BNWL-SA-6064
Conf-770611--39

A RISK ASSESSMENT METHOD FOR NUCLEAR FUEL CYCLE OPERATIONS

For presentation at the American Nuclear
Society 23rd Annual Meeting
June 12-16, 1977
New York, New York

by
P. J. Pelto
W. K. Winegardner

BATTELLE
Pacific Northwest Laboratories
Richland, Washington 99352

PREPARED FOR THE U.S. DEPARTMENT OF
ENERGY UNDER CONTRACT EY-76-C-06-1830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

BNWL-SA-6064

A RISK ASSESSMENT METHOD FOR NUCLEAR FUEL CYCLE OPERATIONS

P. J. Pelto and W. K. Winegardner

I. Introduction

The typical operations in the nuclear fuel cycle are shown in Figure 1. Factors which must be considered in the evaluation of nuclear fuel cycle operations include electrical energy needs, technical feasibility, research and development needs, timing, cost, national and international policies, environmental impact, and both the calculated and the publicly perceived safety. Risk analysis is one method of assessing the safety of nuclear fuel cycle operations. Through such an analysis, consequences of postulated releases of radioactive material can be placed in perspective by viewing the events relative to their probability of occurrence.

This paper describes a method for the identification and preliminary evaluation of potential accidents (release sequences) which could lead to the release of radioactive material from nuclear fuel cycle operations. Potential accident sequences are evaluated on the basis of risk. The basic elements of this method are presented along with its application to a conceptual high-level radioactive waste management system.

II. Background

In general, risk analysis of a nuclear related system consists of the following basic steps: (1) Definition of the inventory of radioactive material and its containment/confinement barriers; (2) Identification of potential failure modes; (3) Estimation of the probability and amount of radioactive material released by the potential failure modes; (4) Analysis of the consequences of the radioactive material released; and (5) Estimation of the system risk. Figure 2 shows the information flow and calculational steps for a risk analysis.

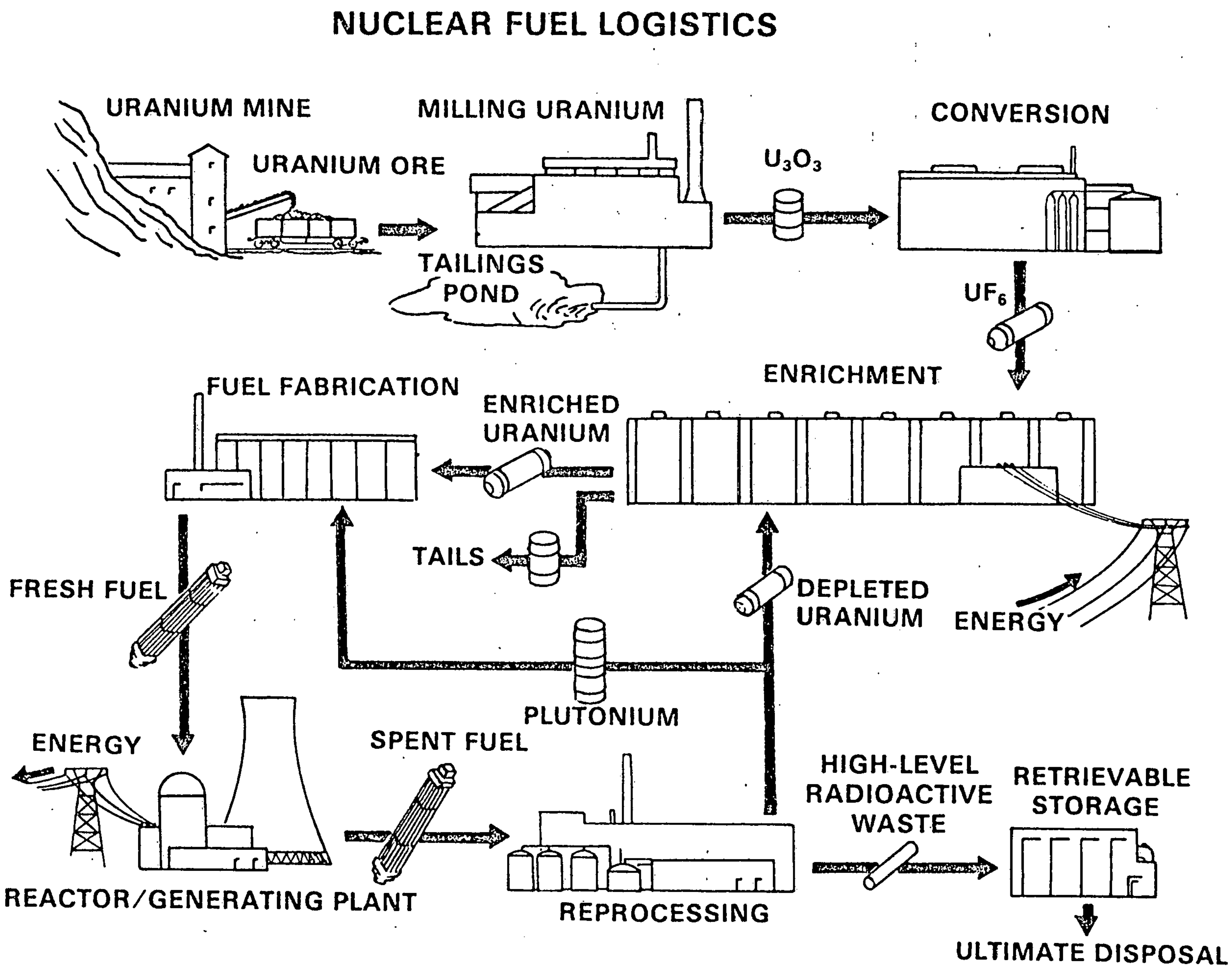

Fig. 1. Nuclear Fuel Logistics[1]

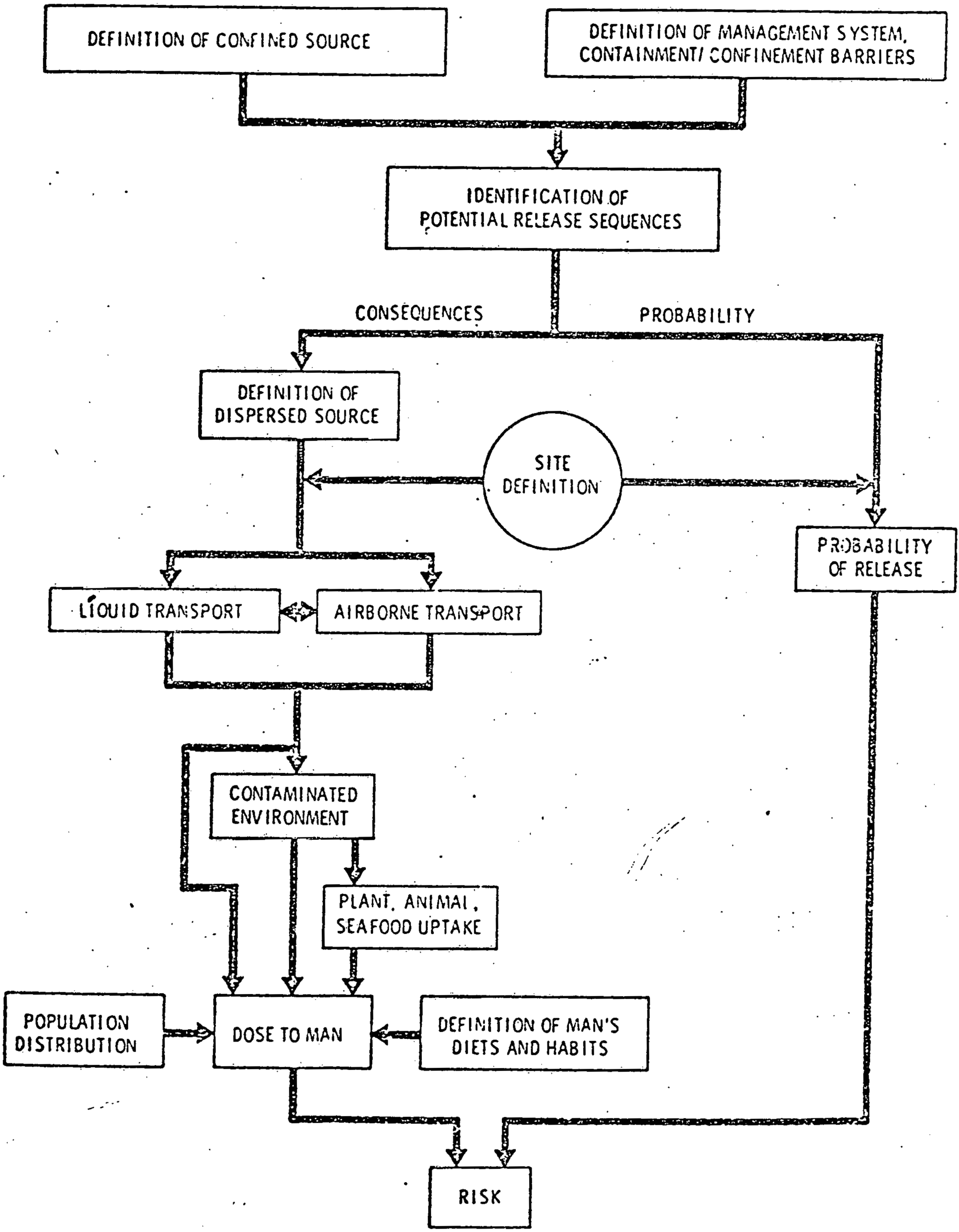
DEFINITION OF CONFINED SOURCE
DEFINITION OF MANAGEMENT SYSTEM, CONTAINMENT/ CONFINEMENT BARRIERS
IDENTIFICATION OF POTENTIAL RELEASE SEQUENCES
CONSEQUENCES
PROBABILITY
DEFINITION OF DISPERSED SOURCE
SITE DEFINITION
PROBABILITY OF RELEASE
LIQUID TRANSPORT
AIRBORNE TRANSPORT
CONTAMINATED ENVIRONMENT
PLANT, ANIMAL, SEAFOOD UPTAKE
POPULATION DISTRIBUTION
DOSE TO MAN
DEFINITION OF MAN'S DIETS AND HABITS
RISK

Fig. 2. Risk Analysis Calculation Flow[2]

In performing a risk analysis potential release sequences ranging from the frequent to the unlikely are identified. These release sequences are evaluated in terms of consequences as well as probability. Knowing both the consequences and the probability, a risk expression can be generated. The most general definition of risk is that it is some function of the probability and the consequences of a potential release sequence. A frequently used definition of risk is the product of the anticipated frequency of a release sequence and its consequences. That is, risk is the mathematically expected consequences of a release sequence. Recognizing the subjective nature of risk and its perception by the public, many studies(3,4,5) have avoided the use of a specific risk expression and simply report curves of probability versus consequences.

The most comprehensive risk assessment to date has been the WASH-1400 study of light water reactors.(3) Safety/risk analyses have been performed to various depths on other nuclear fuel cycle operations; however, none at the detailed level comparable to WASH-1400.

III. Risk Analysis Method

A method for the identification and preliminary evaluation of potential accident release sequences from nuclear fuel cycle operations is discussed in detail in Reference 6. The major elements of this method are given below.

Preliminary Analyses

Several preliminary analyses are performed prior to the systematic identification of potential release sequences. The facility and its operation are described in sufficient detail for the purpose of the analysis. System bounds are established in space (physical boundaries of the system studied), time (time periods of interest for the safety analysis, i.e., mission time), and limit of resolution (degree of system detail considered). Preliminary hazards analyses are then performed to generate a list of hazardous elements in the system and qualitative information on the potential release mechanisms and design measures for prevention and control.

Release Sequence Identification

The next phase of the analysis is the use of more powerful inductive or deductive methods to systematically identify potential release sequences.

Methods that may be applicable include: event trees alone; event trees with fault trees used to supply most of the branch probabilities; the similar cause/consequence analysis in which a fault tree feeds into an event tree through a common critical event and which fault trees again supply most of the branch probabilities; and various fault tree techniques.

Inductive methods, such as event trees, start with assumed initial failures. Additional component failures required to obtain a release (system failure) are then identified. Fault tree analysis is a deductive process. The analyst assumes the occurrence of an event selected as the top, undesired event, constituting system failure. He then systematically works backward to identify component faults which could cause or contribute to the undesired events.

The approach selected was the "to/through" fault tree method. This fault tree construction technique is similar to the leak path approach.[7]. The top, undesired event (accidental release of radioactive material from the operation) is postulated. The analyst traces back in reverse sequence to determine how each containment barrier could have been breached. The initial material released during an accident must move to each barrier and pass through it for release to occur. This process continues until initiating events have been reached. Figures 3 and 4 give a simplified illustration of the to/through fault tree technique. A sequence of events which negates the containment/confinement barriers and results in the occurrence of the top event is termed a release sequence. These sequences correspond to the familiar cut sets of fault tree analysis. The binary limitation of fault trees (i.e., faults must be "on-off") can be circumvented by treating each release sequence (cut set) separately and using a distribution of releases where necessary.

Preliminary Evaluation and Screening

Using this fault tree technique often requires the analysis of very large trees. It is neither feasible nor necessary to rigorously evaluate the large number of release sequences identified by the fault tree. The approach used is to separate the dominant sequences from the low risk sequences by a preliminary evaluation and screening process. Refined analysis can then be performed on these dominant sequences.

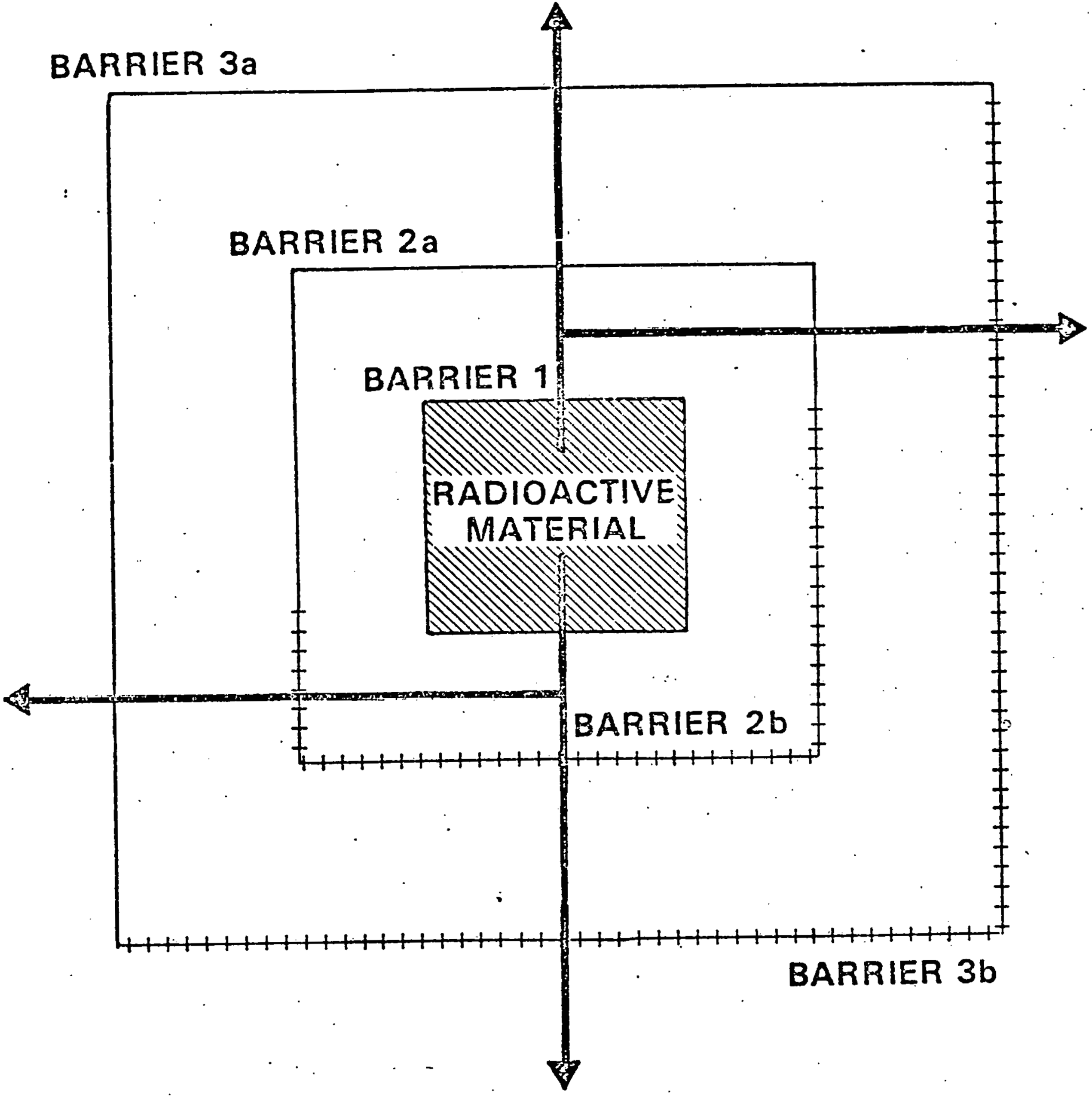

Fig. 3. Barrier Configuration for Example of To/Through Technique for Fault Tree Construction(6)

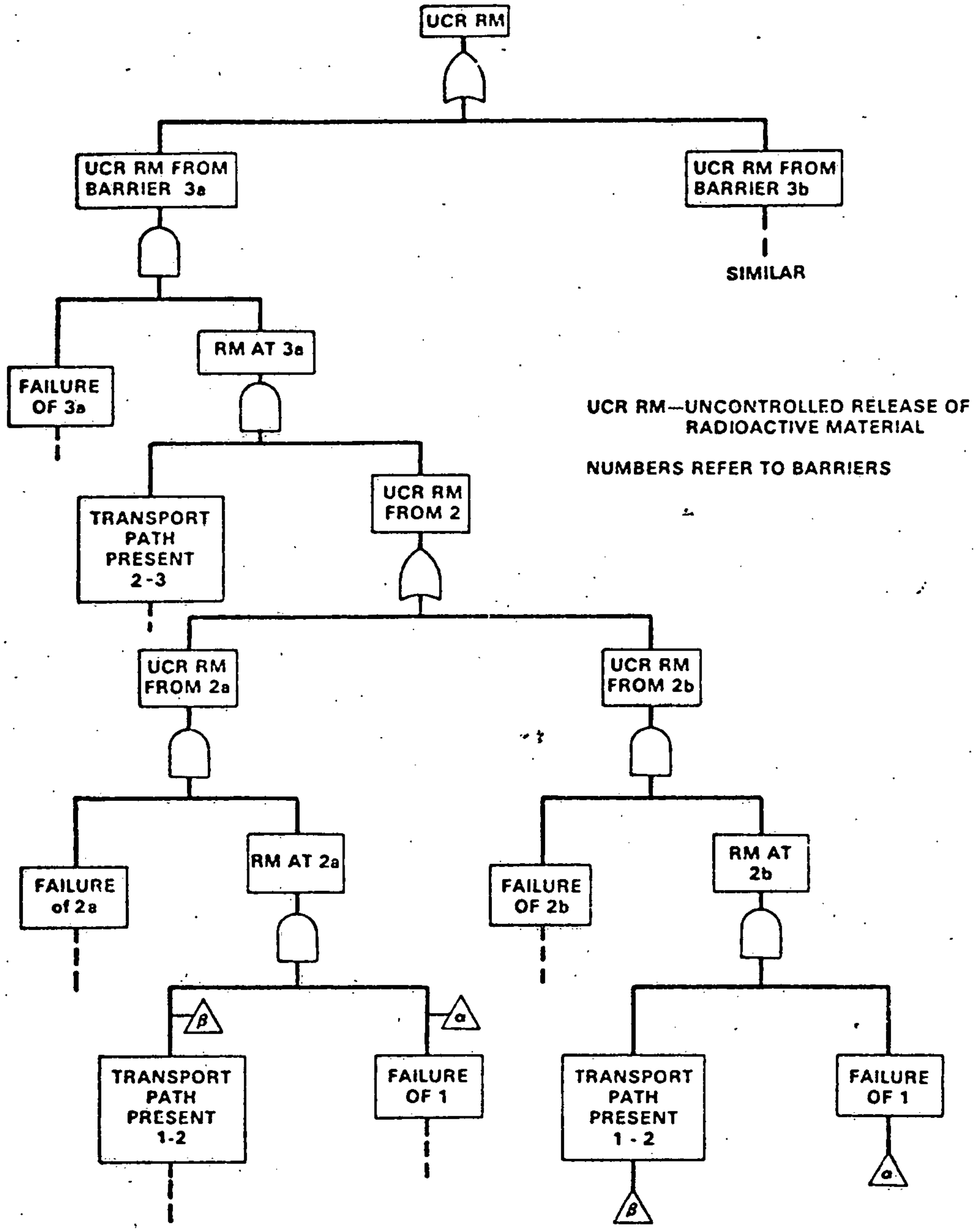

Fig. 4. Fault Tree Representing Release from the Barrier System of the Preceding Figure. The analysis has been simplified by assuming 1) all radioactive material is initially contained within barrier 1; 2) the transport paths 2a→3a, 2a→3b, 2b→3a, and 2b→3b are all identical; and 3) the transport paths 1→2a and 1→2b are identical.(6)

In nuclear risk analysis the significance of an accident sequence is measured by both its probability and its consequence. Therefore the evaluation and screening process must be based on a calculation of risk, not just probability alone. This screening is based on a simplified risk expression and use of derived cutoffs (based on risk) on the probability and length of an accident sequence.

The risk of a release of radioactive material can be defined as a product of five terms, in appropriate units:[6] (A) the probability of the release sequence; (B) the release magnitude; (C) measures of the physical, chemical and radiological characteristics of the released material; (D) a measure of the environmental transport path efficiencies; and (E) a measure of the population distribution and habits. An (F) term for conversion from population dose to health or environmental effects, is optional, as is a (G) term, for conversion of risk to monetary units. As mentioned in Section II, other definitions of risk have been proposed. The effects of alternate measures of risk and their effects on the method discussed in this paper are considered in Reference 6.

When comparing and screening sequences within a fault tree for an operation at one site, the risk expression can be simplified. The E term (population density) is generally independent of failure sequence. Sequences with similar D (environmental transport) terms are grouped and compared only within a group. The C term (material characteristics) can be handled by grouping sequences with similar C terms, or by including C terms with the B terms for release magnitude. Under these conditions, screening and preliminary ranking of sequences can be conducted (for sequences with similar D terms) based simply on comparisons of the product of the A and B terms.

As indicated above the screening and ranking of the potential release sequences requires the probability of the release sequence (A term) and the release magnitude (B term). The basic steps in this procedure include: (1) identify the release sequence; (2) compare release sequence length against the derived cutoff; (3) calculate release sequence probability; (4) compare release sequence probability against the derived cutoff; (5) calculate release sequence release fraction; and (6) rank release sequences on the appropriate A x B comparisons.

Release Sequence Probabilities

The release sequence probabilities are calculated using available data and extensions of the WASH-1400[3] equations. The probability calculations are based on the assumption of small probabilities and constant hazard rates (i.e., exponential failure distributions). Cut sets consisting of repairable components only, nonrepairable components only, or mixtures of both types can be evaluated. On-line or standby components, unavailability contributions from pre-existing failures, failures on demand, and testing and maintenance down-time can be handled.

Release Fractions

A release fraction is assigned to each basic event in the fault tree. The release fraction is defined as the amount of radioactive material passing through a containment/confinement barrier divided by the amount of material to which the barrier is exposed. For an initiating event the release fraction is the fraction of the total inventory of radioactive material initially dispersed. Some basic events do not have a release fraction (e.g., fan fails) and a value of 1.0 (which results in no effect on the calculation) is assigned. Other basic events may have a distribution of releases and up to four distributed values can be assigned. Combining the release fractions with the total inventory of radioactive material available results in the estimated release of radioactive material for the release sequence.

Sources of information for assigning basic event probabilities, unavailabilities, and release fractions are operating data, test data, analysis and engineering judgment. Many events require use of engineering judgment because of the lack of operating experience, test information and analysis.

Use of Cutoffs

In the evaluation and screening process, cutoffs on release sequence length and probability are used to reduce the calculational effort required to evaluate large fault trees. These cutoffs are derived on a risk basis and are conservatively calculated. In calculating the probability cutoff, a reference release sequence is selected and its risk measure is calculated. The probability cutoff is calculated based on the question: "At what probability will even the release of the total system inventory result in negligible risk compared to the reference release sequence?" The release sequence length cutoff is calculated by conservatively assuming the n highest probability basic events compose a single release sequence. The cutoff value is that value of n which results in a probability less than or equal to the probability cutoff.

Computer Program

The identification, preliminary evaluation, and screening process is facilitated by a computerized procedure. A computer package consisting of three codes has been developed to assist in performing a preliminary risk assessment.[6] Figure 5 illustrates the use of these codes in the screening procedure. The names of these programs and their functions are given below:

ACORN - draws a fault tree diagram based on the tree logic description input by the analyst.

MFAULT - identifies release sequences, calculates release sequence probabilities, and screens release sequences on the basis of derived cutoffs.

RAFT - calculates a risk measure and orders release sequences in terms of decreasing risk measure.

Detailed Analysis

The screening processes facilitates the determination of which release sequences are dominant risk contributors and warrant additional analysis. The output from the screening process generally does not result in a complete or suitable determination of the system risk. Areas which require further analysis are spectrum considerations (events which may have frequency versus severity distributions), identification of common cause failures and mathematical treatment of identified dependent events, and sensitivity and importance studies.

Detailed probability and consequence studies of the dominant release sequences should follow. These detailed studies can be performed using the release sequences directly or by performing a more detailed fault or event tree analysis.

Comparison of Methods

The fault tree analysis method employed by PNL has some advantages and weaknesses relative to other safety analysis methods, such as event tree

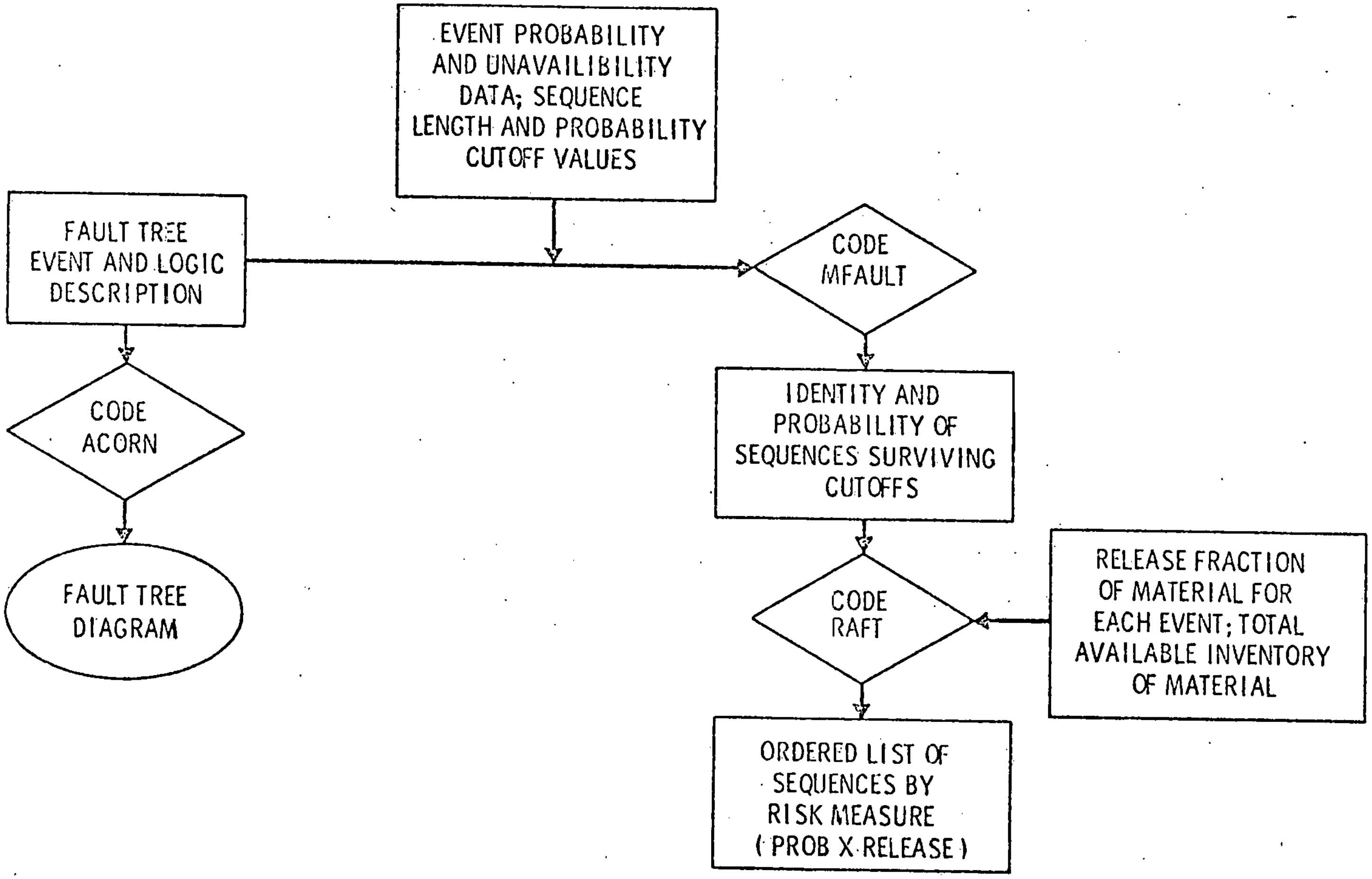
EVENT PROBABILITY AND UNAVAILIBILITY DATA; SEQUENCE LENGTH AND PROBABILITY CUTOFF VALUES
FAULT TREE EVENT AND LOGIC DESCRIPTION
CODE MFAULT
CODE ACORN
FAULT TREE DIAGRAM
IDENTITY AND PROBABILITY OF SEQUENCES SURVIVING CUTOFFS
CODE RAFT
RELEASE FRACTION OF MATERIAL FOR EACH EVENT; TOTAL AVAILABLE INVENTORY OF MATERIAL
ORDERED LIST OF SEQUENCES BY RISK MEASURE (PROB X RELEASE)

Fig. 5. Schematic of Screening Process

and cause consequence analysis. No assumption of initiating or critical events is necessary in the fault tree method. This is an advantage for systems where the key initiators are not known. Other advantages include more direct treatment of common cause failures because all events appear on one fault tree, and potentially a more complete analysis can be conducted because the system is treated as a whole. One disadvantage of this approach is the required analysis of very large fault trees.

Event trees and cause-consequence analysis better facilitate and display the detailed analysis (particularly time phasing) of accidents involving a common initiating or critical event. Using these techniques a complex problem can often be divided into manageable segments. A disadvantage is that there is no formal procedure to develop the required key initiating events. Difficulties often arise in the ordering and the treatment of dependencies of the branch operators (key events or decision points in the event trees or cause-consequence diagrams).

Most safety analysts will agree that there is no best method for performing a safety/risk analysis. Depending upon the system being evaluated a combination of approaches is often advantageous. One potential combination is suggested. A fault tree analysis method as described in this paper would be used to provide a comprehensive identification of potential accidents and to separate those that should be examined in more detail. Detailed analysis of such accidents could follow by means of event trees or cause-consequence analysis. If the key initiating events are known with confidence, the comprehensive type of fault tree analysis may not be necessary.

IV. Application of the Method to a Conceptual High-Level Waste Management System

The risk analysis method described in this paper has been used in the preliminary assessment of a conceptual, pre-disposal system for the management of commercial high-level radioactive waste.[8,9] A description of the conceptual system for managing this waste and the results of the assessment are discussed below.

Fuel Reprocessing and High-Level Waste Management

The zirconium clad, uranium dioxide (slightly enriched in the fissile U-235 isotope) fuel elements of commercial electrical power generating nuclear reactors must be replaced periodically. Replacement is required primarily because of fissile (fuel) material depletion and the accompanying buildup of unwanted fission products that compete with the fission (power producing) process. This irradiated or spent fuel can be shipped to a fuel reprocessing plant to recover residual fuel (uranium and plutonium) material for possible reuse.

After at least a few months to permit decay of relatively short-lived fission products, the spent fuel would be shipped from the reactor to a fuel reprocessing plant. Here, again after appropriate decay, it would be mechanically chopped into short lengths, dissolved in nitric acid, and the dissolved uranium and plutonium separated from the fission products. Separation can be accomplished with a solvent extraction process in which the aqueous acidic solution is contacted with an immiscible organic extractant. Conditions are adjusted to transfer most of the fuel material to the organic phase. Almost all of the non-volatile fission products and transuranic actinides (except Pu) remain in the aqueous phase. In addition, this dilute aqueous acidic solution of chemical salts contains any U and Pu fuel losses as well as nonradioactive chemicals added during reprocessing. It is the operating activities associated with the pre-disposal management of this latter intensely radioactive stream, termed high-level waste, that is the subject of the current risk assessment.

Major waste management activities assumed for the conceptual pre-disposal system (Figure 6) include liquid storage, solidification, water basin storage, rail transport, and retrievable surface storage. The waste is assumed to be managed for about 10 years at the reprocessing plant and is in liquid form for one-fourth of this period. It is assumed that cooled stainless steel tanks, installed in steel-lined concrete vaults are used for the interim storage of concentrated high-level liquid waste.

Present federal regulations require that the reprocessing plant's inventory of high-level liquid waste be limited to that produced in the prior five years and that the waste be converted to a dry solid to comply with this inventory limitation.[10] For the current study, it is assumed that waste with about three years of post irradiation decay is transferred to a shielded hot cell where it is solidified by calcination followed by conversion to a monolothic glass. Atomized droplets of waste are evaporated

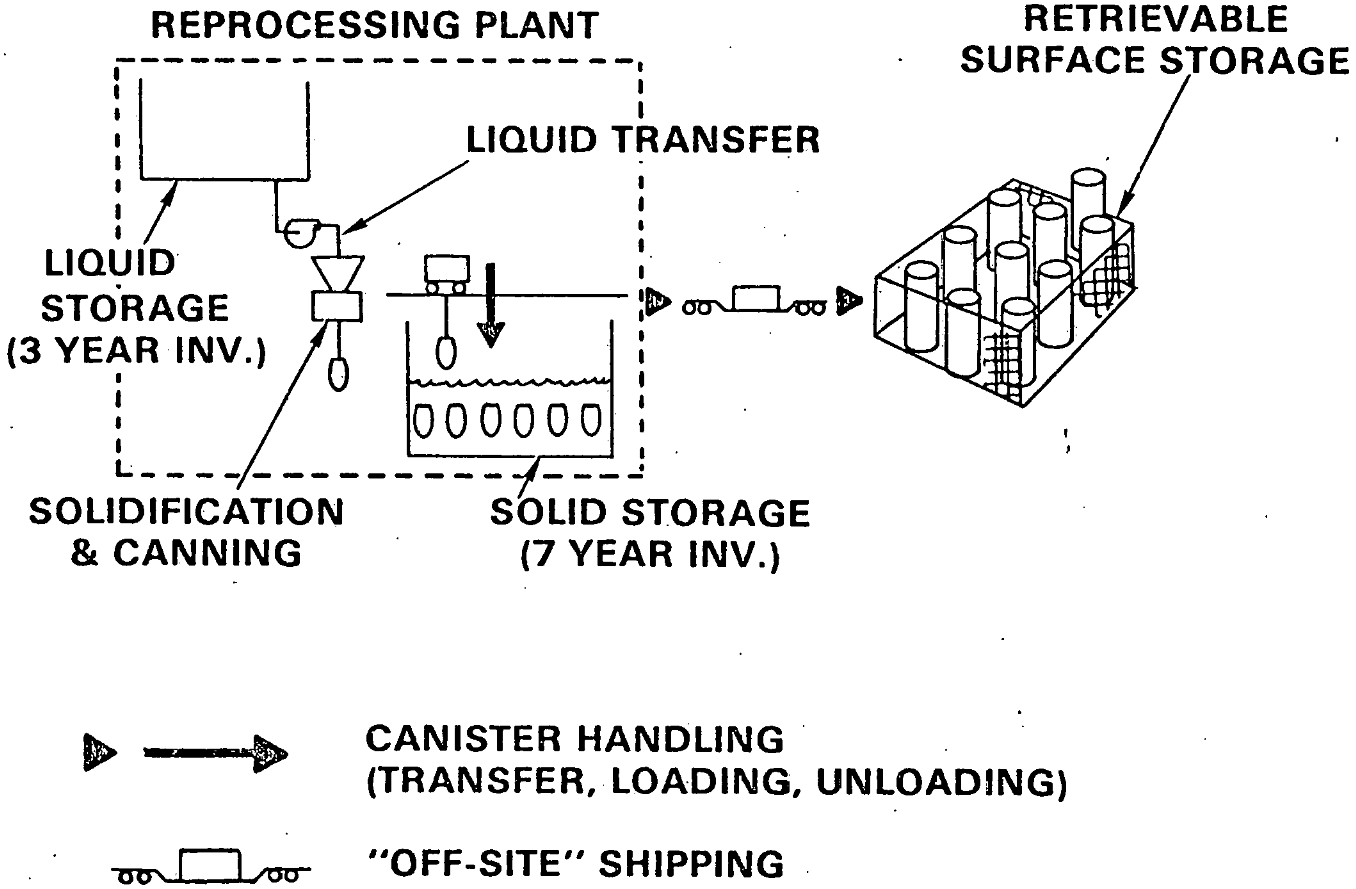
REPROCESSING PLANT
RETRIEVABLE SURFACE STORAGE
LIQUID TRANSFER
LIQUID STORAGE (3 YEAR INV.)
SOLIDIFICATION & CANNING
SOLID STORAGE (7 YEAR INV.)
CANISTER HANDLING (TRANSFER, LOADING, UNLOADING)
"OFF-SITE" SHIPPING

Fig. 6. Reference High-Level Waste Management System

in a heated chamber resulting in solid oxide particles (calcine). Solid glass frit is added to the calcine and the mixture fused in a melter unit (or canister). Sealed-filled canisters of either calcine or glass-like solid product are transferred to a cooled water-filled concrete basin for an additional seven years of storage at the reprocessing plant.

Federal regulations also require transfer of the solid waste form to a federal repository no later than 10 years following reprocessing. For this study it is assumed that waste with about 10 years of decay is transferred by rail to an interim facility located 2500 miles from the reprocessing plant. The solid waste is transported in 100-ton, air-cooled lead-shielded casks. Each shipment consists of nine waste canisters. The retrievable surface storage concept involves storing individual canisters in vertical heavy-walled steel casks that are sealed by welding. The casks are set outdoors on concrete pads. Heat is dissipated by natural convection.

Tentative Results of Risk Assessment

Dominant failure sequences for the accidental release of radionuclides have been tentatively identified for the various activities of the reference system. Dominant sequences were defined as those with the highest mathematical product of probability and consequences, the latter in terms of quantities of waste released. The initial assessment revealed that dominant scenarios that could conceivably have significant public health and safety impact are highly improbable, e.g., on the order of 10^{-6} per year of operation.

Accidental releases of radioactive material initiated by both process operating events and events external to the plant (e.g., earthquake) were found to contribute to total system risk. Except for the mechanically or electrically induced interruption of cooling water to stored liquid and solidified waste, postulated release scenarios contributing the bulk of the risk generally involved sequences initiated by external events.

Dominant scenarios with conceivable significant public health and safety impact were associated with the storage activities rather than with the relatively active modes of solidification and transportation.

This appears to be primarily because of the larger radionuclide inventories associated with the storage activities. The more dominant scenarios were associated with the airborne pathways.

Re-evaluation of this initial assessment is underway to ensure that insights obtained by comparisons are valid. Areas of future work include: (1) performing sensitivity studies; (2) establishing error bounds; and (3) performing more detailed analysis on the dominant potential release sequences.

Several basic difficulties exist in assessing the risk of the operational steps in waste management systems. An important one is the lack of directly applicable and readily available data. In the performance of the safety analysis of a conceptual high-level waste management system, information gaps were encountered. This was expected as there has been little operating experience for high-level waste management activities. Only a relatively small amount of experimental work has been done in identifying and analyzing the consequences of potential accidents. In fact the current assessment has already prompted additional investigations of the breakup and volatility characteristics of solid high-level waste products under potential accident conditions.[11,12]

The basic information needs for improving the safety assessment, and therefore its usefulness, can be placed in the following closely-related categories: (1) Additional information on the probability of breaching containment/confinement barriers versus the severity of the breach; (2) Data on the quantity, transport mechanism, and the chemical-physical form of the radioactive material released from failed barriers; (3) More information on system characteristics and interactions in the accident environment (e.g., ventilation system efficiency under accident conditions); and (4) More information characterizing the solidified high-level waste form (e.g., waste characteristics as a function of storage time and conditions).

Another factor which limits the detail and accuracy of the risk assessment of waste management operational steps is the conceptual nature of present designs. This results in a limited treatment of common cause failures and human error. It also results in difficulties in treating severe external environments (e.g., earthquake).

Safety studies made during the conceptual phases of waste management system design are limited in the detail of analysis. The sooner the analysis is made, the easier it is to effect any safety-related changes in the system under study or the conceptual design. The later in the waste management system life-cycle the study is performed, the more information is available and the greater the accuracy of the results. A tradeoff is involved between the timeliness and the depth of accuracy of the analysis.(9,13)

V. Conclusion

A method for the identification and preliminary evaluation of potential accident release sequences from nuclear fuel cycle operations has been developed. This method has been applied to a conceptual high-level waste management system and preliminary results have been obtained. Refinement of this study is currently underway.

Potential benefits from a risk assessment of waste management systems and other fuel cycle facilities include: (1) Comprehensive and systematic assessment in the sense that the entire spectrum of possible accidents are considered; (2) Development of perspective on the relative safety of system components; (3) Identification of R&D needs for supplying missing data; (4) Preliminary input for management decision-making and improved system design; and (5) Establishment of a rational basis for choosing between alternative systems.

REFERENCES

1. R. M. Fleischman and R. C. Liikala, "Isotopic Composition and Radiological Properties of Uranium in Selected Fuel Cycles," Conference on Occupational Health Experience with Uranium, ERDA 93, April 1975.

2. T. H. Smith, W. K. Winegardner, G. Jansen, L. D. Williams and T. I. McSweeney, "A Methodology for Risk Analysis of Nuclear Waste Management Systems," presented to the American Nuclear Society 20th Annual Meeting, BNWL-SA-4899, Battelle, Pacific Northwest Laboratories, Richland, WA, June 1974.

3. USAEC, Reactor Safety Study, An Assessment of Accident Risks in Commercial Nuclear Power Plants, WASH-1400, October 1975.

4. T. I. McSweeney, R. J. Hall et al., "An Assessment of the Risk of Transporting Plutonium Oxide and Liquid Plutonium Nitrate by Truck," BNWL-1846, Battelle, Pacific Northwest Laboratories, August 1975.

5. C. F. Smith and W. E. Kastenberg, "On Risk Assessment of High Level Radioactive Waste Disposal," Nuclear Engineering and Design, Vol. 39, pp. 293-333.

6. T. H. Smith, P. J. Pelto, D. L. Stevens, G. D. Seybold, W. L. Purcell, and L. V. Kimmel, A Risk-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accidental Release Sequences in Nuclear Fuel Cycle Operations, BNWL-1959, Battelle, Pacific Northwest Laboratories, Richland, Washington, January 1976.

7. R. R. Fullwood and R. C. Erdmann, "On the Use of Leak Path Analysis in Fault Tree Construction for Fast Reactor Safety," Proceedings of the Fast Reactor Safety Meeting, USAEC, CONF-740401-P3, pp. 1493-1507, April 1974.

8. W. K. Winegardner, et al, "Systems Safety Evaluation," in Quarterly Progress Report Research and Development Activities Waste Fixation Program, January through March 1976, BNWL-2080, Battelle, Pacific Northwest Laboratories, Richland, Washington.

9. P. J. Pelto, T. H. Smith and J. W. Bartlett, "Risk Assessment Methods for Nuclear Waste Management Systems," presented to EPA Workshop on Issues Pertinent to Development of Environmental Protection Criteria for Radioactive Wastes, BNWL-SA-6135, Battelle, Pacific Northwest Laboratories, Richland, Washington, February 1977.

10. Code of Federal Regulations Title 10, Energy, (Section 50, Appendix F), Government Printing Office, Washington, D.C., 1976.

11. T. H. Smith and W. A. Ross, Impact Testing of Vitreous Simulated High-Level Waste in Canisters, BNWL-1903, Battelle, Pacific Northwest Laboratories, Richland, Washington, May 1975.

12. W. J. Gray, Volatility of a Zinc Borosilicate Glass Containing Simulated High-Level Radioactive Waste, BNWL-2111, Battelle, Pacific Northwest Laboratories, Richland, Washington, October 1976.

13. T. H. Smith, R. J. Hall and L. D. Williams, "Analytic Methods for Fuel Cycle Safety Sources," in IEEE Transactions on Reliability, Vol. R-25, No. 3, pp. 184-190, August 1976.