

THE AEROSPACE CORPORATION



Suite 4000, 955 L'Enfant Plaza, S.W., Washington, D.C. 20024. Telephone: (202) 488-6000

4810-01.84.kws.04
7 February, 1984

Mr. Kien C. Chang
Mail Stop 623-SS
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

WM Record File
A-4165

WM Project LD, H, LK
Docket file
PDR
LPDR B, N, S

Distribution:
KC

Dear Mr. Chang:

(Return to Mail, 523-53)

DRAFT EVENT TREES

Attached are ten (10) copies of our draft document entitled, "Event Trees Depicting Release of Radionuclides from High-Level Radioactive Waste Packages". An Appendix to the document (included as a separate volume) contains the actual trees.

Please contact us if you have any questions.

Very truly yours,

Kenneth W. Stephens
Manager, Technology Assessments
Eastern Technical Division

KWS/gbf

cc: G.E. Aichinger SD/PMR (letter only)

Attachments

84 FEB -8 P 3:35

WM DOCKET CONTROL CENTER

B409120365 B40207
PDR WMRES EECAEROS
A-4165 PDR

An Equal Opportunity Employer

GENERAL OFFICES LOCATED AT 3500 EAST EL SEGUNDO BOULEVARD, EL SEGUNDO, CALIFORNIA

DRAFT

EVENT TREES DEPICTING RELEASE
OF RADIONUCLIDES FROM HIGH-LEVEL
RADIOACTIVE WASTE PACKAGES

January 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 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, the Nuclear Regulatory Commission 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 relate the research to the 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. The Aerospace project covers a period of 3 years, with all four tasks to be accomplished within the first year (fiscal year 1984), specifically for a basalt repository. The same basic scope for repositories in tuff and salt formations will be covered in the remaining 2 years, concurrent with further refinement of the analytical techniques.

CONTENTS

	<u>Page</u>
PREFACE	iii
INTRODUCTION	1
EVENT TREE METHODS	2
EVENT TREES FOR BASALT WASTE PACKAGES	3
Approach	3
Event Tree Discussions	6
CHLW Package Failure--Corrosion	6
CHLW Package Failure--Hole in Overpack Weld and Corrosion	8
CHLW Package Failure--Ceiling Collapse and Corrosion	8
CHLW Package Failure--Corrosion Followed by Loading From Ceiling Collapse	9
CHLW Package Failure--Drilling Into Repository Area	11
CHLW Package Failure--Drilling Into Waste Package	12
CHLW Package Failure--Mechanical Failure of Waste Form and Internal Corrosion	13
CHLW Package Failure--Earthquake	14
SF Waste Package Failure--Corrosion	15
SF Waste Package Failure--Handling/Quality Control and Corrosion	16
SF Waste Package Failure--Earthquake and Corrosion	16
WORK TO BE DONE	18
Expansion of Events	18
Synergistic Interactions Among Failure Modes	19
Mathematical Analysis Techniques	19
Data Requirements	20
REFERENCES	22
APPENDIX A. Event Trees	23
APPENDIX B. Mathematical Considerations in Fault Tree/Event Tree Analysis	24

EVENT TREES DEPICTING RELEASE OF RADIONUCLIDES FROM HIGH-LEVEL RADIOACTIVE WASTE PACKAGES

INTRODUCTION

This report presents the first version of event trees for radionuclide releases from waste packages for commercial high-level waste (CHLW) and spent fuel (SF) in a basalt repository (Westinghouse, 1982). This work is part of the overall project described in the Aerospace Program Plan (1983a). The complete project includes preparation of fault trees and event trees, an examination of other methods for analyzing waste package reliability, and quantitative reliability analyses of Department of Energy waste package designs, including projections of package lifetimes and radionuclide releases to the basalt. The event trees presented here are intended to provide a medium for discussion of the events resulting in radionuclide releases and a starting point in developing a methodology for quantifying waste package reliability.

Fault trees depicting the failure of high-level radioactive waste packages, which form the basis for the event trees, were presented in an earlier Aerospace document (1983b). That report discussed fault tree and event tree methodology in general, as well as examples of how those techniques have been used for other applications.

The event trees are presented in Appendix A (bound separately). Discussions regarding how the trees were developed and where the basic source information was obtained are provided in the body of the report.

Work remaining in refining the trees has been identified in the final section of this report. As comments are received and as developmental work continues,

these trees can be modified and additional trees can be generated as necessary. It is widely recognized that successful fault tree/event tree analysis requires extensive review and participation by as many knowledgeable persons as possible and that there must be sufficient time for reflection, incubation, and reiteration. In this regard, the Nuclear Regulatory Commission and its contractors should provide as much comment and participation as possible.

The section on work to be done includes a discussion of mathematical analysis techniques. Appendix B provides additional background on the analytical approaches.

EVENT TREE METHODS

As discussed in the fault tree document (Aerospace, 1983b), fault tree/event tree analysis has been used since 1961 for a variety of complex systems analyses, including the Reactor Safety Study (NRC, 1975). Persons desiring an overview of fault tree/event tree methods should consult the Nuclear Regulatory Commission procedures guide for probabilistic risk assessment (NRC, 1983).

Fault trees are developed by starting with an end event as the top of the tree and working backward through the precursor events. Event trees, on the other hand, begin with a defined initiating event and then work forward to examine the consequences of the event, the factors influencing mitigation of its effects, and the results of the sequence of events.

The convention followed for event trees is to divide the branches at each junction in the tree into a "success" (top branch) and a "failure" (bottom branch). The resulting sequence is thus identified by the possible paths that can be taken. For situations in which the safety system (barrier) can fail partially, but not necessarily totally, the success and failure states could have more branches, with each representing a specifically defined degree of failure (McCormick, 1981). However, in this report, the event trees have been restricted to the typical binary (success/failure) form. When the state of knowledge with respect to barrier failure processes is better understood, the failure branches could be

expanded accordingly. Added combinations would of course increase the complexity of the trees.

EVENT TREES FOR BASALT WASTE PACKAGES

Approach

Figures 1 and 2 show the reference waste package designs for CHLW and SF (Westinghouse, 1982) used in developing the fault trees and event trees. These designs are described in more detail in an earlier Aerospace report (1983b).

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.

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 water is the most probable initiator of corrosion. Thus, for each of the waste package designs (CHLW and SF), 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 A-1 and A-9) 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, and for the SF package, the Zircaloy cladding was assumed to have been breached in handling. 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

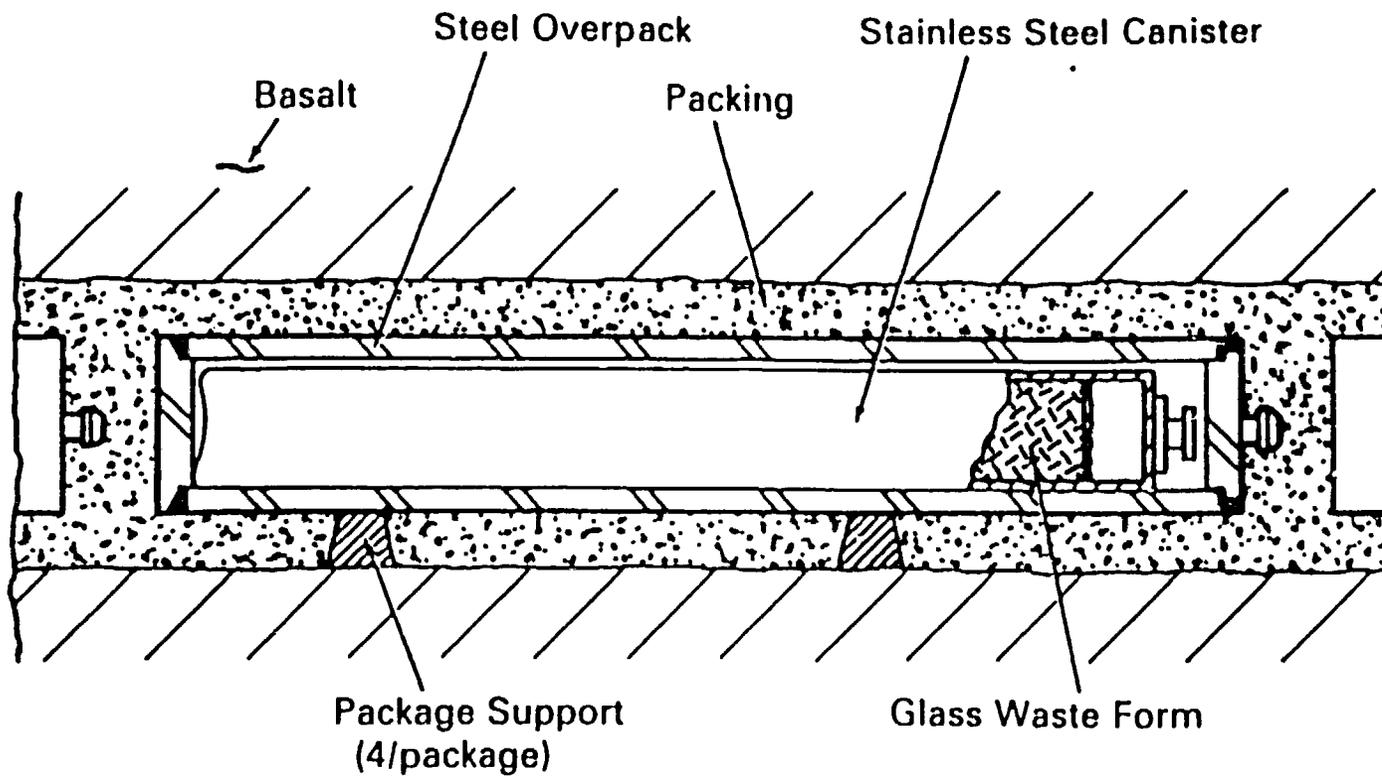


Figure 1. Reference Waste Package Conceptual Design for Commercial High Level Waste in Basalt (Westinghouse, 1982)

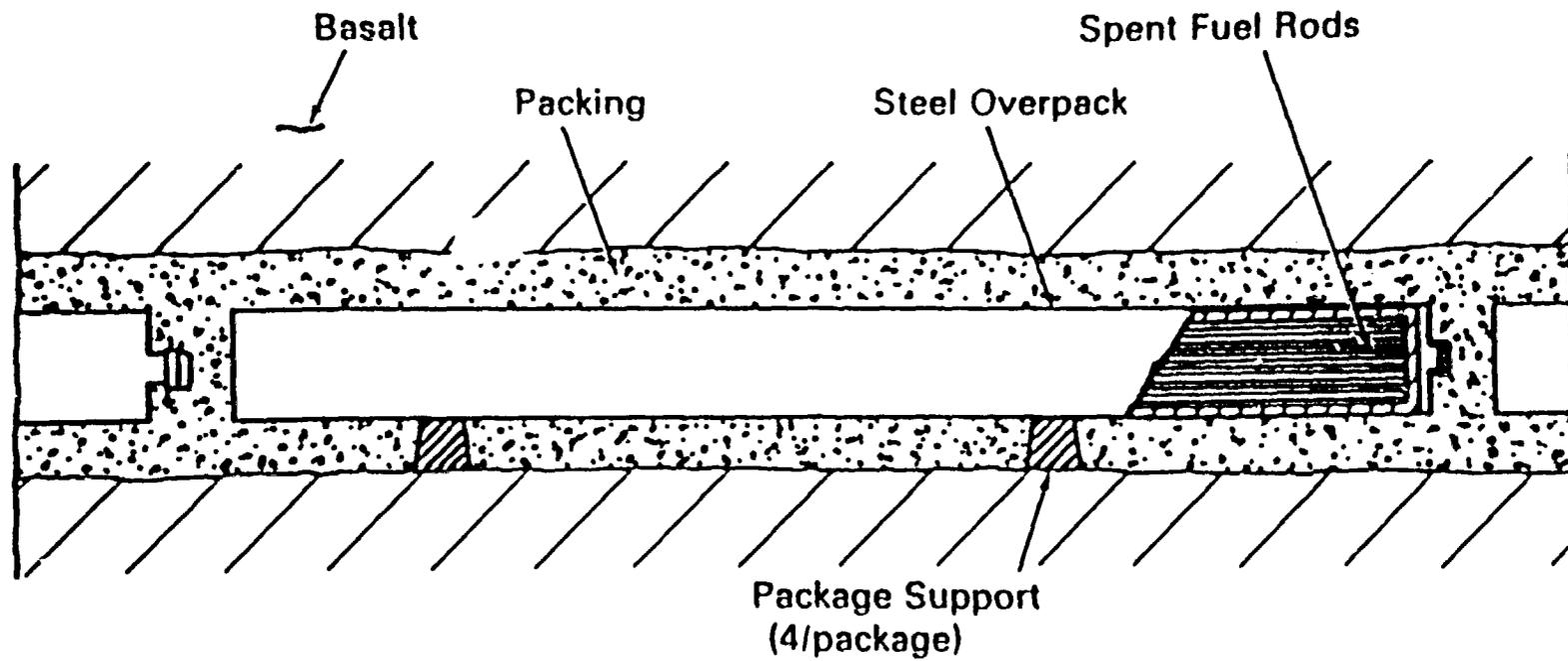


Figure 2. Reference Waste Package Conceptual Design for Spent Fuel in Basalt (Westinghouse, 1982)

scenarios that may not be dominant were included to illustrate how these scenarios could be represented. These include human intrusion into the repository (drilling), corrosion from within the package without water being the main contributor, and catastrophic events, such as an earthquake.

There is by no means unanimity in the scientific community regarding the significance of individual failure modes included in the fault trees and event trees. However, the trees provide a medium for discussion and, as they evolve, will serve to clarify the body of knowledge regarding the potential failure mechanisms. Later, if a consensus develops regarding the credibility of particular failure modes, it may be possible to adjust the trees by deleting failure modes and to simplify the calculations without harm to the overall analysis. However, any such deletion of failure modes would occur only after careful deliberation and would be well documented.

Event Tree Discussions

Of the many event trees that were considered, 11 have been developed for this document to illustrate the scenarios discussed above. Each of these event trees is discussed below.

CHLW Package Failure--Corrosion (Figure A-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 A-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 soluble 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 branch represents package failure. For example, given that the corrosion case diagramed 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 were postulated. Therefore, no subevents were developed for the success branches.

To derive the probability of occurrence of each event depicted in the tree, the conditions and subevents resulting in its occurrence must be incorporated. This requires a variety of input variables and their corresponding uncertainties. To determine the probability of water/steam penetrating 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 will require a determination of items such as the leach rate from the waste form and mass transport through the packing. These calculations would probably use models that are external to the event trees.

CHLW Package Failure—Hole in Overpack Weld and Corrosion (Figure A-2)

The scenario of failure depicted in Figure A-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 A-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 A-1.

The sequence of events diagramed in Figure A-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.

CHLW Package Failure—Ceiling Collapse and Corrosion (Figure A-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 A-3. For this scenario, the source of the loading was assumed to be provided by a collapse of the repository ceiling. The event tree comprises two major branches. Both branches are made 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 A-1). It is also expected that some mechanisms, such as stress corrosion cracking, would play a greater role than in Figure A-1. As discussed above, to determine the probability of occurrence of the events presented, the subevents, controlling factors, and interdependence between mechanisms should be incorporated.

CHLW Package Failure—Corrosion Followed by Loading From Ceiling Collapse (Figures A-4a and A-4b)

The scenario presented in Figures A-4a and A-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 A-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 A-4a is the same, so these four are depicted by the logic structure on Figure A-4b. Even though the logic of the branches is the same, the probabilities assigned to events of Figure A-4b are not necessarily the same when attached to each branch of Figure A-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 have fractured or remained intact. For both of these options, the water leaches the radionuclides, as presented in Figure A-4b. The leaching rates would be greater for the fractured glass versus the nonfractured glass, and correspondingly, the probabilities and rates of radionuclide release would be affected. Figure A-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 A-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 A-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.

CHLW Package Failure—Drilling Into Repository Area (Figure A-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. This assumes that the drilling penetration comes near the depth of the emplaced packages. 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 A-5 presents an event tree initiated by the event "drilling into repository area," and continued by the same sequence of events presented in Figure A-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 A-5 probabilities will not necessarily be equal to the probabilities that will be assigned to events in Figure A-1. For example, the probability of water reaching the packing* will most likely be greater in the Figure A-5 scenario than in the Figure A-1 scenario.

The probability of radionuclide release to the basalt in the scenario in which drilling into the repository area (Figure A-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 A-1). This is because the drilling scenario is a more restrictive case than the base case of Figure A-1—the differences in probabilities of radionuclide release between the two cases will depend in the former case (Figure A-5) on the probability of drilling into the repository area times the greater probability of water intrusion, breaching by corrosion, and radionuclide flow versus the probability of water intrusion, breaching by corrosion, and radionuclide flow in the latter case (Figure A-1). Further investigation will determine the probabilities to be used in the calculations.

CHLW Package Failure—Drilling Into Waste Package (Figure A-6)

The event tree initiated by the event of drilling into a waste package is presented in Figure A-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 contains two subscenarios: (1) the canister might also be 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 would flow immediately to the basalt through the drill hole.

The upper branch is similar to the scenario given for the corrosion case shown in Figure A-1, but there are some major differences. In Figure A-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.

The likelihood of drilling into the repository area and into a waste package is remote. 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 and new objectives may prompt drilling on this site.

CHLW Package Failure--Mechanical Failure of Waste Form and Internal Corrosion (Figure A-7)

As discussed in the earlier document (Aerospace, 1983b), internal corrosion modes have been postulated. The event tree presented in Figure A-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 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. It is

postulated that by then the packing has developed channels and fissures at suitable locations so that the radionuclides will 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 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.

CHLW Package Failure--Earthquake (Figure A-8)

Figure A-8 is a diagram of the scenario in which the waste package either fails completely or is not breached at all by the occurrence of a catastrophic

event. For the purposes of presentation, an earthquake was assumed to be the initiating event. In this case, it was assumed that if the waste package remained intact, no further mechanisms contributed to the failure of the engineered barriers. However, any number of subevents resulting in failure could be added to this branch (e.g., the events resulting from intrusion of water). The lower branch represents the immediate failure of the barriers provided by the packing, overpack, and canister. As a result, the waste form either would be placed directly in contact with the basalt host rock or left unprotected from any subsequent mechanisms that might result in radionuclide release (e.g., the direct contact of groundwater with the waste form). To determine the probability of complete failure of the waste package, the mechanisms and subevents resulting in failure as well as the input conditions should be incorporated.

In this event tree, an earthquake was used as an example of how catastrophic events can be represented. If such events can be dismissed a priori as being noncredible by virtue of low probability or if the waste package design and site selection processes cause the impact of such events to be of little consequence, catastrophic events would not necessarily have to be included in event trees. Also, event trees could be added to represent situations such as less severe earthquakes that would cause less than total failure of the waste package. An example of how effects of an earthquake combined with other events can be depicted is illustrated later in Figure A-11.

SF Waste Package Failure—Corrosion (Figure A-9)

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 A-9. 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, 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 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 A-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.

SF Waste Package Failure—Handling/Quality Control and Corrosion (Figure A-10)

The scenario presented in Figure A-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 A-9. However, because the Zircaloy is already breached, the information used to determine the probability of occurrence and time to failure would differ.

SF Waste Package Failure—Earthquake and Corrosion (Figure A-11)

The event tree presented in Figure A-11 considers a series of events that begin with 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 the earthquake and proceeds to the possibility of water or steam contacting the packing and then reaching the overpack surface.

At this point, two major branches are established: the upper branch (the overpack is not breached by the earthquake) 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 A-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 A-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 A-11 produces two basic source terms, 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.

WORK TO BE DONE

As discussed previously, event trees and fault trees are interrelated; fault trees graphically show potential events that result in determining the probability of system failure, whereas event trees use the same events to focus on specific sequences of events leading to failure. Because of their interrelationship, the work remaining to be done affects both fault and event trees. In the fault tree report (Aerospace, 1983b), several areas requiring further consideration were mentioned: expansion of some events, synergistic interactions among failure modes, mathematical analysis techniques, and data quantification needs. These items and their effect on the development and quantification of the fault and event trees are discussed below.

Expansion of Events

In fault tree analysis, the lowest level of detail in the tree is represented by two types of events: those represented by circles, which are considered basic events needing no further expansion, and those represented by diamonds, which denote that the event might be expanded further. Use of a diamond does not imply that the event must be expanded in order to make effective use of the tree.

For the existing fault trees, a number of events have been left as diamonds. The intent is to expand as many of these events as is practical. However, a sizable portion of them have actually been carried as far as the state of knowledge at this time allows. Accordingly, such events will be considered "basic" events until expansion is feasible. When the trees are quantified, probabilities can be attached to the bottom-level events, whether they are represented by diamonds or circles. The lower an event is in the fault tree, the less likely it is to have a dominant effect on the top event in the tree. Thus, it may not be cost effective to expand all the lower events to the ultimate limit. In this regard, reviewer comments on the significance of particular bottom-level events will help focus future efforts. Because event trees depict the sequential relationships among these events, expansion of the fault trees may require modification to the event trees.

Synergistic Interactions Among Failure Modes

In the existing fault and event trees, relationships involving more than one failure mode have been diagrammed to the extent of current information (e.g., corrosion plus structural loading). However, the question of actual synergism has been raised, especially for chemically related failure modes. If synergistic relationships can actually be hypothesized in sufficient cause-effect detail, they can be added to the trees. The current state of knowledge does not permit that, but synergisms may be incorporated at some future date if better information is available.

Mathematical Analysis Techniques

CHLW package failure requires the failure of the four package barriers: packing, overpack, canister, and waste form. As described in this and a previous Aerospace report (1983b), the waste package is represented in fault trees as a parallel system in which all barriers must be in a failed state by a particular time for the waste package to have failed. According to the Boolean laws of probability generally used in computer assessment of these trees, the probability of the top (final) event is the product of the probabilities of each of the four barrier failures. This mathematical technique, however, has difficulty accounting for the interdependence of the various waste package barriers. This interdependence arises from the effects that the time of occurrence of the failure of one barrier can have on the failure rate of subsequent barriers. This time dependency can easily be confused with two other types of time-variant probabilities: the cumulative effective of a constant failure rate and a time-variant failure rate. It is important to distinguish among these types because the latter two can be handled by standard computer codes, while the first type of time dependency requires a more sophisticated mathematical treatment than Boolean algebra.

Probability distributions describing sequential barrier failures are computed from integral expressions of joint probability distributions, as described by Martz and Waller (1982) and Dhillon and Singh (1981). However, because of the

complexity of the relationships, defining, solving, and checking these equations for the entire waste package fault tree is a very difficult task that may not be feasible in practice. A more detailed discussion of this technique is found in Appendix B.

An alternative approach to determine the distribution of failure probabilities over time is to first examine the occurrence times of each failure mode. If the failure times can be computed for a large number of simulated failure events, then the desired overall failure probability distribution can be developed. Failure times are then determined by simulation using random (Monte Carlo) selection from probability distributions reflecting the uncertainties in the input data.

Multiple failure modes in a single event tree branch can be accommodated with this approach. Finding shortest event times is much easier than computing the joint probability distribution functions for multiple failure modes. Use of multiple failure modes within one event tree branch is important because it allows a substantial reduction in the number of event trees that must be developed.

An additional consideration is the event sequences. Complex event sequences are produced when the order of occurrence of the key events cannot be specified in advance. Complex event sequences are difficult to model using conventional programming languages. Therefore, the use of computer languages specially designed for discrete event simulation can greatly reduce the programming effort. These topics are discussed further in Appendix B.

Data Requirements

The data requirements for the alternative approach described above are the same as the requirements for a direct computation of probabilities using standard mathematical techniques. The input would come from analysis of research data, such as that provided by laboratories working on the waste repository program. Examination of data to date, however, reveals that although a great body

of research exists regarding the topics of interest, most of the results have not been reported in a probabilistic form that readily lends itself to fault tree/event tree analysis. Consequently, quantification efforts pursued prior to the completion of at least a portion of the work now in progress by the Department of Energy and others should be considered only as prototypical and would involve considerable approximation, judgment, and perhaps speculation.

The order of tasks in this project is such that the development of fault trees/event trees will be followed by a review of the methods used by the Department of Energy and others for waste package performance assessment. Subsequently, a decision will be made jointly with the Nuclear Regulatory Commission regarding the technique to pursue for determining waste package lifetimes and radionuclide release quantities. The technique chosen may consist of fault trees/event trees, another method, or a combination. At this time, the level of information available on the techniques the Department of Energy will use is not sufficient to make a determination of the preferred technique for quantification in this project. Accordingly, the issue of availability and adequacy of data for fault tree/event tree quantification will remain open for the time being.

REFERENCES

The Aerospace Corporation, 1983a, "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, 1983b, "Fault Trees Depicting Failure of High-Level Radioactive Waste Packages," Draft, Washington, D.C.

d'Alessandro, Marco, and Arnold Bonne, 1983, "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.

Dhillon, B.S., and C. Singh, 1981, "Engineering Reliability, New Techniques and Applications," Wiley-Interscience.

Martz, H., and R. Waller, 1982, Bayesian Reliability Analysis, Wiley and Sons.

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 II and III.

NRC, 1983, "PRA Procedures Guide—A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, Nuclear Regulatory Commission, Volumes 1 and 2.

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

APPENDIX A. EVENT TREES

Bound Separately

APPENDIX B.
MATHEMATICAL CONSIDERATIONS IN FAULT TREE/
EVENT TREE ANALYSIS

COMPUTING PROBABILITIES

CHLW package failure requires the failure of the four package barriers: packing, overpack, canister, and waste form. The waste package is represented in fault trees as a parallel system in which all barriers must be in a failed state by a particular time for the waste package to have failed. According to the Boolean laws of probability generally used in computer assessment of these trees, the probability of the top (final) event is the product of the probabilities of each of the four barrier failures. In fault trees, a parallel system is represented as events connected by an AND gate. In event tree format, the same events are shown in a linear sequence, each step of which must be taken to result in system failure. In either case, the probability of failure is the product of the probability of failure of each of the four barriers.

Most computer codes used to evaluate fault trees use the simple multiplication and addition of probabilities for AND and OR gates to produce the system failure probability. This ignores the effect of the time of failure of one barrier on the probability of failure of the next barrier. When barrier failure by wet corrosion is considered, the importance of the interdependence of failures is obvious. Clearly, the occurrence of corrosion failure of the overpack with subsequent water penetration to the canister has much to do with the probability of corrosion failure of the canister. This interdependence requires a closer look at time dependencies in general.

TIME DEPENDENCIES

There are several distinct types of time dependencies in the probabilities associated with failure of the waste package. The following types are discussed

below: cumulative effect of a constant failure rate, time-variant failure rate, and convolution with prior events.

- Cumulative Effect of a Constant Failure Rate--The simplest situation is that of a component with a failure rate that does not change with time, e.g., the probability of failure of an unstable atom by radioactive decay. However, if one computes the probability that it has decayed over a certain span of time then that probability is time dependent. If λ = the instantaneous failure rate, then the probability that failure occurs sometime within time span, t , is

$$P1 = 1 - \exp(-\lambda t) \quad (1)$$

Any random event clearly depends on time in this sense. This does not pose a problem for the fault tree approach. The probabilities for each primary event in the fault tree can be recomputed for any elapsed time period. When new primary event probabilities are established, the probabilities of the top event can be computed for each time period using Boolean logic or a standard computer program.

- Time-Variant Failure Rate--Some components are subject to failure rates that change with time. Electrical and mechanical devices, for example, often have failure rates that vary corresponding to break-in and wear-out periods. One might expect the overpack failure rate due to corrosion to increase with time because of increasing corrosion damage. Under these circumstances, the probability of overpack failure over a specified time period would be influenced by the dual effects of the increasing failure rate, $\lambda(t)$, and the accumulated changes due solely to the passage of time. The equation for the probability of failure within time span, t , is

$$P2 = 1 - \exp\left(-\int_0^t \lambda(y) dy\right) \quad (2)$$

Vesely (1970; 1971) recognized the importance of time-variant failure rates and developed the PREP-KITT codes that compute this type of time-dependent probability for nuclear reactors. He describes these methods as Kinetic Tree Theory.

Component failure probabilities derived for either of these two kinds of time dependency can be manipulated using Boolean logic to produce the probability of the top event (package failure). Thus, for any particular span of time, the probabilities may be multiplied or added depending on whether they are connected by AND or by OR gates.

- Convolution With Prior Events—A situation fundamentally different from cumulative effects or time-variant failure rates arises when the probability of one event depends on the time of occurrence of a prior event. This situation is called "load sharing" (Martz and Waller, 1982) "sequential systems" (McCormick, 1981), or "standby systems" (Dhillon and Singh, 1981). The nuclear waste repository clearly has elements of a sequential system. When considering the progress of water from the repository to the waste form by the corrosion mechanism, one would expect the probability that radionuclides have been leached from the glass to depend on when the canister was breached by corrosion, which in turn depends on when the overpack failed, which in turn depends on when the backfill failed. Equations developed for the nuclear waste repository (Pritzker and Gassman, 1979) are as follows:

$$f_0(t) = \int_0^t f_a(t_1) \int_{t_1}^t f_b(t_2 - t_1) \int_{t_2}^t f_c(t_3 - t_2) f_d(t - t_3) dt_3 dt_2 dt_1 \quad (3)$$

where f_0 = overall failure density function;

f_a, f_b, f_c, f_d = the failure probability density functions for the barriers in standby redundancy with sequence a, b, c, d;

t = time of failure of barrier d;

t_1 = time of failure of barrier a;

t_2 = time of failure of barrier b; and

t_3 = time of failure of barrier c.

In addition to the top four events, other events within the fault tree may be similarly interdependent. To produce theoretically sound calculations of package failure using the convolution approach, very complex integral expressions of composite probability distributions must be developed. Defining, solving, and checking these equations for the entire fault tree is a very difficult task that may not be feasible in practice.

There may be fault tree computer programs that provide for analysis of standby systems, but in the documentation reviewed so far, there is no mention of this type of program. Several programs deal with independent events with time-variant probabilities, but they do not appear to deal with probabilities that depend on the time of occurrence of prior events in the sense of the convolution integral.

Time of Failure Versus Probability of Failure

The difficulties of convolution of prior events lead to consideration of alternative approaches. One useful approach is to examine the time of occurrence of each failure. With this approach, one postulates that the failures will in fact occur, and the key question becomes whether the time of failure is before or after the time period of interest. This does not change the criterion for failure. However, the focus is now on computing and combining failure times rather than failure probabilities. This new focus greatly facilitates computations and the use of Monte Carlo simulation.

Computing Failure Times

Expected failure time for each barrier can be computed from the same type of observational data required for direct computation of failure probabilities. Several papers discuss the use of cumulative probability distributions to describe the time of occurrence of events related to waste package performance. For example, Baca and Wilde (1983) show a projected median time of 875 years for a 0.15-m packing thickness to contain radionuclides (ignoring other barriers). They express their data as a cumulative lognormal distribution showing that the time of occurrence of radionuclide release can take on a variety of values. The cumulative distribution curve was developed using a set of hydrogeologic parameters reflecting the uncertainty and spatial variability in the true values at the Hanford site. The authors cite the usefulness of such curves in Monte Carlo simulation determination of containment time for the waste repository.

Simple Event Sequences

If a simple linear sequence of events leading to failure of the waste package is proposed, then the total time for failure can be readily determined as the sum of the times for each event. Specifically, the time required for waste package failure might be described as follows: Water penetrates the packing in time, t_1 ; water corrodes through the overpack in t_2 additional years; it corrodes through the canister in t_3 more years; it leaches radionuclides from the waste

form t_4 years later; radionuclides escape the packing after t_5 more years. The total time for package failure could be computed as the sum: $t_1+t_2+t_3+t_4+t_5$. Because of uncertainty and variability in the parameters controlling the process times required, these times could be treated as random variables, and the times could be drawn from the appropriate probability distributions using Monte Carlo sampling. Each pass through a Monte Carlo program would result in a new set of times and therefore a new total elapsed time for package failure. The trials would be repeated until the mean time over all trials converged on a single value. The statistical law of large numbers guarantees that the mean of these samples will converge on the true mean if enough trials are conducted. Only a simple computer program would be required to expedite the numerous samplings and subsequent additions for a linear sequence of barrier failure events.

Multiple Failure Modes

The simple sequence model can cover more failure types than one might first suppose. If the event tree branches are identified with specific barriers, the same tree branch can be used in assessment of a variety of failure modes for that barrier. For example, if the tree branch corresponds to breaching the canister, then the various types of corrosion might be distinct failure modes listed for that branch. This approach produces fewer numbers of trees at the expense of having fairly complex formulas at each branch for computing failure times.

A key problem in this analysis is how to compute the time required for one branch failure if that branch has several failure modes. If there were no random variability in the process times for each failure mode, then the time required for branch failure would simply be the time of the fastest failure mode. This is the situation implied by the use of deterministic models that analyze in great detail whatever is believed to be the fastest destructive process, while ignoring the slower destructive processes.

However, uncertainties in the environmental conditions that would be applied to the barriers (e.g., ion concentrations, temperatures) produce uncertainty in the occurrence times of each process. This implies uncertainty in the knowledge of which failure mode will really be dominant in that branch. This uncertainty would be very difficult to handle correctly using deterministic models, but is fairly straightforward when using Monte Carlo models.

Using the Monte Carlo approach, for each trial run, a new sample would be taken from the appropriate probability distribution to determine the occurrence time for each of the possible failure modes. The minimum of these times would be the occurrence time for the branch for that Monte Carlo trial. As the process is repeated over many trials, each failure mode would contribute appropriately to the determination of the failure time of the branch. Thus, rare but fast-acting failure modes such as earthquakes could be assessed along with likely but slow-acting modes such as general corrosion.

Even failure modes that have no development time, such as preexisting flaws in the barrier, could be assessed along with the other modes. A certain fraction of the Monte Carlo runs would encounter a zero time-to-failure for barriers corresponding to the probability that the barrier is flawed.

Complex Event Sequences

With a fixed design for the waste package, the sequence of barriers that must be breached is constant, implying a corresponding constant sequence of event tree branches. However, certain events may occur that would alter the sequence. Earthquakes or mining and drilling operations for example may occur at any stage in the system life. Introduction of such new events alters the event sequence and perhaps should be modeled by new event trees. Catastrophic events are capable of widely varying degrees of damage to the barrier system. The packing might be partially removed, water channels might be opened to the repository, the overpack and canister might be damaged, etc. In addition to catastrophic events, certain types of failure modes also can alter the sequence of barrier failure events. Internal barrier failure modes such as radiation

damage and nonaqueous corrosion operating concurrently with attack on external barriers confounds attempts to establish a fixed linear sequence of events.

If there is no fixed linear sequence of events, it may be difficult to sum event times to get the failure time for the waste package. It might be possible to delineate the most important event trees, each representing a fixed linear sequence, and compute the failure time probability distribution for each tree. Quantifying several of the important event trees would be interesting and instructive, but determining the probability of failure for the overall system requires quantification of essentially all possible event trees.

Because there are many ways to sequence events, it is difficult to enumerate them all. Simultaneous internal and external corrosion, earthquakes, tunnel collapse, drilling, water intrusion, etc., can happen in any sequence, and the order of occurrence of these events can have major effects on the computation of failure times for the barriers. Development of a conventional computer program requires a fixed prescription of event sequences. Because enumeration of these sequences in advance poses difficulties, a better approach might be to develop an algorithm that generates the event sequences as it computes the failure times. To understand how this might be done, it will be useful to first discuss the basics of discrete event modeling.

Discrete Event Modeling

Simulation programs model a system as it evolves over time by executing equations that produce changes in the state variables. Typical state variables for package failures would include continuous variables such as corrosion pitting depth, remaining load bearing capacity of the overpack, etc. State variables might also include discrete indicators of system status such as "canister breached" or "packing breached," etc.

The equations that pertain to a particular process are usually grouped together in a subroutine. In conventional programming, these subroutines are called in a fixed sequence by the main program. In a discrete event simulation

program, subroutines need not be called in a fixed sequence; the sequence is determined by the dynamics of each particular simulation run. In such programs, each set of process equations can be defined as an "event routine," and may be scheduled by an event timing routine.

A key feature in simulation programming is that one event may cause the scheduling of another event, which in turn can schedule another event, so that a whole sequence can be scheduled by the initial occurrence of a single event. For example, an earthquake that breaches the packing and stresses the overpack might be modeled by an earthquake event and an overpack failure event. Equations coded in the earthquake event routine could determine the time required for corrosion destruction of the overpack using the information that the packing was breached and the overpack is under stress. Synergistic effects on destruction time, to the extent that they can be quantified, can be programmed into this event routine. The earthquake event routine would schedule the occurrence of an overpack failure event for a future time. That future time would be the current simulated time plus the corrosion destruction time just determined.

Several processes might be able to destroy the overpack, so there could be overpack failure events scheduled by each process. The timing routine, a special subroutine preprogramed into some simulation languages, keeps track of all events. The timing routine triggers execution of each event in order according to its scheduled time.

Each Monte Carlo pass through the simulation routine can generate a different event sequence and timing. Thus, both the causal modes and the time of failure of the waste package can vary from run to run. There is no guarantee that a Monte Carlo approach, even with thousands of repeated trails, will produce all possible event sequences. However, the sequences produced will occur with frequencies approaching their true occurrence probabilities. Thus, any sequences that are missed should be exceedingly rare in nature.

Systems that can be altered by random, interactive events occur in many applications, not just the nuclear waste package. Recognizing the importance of this kind of problem, the RAND Corporation developed a systematic approach to discrete event modeling about 20 years ago. Under contract for the Air Force, they developed a computer language, SIMSCRIPT, specifically for discrete event modeling (Russell et al., 1973). Since that time, the language has enjoyed wide use, has undergone continuous improvements, and is now considered to be one of the best discrete event simulation languages available. Proponents of the method commonly cite a 5:1 advantage in programming time for SIMSCRIPT versus FORTRAN.

The use of SIMSCRIPT or a similar language makes the programming required for evaluation of the reliability of the waste package using the Monte Carlo approach manageable. Such a program could provide information on the relative impact that each failure mode is likely to have on the overall system. Thus, design and licensing decisions could be based on an overall integrated systems approach.

REFERENCES

Baca, R.G., and R.T. Wilde, 1983, "Principal Elements of the Basalt Waste Isolation Project Performance Assessment Studies," Civilian Radioactive Waste Management Information Meeting.

Dhillon, B.S., and C. Singh, 1981, "Engineering Reliability, New Techniques and Applications," Wiley-Interscience.

Martz, H., and R. Waller, 1982, Bayesian Reliability Analysis, Wiley and Sons.

McCormick, N.J., 1981, Reliability and Risk Analysis, Academic Press.

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

Russell, E.C., P.J. Kiviat, R. Villanueva, and H.M. Markowitz, 1973, "SIMSCRIPT II.5 Programming Language," Consolidated Analysis Centers, Inc.

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

_____, 1971, "Reliability and Fault Tree Applications at the NRTS," IEEE Transactions in Nuclear Science 18.