrier is shown as a distinct event to account for any difference in the time the event occurs.

This event tree assumes that the waste package fails from the outside and that only corrosion processes cause the overpack and canister to fail. The result is a cascading tree in which the upper branches represent the package success in retaining radionuclides; the lowest branches represent package failure. For example, given that the corrosion case diagrammed requires aqueous conditions, if water does not penetrate the packing, there can be no water-related corrosion of the overpack. Consequently, no release of radionuclides can occur. Therefore, the failure of water to reach the overpack is considered a total success in this event tree. Similar logic permits the success branch of each succeeding pair of events to be considered a total success. If the engineered barriers are not breached, or if the water or radionuclides fail to flow through the breach, no additional failure scenarios are postulated. Therefore, no subevents are developed for the success branches.

To apply this sequence to a modeling effort to derive the probability of occurrence of radionuclide release to the basalt, a variety of input variables and their corresponding uncertainties would have to be determined. To determine the probability of water/steam contacting the packing and reaching the overpack or the probability of radionuclide migration through the packing to the basalt, the behavior of the packing has to be understood. Therefore, the packing characteristics and any events affecting the ability of the packing to control the flow of water and radionuclides should be incorporated in the calculation of probabilities. This would include events such as those causing the presence of cracks or channels, inadequate swelling, or inadequate sorption. Information necessary as input would include chemical and physical conditions such as temperature, pressure, water chemistry, and radiation. Similarly, with respect to breaching of the overpack and canister by corrosion, the different types of corrosion (e.g., general, pitting, and crevice corrosion) and the interactions between them must be evaluated. In addition, quantification of the radionuclide releases associated with the "failure" outcomes of the event trees would require a determination of items such as the dissolution and leach rate from the waste form and mass transport through the packing. These evaluations would use process models that are external to the event trees.

## 2. CHLW Package Failure--Hole in Overpack Weld and Corrosion (Figure C-2)

The scenario of failure depicted in Figure C-2 assumes that a quality control error has resulted in the emplacement of a waste package containing a hole in the overpack. Therefore, for radionuclide release to occur, only three barriers (packing, canister, and waste form) must fail. This case assumes that water/steam drives the failure mechanisms of these three barriers. As in Figure C-1, the event tree shows the events required for water/steam to reach the waste form and for radionuclide migration through the breached barriers to the basalt. However, because the overpack was breached prior to the intrusion of water/steam, no corrosion mechanisms are required for overpack failure. Consequently, the timing of water movement through the overpack breach to the canister as well as the time of occurrence of the subsequent events would differ from the scenario of Figure C-1.

The sequence of events diagramed in Figure C-2 assumes that the waste package fails primarily from the outside and that water/steam must reach the waste form in order to cause radionuclide release. Therefore, the upper branches of the event tree represent total success; the lower branches depict package failure. To determine the probability of water/steam penetrating the overpack, corrosion of the canister, radionuclide release from the waste form, or radionuclide migration through the packing, the subevents, controlling factors, and interdependence between mechanisms should be incorporated as discussed above. Also, the probability of the initiating event, a quality-control failure, would have to be evaluated.

### 3. CHLW Package Failure—Ceiling Collapse and Corrosion (Figure C-3)

Failure of a CHLW package due to a combination of loading and the presence of water/steam and the related corrosion mechanisms is diagramed in Figure C-3. For this scenario, the source of the loading was assumed to be provided by a collapse or settling of the repository ceiling. The event tree comprises two major branches. Both branches consist of a similar sequence of events resulting in either package success or failure. These major branches are derived from the effect of the collapse of the repository ceiling onto the packing. If the packing is degraded (e.g., a direct pathway, such as a fissure, from the basalt to the overpack is provided), the timing and rate of water reaching the overpack would differ from a situation in which the packing was not disturbed. Consequently, although the subsequent events in each branch are the same, the rates and, hence, the probabilities of occurrence would be different.

For radionuclide release to occur, four barriers (packing, overpack, canister, and waste form) must fail. The event tree depicts the sequential failure of these barriers due to a combination of the effects of loading and corrosion. Because of the pressure being exerted on the waste package, it is anticipated that the failure rates would be enhanced (as compared with the corrosion case described in Figure C-1). It is also expected that some mechanisms, such as stress corrosion cracking, would play a greater role than in Figure C-1. As discussed above, to determine the probability of occurrence of the events presented, the subevents, controlling factors, and interdependence between mechanisms must be incorporated.

#### 4. CHLW Package Failure--Corrosion Followed by Loading from Ceiling Collapse (Figures C-4a and C-4b)

The scenario presented in Figures C-4a and C-4b concentrates on corrosion of the overpack to some degree of degradation followed by the tunnel ceiling collapse onto the overpack. As in the scenario depicted in Figure C-1, the contact of water/steam with the packing is the initiating event. For the remainder of the scenario to occur, it was also assumed that the water/steam penetrates the packing and corrodes the overpack, thus reducing the mechanical strength of the overpack. Subsequent loading on the overpack from the tunnel collapse may or may not immediately breach the overpack. Two subscenarios have been given consideration: (1) the corroded overpack is loaded with rock from a tunnel collapse without immediate breach of the overpack (additional corrosion under loaded conditions may weaken the overpack sufficiently to cause breaching) and (2) the corroded overpack is breached immediately upon collapse of the tunnel. These two scenarios are discussed below as lower and upper branches for the breached and nonbreached cases, respectively. It should be noted that the logic structure of four subbranches on Figure C-4a is the same, so these four are depicted by the logic structure on Figure C-4b. Even though the logic of the branches is the same, the probabilities assigned to events of Figure C-4b are not necessarily the same when attached to each branch of Figure C-4a.

After the tunnel collapse and the resulting breach of the overpack, the lower branch shows that water/steam flows into the overpack to the canister. If the canister is also breached, water/steam may flow to the waste form. The waste form may fracture or remain intact. For both of these options, the water leaches the radionuclides, as presented in Figure C-4b. The dissolution and leach rates would be greater for the fractured glass versus the nonfractured glass if the fluid is not in a saturated state, and correspondingly, the probabilities and rates of radionuclide release would be affected. Figure C-4b considers the flow of radionuclides through the barriers and through the disturbed packing as well as the nonrelease of radionuclides.

In the branch in which the canister is not immediately breached by the force of the tunnel collapse when the overpack is breached, the canister might continue to corrode under load (especially by stress corrosion and crevice corrosion) until breaching occurs. Water might then flow through the breach to the waste form. The waste form might also be treated by the same scenario as given in Figure C-4b.

The upper branch represents the sequence of events in which the overpack does not breach immediately upon tunnel collapse. The overpack might continue to corrode (especially by stress corrosion and crevice corrosion) and eventually breach. This would allow water/steam to flow to the canister. The canister might then be breached by a combination of loading and corrosion. The scenario continues with water/steam reaching the waste form and so on as given in Figure C-4b.

Additional scenarios could have been added to this event tree, but these subscenarios are either addressed in other figures or could be added later, if deemed appropriate.

#### 5. CHLW Package Failure--Drilling into Repository Area (Figure C-5)

If drilling into the repository area occurs in the future, the rate of water intrusion into the repository area is likely to be accelerated. The drilling might pass through the package level and continue to lower depths, but the drilling process would still inject drilling fluids (water, oil, polymers, etc.) into the repository area and allow groundwater (fresh or saline) to flow down along the outside of the well casing, if casing is used, or allow groundwater flow through the drill hole if no casing is used. In any event, the casing could eventually fail and allow groundwater an unobstructed path to the repository area.

Figure C-5 presents an event tree initiated by the event "drilling into repository area" and continued by the same sequence of events presented in Figure C-1. The scenario continues with the probability that water reaches the packing, overpack, canister, and waste form, respectively. Radionuclides would

have some probability of flowing through the breaches to the basalt. Note, however, that the Figure C-5 probabilities will not necessarily be equal to the probabilities that will be assigned to events in Figure C-1. For example, the probability of water reaching the packing will most likely be greater in the Figure C-5 scenario than in the Figure C-1 scenario.

The probability of radionuclide release to the basalt in the scenario in which drilling into the repository area (Figure C-5) occurs may be less than the probability of a radionuclide release to the basalt in the scenario in which water merely wets the packing from water flow through the basalt (Figure C-1). This is because the drilling scenario is a more restrictive case than the base case of Figure C-1. In the former case (Figure C-5), the differences in probabilities of radionuclide release will depend on the probability of drilling into the repository area and on the greater probability of water intrusion, breaching by corrosion, and radionuclide flow. Further investigation will determine the probabilities to be used in the calculations.

At present, it is not foreseen that there would be any drilling for oil or gas recovery, but centuries after repository closure, the surface markers may be obscured or new objectives may prompt drilling on this site. Drilling possibilities are discussed in detail by Hunter (1983).

#### 6. CHLW Package Failure—Drilling Into Waste Package (Figure C-6)

The event tree initiated by the event of drilling into a waste package is presented in Figure C-6. The scenario considers events in which the packing, overpack, canister, and waste form are penetrated in the drilling process. The scenario also considers events in which only some of the waste package barriers are penetrated. If a barrier is not breached by drilling, it was assumed that it could be breached later by the corrosion processes.

The initiating event assumes the packing has been penetrated by drilling and the drilling process has resulted in the removal of packing materials. Additionally, the process is assumed to introduce drilling fluids and water to the overpack. The overpack might also be penetrated by the drilling process, and drilling fluids (water, oil, or polymers) might be introduced to the canister. This event is represented in the event tree by the lower branch. The upper branch considers that the overpack was not penetrated by the drilling process, but that drilling fluids or water have penetrated the packing and are in contact with the overpack.

The lower branch, which begins with the overpack being breached by the drilling process and the intrusion of fluids, contains two subscenarios: (1) the canister is breached along with the overpack by the drilling process and fluids might contact the waste form and (2) the canister is not breached by the drilling process, but fluids are in contact with the canister. In the first case, when the canister is breached by drilling, the fluids might leach the waste form and the radionuclides might flow through the drill hole to the basalt. The next possible step could be that the radionuclides go to the surface (biosphere), but this event tree analysis stops at the basalt/package boundary.

If the canister is not breached by the drilling process (the second case), it is assumed that corrosion could breach the canister. If it does, the drilling fluids could flow through the breach and then begin to leach radionuclides. Once the radionuclides flow through the canister breach, they could flow toward the basalt through the drill hole.

The upper branch is similar to the scenario given for the corrosion case shown in Figure C-1, but there are some major differences. In Figure C-6, it was assumed that the packing was penetrated by the drilling process; therefore, a free exchange of drilling fluids with the overpack surface would be possible. Overpack corrosion might result in a breach, and drilling fluids might flow through the breach to the canister. The scenario continues with corrosion and breaching of the canister, followed by flow of drilling fluids through the breach to the waste form. Radionuclides then might be leached from the waste form

and begin to flow through the breaches. Once the radionuclides have cleared the canister, they are considered to be in contact with the basalt because the drill hole and lack of packing offer no barrier to radionuclide flow to the basalt.

7. CHLW Package Failure—Mechanical Failure of Waste Form and Internal Corrosion (Figure C-7)

As discussed earlier, internal corrosion modes have been postulated. In all likelihood, the possibility of significant damage to the canister by internal corrosion is remote. Nevertheless, this scenario has been included for completeness. The event tree presented in Figure C-7 represents a scenario for the release of radionuclides from a CHLW package in which the failure begins at the glass waste form and proceeds through successive barriers until it reaches the basalt without the assistance of an aqueous (water/steam) medium. The scenario assumes that the glass waste form granulates and in turn accelerates canister corrosion relative to corrosion of the canister in contact with nongranulated glass or devitrified glass. Once the canister is breached and sufficient opening exists in the breach or breaches, the granulated waste form can trickle through to the inside surface of the overpack. The combination of canister corrosion products (materials) and the waste form is then postulated to corrode and ultimately breach the overpack. After overpack corrosion products spall away from the overpack and form a sufficiently large separation in the overpack, the radionuclides will trickle through the breach to the packing as sand would trickle through an hourglass. It is postulated that by then the packing will have developed channels and fissures at suitable locations so that the radionuclides would eventually trickle through the packing and contact the basalt formation.

Because radionuclide release to the basalt occurs without water or steam present, the corrosion rate of the canister is controlled by the chemicals in the waste form. Corrosion proceeds from the inside of the canister to the outside, and the corrosion rate of the overpack is controlled by the chemicals from the waste form and the canister corrosion. Because there is no water or steam, the radionuclides are transported through the breaches of the canister, overpack, and packing to the basalt by gravity.

The glass waste form can crack as a result of mechanical stresses and thermal variations, as well as glass devitrification. These mechanisms can yield waste form granules that spall from the main waste form mass and are small enough to flow down through a breach.

The corrosion mechanisms operating on the canister and overpack are affected by the mechanical stresses and defects present in each barrier, as well as by the thermal and radiation influences. The corrosion mechanisms considered are pitting, crevice and general corrosion, and stress corrosion cracking. The composite effect of these mechanisms will be determined in a probabilistic manner to yield a time of breach and the possible consequent rate of flow of radionuclides through the breach.

Branches in this event tree sequence that cite no corrosion of the canister or overpack or that cite nonflow of radionuclides through breaches are assumed to indicate permanent stoppage of radionuclide attempts to reach the basalt host rock.

#### 8. SF Waste Package Failure—Corrosion (Figure C-8)

Failure of a spent fuel waste package due to the presence of water/steam and the related corrosion mechanisms is diagrammed as a base case in Figure C-8. Water/steam drives the mechanisms given in the scenario, and its contact with the packing is used as the initiating event. Historically in waste repository studies, the spent fuel cladding has not been credited as a barrier against radionuclide release. However, there is reason to believe that, at least to some degree, the Zircaloy cladding and the fuel matrix would prevent or retard release. Therefore, for radionuclide release to occur, it was assumed that four barriers (packing, overpack, Zircaloy cladding, and spent fuel waste form) must fail. Because this tree begins with the packing and proceeds to the waste form and back to the packing and because the presence of water is necessary for failure, the success of a barrier to control the flow of water or to completely retain the radionuclides is considered a total success. Therefore, although different barriers are used and different input variables are required, the events

presented in this tree are essentially the same as those for the failure of the CHLW package by corrosion (Figure C-1). The probabilities and times to failure would probably be different. Also, information similar to that needed for the CHLW case would have to be incorporated for this scenario.

#### 9. SF Waste Package Failure--Corrosion Followed by Criticality (Figure C-9)

The event tree presented in Figure C-9 considers a series of events that start with the presence of water/steam at the waste package, leading to corrosion of the overpack and Zircaloy (as as SF base case in Figure C-8), and eventually concludes with a radionuclide release to the basalt rock through the SF mass attaining criticality. The fuel pellets slowly disintegrate (and may undergo some oxidation) and concentrate as a fuel powder. Given the right equivalent enrichment of  $^{235}\text{U}$  fuel, criticality of the mass can occur (Weren et al., 1983). Criticality is assumed to occur when the effective neutron multiplication factor ( $K_{eff}$ ) is equal to or greater than 0.95. It is easier to reach  $K_{eff} \geq 0.95$ , when water moderates the neutrons than when the mass is dry and there is no moderator.

For the case in which the mass does not attain criticality, the upper branch indicates that the radionuclides would not reach the basalt host rock and the lower branch indicates that the radionuclides are dissolved or leached from the spent fuel mass that is assumed to be surrounded by water/steam. The dissolved, leached, and colloidal radionuclides would then be thwarted from reaching the basalt host rock or would successively pass through an overpack breach and through the packing to the basalt host rock.

In the failure branch, the radionuclides concentrate, go critical, and flow through the overpack, but could be prevented from reaching the basalt host rock. This final nonevent might exist, for example, if the mass that went critical were to produce a molten zone that could solidify the water recedes from the mass. That the radionuclides would not reach the basalt rock once criticality is achieved would be surprising--the high temperature of the critical mass would likely melt the overpack and damage the packing such that the

radionuclides would be transported by steam or diffusion to the basalt host rock. The most likely branch, therefore, is the lower one in which the radionuclides flow quickly to the basalt once the mass achieves criticality.

The probability of the spent fuel mass going critical in the repository is highly unlikely (Weren et al., 1983) has calculated that it is reasonable to believe that if the fuel is "burnt up" to an equivalent  $^{235}\text{U}$  of about 1.4 weight percent or less, the package would remain subcritical under any postulated condition. Spent fuel should have an equivalent  $^{235}\text{U}$  of much less than 1.4 weight percent. In order to determine whether spent fuel criticality is a significant event, the probability of occurrence should be ascertained.

#### 10. SF Waste Package Failure--Handling/Quality Control and Corrosion (Figure C-10)

The scenario presented in Figure C-10 assumes that a quality control error has resulted in the emplacement of an SF waste package in which the Zircaloy cladding has failed prior to closure of the repository. Therefore for radionuclide release to occur, only three barriers (packing, overpack, and the SF waste) must fail. This case assumes that water drives the failure of these barriers. The water must penetrate the packing for the overpack to be breached by corrosion. Due to the assumed breach in the Zircaloy cladding, the water might then flow directly through the overpack to the SF and leach the radionuclides. This case is similar to that presented for the SF in Figure C-8. However, because the Zircaloy is already breached, the information used to determine the probability of occurrence and time to failure would differ.

#### 11. SF Waste Package Failure--Earthquake and Corrosion (Figure C-11)

The event tree presented in Figure C-11 considers a series of events that includes an earthquake that affects the SF waste package. The scenario presents several effects of the earthquake on the waste package and shows some instances of radionuclide release to the basalt, as well as nonreleases to the basalt.

The event tree begins with water or steam contacting the packing and then reaching the overpack surface. Then an earthquake possibly occurs. At this point, two major branches are established: the upper branch (the overpack is not breached by the earthquake or no earthquake occurs) and the lower branch (the overpack is breached during the earthquake).

The lower branch continues with the event "water/steam flows through the overpack breach to the Zircaloy cladding." In this scenario, it is assumed that the cladding is not breached by the earthquake, so the next event considered is whether or not the Zircaloy cladding was breached by corrosion in conjunction with mechanical mechanisms initiated by loading from the overpack and other debris. Once the cladding is breached, the process of releasing radionuclides to the basalt is similar to that presented in the scenario of corrosion of SF waste package, Figure C-9. After the cladding is breached and radionuclides are leached from the SF, the radionuclides successively flow through the breach in the overpack and through the packing to the basalt. This is the end point of the lower branch.

The upper branch illustrates the case in which the overpack survives being breached by the earthquake. The overpack is assumed to be loaded with some of the debris of the earthquake and to corrode. The mechanical and corrosion mechanisms are considered to interact and possibly lead to a breach of the overpack. After breaching, the water/steam would be able to flow through the overpack breach and thus contact the Zircaloy. It is assumed, as part of the scenario, that some of the load on the overpack would load the Zircaloy cladding and contribute to the corrosive and mechanical mechanism that would likely cause a breach in the cladding. The remaining events are similar to those in the lower branch of Figure C-11, i.e., the events of leaching the radionuclides from the SF and the subsequent flow of the radionuclides to the basalt.

The event tree of Figure C-11 produces two basic source term flow rates, one from the upper branch and one from the lower branch. These source terms will be made up of the quantities of each radionuclide that can be released, as well as the period of release. Other source terms in this event tree are null, because they indicate no release.

## **VI. MATHEMATICAL CONSIDERATIONS**

**Fault tree and event tree methods are based on the same fundamental considerations. Although they are structurally distinct, they are subject to many of the same strengths and weaknesses. Applications in which one is useful generally are applications in which the other is useful and complimentary. In the discussions that follow, some of the limitations of these related methodologies as applied to quantification of the waste package are revealed. Some of the same basic difficulties occur in both methods but are manifested differently; hence, the methods are discussed separately. In general, both methods are based on simplifying assumptions that are too limiting for the complexities posed by the waste package leading one to investigate other methods that appear to be more appropriate for the problem at hand. This investigation is Task I of this project.**

**Complete numerical quantification of the fault trees and event trees has not been attempted because the results would not have been meaningful given the limitations of the methodologies discussed below. However, a numerical example is provided to illustrate the magnitude of the problem encountered in using the fault tree method for quantifying the waste package reliability.**

### **A. FAULT TREE ANALYSIS**

**Booleau logic is generally the mathematical technique used for combining event probabilities in fault trees. The application of fault trees and Boolean logic in quantitative assessments of the waste package has identified certain difficulties that can be described in four categories:**

- Nonindependence of primary events,**
- Representation of standby systems as parallel systems,**
- Representation of continuous processes by discrete events, and**

- Combined effects of internal and external degradation.

### 1. Nonindependence of Primary Events

Computation of event probabilities in a fault tree using standard computer codes usually is based on the assumption of independence of the primary events. (Primary events are the bottom events of the fault tree.) A standard procedure in fault tree codes is to transform the tree logic to a collection of cut sets. Each cut set is a selected group of primary events chosen so that if all the events in any one cut set occur, the system fails. If the primary events in a given cut set are independent, then the probability that they all occur is the multiplicative product of the individual probabilities for each event in that set. Thus, the portion of the system failure probability that is attributable to that particular cut set is computed as a simple multiplication. For any tree structure, there is a specific number of cut sets, each with a unique collection of primary events. Thus, the probability of the top event (system failure) can be computed by adding the contributions from each cut set. This is the key process used by most fault tree codes. However, if the primary events are not statistically independent, then the product rule for cut set probabilities does not hold, and gross errors in the computation of cut set probabilities will result. This leads to erroneous calculations for the probability of system failure.

Many of the primary events in the current fault tree representation of waste package failure involve crossing certain threshold values of environmental variables such as temperature, radiation intensity, water presence, and ion concentrations. Unfortunately, these variables are highly interrelated, even to the point of requiring sophisticated mathematical models to determine their values. Secondly, these variables can be influenced by the waste package degradation itself, creating a feedback relationship between the status of the waste package and the primary events representing the environmental variables. In addition, catastrophic events, such as earthquakes, earth movement, or human intrusion can affect several of the environmental variables at the same time simply by changing the underground hydrology. This type of situation can be called "common cause" dependence.

Because it is impossible to justify the assumption of statistical independence of primary events, computation of system failure requires more complex analysis than just the straightforward execution of fault tree codes—or of any method that relies on statistical independence of events.

In addition to the lack of independence in the primary events, another type of dependency is induced by the structure of the waste package itself. To the extent that the degradation of inner barriers is delayed because of protection from the outer barriers, there is a time lag between the barrier failures.

## 2. Representation of Standby Systems as Parallel Systems

The time-lag dependency is quite distinct from the primary event dependencies discussed above and is explored in this section. Consider a simplified four-barrier waste package scenario in which the dependence of primary events is not a problem, and assume further that the failure probability distributions for each of the barriers can be computed without difficulty. Because all four barriers must fail in order for the system to fail, it is natural when using the fault tree approach to connect the four barriers by an AND gate as has been done in Appendix A. The four barriers are represented by the top four events in Figure A-2. This logical representation is equivalent to a parallel system representation in signal-flow graph notation (Figure 5).

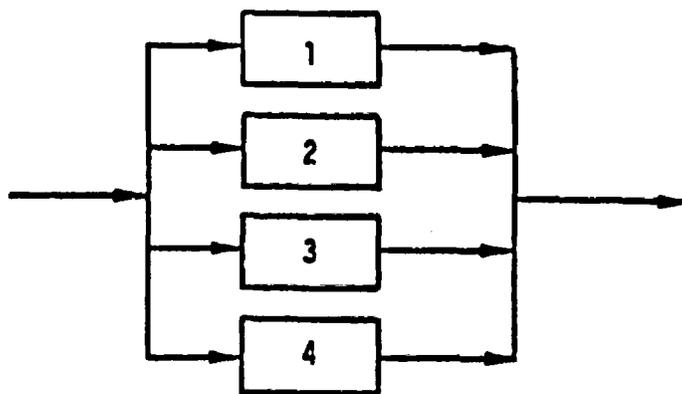


Figure 5. Signal-Flow Graph for a Parallel System

In this notation, the system has not failed as long as there is any path that will allow continuity of the signal flow from left to right. Thus, as long as any of the component barriers (1, 2, 3, or 4) is still intact, the signal can pass through, and the system has not failed. Only if all four components have failed will the system have failed.

The signal-flow graph notation is useful because it enhances the perception of the parallelism of the system and, more important, because it provides an easy representation of standby redundancy. Standby redundancy would be the appropriate representation of the waste package in a situation in which the failure of a second component is dominated by degradation processes that start only after the first component has failed. Corrosion of the canister initiated by water penetration through the overpack is an example. The concentric barriers of the waste package are best represented as a standby system.

Figure 6 is the signal flow representation of a four-component standby system. Component 1 represents the outermost barrier, the packing; Component 2 represents the overpack; Component 3 represents the canister; and Component 4 represents the waste form. The flow into the components is regulated by a switch that automatically moves to the next component when one component fails. Thus, only one component is used at any time, although all four are ultimately available. The new notation helps in visualizing the time sequence properties of a standby system. If failure of the first component occurs at time,  $t_1$ , then the degradation of the second component begins at that time also. This is equivalent to shifting the time axis  $t_1$  units in the probability density function for the second component as shown in Figure 7.

A shift in the time axis is an important consideration. This means that the probability of failure for any barrier depends not only on the current time but also on the time of failure of the prior barrier. This is in contrast to the parallel system in which all components have failure probabilities that depend only on time elapsed from initial system startup. Parallel systems would be used to describe four barriers that were buried separately and subject to corrosion degradation independently.

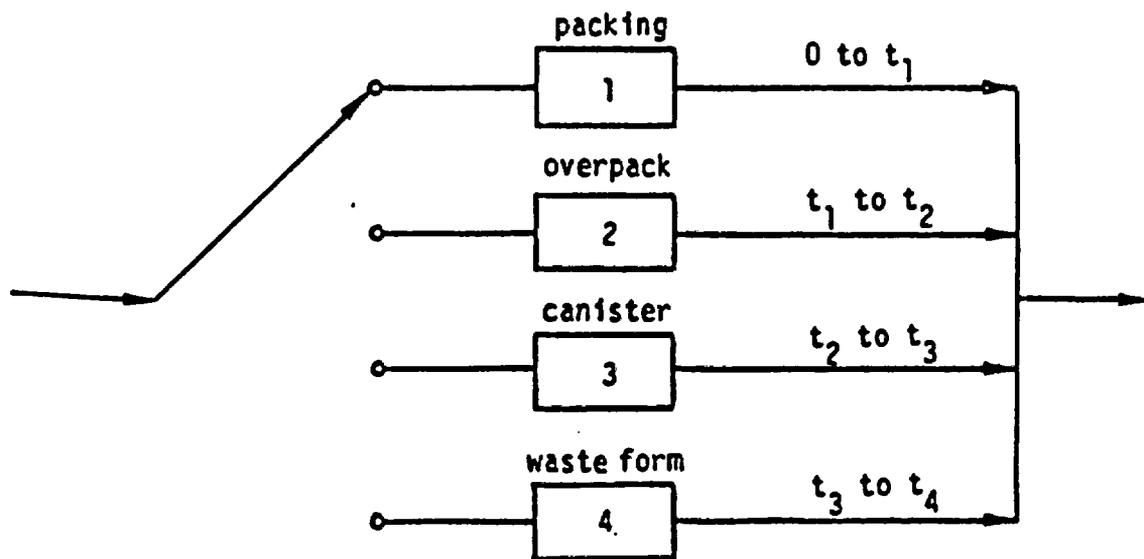
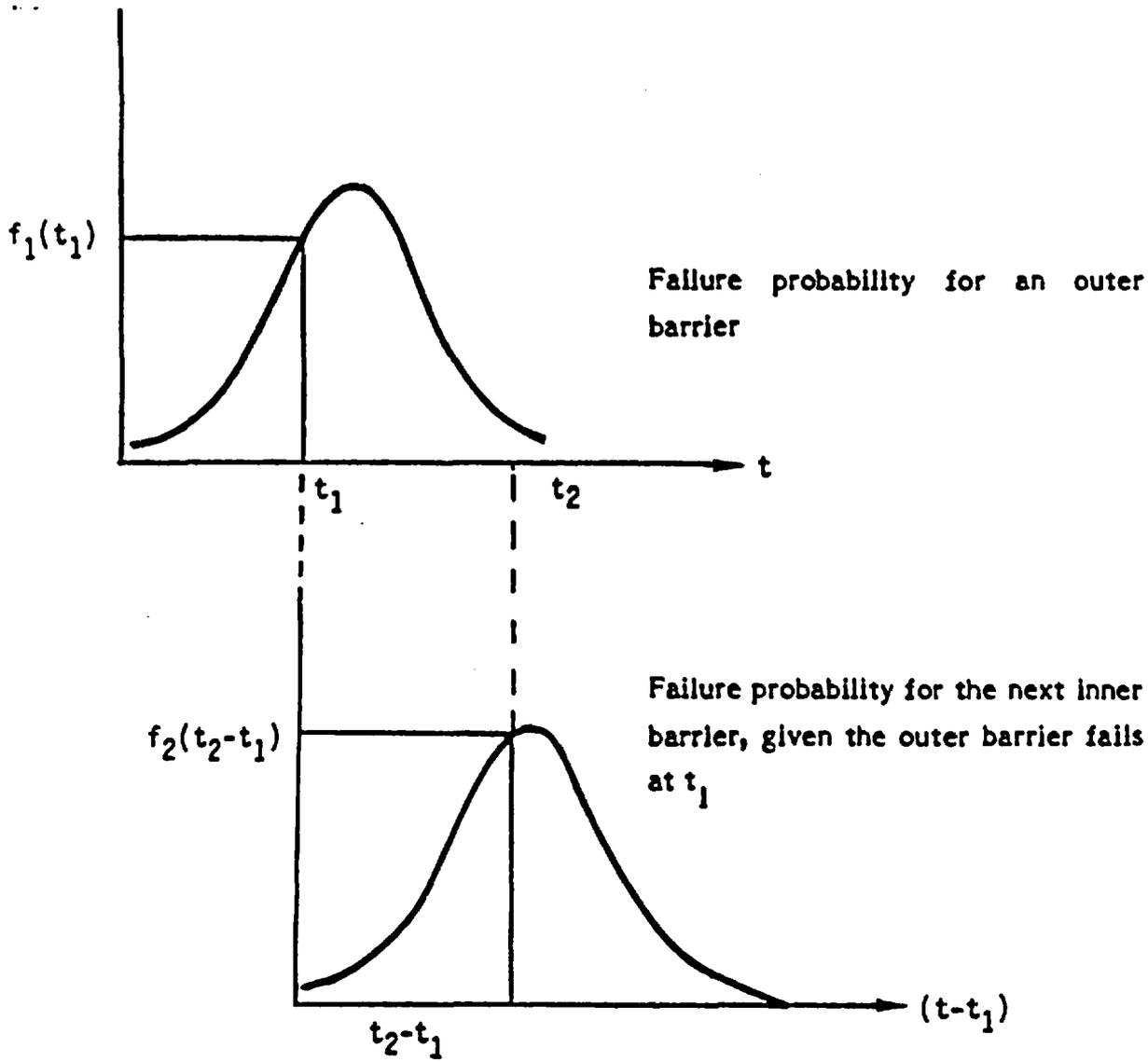


Figure 6. Signal Flow Graph for a Standby System



$t_1$  = random time of failure of first barrier.  
 $t_2$  = random time of failure of second barrier.

Figure 7. Time Shift in Component Failure Probability Density Functions

Although the parallel system is easy to represent in fault tree notation, the standby system is not. The signal flow switch is not easily represented by AND and OR gates, and the time-lag is not representable at all because there is no characterization of time in fault tree structures. The two systems are also quite different mathematically, as evidenced by expressions for the probability of system failure for both cases.

Let  $f_1(t)$ ,  $f_2(t)$ ,  $f_3(t)$ , and  $f_4(t)$  be the probability density functions for components 1, 2, 3, and 4. The probability that the  $i$ th component has failed by time,  $t$ , is as follows:

$$F_i(t) = \int_0^t f_i(t) dt$$

With the parallel system, and with assumed independence of component failure events, the probability that all four barriers have failed by time,  $t$ , would be calculated as the product of the individual probabilities:

$$P_1(t) = \int_0^t f_1(t) dt \int_0^t f_2(t) dt \int_0^t f_3(t) dt \int_0^t f_4(t) dt \quad (1)$$

and

$$P_1(t) = F_1(t) \cdot F_2(t) \cdot F_3(t) \cdot F_4(t) \quad (2)$$

where the  $F_i(t)$ 's are the cumulative probability functions.

The parallel system equations show that parallel systems depend on time in a simple manner. Independent component failure probabilities can be generated for any particular time,  $t$ , and system failure for that time can be computed by multiplying these probabilities just as is suggested by the AND gate notation in

the fault tree. Kinetic tree programs are available for this type of problem (Vesely, 1970).

The failure probability for standby systems can be described by

$$P_2(t) = \int_0^t \int_{t_1}^t \int_{t_2}^t \int_{t_3}^t f_1(t_1) f_2(t_2-t_1) f_3(t_3-t_2) f_4(t_4-t_3) dt_4 dt_3 dt_2 dt_1 \quad (3)$$

where  $t_1$ ,  $t_2$ ,  $t_3$ , and  $t_4$  are the failure times for components 1, 2, 3, and 4, respectively (Pritzker and Gassman, 1979).

The time shifts in the arguments of the density functions and the restricted lower limits of integration are needed to account for the time delays in initiation of the component degradation processes.

The failure probability for standby systems, using the convolution integral equation (3), is a special case of a more general relationship involving integration of the joint probability distribution function. Under the assumption that individual barrier probability distributions are independent except for the time factor, the joint probability distribution can be decomposed into the product form shown in equation (3).

Because typical fault tree computer codes can assess parallel systems similar to that in equation (1) but cannot assess standby systems similar to equation (3), it is important to see whether there is a significant numerical difference between the two. If the difference is substantial, the fault tree method that works for parallel but not standby systems should not be used to quantify waste package failures.

To produce numerical examples, equations (1) and (3) must be integrated using specific density functions. Equation (1) is easy to integrate for most

standard probability distributions. However, equation (3) is difficult to integrate analytically, and numerical integration using a computer would be required in most cases. A relatively simple closed form solution can be developed for equation (3) for the special case in which all components have an exponential probability density with the same mean time to failure. Therefore, to compare the two systems, both equations (1) and (3) were solved using the same assumptions of exponential failure probability densities with the same mean time to failure.

With these assumptions, the failure probability for four parallel components is as follows:

$$P_1(t) = [1 - \exp(-\lambda t)]^4 \quad (4)$$

where  $1/\lambda =$  mean time to failure.

The corresponding equation for the standby system is

$$P_2(t) = 1 - \sum_{i=1}^4 (\lambda t)^i \exp(-\lambda t) / i! \quad (5)$$

These two systems were compared for components with mean time to failure of 500 years, for time periods of 250, 500, 1000, and 2000 years (Table 3).

**Table 3. Failure Probabilities for Parallel and Standby Systems with Four Components\***

Parallel Time (years)	(P <sub>1</sub> ) (Fault Tree)	Standby (P <sub>2</sub> )
250	0.024	0.002
500	0.160	0.019
1000	0.559	0.143
2000	0.929	0.567

\*Each component has a mean time to failure of 500 years.

The standby system has smaller failure probabilities than the parallel system. This is to be expected from the protection offered by the outer barriers to the inner barriers.

For this case, an estimate was made of the comparative magnitude of the time-lag effect on the waste package system reliability. Calculations (Table 3) were made for the standard fault tree method (parallel system) and a method that accounts for the time-delayed degradation provided by the nested barriers. Results for the first 500 years, for example, show that the fault tree analytic method generated failure probabilities approximately an order-of-magnitude higher than predicted by the time-delayed degradation method. The latter method provides a more realistic representation of waste package physical degradation than does the parallel (fault tree) method.

The standby system, like the parallel system, is not by itself an adequate representation of the waste package. The standby system assumes no significant degradation of a barrier until all prior barriers have failed, but several mechanisms for early degradation have been identified in the qualitative fault tree analysis (Appendix A). Nevertheless, the waste package strongly resembles a standby system, because the failure rates of inner barriers are expected to increase dramatically when the protective barriers have failed. Thus, computations based on parallel systems (i.e., an AND gate connecting the four

barriers) cannot be trusted, because the probabilities for parallel systems have been shown to be substantially different from those of standby systems.

Having found the standby system to be a better representation of the waste package than the parallel system, there still is the problem of lack of independence of primary events discussed earlier. Equation (3) accounts for dependencies generated by the time-lag structure of standby systems, but it does not correct for the primary event dependencies. In addition, there are the difficulties associated with representation of continuous processes and with representation of combined effects of internal and external degradation.

### 3. Representation of Continuous Processes by Discrete Events

Describing continuously varying processes in terms of discrete branches of a fault tree (or event tree) is a difficult problem. For example, two events can occur together to cause a breach of the overpack: (1) a geological event creating pressure on the overpack and (2) the weakening of the overpack by corrosion. Both the geologic pressure and the remaining strength of the overpack are continuous variables. For any given level of overpack strength, there is a continuum of values of geologic pressure that could result in overpack breach. For each of these, there is a continuum of possible overpack strengths (after corrosion processes have been at work). It appears that a very large number of combinations of discrete branchings would be required for a quantitative fault tree description of such two-dimensional, continuous processes. Thus, while at first it may appear that multiple branchings might be useful, the approach now seems impractical because of the very large number of branching combinations that would be required. Two-dimensional, continuous variable problems such as this can be solved using the calculus of probabilities or by using simulation modeling. The difficulty comes from limiting oneself to the two-state algebraic manipulations provided by the fault tree approach.

### 4. Combined Effects of Internal and External Degradation

Several mechanisms for degradation of barriers from the inside to the outside are identified in Appendix A. These processes potentially lead to breach

of the canister or overpack. Similarly, external degradation processes that can lead to barrier breach from the outside to the inside were identified. These two possibilities are connected by an OR gate to produce the "overpack breach by degradation" event.

The same kind of logic is used to produce the canister failure event as well. Interior corrosion generally is believed to be much less significant than exterior corrosion. If degradation by interior processes can be shown to be insignificant, then the problem of combined effects might not be important. However, it is possible that even a very slow corrosion rate on the inside of the canister might result in significant damage by the time all the outer barriers have been breached by exterior processes. Obviously, if there are processes working outward from the interior and inward from the exterior, they will meet at one of the barriers. Quantification of the probability of failure from an outside process must take into consideration the degradation produced by the inside process for this barrier. Although these processes may act independently, they compete for the remaining undamaged barrier material.

Failure from combined effects can be expected to occur more quickly than failure from either process working alone, and time-dependent failure probabilities should be calculated with this in mind. Computations that properly account for all possible combinations of interior and exterior damage that could produce failure would be very awkward to arrange using Boolean algebra; it would require a new OR gate for each possibility. This is another instance where the calculus of probability distributions is needed because of the continuum of possibilities.

##### 5. Alternative Methods for Quantification of Failure and Risk

Limitations of the fault tree method do not imply that waste package failures are not quantifiable. Several analytical tools show promise and are now being investigated. Simulation modeling, as has been described in the interim methodology report (Aerospace, 1984), provides a mechanism for keeping track of accumulated damage to barriers and for assessing the interactions between

dependent variables. Such models can provide the most realistic description of the system including the quantification of release rates as well as failure probabilities. However, simulation can also lead to unwieldy computer programs. Considerable judgment would be required to capture the key relationships in the waste package system without being overwhelmed by details.

Another promising method is to establish a series of probability distributions using the same mathematical submodels that would go into a simulation program. Multiple sampling of these distributions in sequence could be conducted to provide a probability distribution for overall system reliability. The associated programming would be much simpler than with the pure simulation approach, but the use of separate probability distributions implies an uncoupling of any feedback interactions that may exist between the processes represented by the separate distributions. It is not yet known whether there exists a sufficient number of natural break points, where interactions between processes can be ignored, to make this method an adequate representation of reality.

A third approach, a generalization of the standby system equations discussed earlier, has been suggested (Aerospace, 1984). In a manner similar to the approach just described, probability distributions would be established from exercising the mathematical submodels for each process. The main difference is that the probabilities would be used in a well-defined mathematical structure representing a multicomponent standby system. The system description developed thus far is more general than the standby system example described earlier in that it allows for the possibility of failure of some components while they wait in standby. This is an important feature given the inside to outside degradation mechanisms that have been identified for the waste package.

## B. EVENT TREE ANALYSIS

Difficulties have been identified in connection with application of event trees in quantitative assessment of the waste package, like the problems that

arose in the use of fault trees. The difficulties discussed below are classified in three categories:

- Representation of continuous changes by discrete states,
- Time dependencies in event probabilities, and
- Completeness and overlap of scenarios.

### 1. Discrete versus Continuous State Variables

The branching process used in event trees forces categorization of the waste package system into discrete states. Representation of degrees of degradation of the canister would require multiple branchings, which when pursued for each of the barriers, produces an awkward multiplicity of combinations that are difficult to quantify and may not model the system with sufficient accuracy. This is essentially the same problem that was discussed previously for the fault trees. When modeling the actual processes and interactions, continuous state variables will be required to describe the system, and a simulation program may be needed to do the calculations.

### 2. Time-Dependent Probabilities

Event trees can be an adequate representation for some systems. For example, in a nuclear reactor, a safety valve might be activated after the failure of some other component. If the probability of failure of the safety valve were truly independent of the status of the first component, then the probability of joint occurrence of failure of both components could easily be computed as a simple multiplication. Statistical independence of component failures is often a reasonable assumption, and in such cases, the event tree methodology is useful for quantification of the system failure probability.

An event tree structure could also be used with conditional probabilities if the probabilities of successor failure events could be computed based solely on the knowledge of whether the predecessor failure events had occurred. A good

example of this might be a network of batteries providing power to an electric car. If the failure of one battery creates an overload that leads, in a quantifiable manner, to failure of the other batteries, then an event tree using conditional probabilities could be an appropriate representation.

The waste package unfortunately poses an even more complex problem. Many of the failure events (e.g., corrosion of the metal barriers, leaching of nuclides, transport of nuclides through the packing) are not only dependent on whether certain predecessor events occur but also are strongly dependent on how much time has elapsed since their occurrence. The event tree structures are not sensitive to this kind of time dependency, the same event tree could represent any one of a continuum of time spacings between events. Calculation of the conditional probabilities needed to quantify the event tree must take into consideration all these possibilities in timing, leading to the convolution integral approach (equation 3) described earlier in connection with fault trees.

### 3. Completeness and Overlap of Scenarios

Event tree branches should comprise mutually exclusive sequences of events if they are to be used to quantify the waste package failure probabilities. Two branches are mutually exclusive if at least one event in each branch is entirely different from all the events in the other branch. Otherwise, if all events in the two branches have something in common, then the branch probabilities could not be added together without double counting some of the probabilities.

With the waste package, it is always the same barriers that must fail, so ordinarily one would expect to generate different tree branches corresponding to different failure modes of the barriers. This is difficult to accomplish in practice, however; because many of the failure modes have something in common. (Stress fracturing may be enhanced by corrosion, and crushing of the overpack from geologic pressure is much more likely after corrosion weakening, etc.) Even if direct commonality between the failure modes is not evident, they often share common environmental conditions. Because many of the failure modes involve interrelated processes, it is difficult to see how the probabilities of the individual branches can be added together.

Another difficulty with the event tree approach to quantification of waste package failure is the need for completeness in the list of possible scenarios. In other words, the event tree branches ideally should comprise an exhaustive set of event sequences as well as an exclusive set as described above. If scenarios are omitted, then the corresponding branch probabilities will not be added to the total probability of failure, leading to an underestimate. It is generally understood that if only the most improbable scenarios are omitted, little error is produced. In practice however, little seems to be done to systematically control this omission process. The best approach is probably that used by Sandia National Laboratories (Cranwell et al., 1982) where the rejected scenarios are discussed and recorded for the benefit of future analysis.

Development of a set of mutually exclusive and exhaustive event tree branches is doubly difficult for the waste package problem because of the effects of time of occurrence of the events. Because there are many ways to sequence the same events, it is difficult to enumerate all the possible combinations (i.e., be exhaustive) without producing too much overlap. Earthquakes, tunnel collapse, drilling, or water intrusion can happen in any sequence, and the order of occurrence of these events can have major effects on the computation of barrier failure times. It is very difficult to reconcile these possibilities using event trees alone. Event tree methodology does not adequately deal with event timing and with random sequence ordering; for these kinds of problems, more comprehensive methods such as computer simulation are needed.

## VII. CONCLUSIONS AND RECOMMENDATION

On the basis of the work to date, the following conclusions have been developed:

- Fault trees and event trees can be valuable qualitative tools to display failure modes on event sequence.

The act of generating fault trees/event trees is itself constructive in that it serves to focus on the identification of possible failure modes by requiring that the analyst articulate the relationships among the system components. This activity suggested relationships not previously considered.

- The standard methods used to quantify the trees in other applications cannot be used in the waste package context because they do not provide a realistic representation of the waste package degradation.

Typically, the trees are analyzed using boolean algebra techniques that presume independence of primary events—this condition is not satisfied for the waste package, which is subject to common environmental conditions and coupled events. The nested barriers mean that the respective times of failure are interrelated and occur over long periods of time; the standard quantification techniques presume that events occur within the same general time frame. In addition, the processes governing waste package performance (e.g., corrosion) are continuous and do not lend themselves to manageable representation by the discrete logic gates used in the trees. These considerations cast doubt on the credibility of the numerical results obtained using the trees. Given the necessity for maintaining confidence in the tools used in support of licensing decisions, it is important to consider alternative quantification methods.

It is recommended from these conclusions that:

- Techniques other than fault trees and event trees should be explored for quantitative analysis of waste package performance.

Alternative quantification methods are currently being pursued in the Methodology Review portion of this project.

## REFERENCES

The Aerospace Corporation, 1983, "Preparation of Engineering Analysis for High-Level Waste Packages in Geologic Repositories, Program Plan," ATR-83 (3810-01)-IND, Washington, D.C.

The Aerospace Corporation, 1984, "Methodologies for Assessing Long-Term Performance of High-Level Radioactive Waste Packages," Draft Interim Report, Washington, D.C.

Ahn, T.M., and P. Soo, 1982, "Container Assessment-Corrosion Study of HLW Container Materials," NUREG/CR-2317, Vol. 1, Brookhaven National Laboratory.

Bertozzi, G.M. d'Alessandro, and F. Girardi, 1977, "Evaluation of the Safety of Storing Radioactive Wastes in Geological Formations: A Preliminary Application of Fault Tree Analysis to Salt Formations," BNWL-TR-272, Battelle Pacific Northwest Laboratories, Proceedings of OECD Workshop, Ispra, Italy.

Bhaskaran, G., and J.E. McCleery, 1979, "Accident Event Analysis and Mechanical Failure Probabilities--Retrieval System for Emplaced Spent Unreprocessed Fuel (SURF) in Salt Bed Repository," UCRL-15111, Lawrence Livermore Laboratory.

Bida, G., and D. Eastwood, 1983, "Packing Material Testing Required to Demonstrate Compliance with 1000-year Radionuclide Containment, Semiannual Report on Waste Package Verification Tests," NUREG/CR-2755, BNL-NUREG-51544, Brookhaven National Laboratory.

BNL, 1983a, "Review of DOE Waste Package Program, Subtask 1.1--National Waste Package Program April 1982-September 1982," NUREG/CR-2482, BNL-NUREG-51494, Vol. 3, Brookhaven National Laboratory, P. Soo Ed.

BNL, 1983b, "Review of DOE Waste Package Program, Subtask 1.1--National Waste Package Program, October 1982-March 1983," NUREG/CR-2482, BNL-NUREG-51494 Vol. 4, Brookhaven National Laboratory, P. Soo Ed.

BNL, 1983c, "Review of Waste Package Verification Tests Semiannual Report covering the period October 1982-March 1983," NUREG/CR-3091, BNL-NUREG-51630, Vol. 2, Brookhaven National Laboratory, P. Soo Ed.

Claiborne, H.C., et al., 1984, "Draft Staff Technical Position on Repository Environmental Parameters Relevant to Assessing the Performance of High-Level Waste Packages," NUREG-1076 (Review Draft), Oak Ridge National Laboratory.

Cranwell, R., et al., 1982, "Risk Methodology for Geologic Disposal of Radioactive Waste: Final Report," NUREG/CR-2452.

d'Alessandro, Marco, and Arnold Bonne, 1980, "Fault Tree Analysis for Probabilistic Assessment of Radioactive Waste Segregation: An Application to a Plastic Clay Formation at a Specific Site," Proceedings, 26th International Geologic Congress in Paris.

Davis, M.S., and D.G. Schweitzer, 1982, "Review of DOE Waste Package Program, Subtask 1.1--National Waste Package Program," NUREG/CR-2482, BNL-NUREG-51494 Vol. 1., Brookhaven National Laboratory.

Hunter, R.L., 1983, "Preliminary Scenarios for the Relevance of Radioactive Waste from a Hypothetical Repository in Basalt of the Columbia Plateau," NUREG/CR-3353, Sandia National Laboratories.

Larsen, Waldmar F., 1974, "Fault Tree Analysis," AD-774843, Picatinny Arsenal, Dover, New Jersey.

Lee, W.L., K. Nair, and G. Smith, 1978, "Basalt Waste Isolation Disruptive Events Analysis," RHO-BWI-C-43, Rockwell Hanford Operations, Richland, Washington.

Logan, S.E., and M.C. Berbano, 1977, "Geologic Modeling in Risk Assessment Methodology for Radioactive Waste Management," Proceedings of OECD Workshop, Ispra, Italy.

McCormick, Norman J., 1981, "Event Tree Analysis," Reliability and Risk Analysis, Academic Press.

NRC, 1975, "Reactor Safety Study," WASH-1400 (NUREG 75/014), Nuclear Regulatory Commission, Main Report and Appendixes I and II.

NRC, 1981, "Fault Tree Handbook," NUREG-0492, Nuclear Regulatory Commission.

Pritzker, A., and J. Gassman, 1979, "Application of Simplified Reliability Methods for Risk Assessment of Nuclear Waste Repositories," Nuclear Technology 48.

Reilly, J.T., 1978, "A Review of Methods for the Integration of Reliability and Design Engineering," GA-A14748, General Atomic Company.

Siskind B., et al., 1983, "Review of Waste Package Verification Tests Biannual Report," BNL-NUREG-33565, Brookhaven National Laboratory, Draft.

Stahl, D., and N.E. Miller, 1983, "Long-Term Performance of Materials Used for High-Level Waste Packaging," NUREG/CR-3405 Vol. 1., Battelle Columbus Laboratories.

Vesely, W.E., 1970, "A Time Dependent Methodology for Fault Tree Evaluation," Nuclear Engineering and Design 13.

Weren, B.H., et al., 1983, "Nuclear Criticality Safety Analysis of a Spent Fuel Waste Package in a Tuff Repository," UCRL-15575, Lawrence Livermore National Laboratory.

Westinghouse Electric Corporation, 1982, "Waste Package Conceptual Design for a Nuclear Repository in Basalt," RHO-BW-CR-136P/AESD-TME-3142.

Woodley, R.E., 1983, "The Characteristics of Spent LWR Fuel Relevant to Its Storage in Geologic Repositories," HEDL-TME 83-28, Hanford Engineering Development Laboratory, Richland, Washington, Draft.

**FINAL DRAFT**

**THE ROLE OF FAULT TREES AND EVENT TREES IN DEPICTING  
FAILURE OF A HIGH-LEVEL RADIOACTIVE WASTE PACKAGE IN  
A BASALT REPOSITORY**

**APPENDICES**

**August 1984**

**Prepared for**

**Office of Nuclear Material Safety and Safeguards  
U.S. NUCLEAR REGULATORY COMMISSION  
Washington, D.C.**

**Prepared by**

**Eastern Technical Division  
THE AEROSPACE CORPORATION  
Washington, D.C.**

## LIST OF FIGURES

### Figure

- A-1 Top Events for Radionuclide Release From Waste Forms to Basalt After Repository Closure
- A-2 Top Event Fault Tree for Radionuclide Release From Commercial High-Level Waste Package to Basalt After Repository Closure
- A-3 A1000—Radionuclide Release From Glass to Canister by Water/Steam
- A-4 A1001—Waste Form Characteristics Altered To Facilitate Radionuclide Release
- A-5 A2000—Radionuclides Released From Glass to Canister by Nonaqueous Means
- A-6 B1000—Canister Allows Radionuclides Aqueous Transport (Through Canister) to Overpack
- A-7 B1001—Canister Weakened Via Degradation From Outside Canister
- A-8 B1002 and B2002—Canister Weakened Via Degradation From Inside Canister
- A-9 B1003 and B2003—Canister Breached Via Degradation From Inside Canister
- A-10 B1004—Canister Breached Via Degradation From Outside Canister
- A-11 B2000—Canister Allows Radionuclide Nonaqueous Transport (Through Canister) to Overpack
- A-12 B2001—Canister Weakened Via Degradation From Outside Canister (Dry)
- A-13 B2004—Canister Breached Via Degradation From Outside Canister (Dry)
- A-14 C1000—Overpack Allows Radionuclides Aqueous Transport (Through Overpack) to Packing
- A-15 C1001 and C3001—Overpack Weakened Via Degradation From Outside Overpack
- A-16 C1002, C2002, C3002, and C4002—Overpack Weakened Via Degradation From Inside Overpack

LIST OF FIGURES (continued)

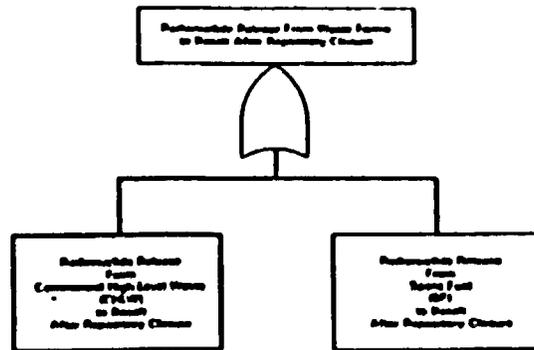
Figure

- A-17 C1003, C2003, C3003, and C4003—Overpack Breached Via Degradation From Inside Overpack
- A-18 C1004 and C3004—Overpack Breached Via Degradation From Outside Overpack
- A-19 C2000—Overpack Allows Radionuclides Nonaqueous Transport to Packing
- A-20 C2001 and C4001—Overpack Weakened Via Degradation From Outside Overpack (Dry)
- A-21 C2004 and C4004—Overpack Breached Via Degradation From Outside Overpack (Dry)
- A-22 D1000 and D3000—Packing Allows Radionuclides Aqueous Transport to Basalt
- A-23 D1001—Packing Unable to Adequately Limit Diffusional Radionuclide Transport
- A-24 D1002—Void Space Interconnections Greater Than Desired
- A-25 D2000 and D4000—Packing Allows Radionuclides Nonaqueous Transport to Basalt
- B-1 Top Events for Radionuclide Release From Waste Forms to Basalt After Repository Closure
- B-2 Top Event Fault Tree for Radionuclide Release From Spent Fuel Package to Basalt After Repository Closure
- B-3 E1000—Radionuclides Released From Spent Fuel to Overpack by Water/Steam
- B-4 E1001—Fission Gas Product Release Occurs
- B-5 E1002—Radionuclides Released to Water by Dissolution
- B-6 E2000—Radionuclides Released From Spent Fuel to Overpack by Nonaqueous Means
- B-7 C3000—Overpack Allows Radionuclides Aqueous Transport to Packing

LIST OF FIGURES (continued)

Figure

- B-8 C9000—Overpack Allows Radionuclides Nonaqueous Transport to Packing
- C-1 CHLW Package Failure—Corrosion
- C-2 CHLW Package Failure—Hole in Overpack Weld and Corrosion
- C-3 CHLW Package Failure—Ceiling Collapse and Corrosion
- C-4a CHLW Package Failure—Corrosion Followed by Loading From Ceiling Collapse
- C-4b CHLW Package Failure—Corrosion Followed by Loading From Ceiling Collapse (cont'd)
- C-5 CHLW Package Failure—Drilling Into Repository Area
- C-6 CHLW Package Failure—Drilling Into Waste Package
- C-7 CHLW Package Failure—Mechanical Waste Form Failure and Internal Corrosion
- C-8 SF Waste Package Failure—Corrosion
- C-9 SF Waste Package Failure—Corrosion Followed by Criticality
- C-10 SF Waste Package Failure—Handling/Quality Control and Corrosion
- C-11 SF Waste Package Failure—Earthquake and Corrosion



**Figure A.1. Top Events for Radionuclide Release From Waste Forms to Environment After Repository Closure**

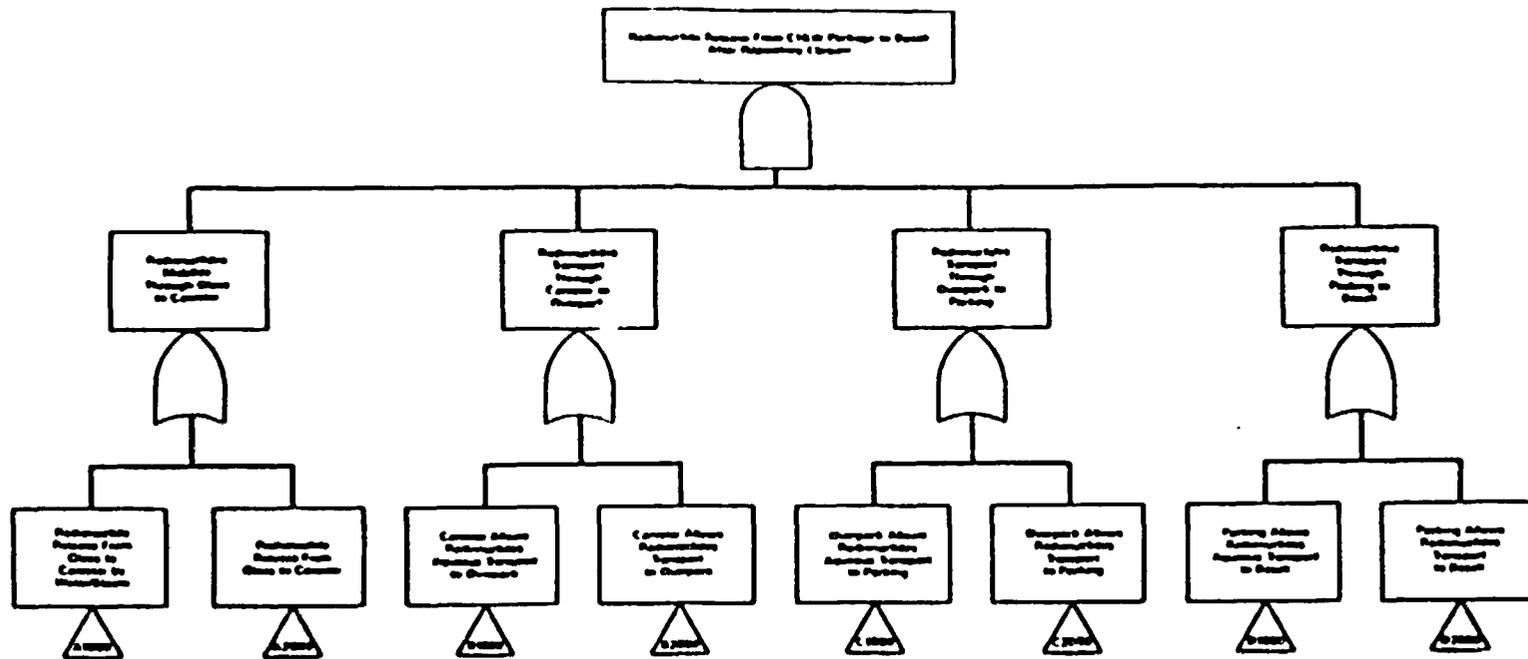


Figure A.2. Top Event Fault Tree for Radionuclide Release from Commercial High Level Waste Package to Beach After Repository Closure

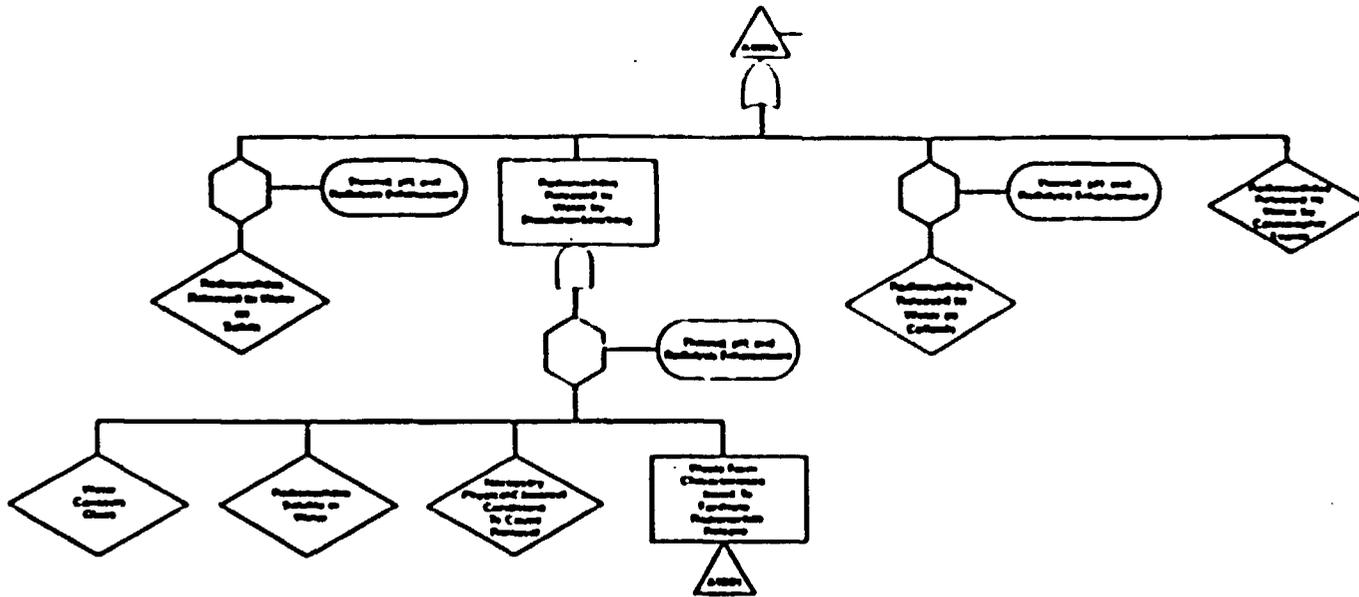


Figure A 2. A1000 - Radiological Release From Class to Control by Water/Shower

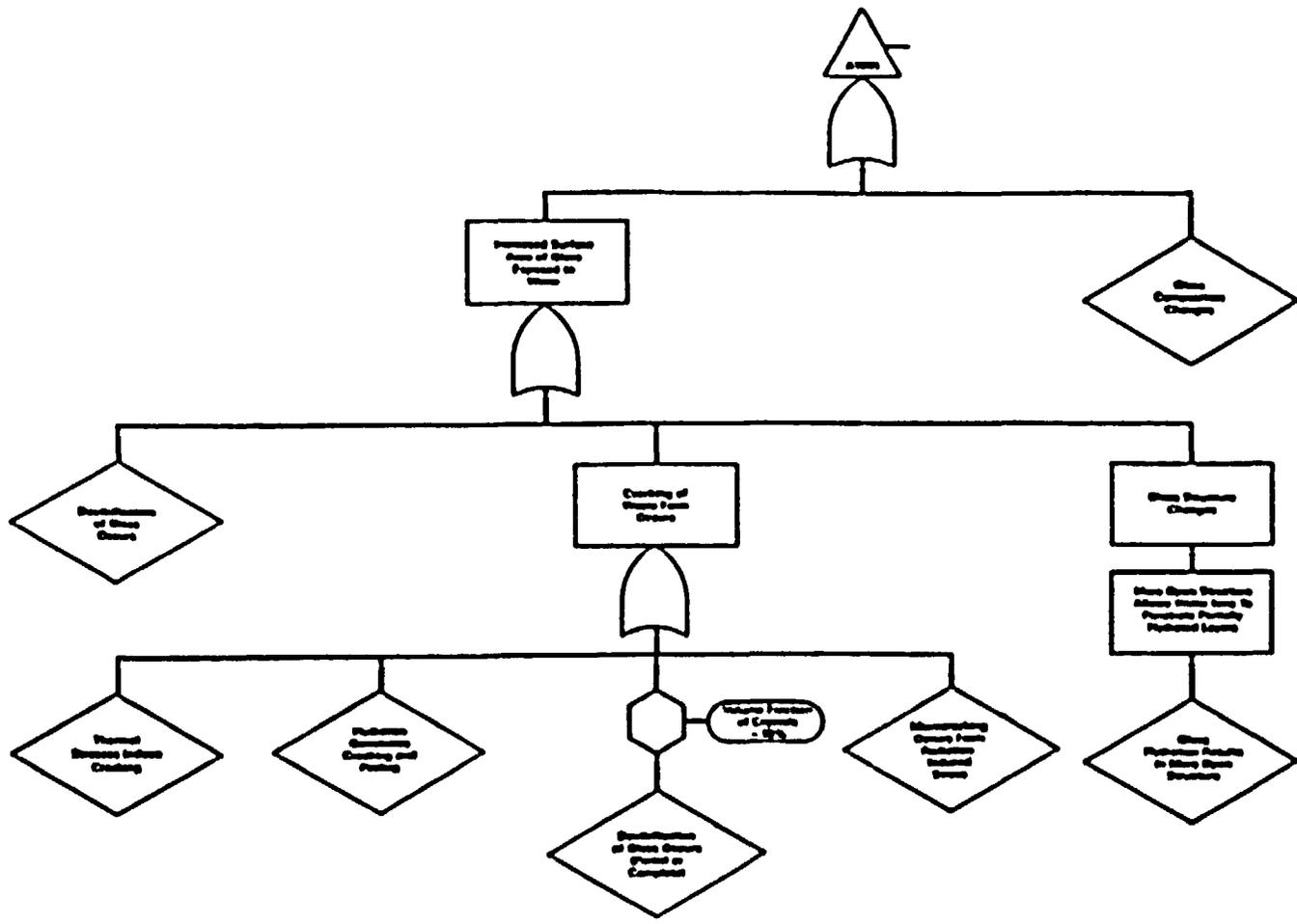


Figure A-4. A1001 - Form Characteristics Altered to Facilitate Redundant Release

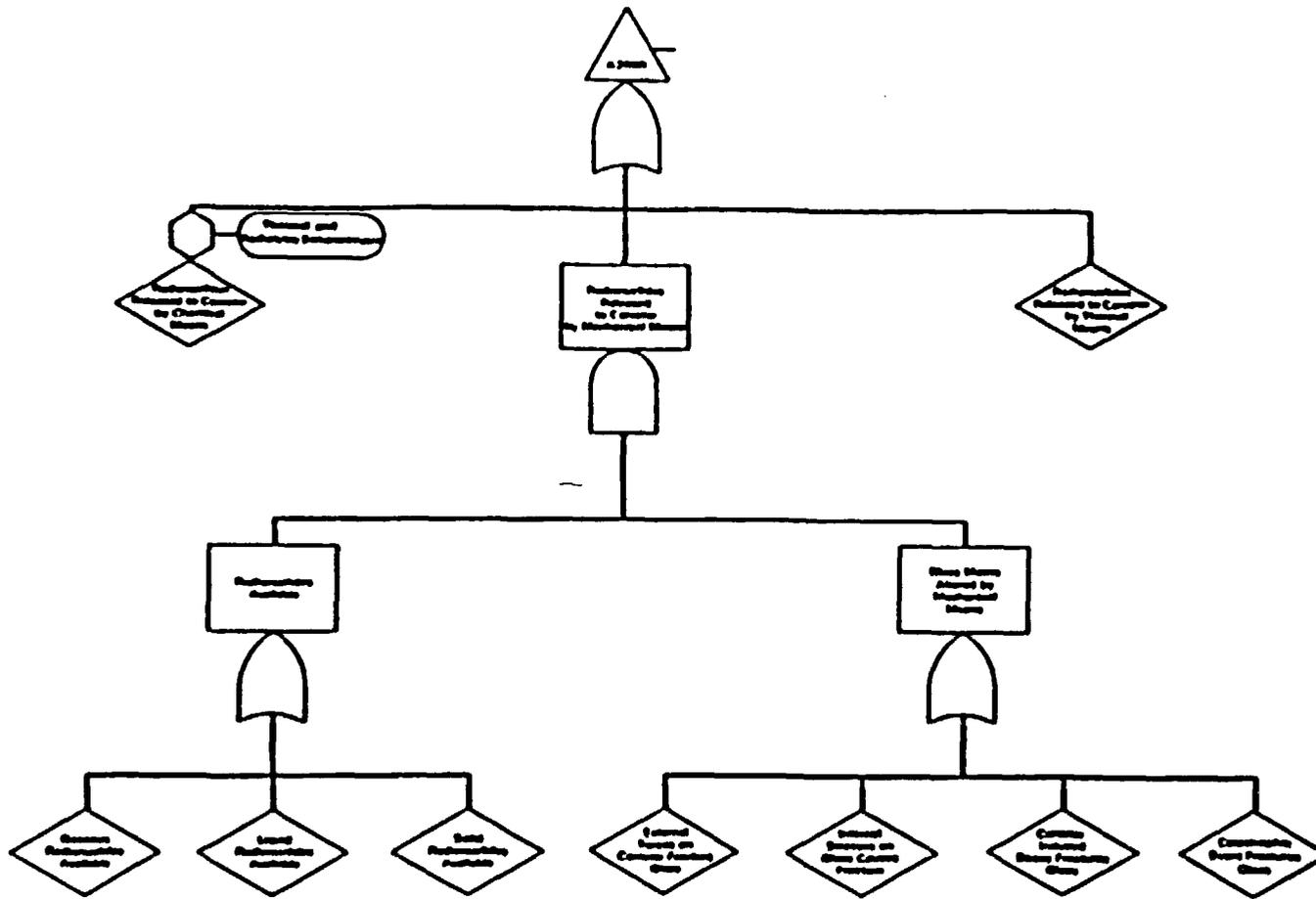


Figure A.5. A2000 - Redundancies Released From Glass to Computer by Resequencing Errors

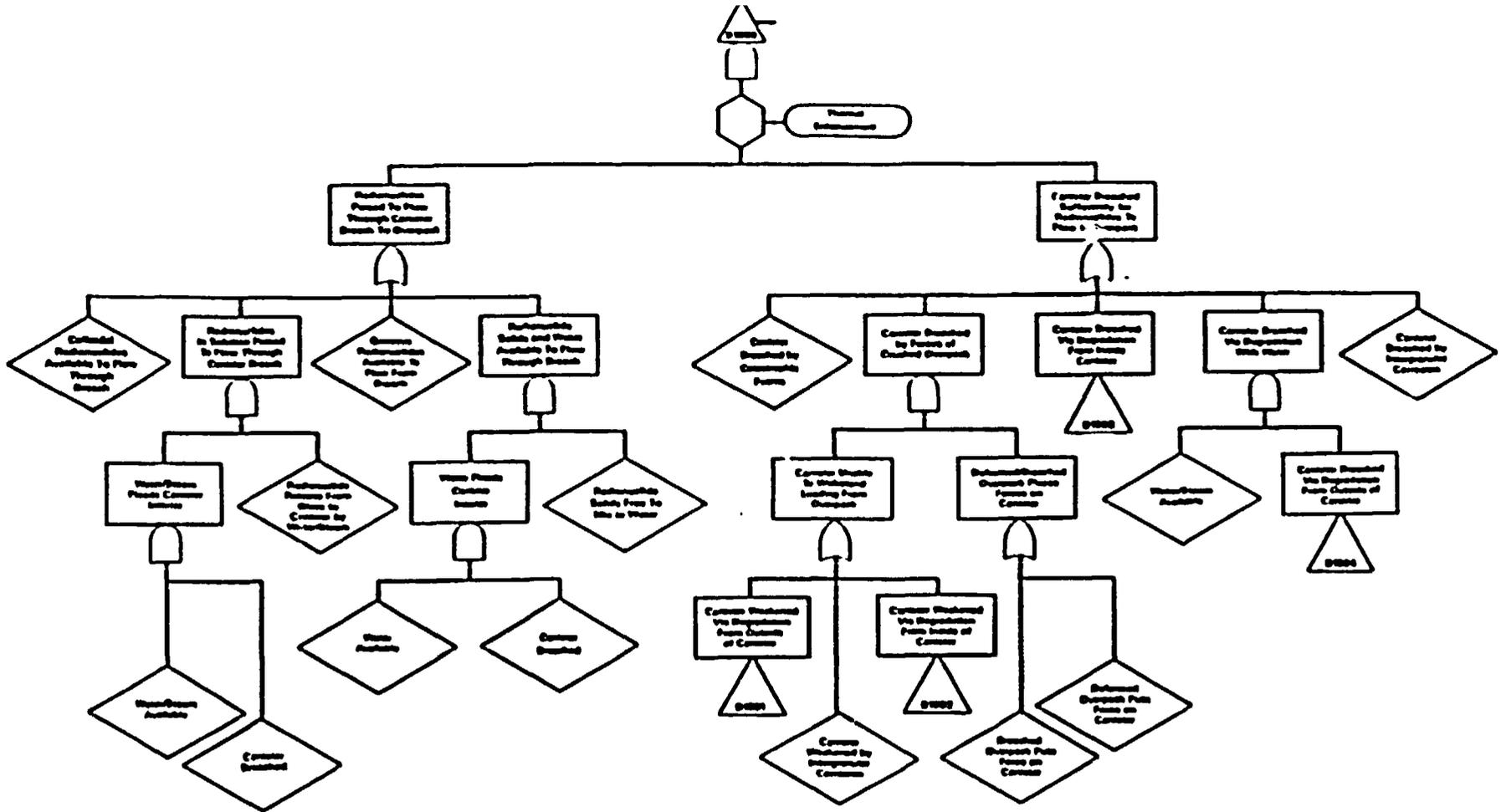


Figure A-8. 91000 - Canister Above Radionuclides Against Transport (Through Canister) to Overpack

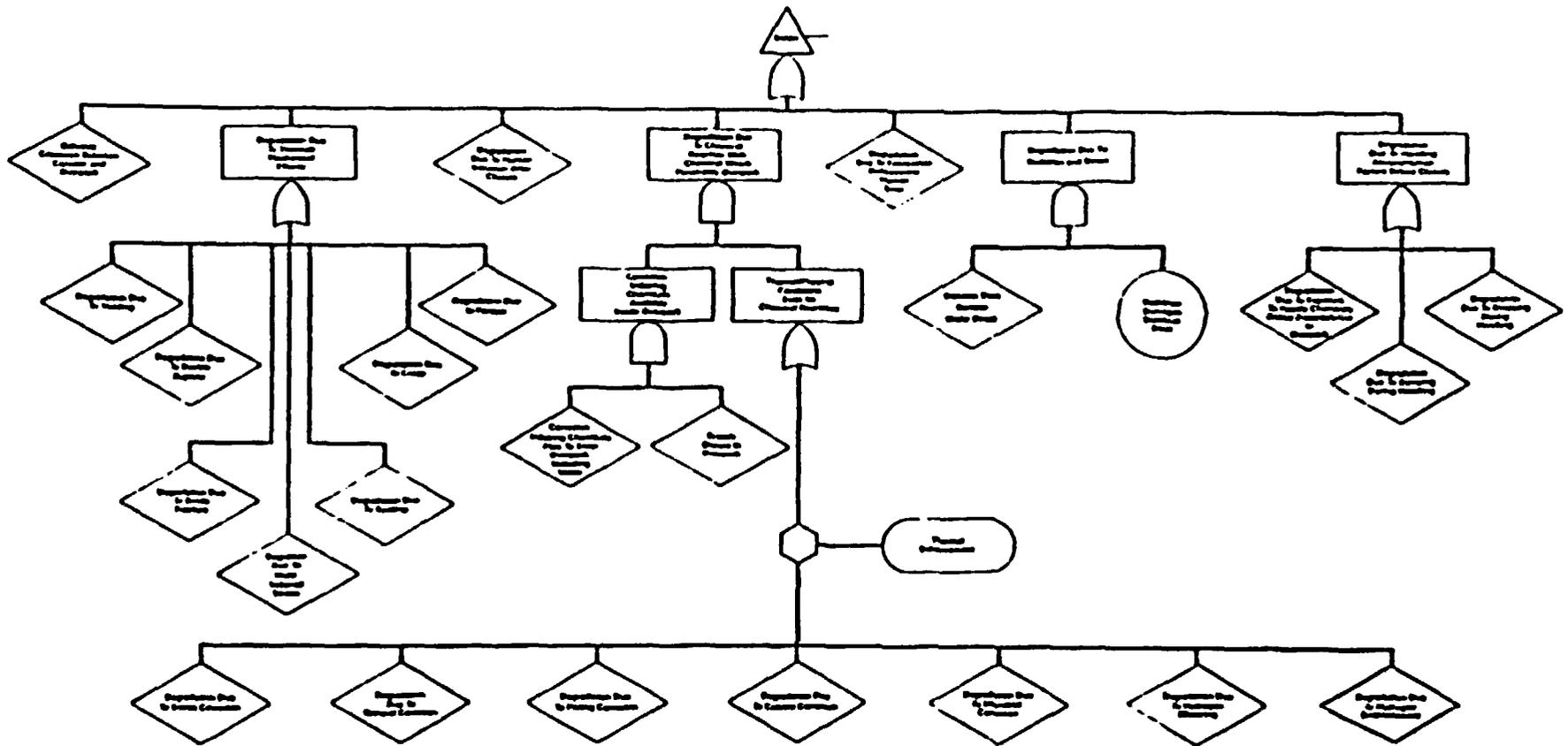


Figure A-7. B1001 - Core Barrel Whiskered Via Degradation From Outside Core Barrel

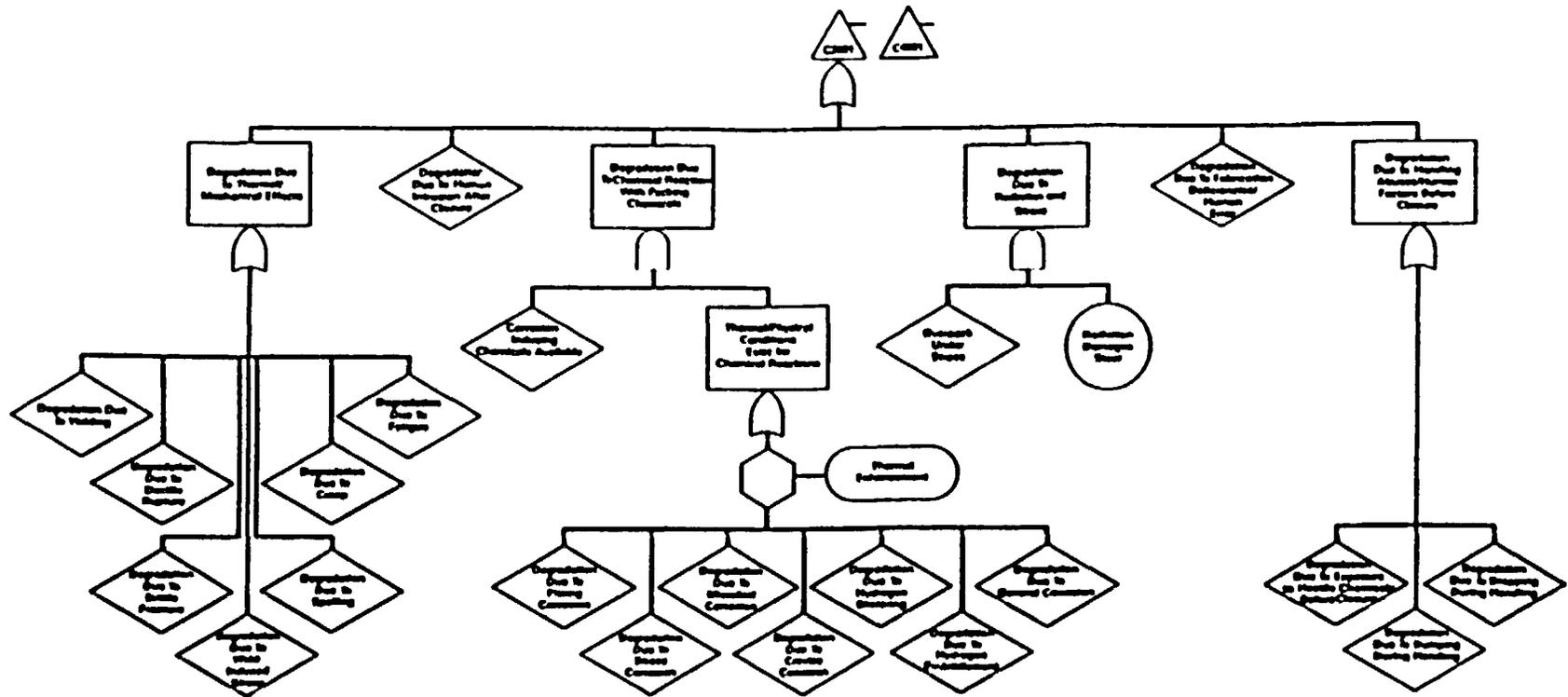


Figure A-26. CSM1 and CSM2 – Overpack Washed Via Degradation From Outside Overpack IDyl

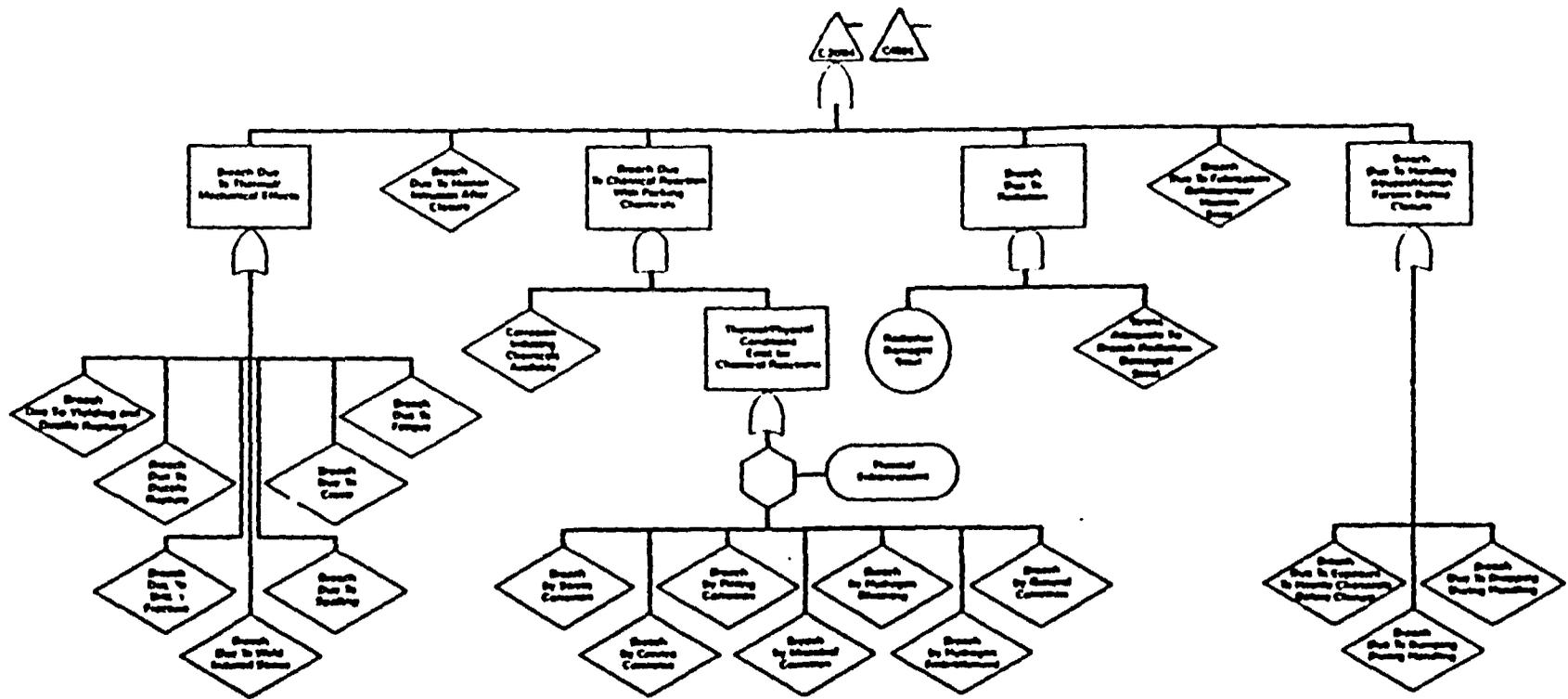


Figure A-21. C2004 and C4004 - Overpass Breached Via Degradation From Outside Overpass (Dry)

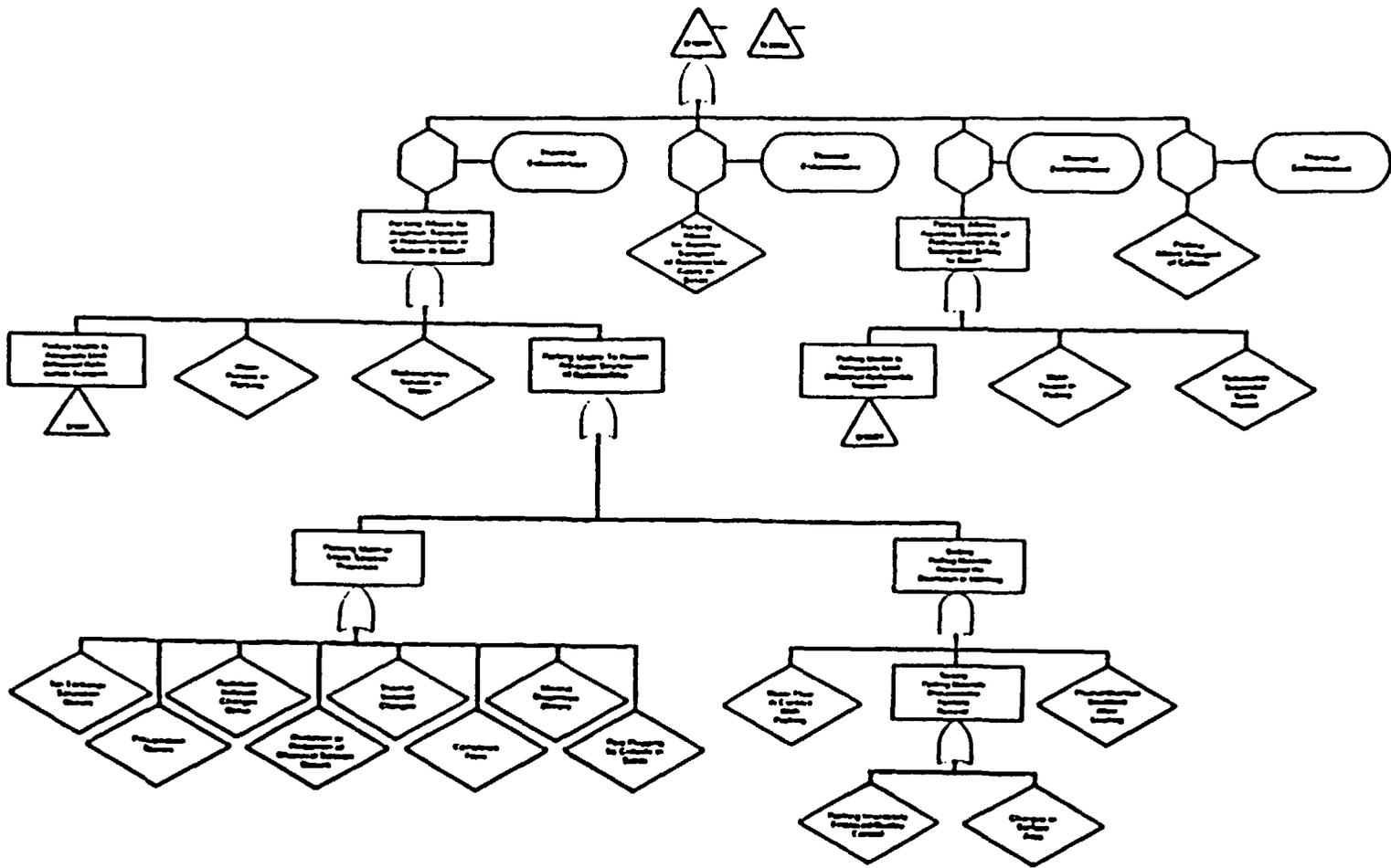


Figure A-22. D1000 and D3000—Packing Above Radionuclide Aqueous Transport to Reactor

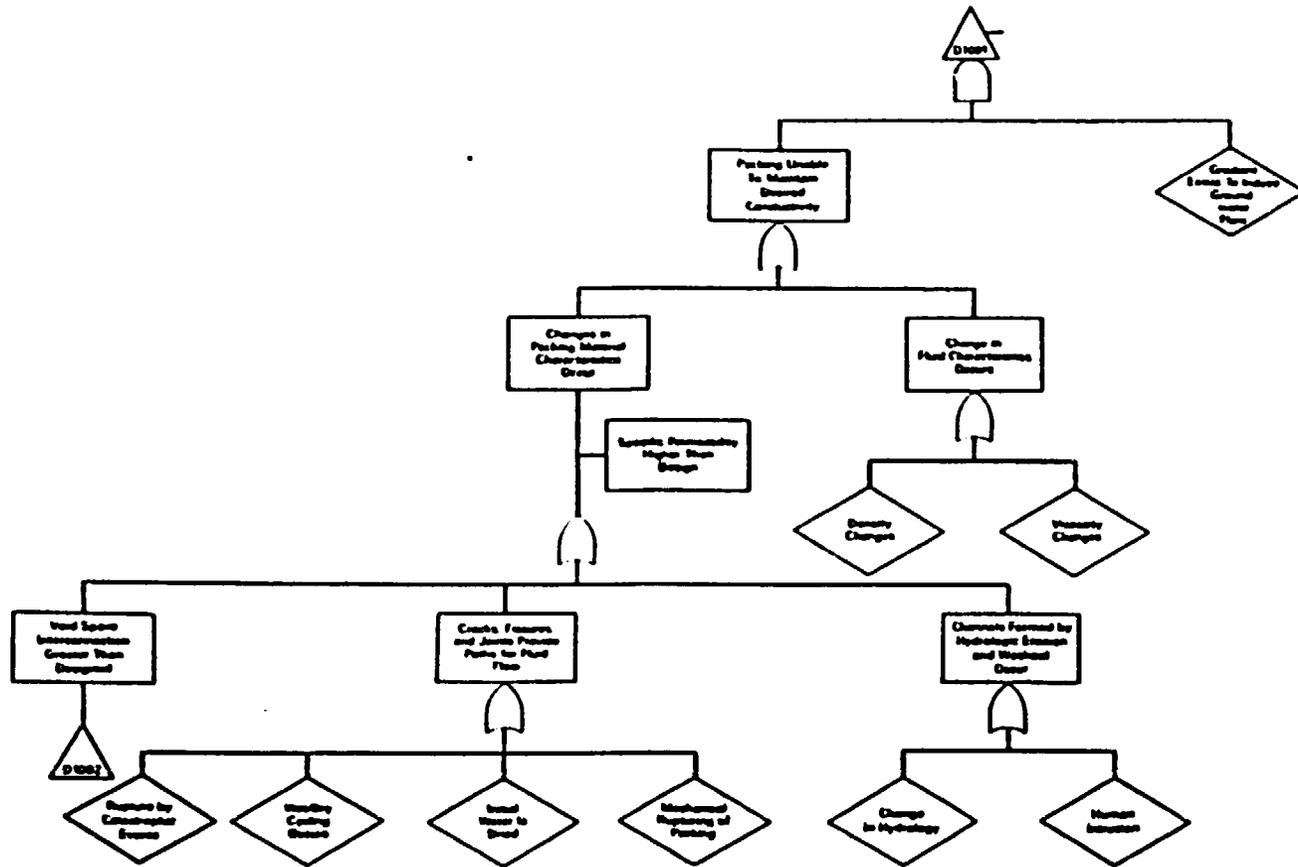


Figure A-23 D1001—Packing Unable to Adequately Limit Diffusional Resistance Transport



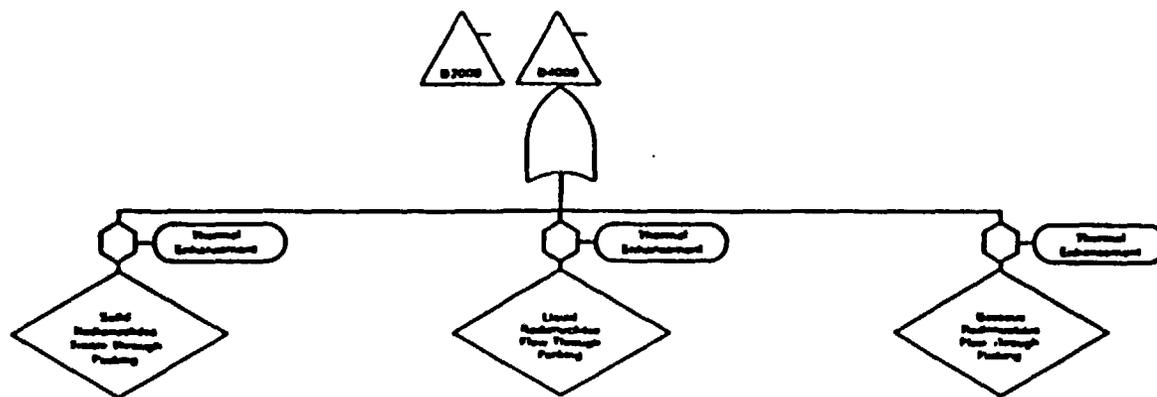


Figure A-25 D2000 and D4000 - Packing Allows Radonuclei's Heterogeneous Transport to Beak

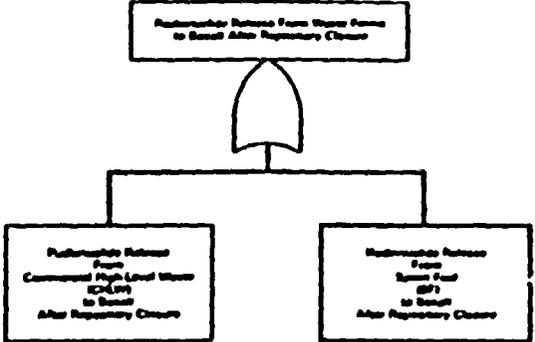


Figure B-1 Top Events for Radionuclide Release From Waste Forms to Small Area Repository Closure

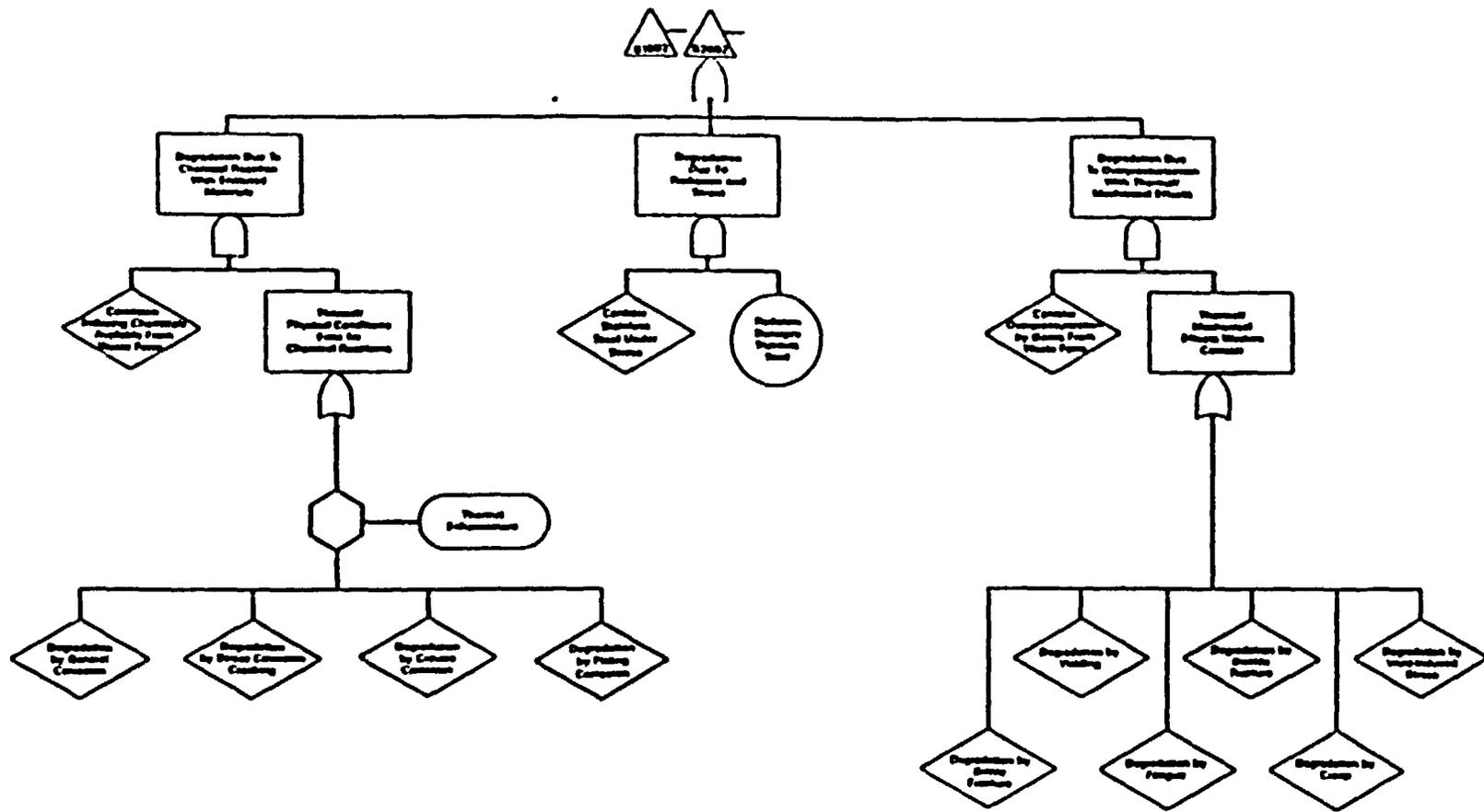


Figure A-8. S1002 and S2002 - Concrete Weakened Via Degradation From Inside Concrete

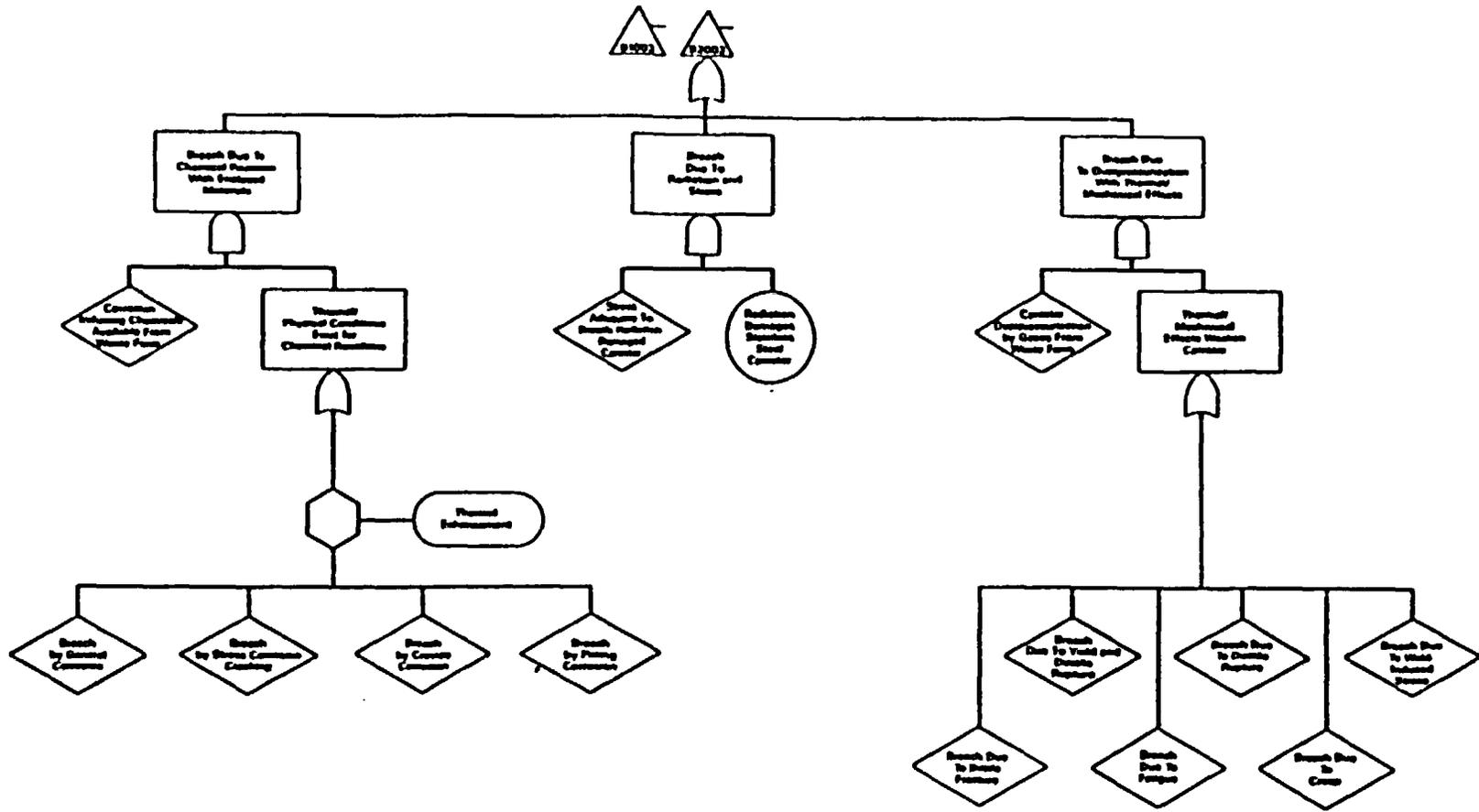


Figure A-9. B1003 and B2003—Control Broken Via Degradation From Inside Control

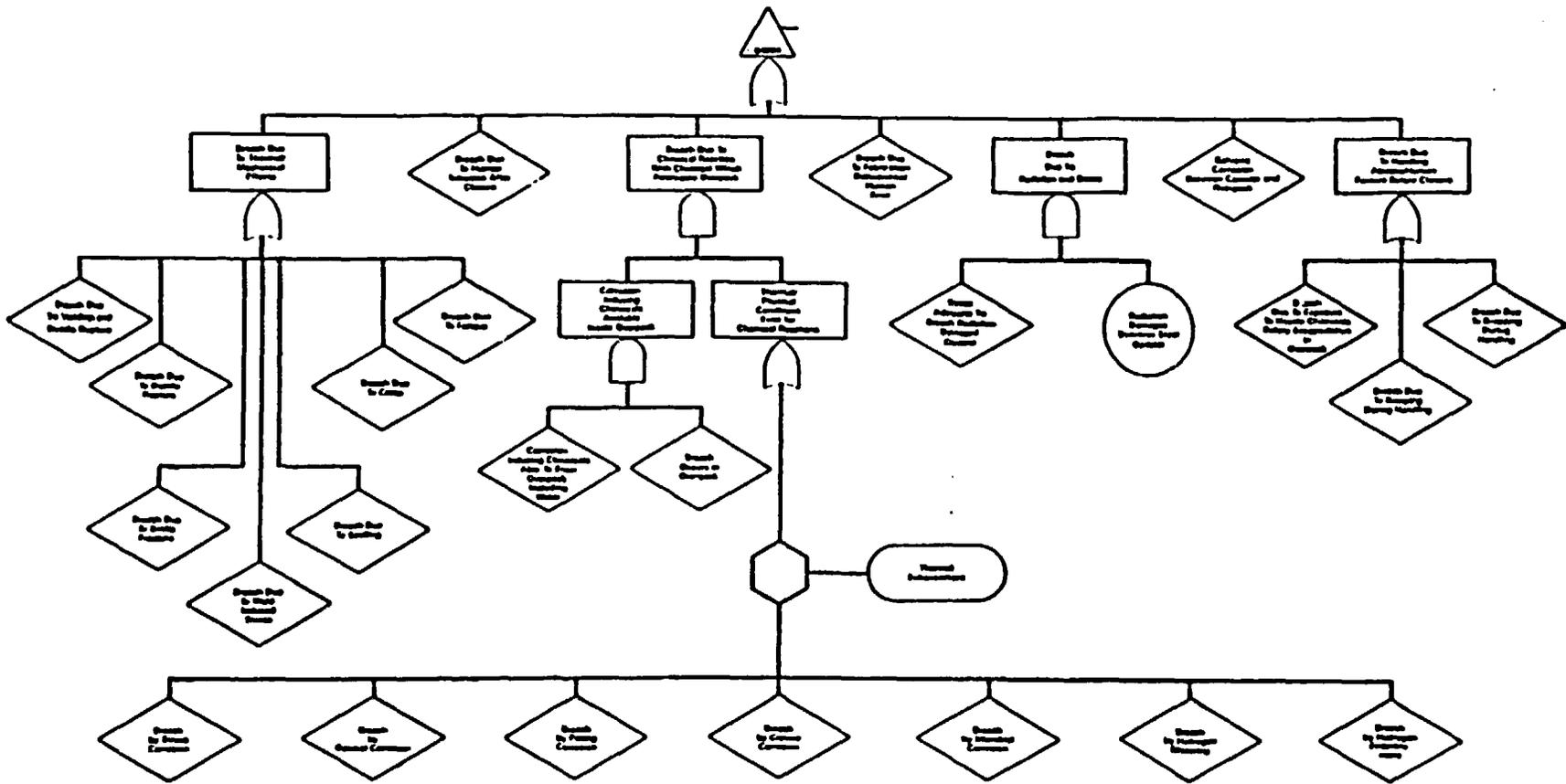


Figure A-10. 81004 - Container Breached Via Degradation From Outside Container

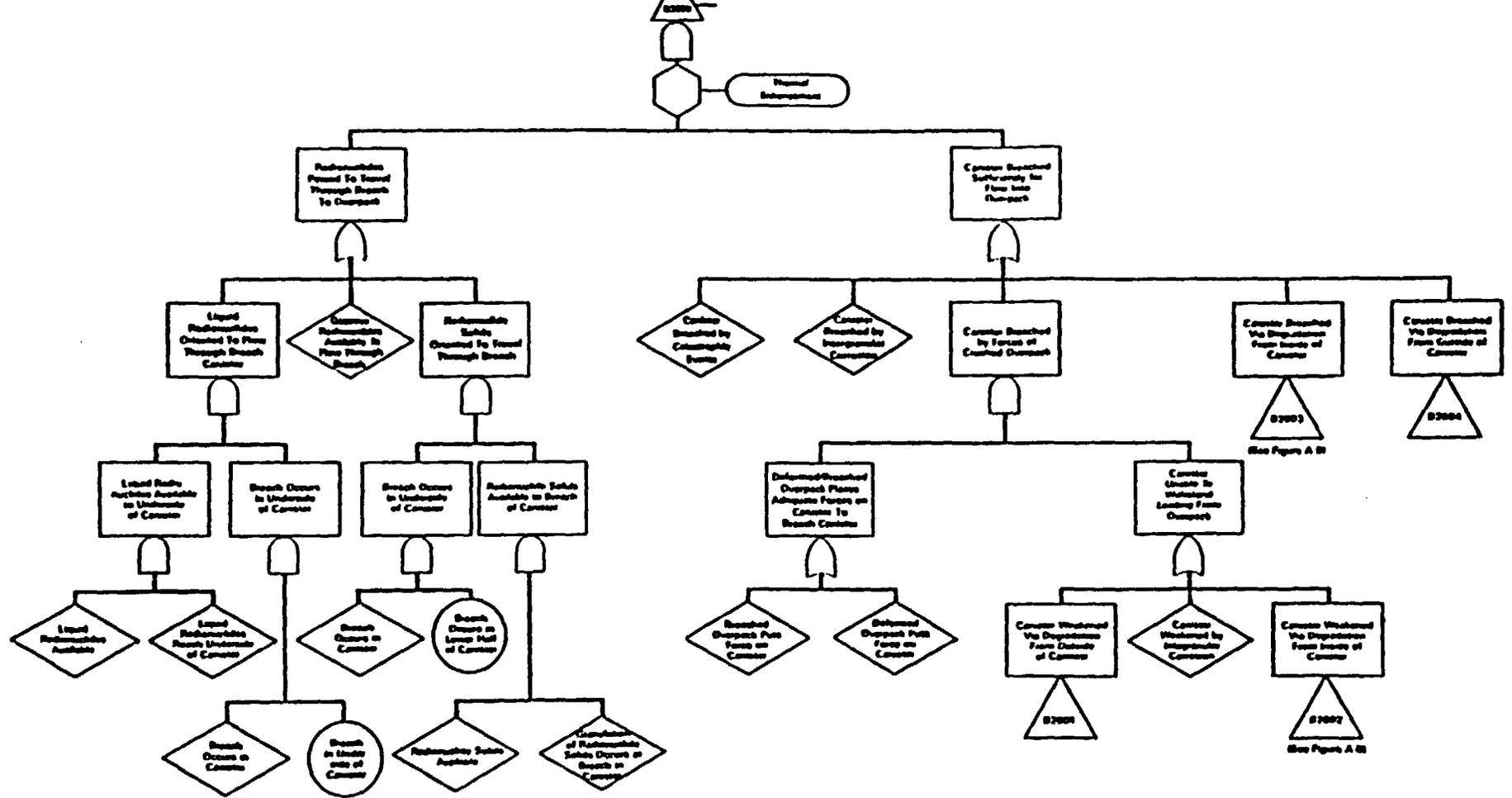


Figure A-11. B2000 - Canister Allows Radiocesium Monoisotope Transport (Through Canister) to Overpack

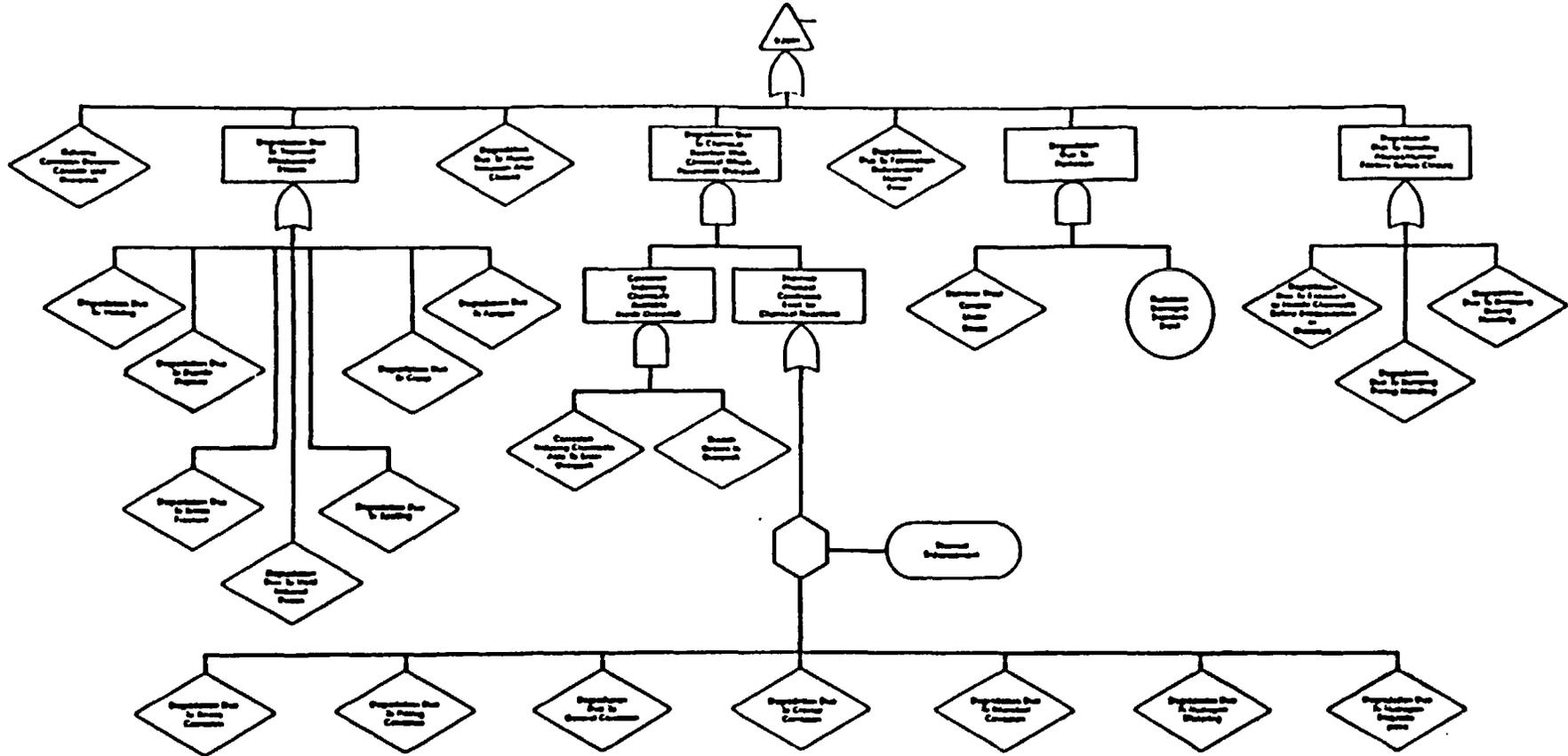


Figure A-12. E2891 - Canister Weakened Via Degradation From Outside Canister (Dry)

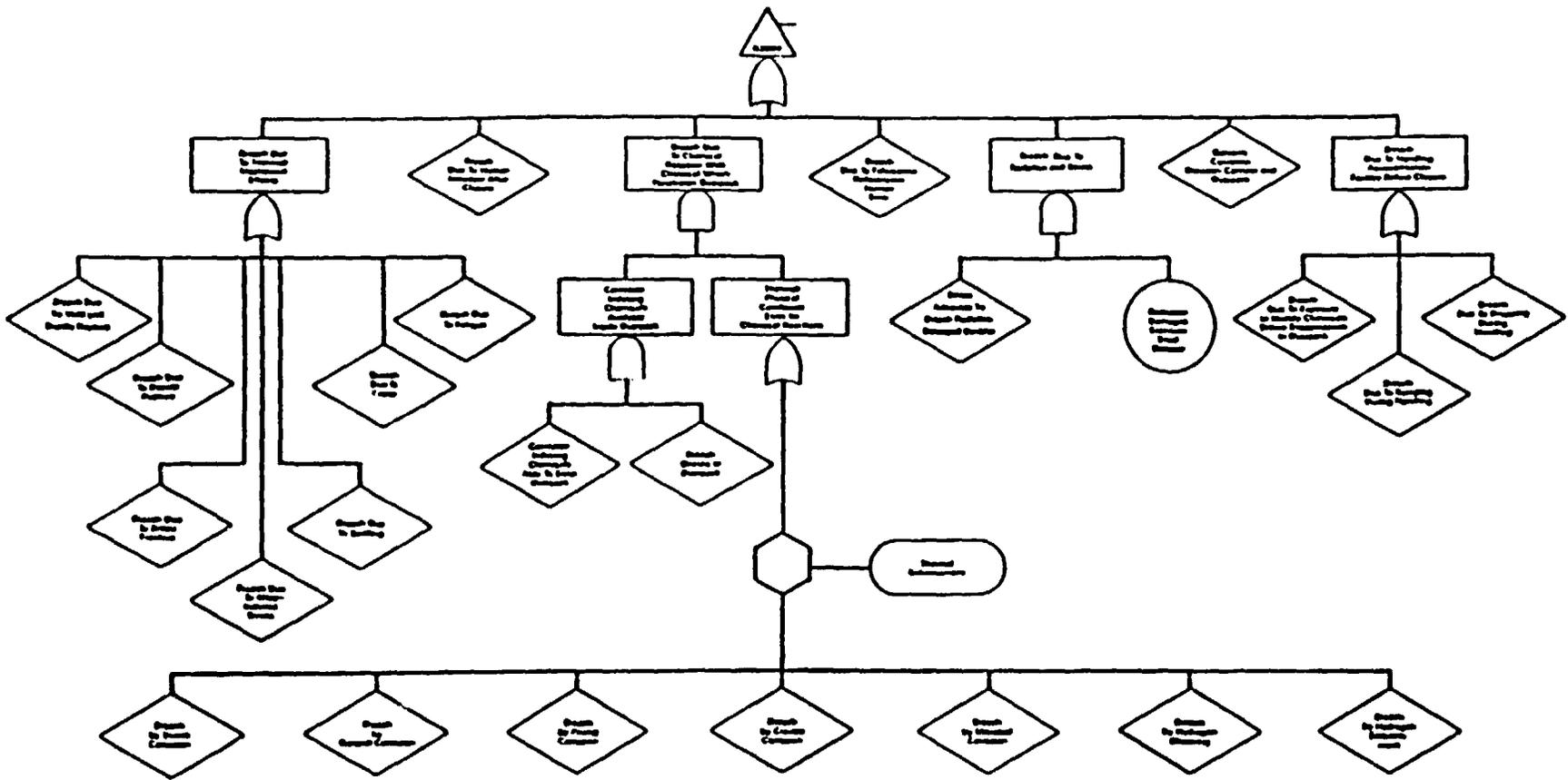


Figure A-13. 62894 - Contactor Breached Via Degradation From Outside Contactor (Dry)

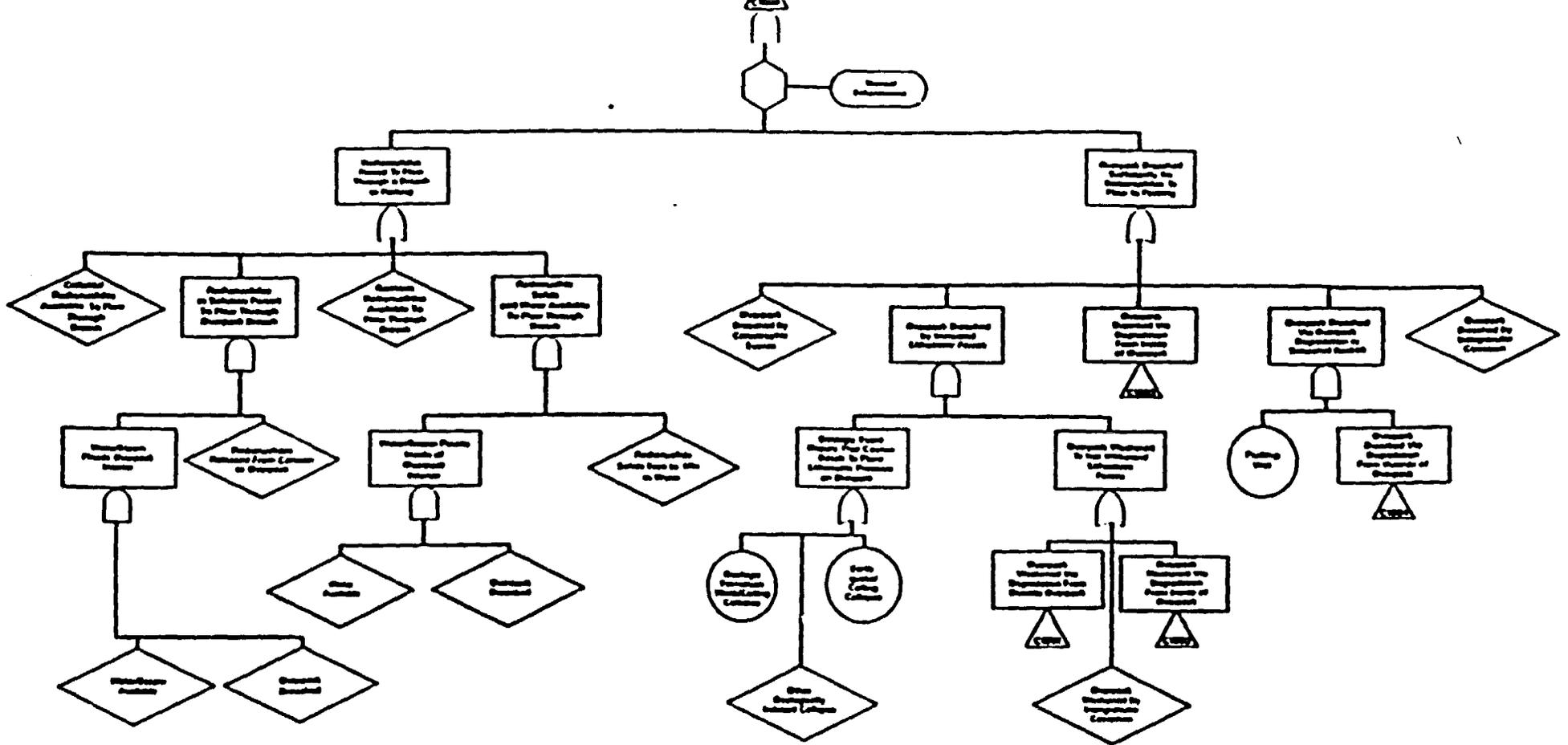


Figure A 54. C1000 - Control Through Relationships Against Transport (Through Overpass) to Parking

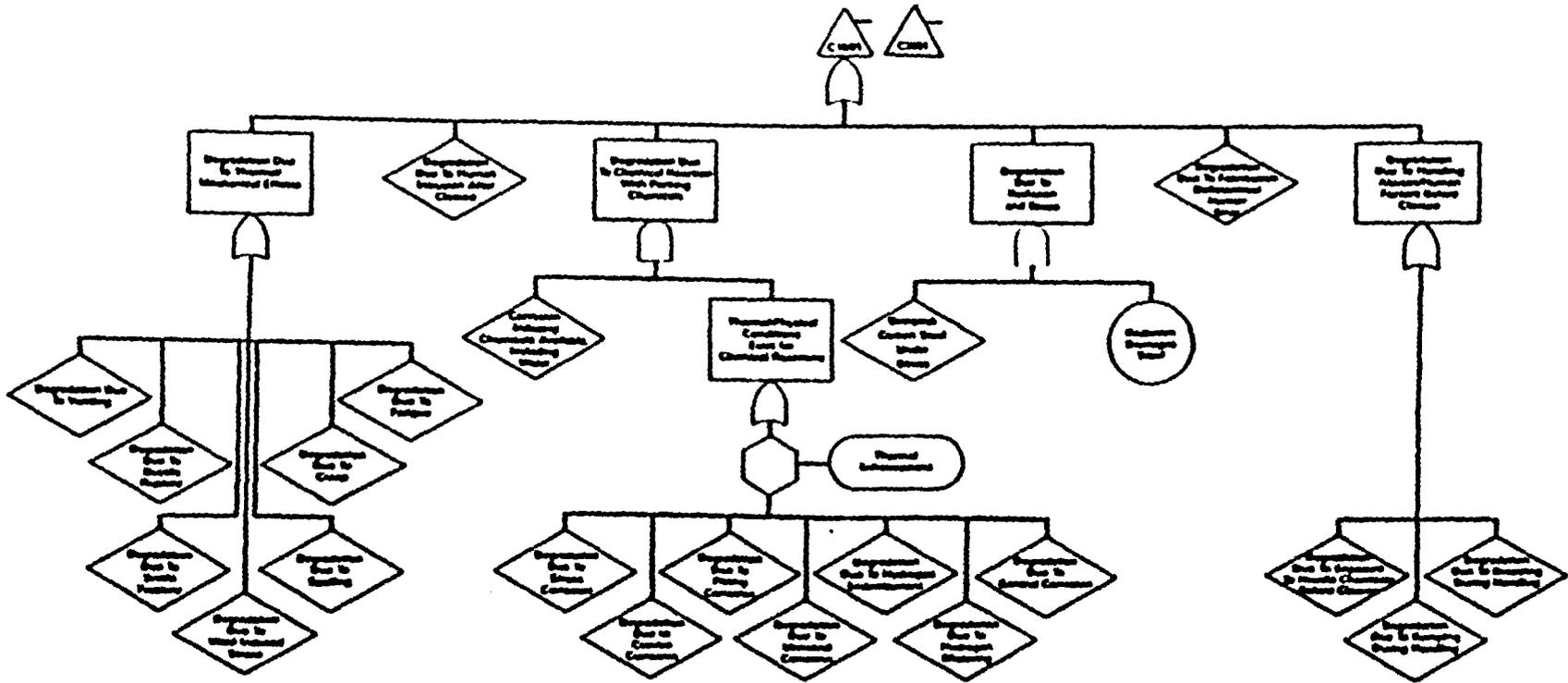


Figure A-16. CMMI and CMMB - Outputs Masked Via Degradation from Outside Outputs



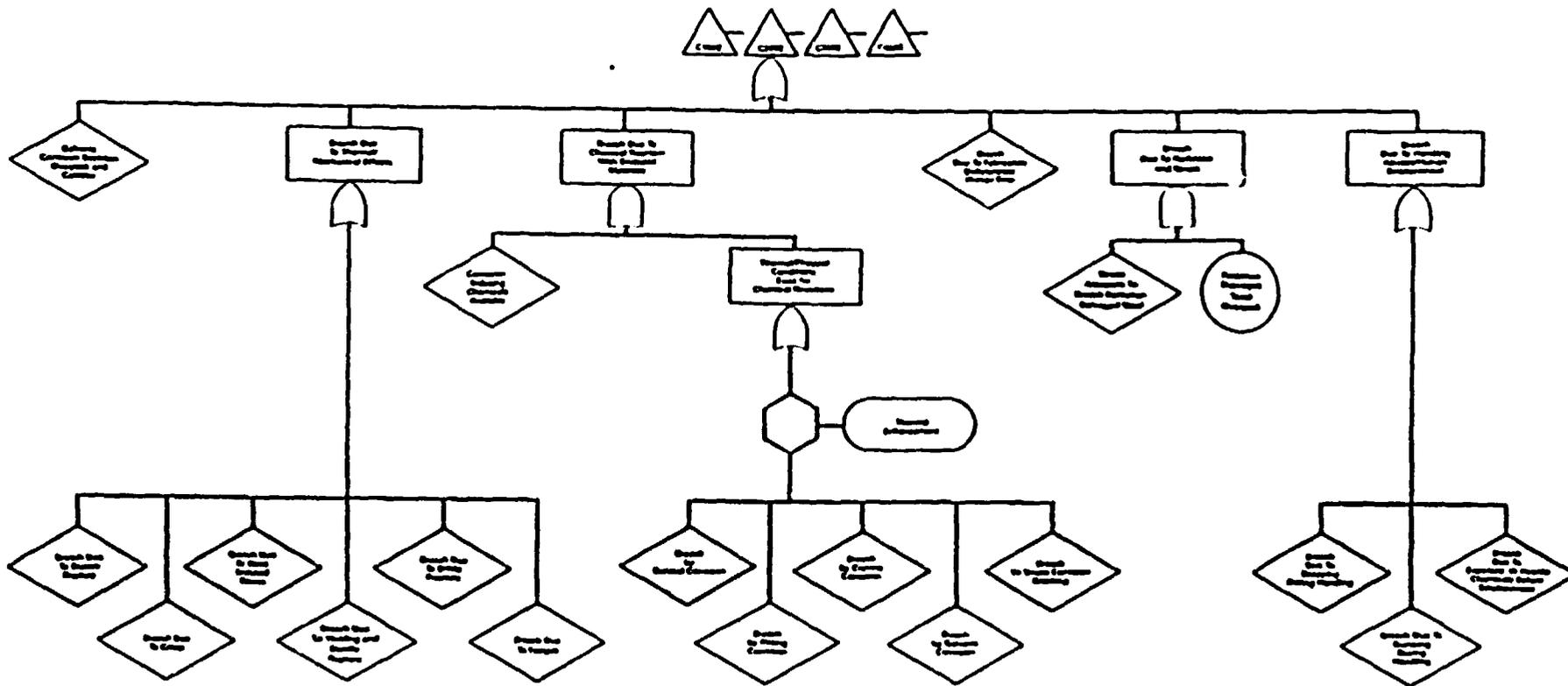


Figure A-17. C-100, C-200, C-300, and C-400—Overpost Reached Via Degradation From Initial Overpost

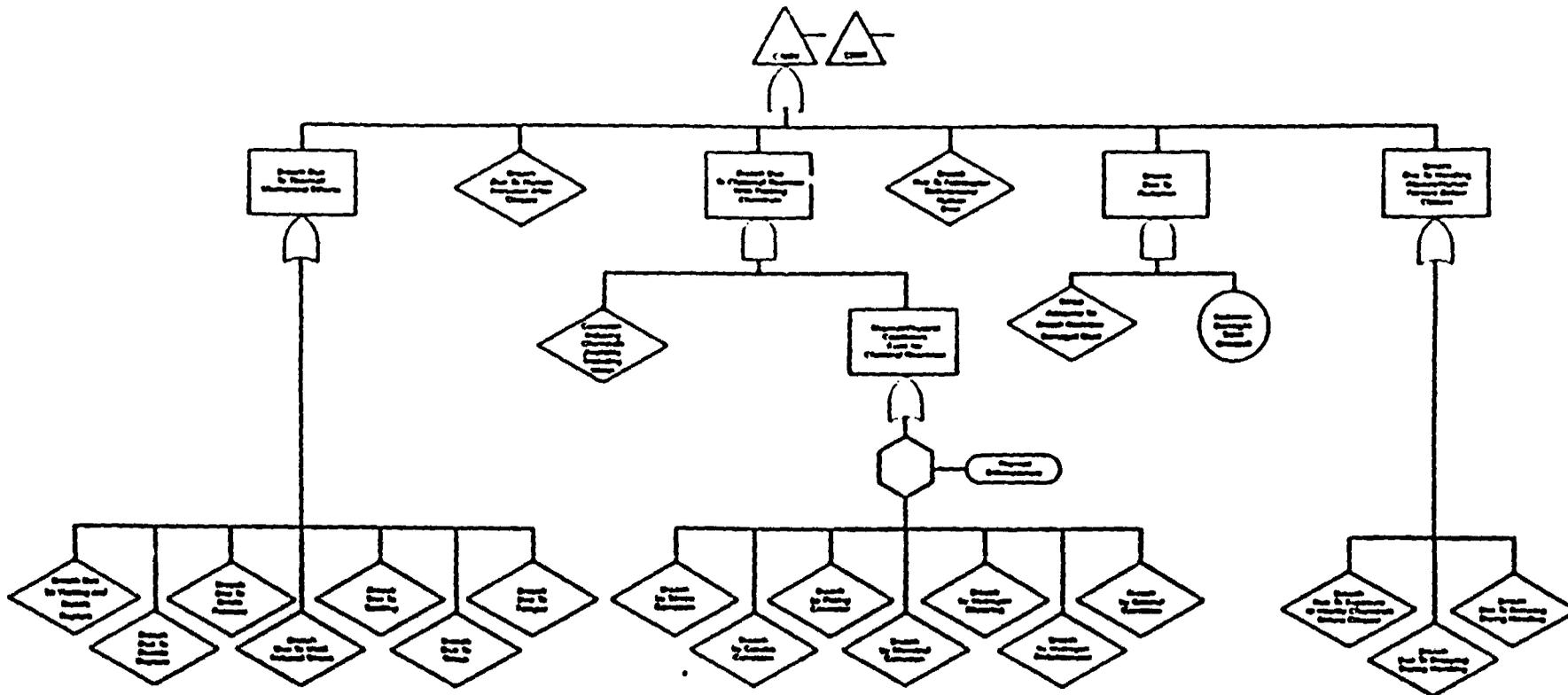


Figure A-12. C1884 and C1884 - Overpack Breached Via Degradation From Outside Overpack



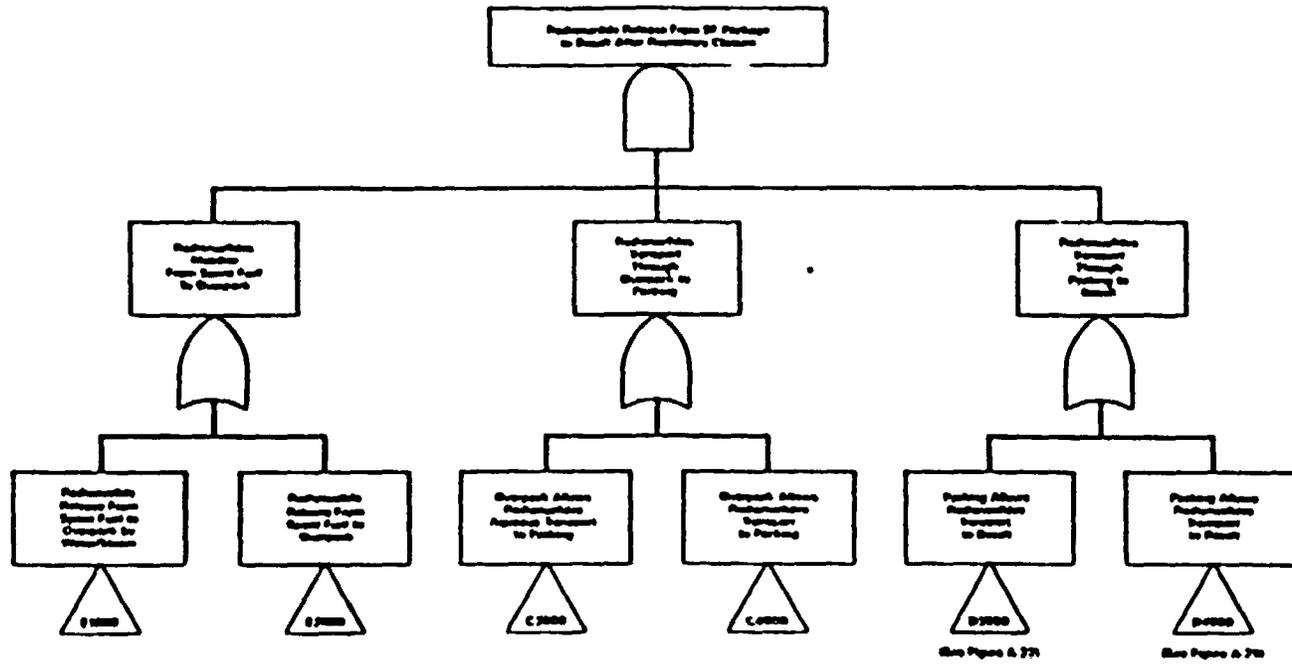


Figure B-2 Top Event Fault Tree for Redundable Return From Beach Fuel Package to Beach After Repetitive Checks



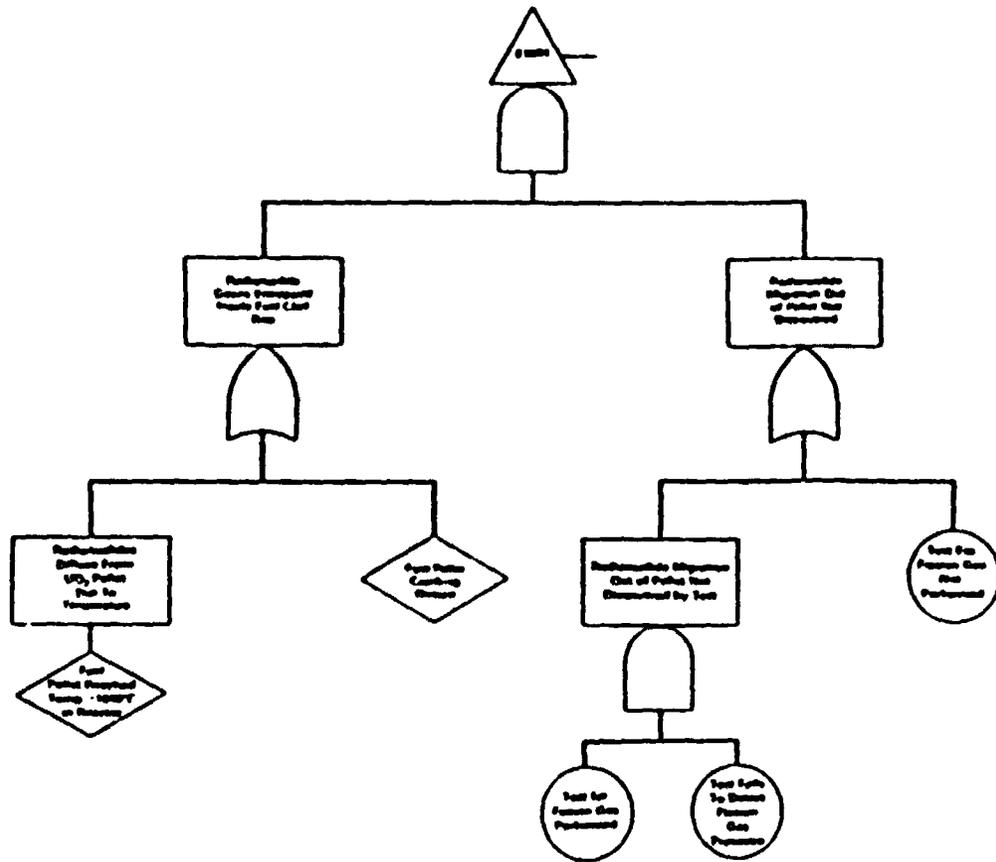


Figure B.4 (E1001) - Piston Gas Product Release Control

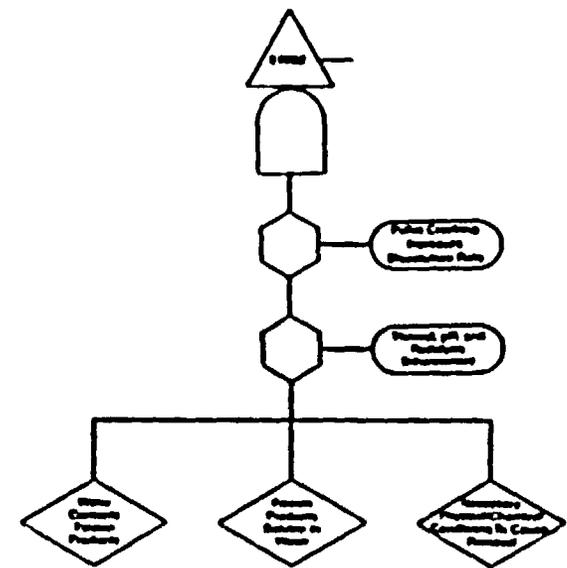


Figure B.5 (E1002) - Piston Gas Product Release Control

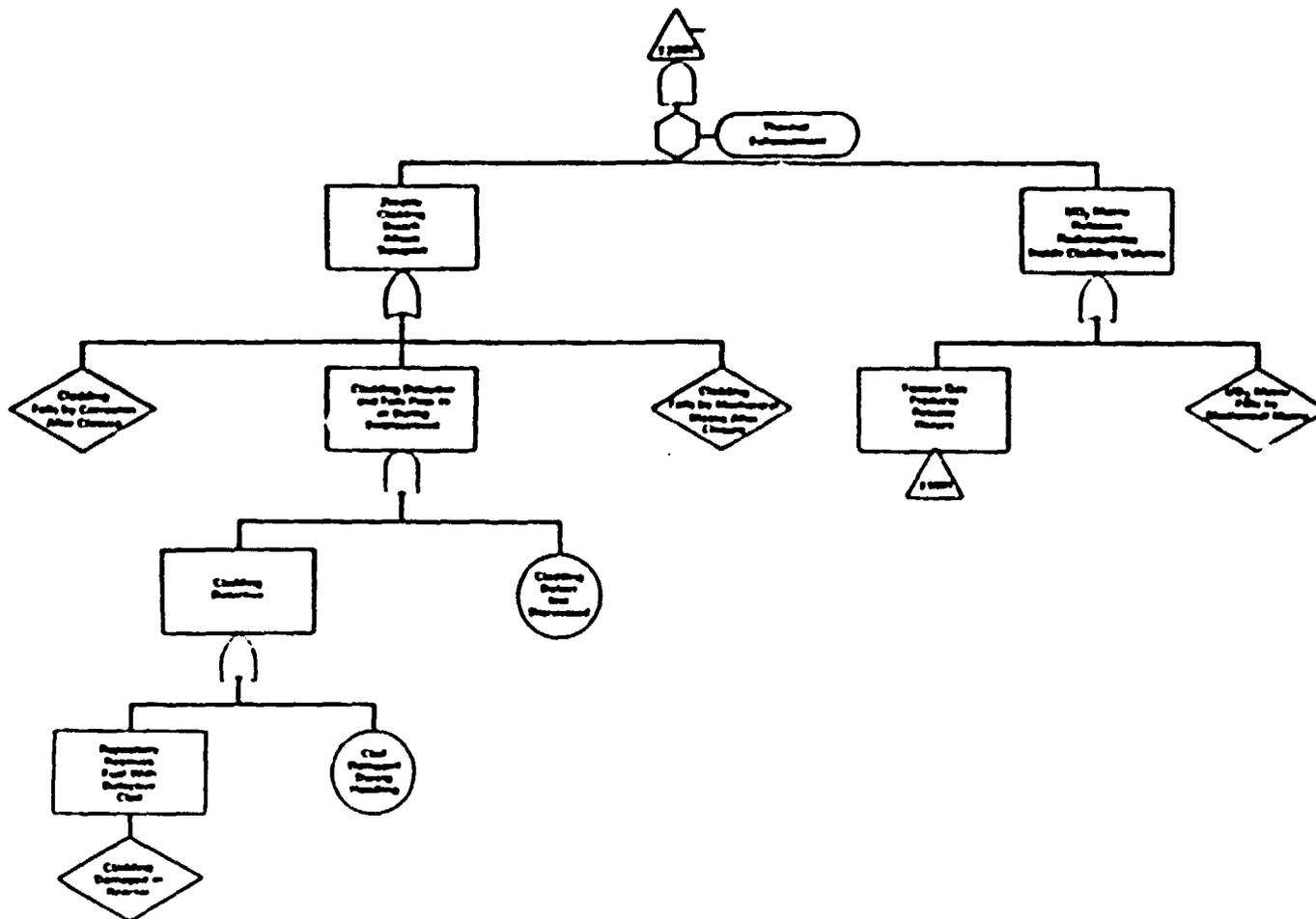


Figure B-6 F7000 - Radionuclides Released From Spent Fuel to Overpack by Nonaqueous Means



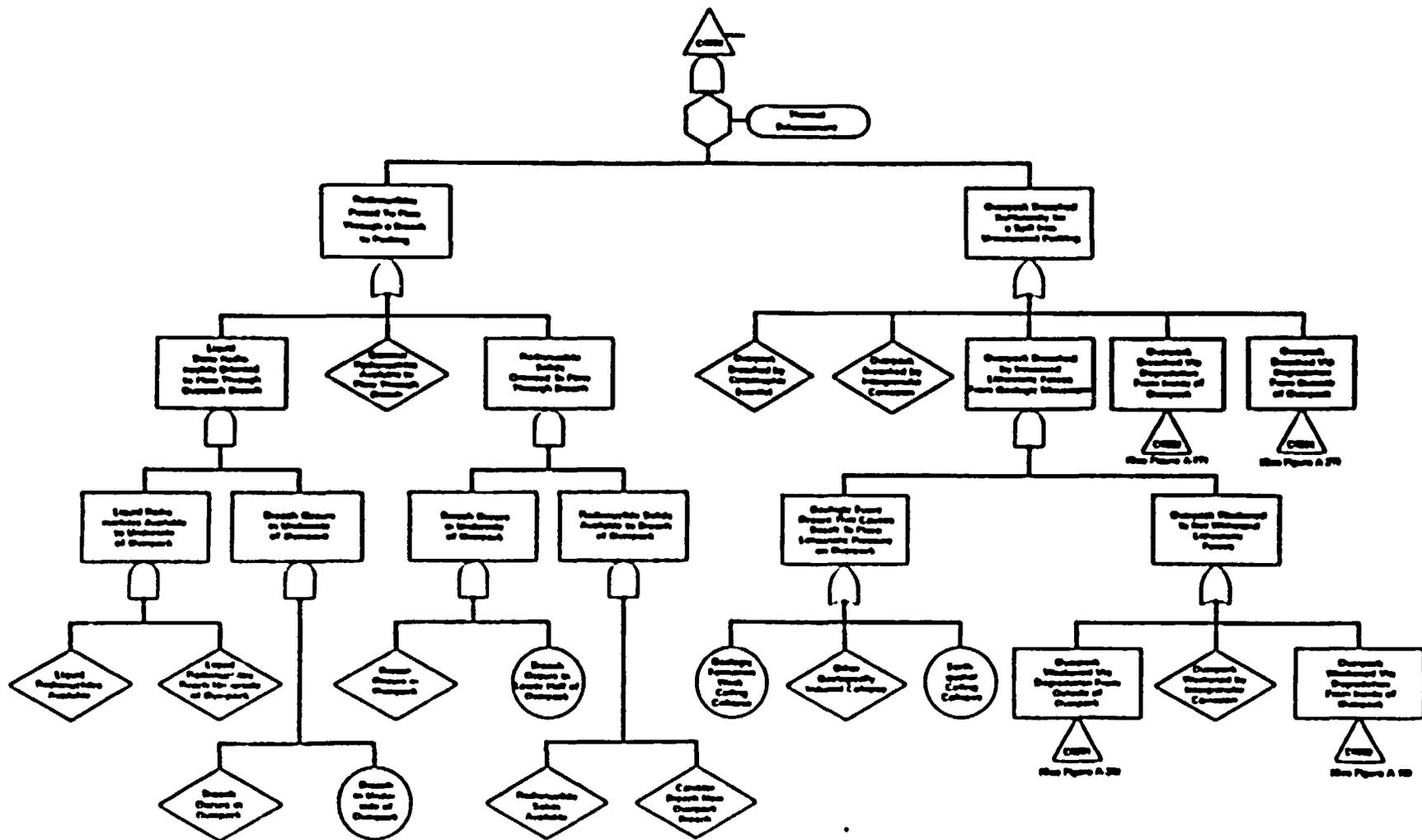


Figure B-2. CRMS - Overpass Allows Redundant Management Transport to Parking

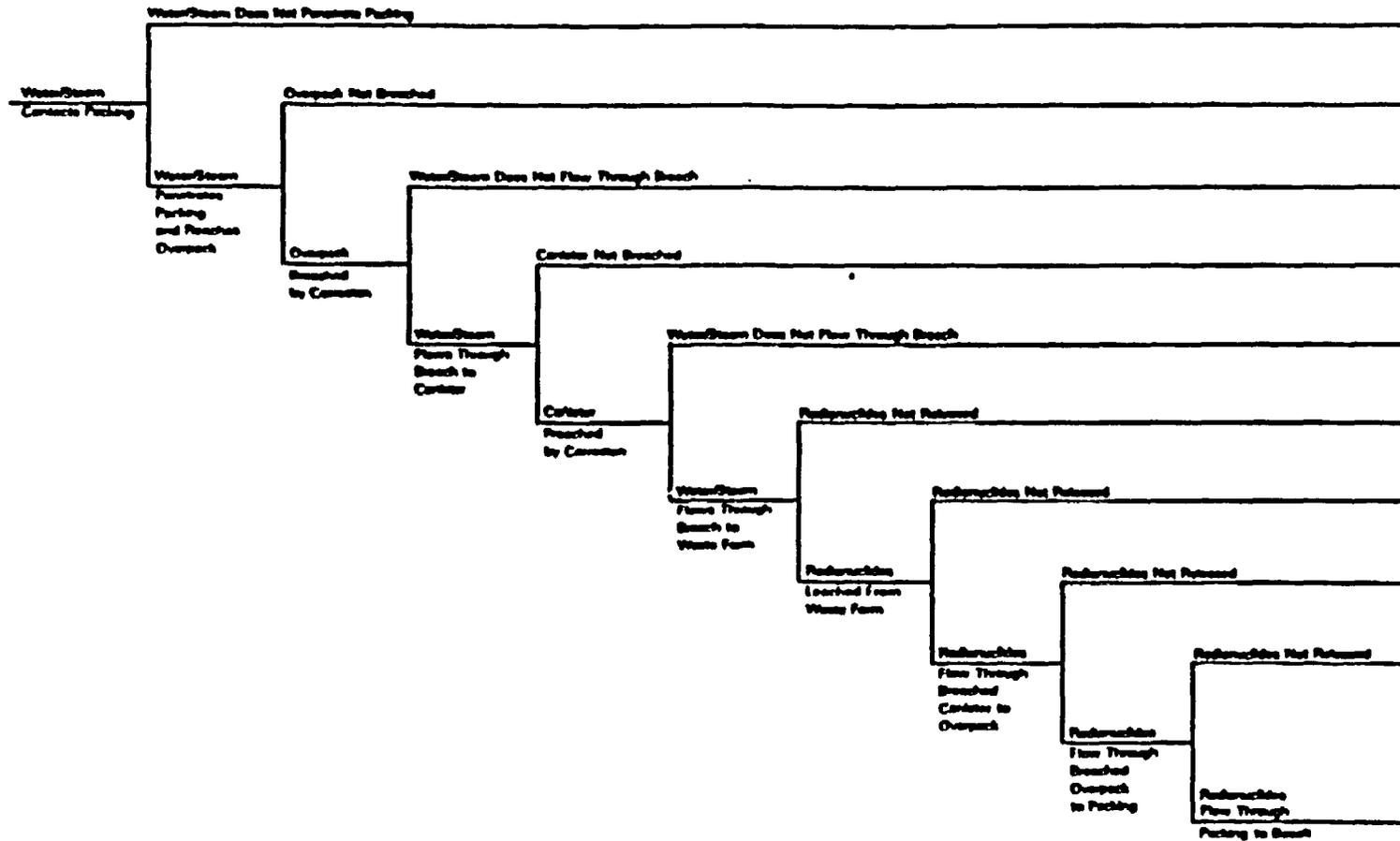


Figure C.1. CHLW Package Failure - Corrosion

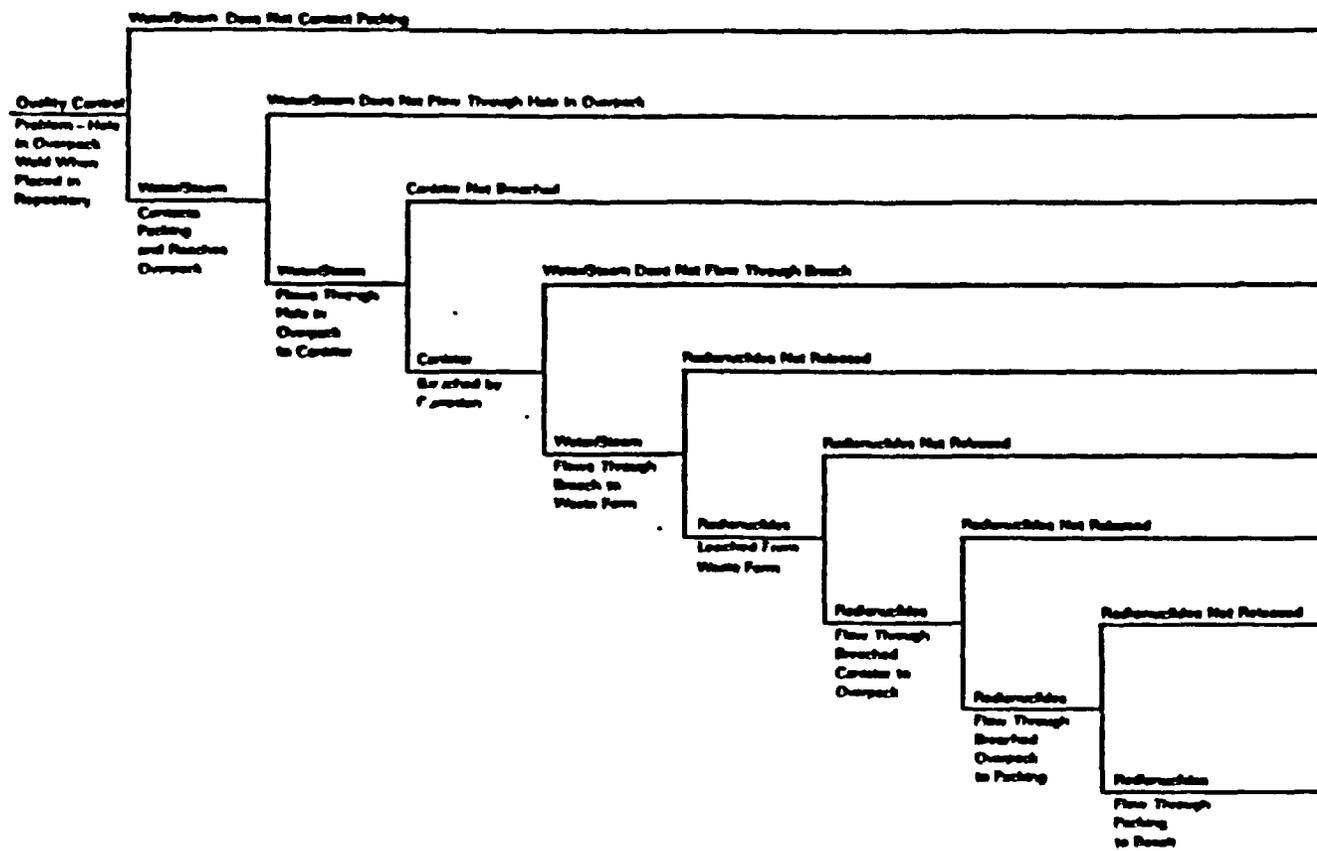


Figure C.2. CHEW Package Failure - Hole in Overpack Weld and Corrosion

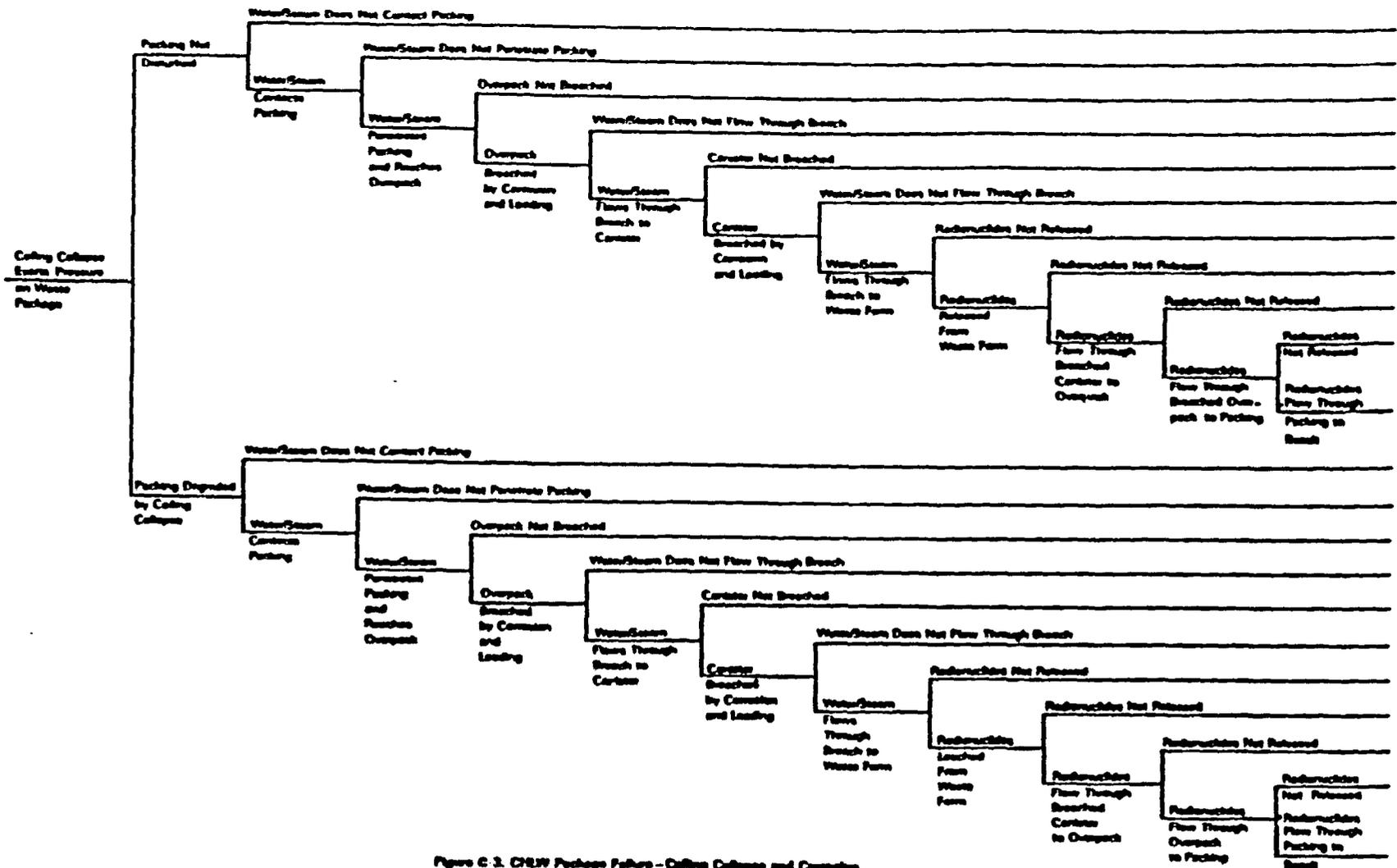


Figure C-3. CRW Package Failure - Coffing Collapse and Corrosion

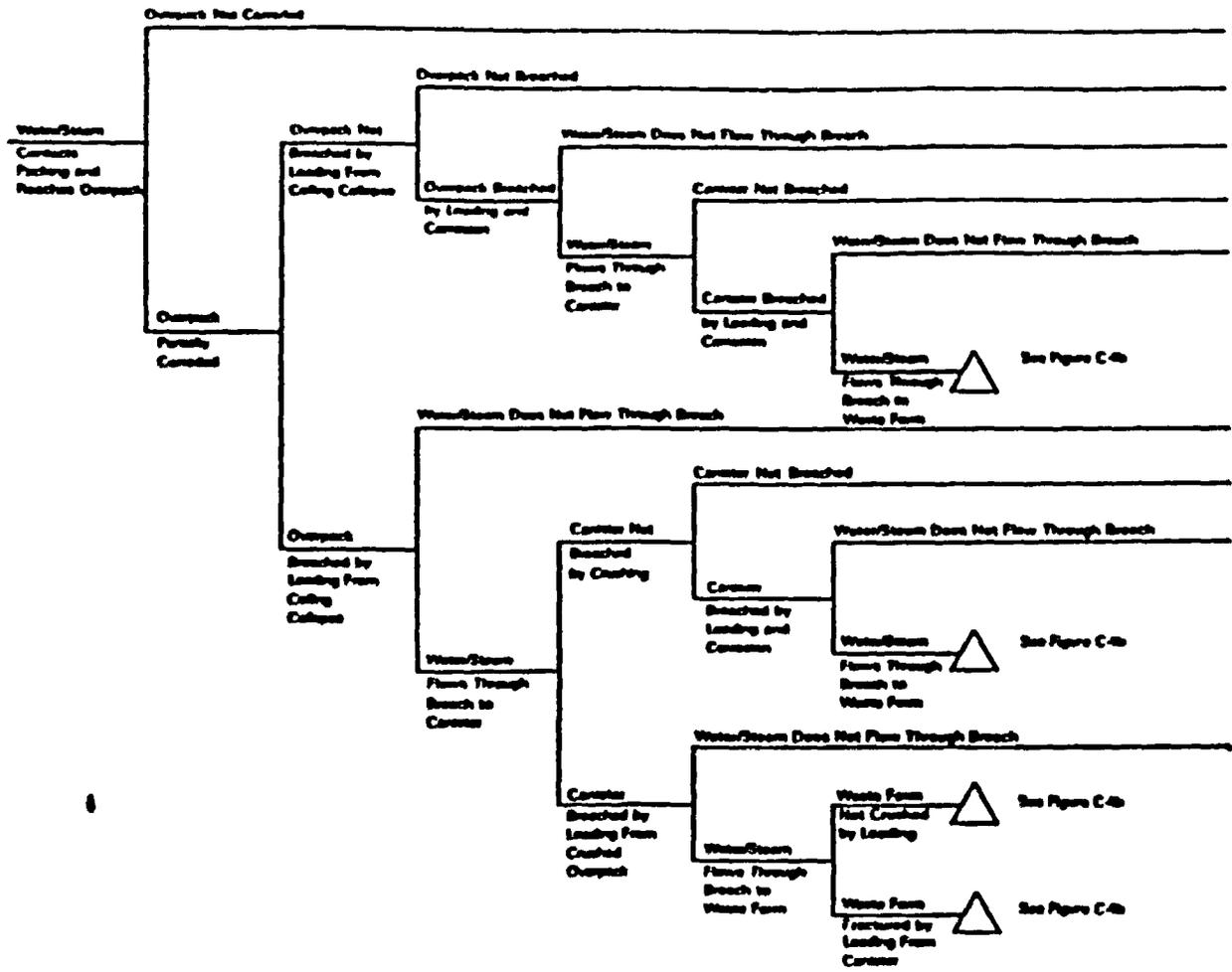


Figure C-4a. CRW Package Failure - Corrosion Followed by Loading From Ceiling Collapse

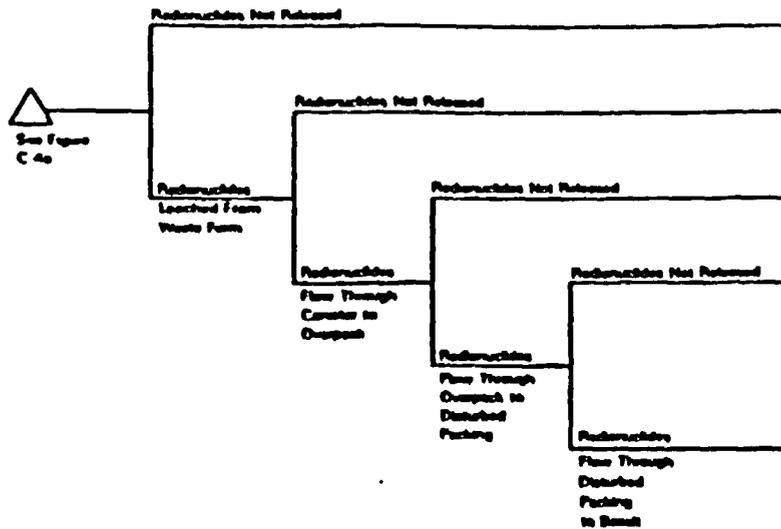


Figure C-4b. CHEW Package Failure - Corrosion Followed by Leaching From Colling Collapse (Cont'd)

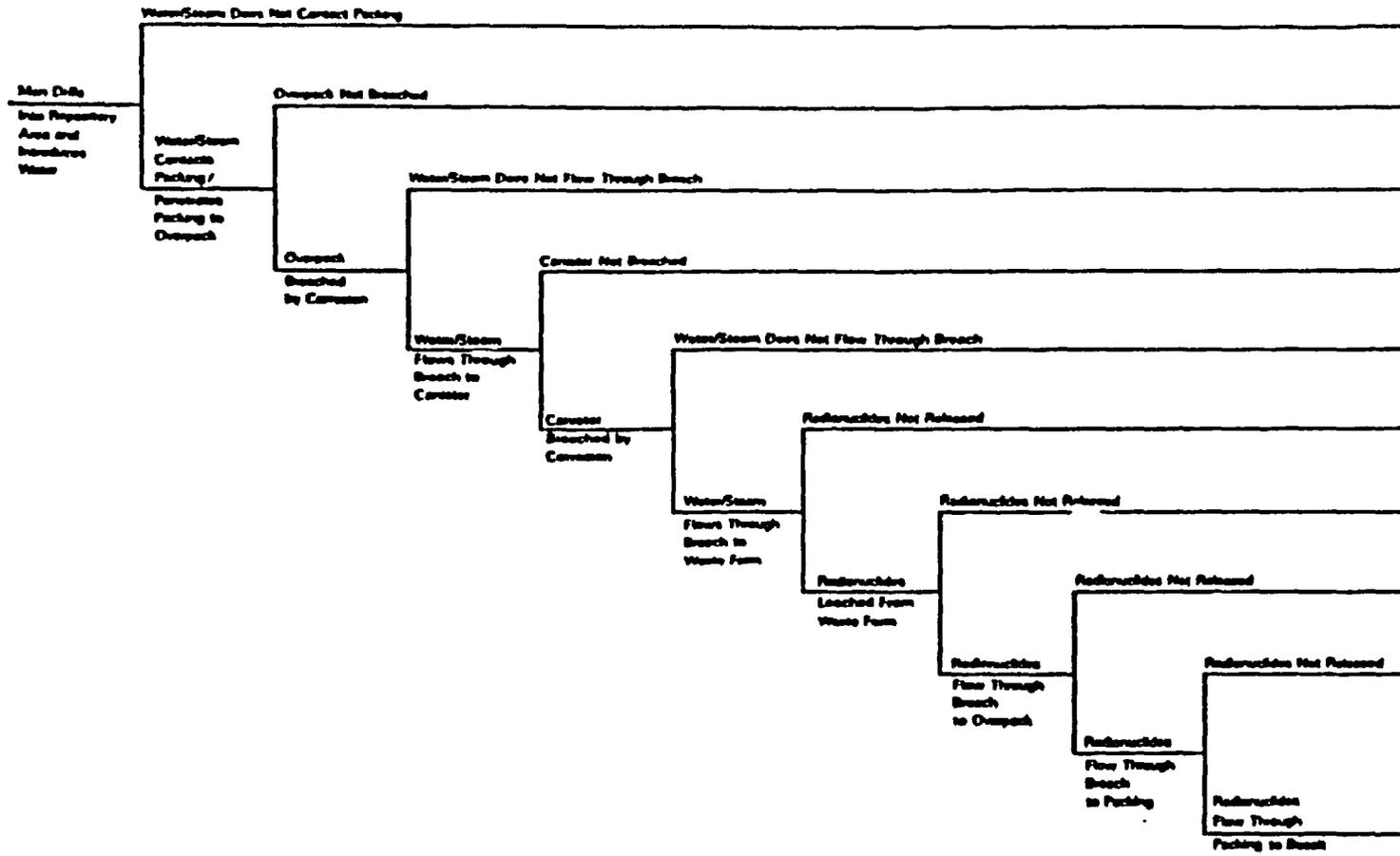


Figure C-8. CHEW Package Failure - Drilling Into Repository Area

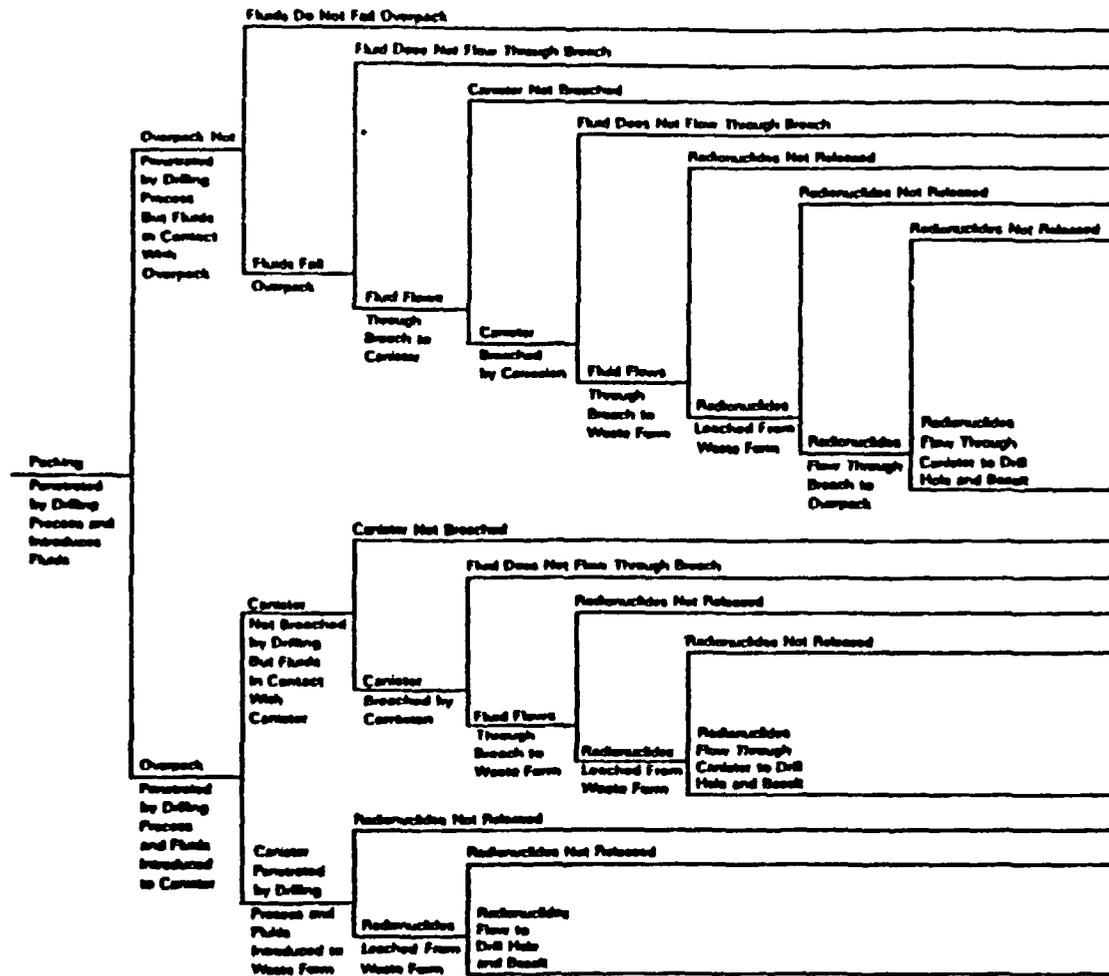


Figure C-6. CRW Package Failure - Drilling into Waste Package

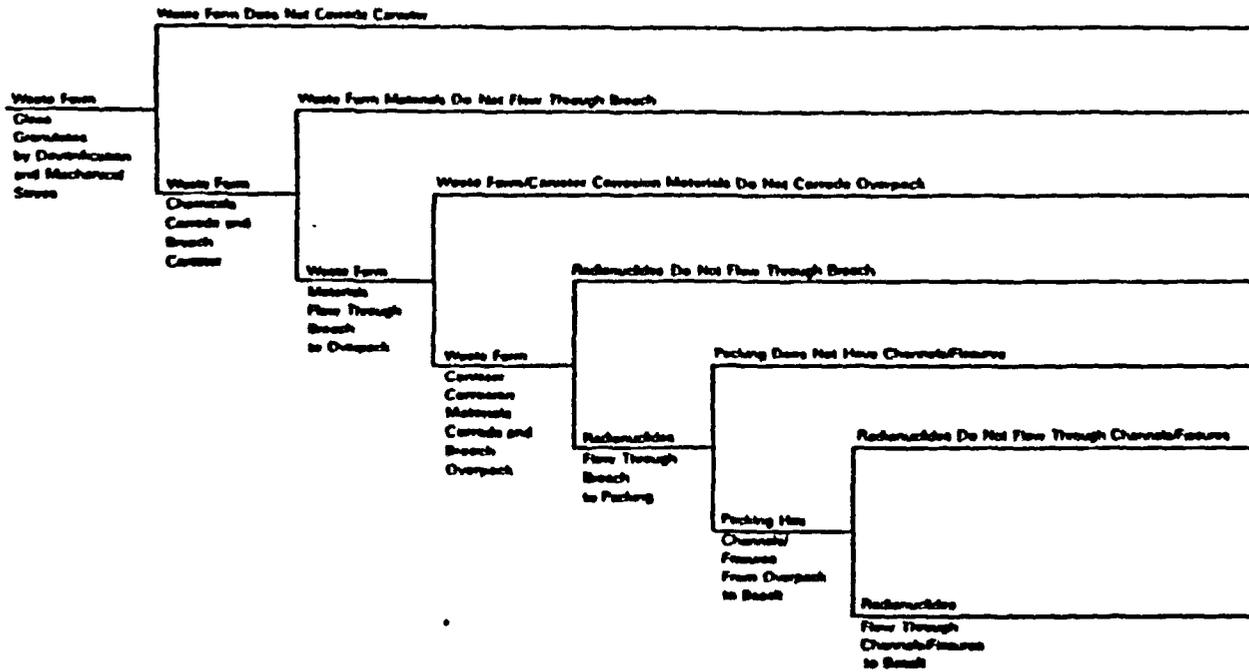


Figure C.7. CHW Package Failure - Mechanical Waste Form Failure and Internal Corrosion

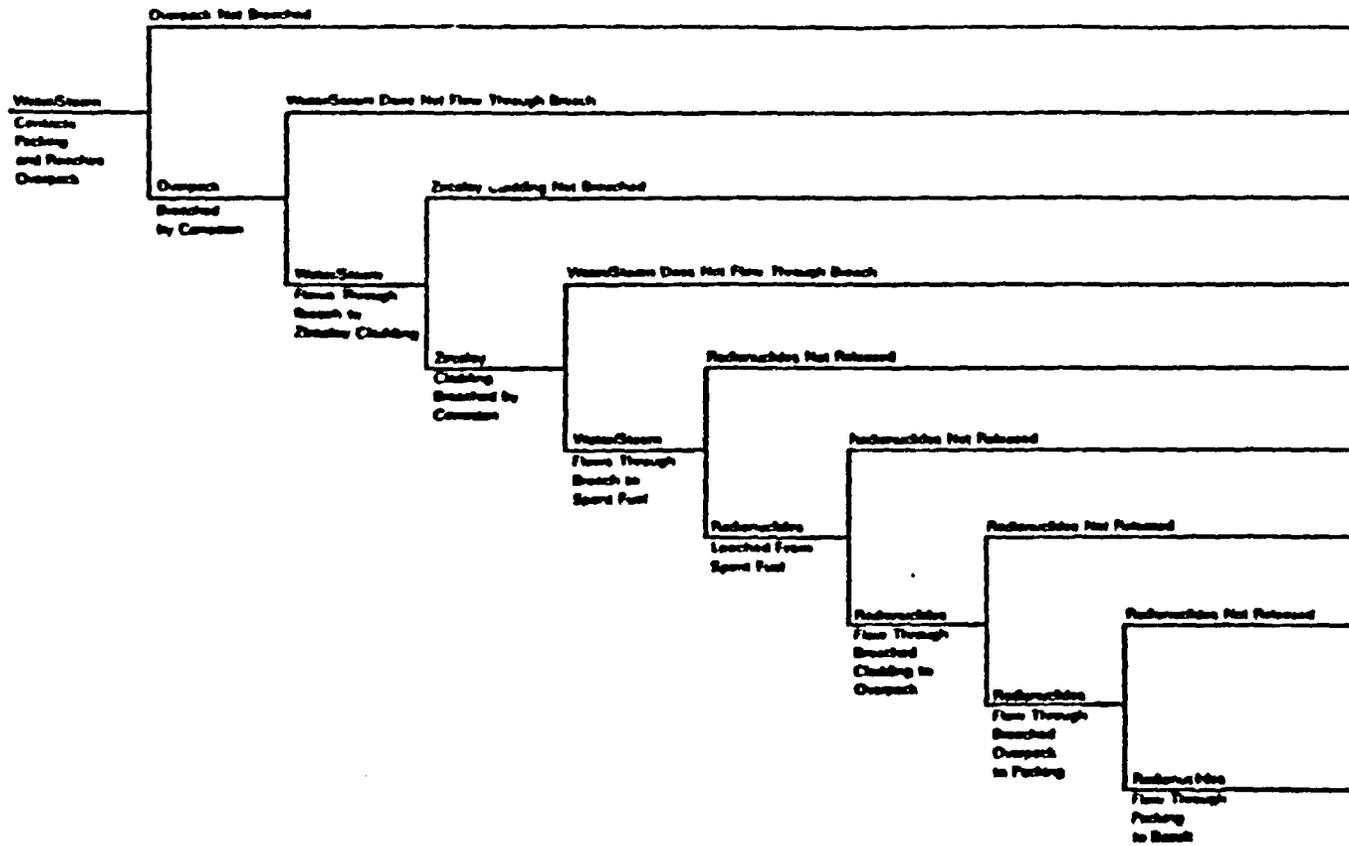


Figure C-8. SF Waste Package Failure - Corrosion

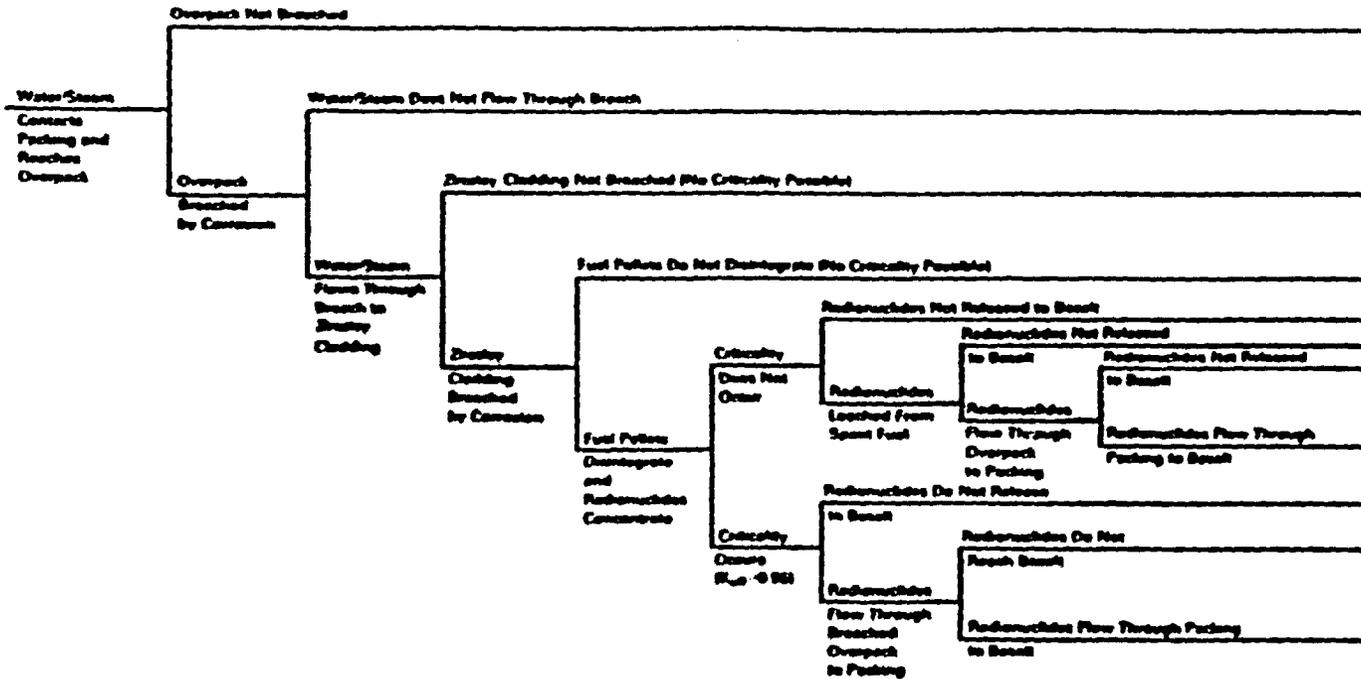


Figure C-8. SF Waste Package Failure—Corrosion Followed by Criticality

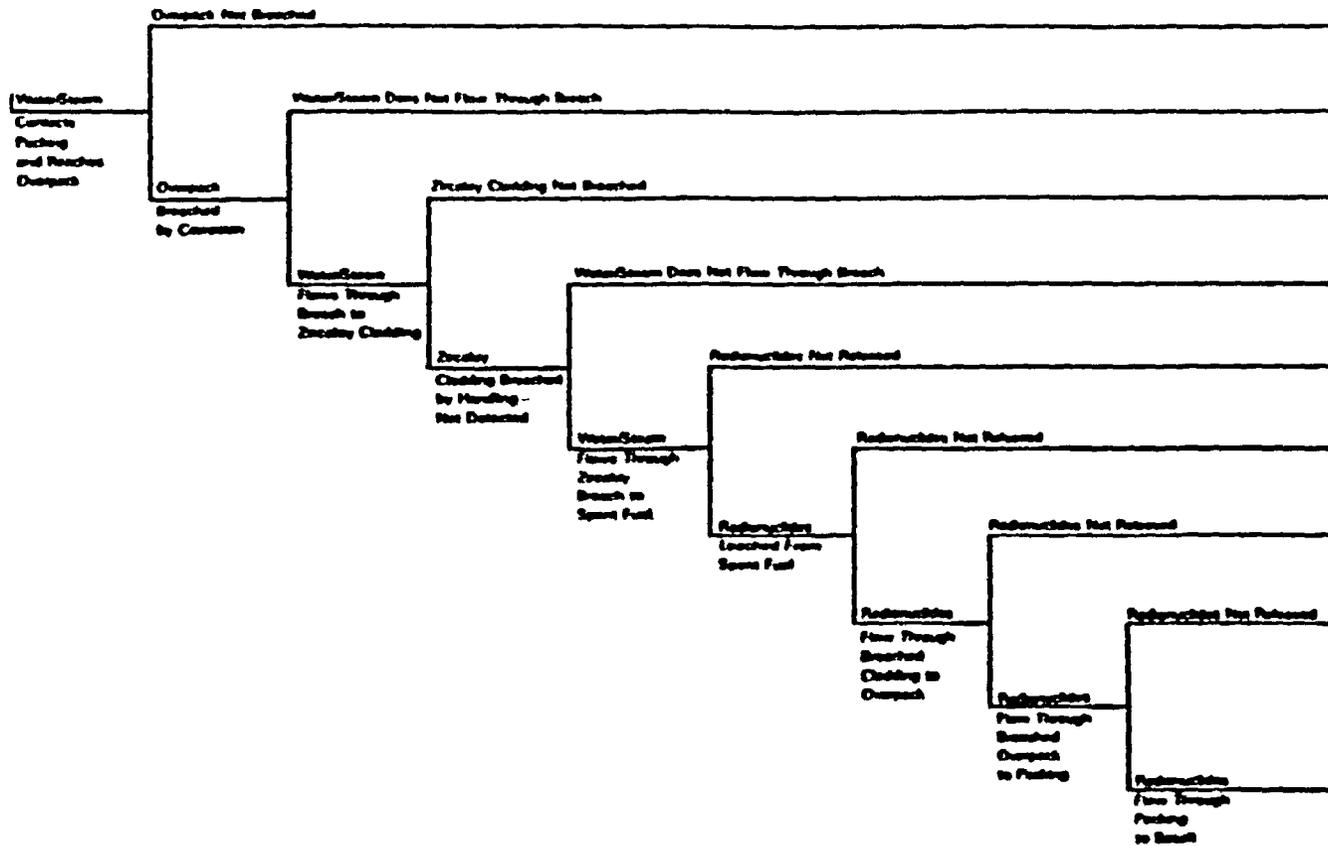


Figure C-18. SF Waste Package Failure - Handling/Quality Control and Corrosion

