RISK ANALYSIS METHODOLOGY
APPENDIX P

Principles and Methods for Combining Failure Probabilities and Risks in Dam Safety Risk Analyses

U.S. Bureau of Reclamation
Technical Service Center
Denver, CO

Version 2.5
May 22, 2003

Contacts: Karl Dise (303) 445-3030

Final Technical Report, Work Release Number 33277-001-166
Subcontract Number 33277
Reclamation Contract 1425-97-CA-81-20003
URSGWC Delivery Order 166
February 9, 2000

U.S. Bureau of Reclamation
Technical Service Center
Denver, CO

Principles and Methods for Combining Failure Probabilities and Risks in Dam Safety Risk Analysis

By Steven G. Vick

Abstract

The U.S. Bureau of Reclamation has instituted a program for probabilistic risk analysis in its dam safety activities. By acknowledging and explicitly addressing the various uncertainties inherent in the evaluation of dam safety, the objective is to improve the understanding of dam behavior and aid in focusing dam safety resources toward those areas where greatest risk reduction benefits can be achieved.

Reclamation=s risk analysis activities and its implementation of related technology have proceeded incrementally, expanding and refining the procedures according to perceived needs and outcomes from progressive applications. Its Dam Safety Risk Analysis Methodology document provides the current status of these efforts. Among the elements it describes are dam failure probabilities and risks derived by combining values determined at some lower level of aggregation. These might include probability or risk values for different loading conditions, loading ranges, failure modes, spatial segments, or other conditions. Not only do these values result from aggregation of their own constituents, but they themselves are often combined in some way to express their collective effect. This report has been prepared in support of the Methodology document to address this and related topics.

The report treats various methods and the underlying principles for combining risk and probability values in the context of current Reclamation practice. Many of these methods have already been adopted, but their technical underpinnings may not be universally appreciated or commonly understood by the technical specialists who use them and the dam safety decisionmakers who interpret them. One purpose of this work is to enhance this understanding within the framework of the basic axioms and related principles that govern the probability mathematics. It adopts a systems approach that views the features of the dam and its downstream environs as system components, and interaction among these components in terms of independent and correlated behavior receives special emphasis. In addition to the mechanics of probability and risk aggregation, attention is devoted to the reasons why these aggregations may be warranted and some of the various forms they may take. This goes to how risk analysis is used to develop probability and risk-based insights into dam behavior, and how this information is best communicated to decisionmakers.

Table of Contents

List of Tables

List of Figures

1.0 Introduction

Performing a risk analysis usually requires that probability values be mathematically manipulated in some way. In fact, its ability to provide for mathematical operations is the underlying reason why numerical probability is used at all, and this is also why quantitative risk analysis offers significant advantages over qualitative (non-numerical) procedures. Simply put, some probabilities are easier to estimate than others, and mathematical operations afford the opportunity to derive probabilities for one condition based on estimates that can be made more conveniently for some other condition. It is difficult, for example, to estimate the probability of failure of a dam directly, but quite possible to estimate the separate probabilities associated with loading, response, and consequences. To arrive at the probability of dam failure then requires some means for aggregating these values.

The same is true for risk. A separate risk value (i.e., the probability of some number of lives lost) is calculated for every end-branch and associated unique branch pathway in an event tree. It would be possible, but not particularly useful, to present each and every one of these risk values individually to the decisionmaker. Instead, combining them various ways - say according to some loading condition, or load range, or failure mode - provides a more readily-usable synthesis of this information that communicates the desired elements of risk more meaningfully.

This Appendix treats some of the issues involved in combining failure probability and risk estimates in situations typically encountered for Reclamation dams. Many of the methods and procedures described are already used in Reclamation risk analysis practices. The objective here is to put forward some of their conceptual underpinnings in the interest of promoting consistency, enhancing risk communication, and ultimately improving the dam safety decisionmaking process. First, system concepts are described, and then some simple mathematical principles derived from the basic probability axioms. It is not anticipated that these discussions will apply to the unique circumstances of every case. They do, however, provide general guidance and a framework for recognizing the various conditions that arise.

2.0 System Concepts

Before treating how probabilities and risks are combined, it is first useful to consider how and why they are separated in the first place. One obvious case alluded to above refers to the individual probabilities assigned to the separate decomposed events in an event tree. Here, each such event is a *component event* of the failure sequence. But components can also be defined in a different sense that considers the dam and its downstream evirons as a system, and here probabilities or risks may be developed separately for various *system components*. The components of a dam system can be classified in three general categories: physical features of the dam, spatial segments of the dam, and PAR downstream from the dam. When more than one dam or dike impounds the reservoir, for example, each such structure might be considered a component of the reservoir system, or as a separate system in itself. Viewing the elements considered in the risk analysis as a system helps structure how they are treated, how they relate to each other, and how their individual failure probabilities and risks are generated.

2.1 System components

The components of the system are its basic building blocks that together describe and define it. The system description is ordinarily implied within the context of a Reclamation risk analysis and is not usually developed formally. Nevertheless, the system and its definition, whether explicit or implied, provide the framework for determining how probability and risk estimates are initially developed, and consequently how they are later combined. The three kinds of components that together comprise the system are described separately below.

- **physical features**

Any dam contains various features that must function successfully for its integrity to be maintained, such as the foundation, abutments, spillway, and dam embankment. Any or all of these features may be subject to conditions that might cause them to fail to function in the desired manner. These, of course, are the failure modes that the risk analysis identifies and evaluates. So on the most basic level, physical features define the components of the dam system, and system failure is associated with the occurrence of failure modes for one or more of them.

- **spatial segments**

A dam can display marked variations in physical conditions usually (but not necessarily) along its length. These might consist of different structure types, such as an earthfill embankment with a concrete overflow section, or geologically distinct foundation conditions like an alluvial deposit with rock abutments. Abrupt variations in height may also occur for a dam spanning a deeply-incised valley with lower adjoining sections. Spatial differences like these can provide the basis for defining separate segments of the dam which then become components of the system, each subject to applicable failure modes or failure consequences. Dams or dikes that are physically separated but confine the same reservoir can be a special case of spatially-segmented system components.

- **downstream environs**

The third element of the system is the downstream region where consequences are incurred. Because Reclamation usually evaluates economic and environmental damages externally from the risk analysis, the affected downstream region is defined by the location of the population at risk (PAR). This region is bounded by the locations of downstream residences, attenuation characteristics of the dam-breach floodwave, or distances sufficient to provide ample warning in relation to floodwave travel time. In the special case of multiple structures on the same reservoir each with individual PAR=s, separate systems (or subsystems) can be defined to reflect these downstream conditions.

2.2 Defining the system

In practice, defining and describing the system and its various components is a sequential process that proceeds in the following steps:

1) *Define system failure*. Conventionally, failure is defined as uncontrolled release of the reservoir. For purposes of risk analysis, Reclamation defines failure as breach of the dam, and its Tier 2 guidelines require this condition to be addressed whether or not any loss of life would result. Occasionally, circumstances may be identified that could involve significant damage to the structure or even loss of life from unexpected seepage discharges, outlet works releases, gate malfunction, or spillway flows well beyond those associated with normal operation. These would not be treated as failure conditions unless they propagate to dam breach. Their associated probabilities and risks can, however, often be developed from information the event tree contains, and they may warrant separate discussion in the risk analysis documentation.

2) *Define spatial segments*. Spatial segmentation and definition of corresponding spatial system components most often follows from different types of foundation conditions, or from differences in their severity sufficient to substantially affect probability estimates from one location to another. Segmentation is based on subsurface data and geologic interpretations, and conditions within any segment are said to be *statistically homogeneous*. This does not imply that they are uniform - variations can still occur from place to place - but that the *statistical properties* (such as mean and standard deviation) describing the spatial distribution of these conditions are the same within any segment. Another basis for segmentation can be abrupt changes in dam height producing different dam-breach floodwave heights and hence different risk. Defining discrete spatial segments accordingly can provide more information for possible modification decisions. In particular, this allows different types of remedial alternatives to be related to their risk-reduction effectiveness at these separate locations, as opposed to prescribing a single type of modification over the entire length of the dam. Considerable discretion and judgment is required in spatial segmentation according to either of these factors. While many finely-discriminated segments can be appealing for probability estimation, the total number of failure modes increases geometrically with the number of segments where they apply. This can quickly lead to a great deal of additional effort and ultimately reduce the clarity of results.

3) *Define failure modes*. For each segment of the system, the failure modes applicable to its conditions are then identified. Failure mode identification, or screening, is described elsewhere in the Methodology Document and is not treated further here.

4) *Define system boundaries*. The dam(s), reservoir, and PAR together define physical boundaries to the system, and it can be useful to Adraw a box@ around it (both figuratively and literally) to designate the features it is, and is not, intended to contain. Figure 1a shows the typical case of a single dam, reservoir, and PAR. Here, a powerhouse is below the dam and above it lies an unstable slope that could potentially destroy it and its occupants. The powerhouse is included in the system boundary along with the town downstream because workers would be affected by a dam-breach floodwave. The unstable area is not included in the system because a landslide would not satisfy the definition of failure as breach of the dam. There could be many failure modes affecting the powerhouse and its workers, such as a landslide, penstock failure, and of course dam breach. But to comprehensively address these would require defining another system - the powerhouse - and performing a separate risk analysis for it. Hence, defining system boundaries

for a dam safety risk analysis requires distinguishing between processes causing dam breach and those associated with O&M issues that do not propagate to breach, acknowledging that the latter may have adverse consequences as well. A contrasting case is shown on Figure 1b, with two dams on the same reservoir each having different PAR=s. Here, two systems requiring separate risk analyses are defined because each system failure has unique downstream consequences. In this case, Tier 1 and Tier 2 guidelines would be applied to each system; the common reservoir does not require a single system.

2.3 Characteristics of dam systems

The system description leads to the relationships among component failure probabilities and risks. Figure 2 shows several forms of *reliability block diagrams* that portray how system components interact. Figure 2a corresponds to the dam system of Figure 1a, where the physical components are subject to three separate failure modes FM_1, FM_2, and FM_3, over two spatial components, Segments 1 and 2. This represents a *series system* such that failure of any one component in series results in system failure. Figure 2b corresponds to the two systems of Figure 1b, where each is subject to the same three failure modes. These are series systems as well. By contrast, Figure 2c shows a *parallel system*, where system failure requires failure of all three components. Here, the components are *redundant* such that the system could still function with any one intact.

Some dam systems, or parts of them, may have redundant components that operate in parallel. For example, if one spillway gate should become jammed, others may be able to pass an inflow flood up to some level. Similarly, outlet works sometimes have significant discharge capacity that provides some degree of redundancy with the spillway. Dam components that operate in parallel, however, are by far the exception, and most dam systems are series systems: if one component fails the system fails. This has implications for evaluating correlated failure modes, as subsequently explained.

Another important aspect of the system description is that it is fixed in time - a Asnapshot@ of the system at the moment the risk analysis is performed. The probability and risk estimates are predicated and contingent upon the particular description, or *state*, of the system as it is defined during the risk analysis, and failure processes that occur under a such a non-varying system state are said to be *probabilistically stationary*. Some processes like alkali-aggregate reaction or particle transport may be time-dependent if they change the physical condition of components and therefore the system state. Others, like increase in PAR over time, can change the system description or its boundaries. Still others can have to do with seismotectonic interpretations and how earthquake potential varies in time and space. However, neither the system state nor description can be projected forward in time to account for such effects or the cumulative damage they may produce. Thus, even though the risk analysis produces estimates of annual failure probability and annual risk that apply in principle to any given year present or future, these estimates apply only to the system description

adopted.[1] The risk analysis can be updated, however, as part of the CFR process or at other times as necessary to reflect known changes in conditions and system state that may have occurred.

3.0 Combining Probabilities

The mathematics of probability provide rules for combining basic system component failure probabilities in ways consistent with the probability axioms. Together these rules and axioms are called the *probability calculus*, and the essential texts on this topic are Benjamin and Cornell (1970), and Ang and Tang (1975, 1984). They contain many probability principles, applications, and examples relevant to dam safety issues, and readers are strongly encouraged to consult them. Before discussing how probabilities are combined, it is useful first to consider which ones to combine and why.

The probability calculus itself does not require that any probabilities be combined, but one may choose to do so for reasons of convention, convenience, and ultimately insight and communication. Conceivably, the product of a risk analysis could be nothing more than a tabulation of the probabilities assigned to each event in the event tree, but this would offer little insight into overall dam behavior, nor would it communicate information in a useful form. Both insight and communication require some kind of synthesis and aggregation of the individual values.

Which probabilities to combine depends on what insights are sought and what is sufficiently important that it needs to be communicated. This is partly a matter of convention and partly judgment. By convention, Reclamation=s Tier 2 guidelines specify that event probabilities be combined to subtotals for static, seismic, and hydrologic loading conditions, and these to the total failure probability for the dam under all such conditions. This is reasonable because the loading conditions are closely related to the kinds of modifications that might be required, and also because the total failure probability allows different dams to be conveniently compared.

Deeper insight into dam behavior requires other probability combinations. Probabilities for each loading range show whether vulnerability is controlled by extreme or by more frequent flood and earthquake initiators. Probabilities for various failure modes combined over all such load ranges can show whether and why one might dominate. And probabilities for different segments can show where failure is believed to be

[1]Methods are available to address non-stationary processes, provided that the variation in system state can be described probabilistically for example as a *Markov process*, but they are considerably beyond the current state of practice in dam safety risk analysis. Otherwise, annual probabilities for stationary processes and constant system state can serve as a lower bound where cumulative damage or other system changes may occur. Vick and Stewart (1996) describe one such case.

most likely. Each such probability combination tells and reveals something different about the dam system, and they are all necessary to develop an understanding of dam behavior that directs where to target attention, investigations, or modifications.

3.1 Probability axioms

Venn diagrams are a pictorial representation of the relationships among events according to set theory, and they provide the underlying basis for the probability axioms. Consider, for example, whether sand or clay exists at some particular location in a foundation, as depicted on the Venn diagram of Figure 3. The corresponding events S and C exist within the *sample space* that is the set of all possible soil and rock types. The presence of either sand or clay is the *union* of the two events S and C, expressed as $S \cup C$ and read as S OR C. Their *intersection* represents a mixture of sand and clay as shown by the overlapping region on Figure 3, expressed as $S \cap C$ and read as S AND C. The remaining regions represent exclusively sand S_0 and exclusively clay C_0. The three events S_0, C_0, and $S \cap C$ are now *mutually exclusive* - no one can exist in the presence of another. Together with all of the remaining elements in the sample space they form a *collectively exhaustive* set of foundation material types which could exist at that location. Probability operates on the relationships among events that the Venn diagram portrays, and its axioms define the conventions these operations adopt:

Axiom I. The probability of an event E is a number greater than or equal to zero but less than or equal to unity:

$$0 \leq p[E] \leq 1$$

Axiom II. The probability of a certain event E_c is unity, where E_c is the event associated with the occurrence of all members of the sample space:

$$p[E_c] = 1$$

Axiom III. The probability of the union of any two mutually exclusive events is the sum of their probabilities:

$$p[E_1 \cup E_2] = p[E_1] + p[E_2]$$

which implies that:

$$\sum p[E_i] = 1$$

Returning to the Venn diagram of Figure 3, the event S can be considered as the union of the intersection $S \cap C$ and the non-overlapping region S_0, and likewise C is the union of the intersection $S \cap C$ and the non-overlapping region C_0. So from Axiom III:

$$p[S] = p[S \cap C] + p[S_0] \quad (1)$$

$$p[C] = p[S \cap C] + p[C_0] \quad (2)$$

Also from Axiom III, for the three mutually-exclusive events S_0, C_0, and $S \cap C$:

$$p[S \cup C] = p[S_0] + p[S \cap C] + p[C_0] \tag{3}$$

Solving eqns. (1) and (2) for $p[S_0]$ and $p[C_0]$ and substituting in eqn. (3), the probability of either sand or clay at the location in question is:

$$p[S \cup C] = p[S] + p[C] - p[S \cap C] \tag{4}$$

The right-hand side of eqn. (4) can be interpreted as the sum of the probabilities of sand and clay considered individually, with the third term subtracted to prevent Adouble counting@ of the overlapping region on Figure 3.

3.2 Independent and conditional probabilities

The *conditional* probability that the clay contains sand is $p[S|C]$ (read as the probability of S GIVEN C). From Figure 3, this is the proportioned ratio of the probability of the overlapping region $S \cap C$ to the probability of C, or:

$$p[S|C] = \frac{p[S \cap C]}{p[C]} \tag{5}$$

In general, conditional probability is the probability that one event A will occur given the knowledge that some other event B has already occurred, or similarly the probability of A predicated on the occurrence of B. Thus, the probability of liquefaction is a conditional probability given the occurrence of some seismic ground motion. From eqn. (5), the combined or *joint* probability of both liquefaction B and the earthquake A is:

$$p[A \cap B] = p[B|A]\, p[A] \tag{6}$$

Other events might be taken as *independent*, such as the occurrence of full-reservoir conditions C and the earthquake A. Here, the conditional probability of the reservoir being full given the earthquake is the same as the probability of full-reservoir conditions, because the occurrence of the earthquake says nothing about the reservoir and vice-versa (at least if reservoir-induced seismicity is neglected). Therefore for independent events:

$$p[C|A] = p[C] \tag{7}$$

Thus, the joint probability of the earthquake and full-reservoir conditions, from eqn. (6) would be:

$$p[A \cap C] = p[C|A]\, p[A] \quad (8)$$

and from (7),

$$p[A \cap C] = p[A]\, p[C] \quad (9)$$

If we further wish to combine all three probabilities to determine the joint probability of the earthquake, liquefaction, and full-reservoir conditions together, then:

$$p[A \cap B \cap C] = p[A]\, p[B|A]\, p[C] \quad (10)$$

Eqn. 10 provides the basis for combining probabilities for any branch pathway in an event tree. Both conditional and independent probabilities are multiplied to find the end-branch probability for the combined occurrence of all events on that particular pathway. Moreover, even though separate branch pathways may contain some common events, each constitutes a unique and therefore mutually exclusive set of events. Therefore, Axiom III specifies that the end-branch probabilities be added to find the total failure probability. Similarly, probabilities for a particular loading range, a particular failure mode, or a particular segment are combined by identifying the relevant branch pathways and adding their end-branch probabilities. In these ways, the probability axioms provide the basic principles for combining event probabilities from event trees to find any aggregated value of interest. All of this, however, assumes that the branch pathways and end-branch probabilities are themselves truly independent, and this raises the important matter of correlation.

3.3 Correlations and common-cause failures

The probability axioms do not specify whether the probability of a particular event should be independent or conditional. This is established from the physical processes involved. The test for independence is if the known outcome of one event would not alter in any way the probability assigned to the other. In practice, probabilistic independence between events is often taken as an assumption, either simply for convenience or because knowledge about the events is not sufficient to specify how they may be related. If, however, there is some possible relationship between them, they are said to be *correlated*, and this affects how their probabilities are combined.

To illustrate, consider the system of a chain comprised of component links, and let E_i be an event that represents failure of some link (Ang and Tang, 1975). Figure 4a shows the case of a single-link chain, and suppose that for this link $p[E_1] = 0.05$. Here the probability of system failure is obviously the same as the failure probability of the link, or 0.05.

Next, consider the two-link system of Figure 4b. The probability of link failure is again 0.05 for both links, and suppose they have been independently fabricated by different suppliers. Now the failure probability of the two-link system is given by eqn. (4) as:

$$p[E_1 \cup E_2] = p[E_1] + p[E_2] - p[E_1 \cap E_2] \quad (11)$$

and from eqn. (6):

$$p[E_1 \cup E_2] = p[E_2|E_1]p[E_1] \quad (12)$$

so,

$$p[E_1 \cup E_2] = p[E_1] + p[E_2] - p[E_2|E_1]p[E_1] \quad (13)$$

$$= 0.05 + 0.05 - 0.05p[E_2|E_1] \quad (14)$$

$$= 0.10 - 0.05p[E_2|E_1] \quad (15)$$

Here, E_1 and E_2 are assumed to be probabilistically independent, so from eqn. (7):

$$p[E_2|E_1] = p[E_2] \quad (16)$$

and the probability of system failure in eqn. (15) with its two independent components becomes:

$$p[E_1 \cup E_2] = 0.10 - 0.05(0.05) \quad (17)$$

$$= \mathbf{0.0975}$$

Now, suppose that the same two links are fabricated from the same steel by the same manufacturer and have identical strengths. E_1 and E_2 will now be *positively correlated* because if one link fails they are both likely to fail. In the extreme case where failure of one makes it certain that the other would fail they are *perfectly correlated* such that $p[E_2|E_1] = 1.0$. For this condition, the probability of system failure in eqn. (15) becomes:

$$p[E_1 \cup E_2] = 0.10 - 0.05(1.0) \quad (18)$$

$$= \mathbf{0.05}$$

which is the same as for the single-link system of Figure 4a. So positively-correlated system components operate identically to a single-component system if they are perfectly correlated. But in reality, how the links are fabricated and by whom will be uncertain. The degree of component correlation is undetermined and system failure probability can only be bounded, by the assumption of independence on one hand and perfect correlation on the other, as lying between 0.05 and 0.0975.

The chain example illustrates the problem of correlated system components, and it is evident that it can apply to dam systems as well. In general, system components assumed to behave independently but which may actually be influenced by interactions of various kinds are said to be subject to *common cause* or *common mode* failure (McCormick, 1981; Henley and Kumamoto, 1992). Several types of common-cause conditions and correlated events are discussed below.

- **correlated loading conditions**

Floods and earthquakes. Probabilistic independence of flood and earthquake loading conditions rests on the absence of any relationship between meteorology and geology: the occurrence

of an earthquake would say nothing about the occurrence of a flood, or its estimated probability.[2] Flood and earthquake probabilities are therefore combined additively according to eqn. (4), with its third term representing their joint occurrence neglected as insignificant. A severe test of this simplification would be the joint occurrence of the 10-year flood and the 10-year earthquake, each having exceedance probabilities of 0.1 on an annual basis. Since the flood duration would be no more than a few days, its exceedance probability during this time would be on the order of 0.1 x 0.01 = 0.001, the probability of the earthquake during this period would be the same, and the joint probability of their simultaneous occurrence would be on the order of 10^{-6}. This shows that the joint probability of flood and earthquake occurrence is indeed negligible and that probabilities for flood and earthquake conditions can be added under the assumption of independence with insignificant error.

Static and flood/earthquake conditions. Static loading conditions in Reclamation practice are taken as independent of flood and earthquake conditions, using threshold loads for seismic and hydrologic failure to distinguish them from static conditions. Here, some correlations do exist. For example, internal erosion (static) events can be correlated with flood-induced increases in reservoir level, and with inertial forces or deformations produced by seismic shaking (Vick, 1993; Vick and Stewart, 1996). These correlations are usually accounted for explicitly, by including branches associated with various flood conditions in the static (internal erosion) event tree, or by including certain particle transport conditions in the seismic event tree. However, these kinds of correlations can be especially easy to overlook, and they require particular attention during the failure mode identification stage of the risk analysis process.

- **correlations between failure modes**

The failure modes associated with any given loading condition are usually assumed to be independent and are developed in the event tree in this way. But there are often correlations between many of them due to various kinds of physical dependencies that are not explicitly addressed. For example, consider a compacted clay embankment on a liquefaction-susceptible foundation subject to two seismic failure modes: foundation liquefaction leading to flowsliding, and inertial (ANewmark@-type) crest deformations leading to overtopping. Typically these would be treated as independent, but they share a

[2] This has not always been so. Only a few decades prior to the creation of the Reclamation Service, the prevalent doctrine was that Arain follows the plow,@ so flood probability then was quite literally conditional on the presence of bare earth from cultivation. John Wesley Powell was instrumental in changing this presumption through his influence on early Federal irrigation policy. This illustrates that probabilistic independence is a function of one=s state of knowledge, and therefore the product of judgment.

common element in that seismically-induced foundation pore pressures influence both of them. In general, failure modes tend to be idealized as independent largely because this is the way they are treated analytically, but a number of correlations can become apparent on close inspection.

Another kind of physical dependence producing common-cause failure conditions occurs when the failure of one system component places additional loading on some other that could cause its failure as well. Take a concrete-gravity dam subject to basal sliding from either low friction angle at the contact or from uncertain drain effectiveness. Incipient movement could disrupt the drains, increasing uplift pressures and increasing the likelihood of sliding. Here the failure modes interact - the occurrence of one enhances the other. This kind of correlation has been observed in actual failures. A certain tailings dam contained design and construction deficiencies related to both the filter and the diversion conduit that made both components subject to individual internal erosion failure modes. The failure investigation showed that both failure modes occurred, but that they operated in a complex interaction between them that would not have been fully described by either one separately (Dam Review Team, 1996). Again, some of these interactions and dependencies between failure modes and system components may be captured explicitly in their event tree development (internal erosion from the embankment into the foundation is one that Reclamation typically emphasizes), but many are not, either because they are too difficult to anticipate as for the example tailings dam, or because the event tree would simply become too complex if they were.

- **spatial correlations**

Consider an embankment dam on an alluvial glacial-outwash foundation with a limited number of borings, some of which encountered intervals of liquefaction-susceptible silt, and suppose that the embankment is divided into several segments to reflect these apparent differences. Suppose then that additional borings were drilled, with still more segments defined accordingly. It is easy to see that, taken to the limit, a nearly infinite number of segments could be defined. If the total embankment failure probability were determined by adding the respective contributions, then it would be arbitrarily controlled by the number of segments defined. Spatial correlation solves this apparent paradox. The segments are not truly independent but spatially correlated - the presence of silt layers in one increases the likelihood that they may extend into or otherwise be found in neighboring segments.

If conditions are spatially correlated, as a common geologic origin would imply, then their probabilities are not strictly additive. The chain example provided earlier illustrates exactly this effect. Where multiple components such as those shown in Figure 4b are perfectly correlated, the example showed how the system failure probability collapses to that of the single-component system of Figure 4a; similarly, the combined failure probability for perfectly-correlated segments would be the same as that for a single-segment dam. On the other hand, if the conditions within each segment had different geologic origins (say jointed rock in one and alluvial outwash in another), only then would their failure probabilities be truly independent and therefore additive. Here, however, the number of segments is not arbitrary. They arise from unique statistically-homogeneous populations that are geologically unrelated. Many typical situations of spatial correlation lie between these two extremes.

- **system correlations**

Another type of common-cause or common-mode failure affects different systems where the failure of one system produces loads on another. An example is the risk analysis for a project (Vick, 1997) where four separate dams, each with distinct downstream populations, impound a single reservoir to produce separate systems like those on Figure 1b. One dam is a gated concrete-overflow structure, another a rockfill dam, and two more are earthfill dikes both with histories of slope instability. In this case, failure of the concrete or rockfill structure would produce rapid-drawdown conditions that could be an initiator for upstream slope failure of either dike. A even more obvious kind of system correlation is the cascade failure of dams in series, and Reclamation has separate procedures for handling these situations in risk analysis applications.

- **unimodal bounds**

The chain example illustrated how bounds could be placed on failure probability for a system using assumptions of completely independent and perfectly-correlated components. More generally, systems can contain varying numbers of components with different failure probabilities and indeterminate degrees of positive correlation. So-called *unimodal bounds* provide a way of combining such component failure probabilities. For series systems like those on Figure 2a and 2b, which typically apply to dams, system failure probability p_F for n components, each having individual positively-correlated failure probabilities p_i, is bounded by the following (Ang and Tang, 1984):

$$\max p_i \leq p_F \leq 1 - [(1 - p_1)(1 - p_2)...(1 - p_n)] \qquad (19)$$

Intuitively, this expression can also be understood by analogy to a chain. The left-hand side, the highest component failure probability, represents that of the weakest link, and the right-hand side represents the failure of any one or more of them. Also, for the special case of small p_i the right-hand side can be approximated as $\sum p_i$, and the inequality becomes:

$$\max p_i \leq p_F \leq \sum p_i, \qquad (20)$$

So here, for positively-correlated failure modes, segments, systems, or any combination of these, their combined failure probability lies between that for the most likely such condition and their sum as if they were independent. Vick and Stewart (1996) provide examples of the application of the unimodal bounds in (19) to positively-correlated failure modes for several dams. From this and other experience, the range on unimodal bounds is typically a factor of 3 or less. In general, the bounds are narrower when there are less than a few failure modes or where one dominates, and wider when there are a greater number with individual probabilities that are more nearly equal. In practice, if bounds from the inequality of (19) are narrow in relation to the imputed precision of probability estimates (say, less than a factor of 2 or so) it is often sufficiently accurate to adopt the right-hand side of the inequality of (20) and add the individual values. Otherwise, the bounds need to be carried through and propagated to the result in expressing the combined probability as a range.

3.4 Special cases

Special circumstances can be encountered for unusually long dams or dikes that are subject to substantial variation in foundation conditions or breach conditions over their length. These situations can ordinarily be handled by including spatial segments as system components and combining segment failure probabilities as previously described.

More advanced techniques are also available for addressing spatial variation in foundation or embankment soil properties in connection with reliability techniques and the geomechanical models they adopt. Vanmarke (1977) presents the basic elements of statistical analysis of spatial variability, while DeGroot and Baecher (1993) describe the related statistical properties of *autocovariance*, *autocorrelation*, and their measurement. These techniques can be especially useful for long dikes on statistically homogeneous clay deposits, and Christian, et. al. (1992) provide an excellent case history of reliability analysis incorporating spatial variability considerations for static slope stability of hydroelectric project dikes.

Another special case involves geologic anomalies or other defects, especially for long dams or dikes. One way to address such discrete features is to treat their possible presence as independent Bernoulli trials with some occurrence probability per unit length, area, or time. If p_i is the unit occurrence probability and the dam length or footprint contains n such regions, then from the binomial theorem the probability p of encountering at least one of them over the entire dam is (for small p_i):

$$p = 1 - (1 - p_i)^n \tag{21}$$

and their mean number is $(n)(p_i)$. Vick and Bromwell (1989) describe an example for the occurrence of karst sinkholes in a dam foundation where unit sinkhole occurrence probability was determined from regional geologic information. Applying this technique requires identifying such a statistically representative sample population of the anomaly for estimating its unit occurrence probability.

4.0 Combining Risks

Like probability, risk contributions need to be combined, and for similar reasons all having to do with how insights are obtained and information conveyed. Reclamation expresses risk as the combination of failure probability and the number of lives lost, obtained by definition from multiplication of the two. A corresponding risk value can refer to the total risk posed by the dam, or to risks associated with any of its loading conditions, failure modes, segments, or some combination of these.

4.1 Expected value

Each end branch of the event tree that propagates to failure carries with it a failure probability and a loss of life value that together characterize the branch pathway it represents. The mathematical concept of

expected value governs how these values are combined to determine the risk associated with any desired condition described by one or more of these pathways.

Expected value is most often illustrated in relation to gambling and long-run winnings from repeated wagers, and for this reason it is closely associated with the relative-frequency probability interpretation used in characterizing repeatable events. Consider the wager depicted on Figure 5a. If outcome A occurs with probability 0.99 the gain is $5, but for outcome B with probability 0.01 $100 is forfeited. Here the consequences associated with the outcomes are monetary in nature, and each [probability, consequence] pair is multiplied and the products are summed to yield the *expected monetary value* or EMV of the wager - in this case $3.95. This is the average amount that one would expect to receive in the long run if many such identical wagers were made. This also illustrates the concept of *monetary risk aversion*. Although its expected value would make the wager of Fig. 5a an attractive long-term proposition, someone with only $20 in their pocket would find it hard to fund a possible loss and would be adverse to accepting such a risk despite the possible gain.

The expected value of the risk analysis event tree in Figure 5b is obtained in the same way. Here, the probability and loss of life are multiplied to find the risk for each end branch, and these risk values are summed over all relevant branches to find E(L), the *expected loss of life*.[3] This is expressed on Reclamation=s Tier 1 guidelines as *annualized loss of life* since failure probabilities are determined on an annual basis. The principle of risk aversion enters here as well, and for this reason the Tier 1 plot includes the absolute number of lives lost in addition to the expected value.

4.2 Independent and correlated components

The expected value computation combines the individual end-branch risk values by simple addition, which implicitly assumes that each branch pathway is independent from any other. As explained in Section 3.3, this is a valid assumption for combining risks derived from different loading conditions because any correlations they contain are usually included explicitly in the event trees.

Each such loading condition will incorporate several different failure modes, which in general will be positively correlated to some degree. At the same time, it is often the case that the consequences of failure modes for any given loading condition are sufficiently similar that they can be assumed equal with little error. For example, breach parameters, warning times, and related factors would not be materially different if

[3] Here expected value applies to a single-event occurrence - dam failure - rather than repeated trials. Blaise Pascal was the first to extend the concept of expected value to such occurrences with nonmonetary consequences in his famous APascal=s Wager@ on the existence of God around 1662, and both the concept and the terminology of expected value have been deeply embedded in probability ever since. However, *expected loss of life* in no way implies that such an outcome is anticipated or presumed for this single-event occurrence.

seismic failure were to occur by upstream flowsliding or downstream flowsliding, at least within ordinary abilities to evaluate these factors. If so, then loss of life would also be the same.

Let L_i represent loss of life from any failure mode having probability p_i, and let the constant value L be that which applies to all failure modes producing similar effects. Then the inequality for positively-correlated failure modes of (20) is preserved when multiplying by the constant L:

$$L(\max p_i) \leq (p_F)(L) \leq L\sum p_i \tag{22}$$

If the risk associated with any failure mode is R_i, then again for constant L:

$$R_i = (p_i)(L) \tag{23}$$

and the combined failure risk R_F from all such failure modes becomes:

$$\max R_i \leq R_F \leq \sum R_i \tag{24}$$

The right-hand side of (24) is simply the expected loss of life computation shown on Figure 5b, and the left-hand side is the highest-risk failure mode. Thus, for positively-correlated failure modes with similar consequences, their combined risk is bounded in the same way as their combined probability.

Complications arise, however, for positively-correlated components whose failure consequences are not the same. If L_i varies, then the inequality of (22) is not necessarily preserved. In other words, the component with the highest failure probability may not constitute the highest risk because its consequences may be lower. In addition to failure modes with different consequences, this situation occurs for dam segments of varying height and breach parameters, or systems with different PAR's. Here, there is no straightforward way to reflect positive correlation, and risks must be combined using the expected-value computations for independent conditions.

4.3 Portraying risk

It is possible to combine risks in many useful and informative ways, but it can be more difficult to portray them visually in a graphic format that effectively communicates the information they contain. In particular, the Tier 1 plot has the capacity to portray the relationships between only a limited number of risk variables without clutter that reduces its effectiveness as a visual risk-communication tool. Figure 6 illustrates this with two Tier 1 plots for an example dam. Together they contain information for three risk-related variables: (1) the risk for static (internal erosion) failure modes, (2) uncertainty in risk estimates represented by the scattergrams from Monte Carlo simulation realizations, and (3) two different system descriptions, one with and the other without a warning system in place. Significantly, it takes two Tier 1 plots to present this

information, and their relationship can be seen only by comparing them side-by-side. While it might have been desirable to also include risk information developed for other loading conditions, failure modes, or individual dam segments, this would not be possible without presenting an entire array of such plots which might tend to obscure the most important factors and make visual comparisons harder to draw.

From a decisionmaker=s standpoint, the format of Tier 1 must allow easy comparison of relative differences in the risk elements included, and it must be sufficiently similar from one risk analysis to another to be familiar and readily recognized. From the standpoint of the risk analysis team, this inevitably requires choices about which risk information is most essential to include on Tier 1 plots and how to portray it. Effective and reasonably uniform formats can be expected to develop over time with close coordination and feedback between Reclamation decisionmakers and risk analysis teams.

5.0 Summary

Combining probabilities and risks depends fundamentally on the system description adopted in their original derivation. Any dam system contains components that together define what can fail, how it can fail, different locations where failure can occur, and what failure would affect. In practice, the system is defined by physical features that are subject to various failure modes and, where needed, by segments that reflect spatial variation in conditions along the length of the dam. The system is bounded by the physical location of these features and by the downstream limits of the PAR.

Combining the probabilities and risks assigned to these various components then depends on how they interact as a system, and the basic axioms of probability together with the concepts of expected value provide the mechanics for doing so. In general, probability and risk contributions are combined additively where they are independent, or where their interactions are included explicitly in the event tree. Components may be idealized as independent, but careful inspection often shows that they are correlated due to physical dependencies, spatial relationships, or transfer of system loads. Where components are positively correlated to an undetermined degree, a combined probability or risk value cannot be specified precisely but can be bounded within reasonable limits in most cases. Table 1 shows several categories of commonly-encountered systems and component types together with some of the probability and risk combination methods typically applicable for addressing them.

Beyond these mechanics is the question of what probabilities and risks should be combined and why. The probability calculus does not address this question, which requires judgments as to what kinds of probability and risk combinations are likely to yield useful insights about dam behavior, and which need to be communicated for decisionmaking purposes. As a vehicle for risk communication, the format of the Tier 1 guidelines has certain inherent limitations in the amount of risk information it can effectively convey. This ultimately requires choices about how much information should be incorporated graphically and how it is presented. These determinations involve collaboration between risk analysis teams and decisionmakers, and they remain to be fully explored.

6.0 References

Ang, A. and Tang, W., 1975, Probability Concepts in Engineering Planning and Design - Volume I, Basic Principles, John Wiley & Sons.

Ang, A. and Tang, W., 1984, Probability Concepts in Engineering Planning and Design - Volume II, Decision, Risk, and Reliability, John Wiley & Sons.

Benjamin, J. and Cornell, A., 1970, Probability, Statistics, and Decision for Civil Engineers, McGraw-Hill.

Christian, J, Ladd, C., and Baecher, G., 1992, "Reliability and Probability in Stability Analysis," Stability and Performance of Slopes and Embankments - II, R. Seed and R. Boulanger (eds.), Geotech. Spec. Pub. No. 31, ASCE.

Dam Review Team, 1996, "Final Report on Technical Causation, Omai Tailings Dam Failure," Guyana Geology and Mines Commission, BiTech Publishers, Vancouver.

DeGroot, D. and Baecher, G., 1993, "Estimating Autocovariance of In-Situ Soil Properties," Journ. Geotech. Eng., ASCE, v. 119, no. 1.

Henley, E. and Kumamoto, H., 1992, Probabilistic Risk Assessment - Reliability Engineering, Design, and Analysis, IEEE Press.

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

Popescu, R., Prevost, J., and Deodatis, G., 1996, "Influence of Spatial Variability of Soil Profiles on Seismically Induced Soil Liquefaction," Uncertainty in the Geologic Environment: From Theory to Practice," C. Shackelford, et. al. (eds.), Geotech. Spec. Pub. No. 58, ASCE.

Vanmarke, E., 1977, "Probabilistic Modeling of Soil Profiles," Journ. Geotech. Eng. Div., ASCE, v. 103, no. GT11.

Vick, S., 1993, "Effects of Seismic Shaking on Internal Erosion of Embankment Dams," report to BC Hydro, April.

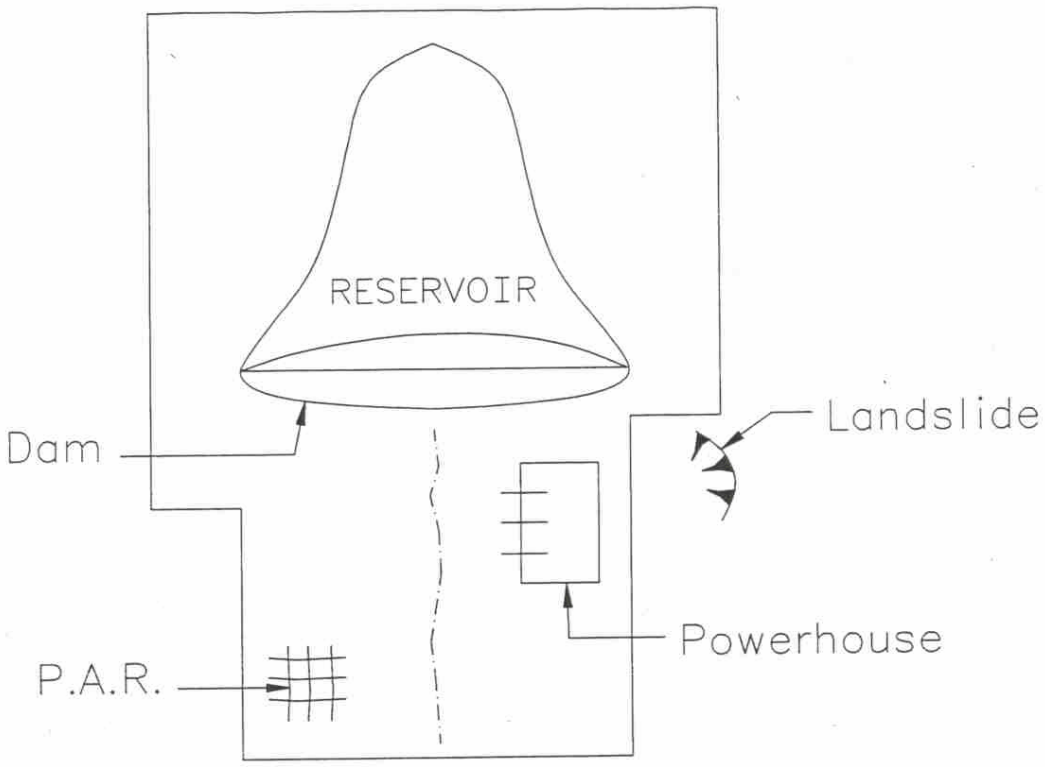
Vick, S., 1997, "Dam Safety Risk Analysis - New Directions," Int. Water Power & Dam Construction, May.

Vick, S. and Bromwell, L., 1989, "Risk Analysis for Dam Design in Karst," Journ. Geotech. Eng. Div., ASCE, v. 115, no. 6.

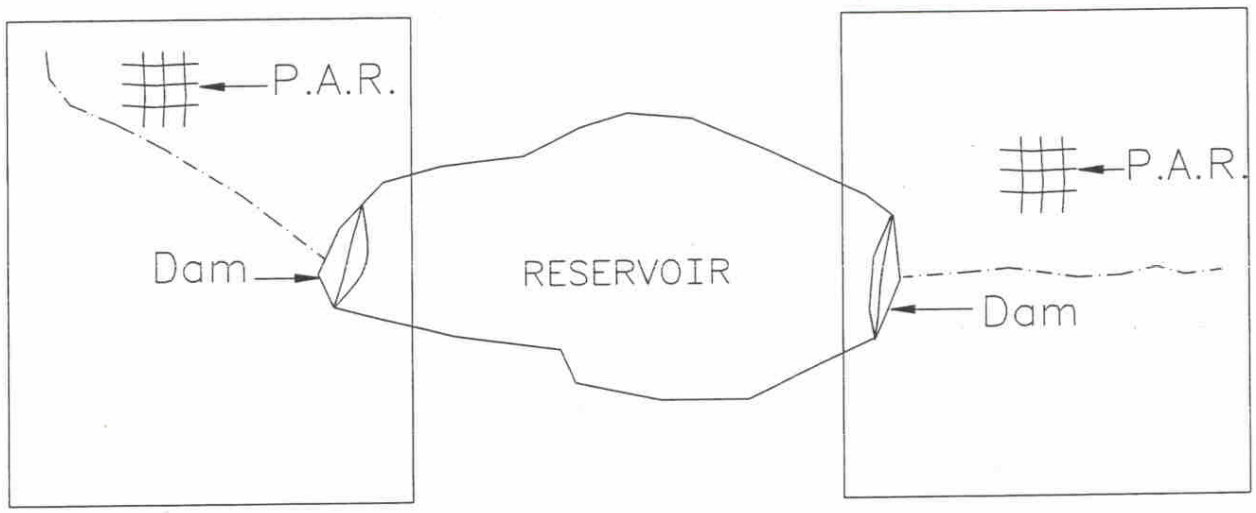
Vick, S. and Stewart, R., 1996, "Risk Analysis in Dam Safety Practice," Uncertainty in the Geologic Environment: From Theory to Practice," C. Shackelford, et. al. (eds.), Geotech. Spec. Pub. No. 58, ASCE.

Table 1. Summary of Probability and Risk Aggregation Techniques

Type of System	Type of Component Failure	Methods for Combining Component Failure Probabilities	Methods for Combining Component Failure Risks
Single dam and PAR	separate loading conditions (static, seismic, hydrologic)	account for correlations explicitly in event tree(s); add probabilities to determine total failure probability	add end-branch risks to determine expected loss of life from dam failure
	separate failure modes for any given loading condition	determine unimodal bounds from eqn. (19); if bounds are narrow, add probabilities to determine failure probability over all such failure modes. Otherwise, retain probability bounds	similar consequences for each failure mode: determine bounds from eqn. (24); add applicable end-branch risks if bounds are narrow. Otherwise, retain risk bounds. different consequences for each failure mode: add applicable end-branch risks to determine risk over all such failure modes
	separate segments of different height and breach conditions (all loading conditions)	determine unimodal bounds from eqn. (19); if bounds are narrow, add probabilities to determine failure probability over all such segments. Otherwise, retain bounds	add segment risks to determine risk over all such segments
	separate segments with different foundation conditions (static and seismic loading conditions only)	same geologic origin or process: determine unimodal bounds from eqn. (19); if bounds are narrow, add probabilities to determine failure probability over all such segments. Otherwise, retain probability bounds	same geologic origin or process: determine bounds from eqn. (24); if bounds are narrow, add risks to determine risk over all such segments. Otherwise, retain risk bounds
		different geologic origin or process: add segment probabilities to determine failure probability over all such segments	different geologic origin or process: add segment risks to determine risk over all such segments
Multiple dams, same PAR	For Tier 2, determine probabilities separately for each dam. For Tier 1, treat each dam as for a segment of a single dam		



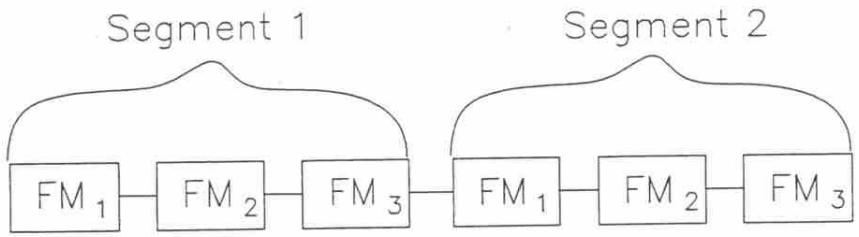
A.) Single Dam, Reservoir, and PAR



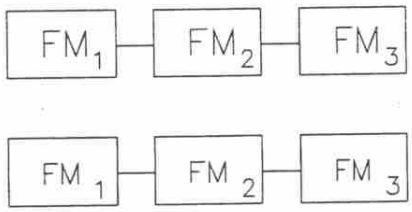
B.) Multiple Dams and PAR's, Single Reservoir

System Boundaries

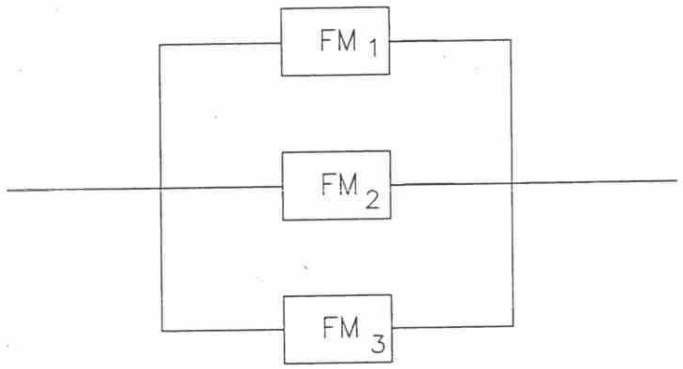
Figure 1



A.) Components in Series, Multiple Segments (Fig. 1a)



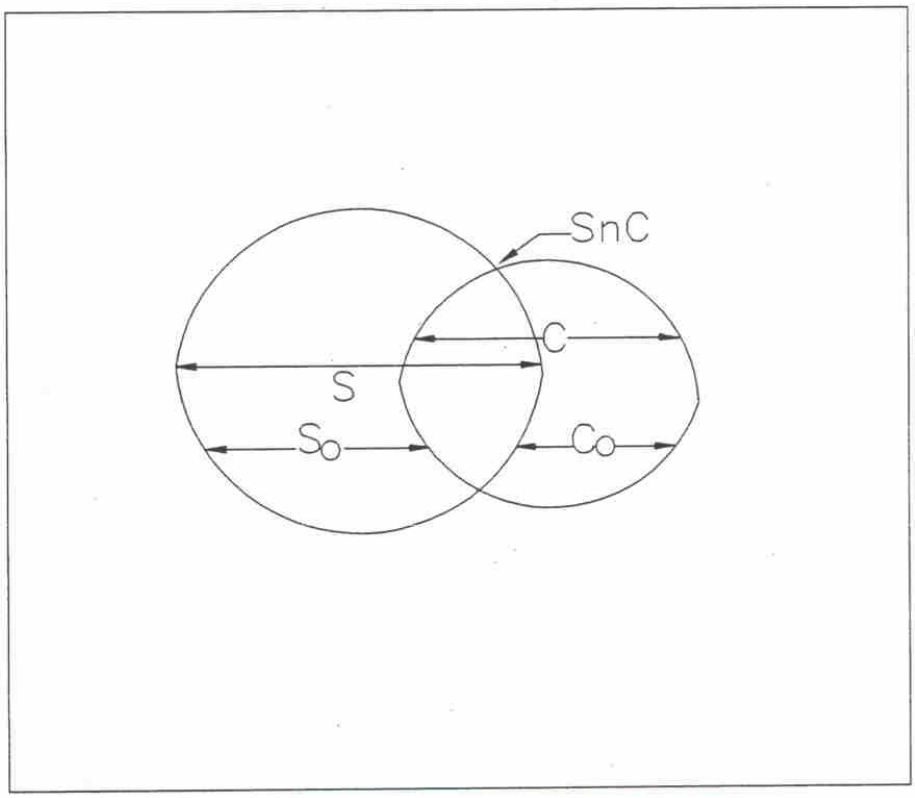
B.) Components in Series, Multiple Systems (Fig. 1b)



C.) Components in Parallel

Series and Parallel Systems

Figure 2

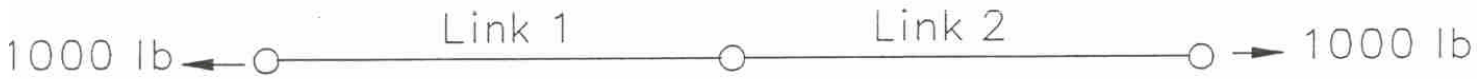


Sample Space: All soil and rock types

Venn Diagram

Figure 3

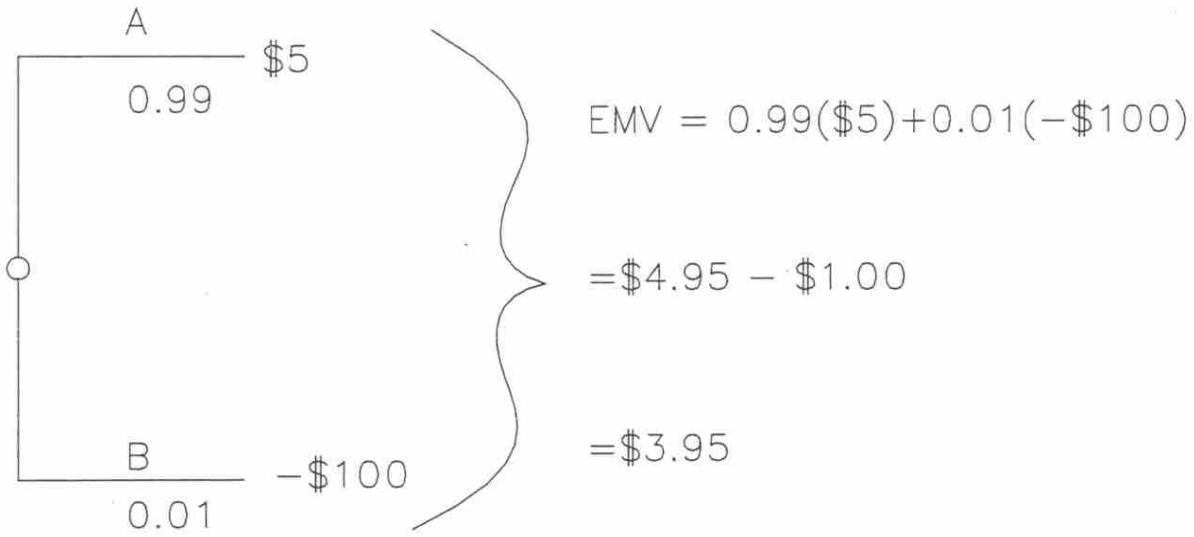
A.) Single Link



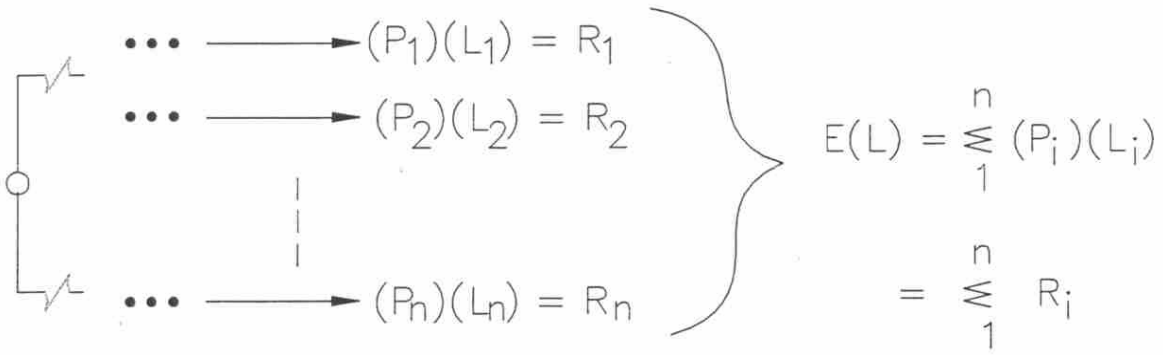
B.) Two Links

Chain
Example

Figure 4



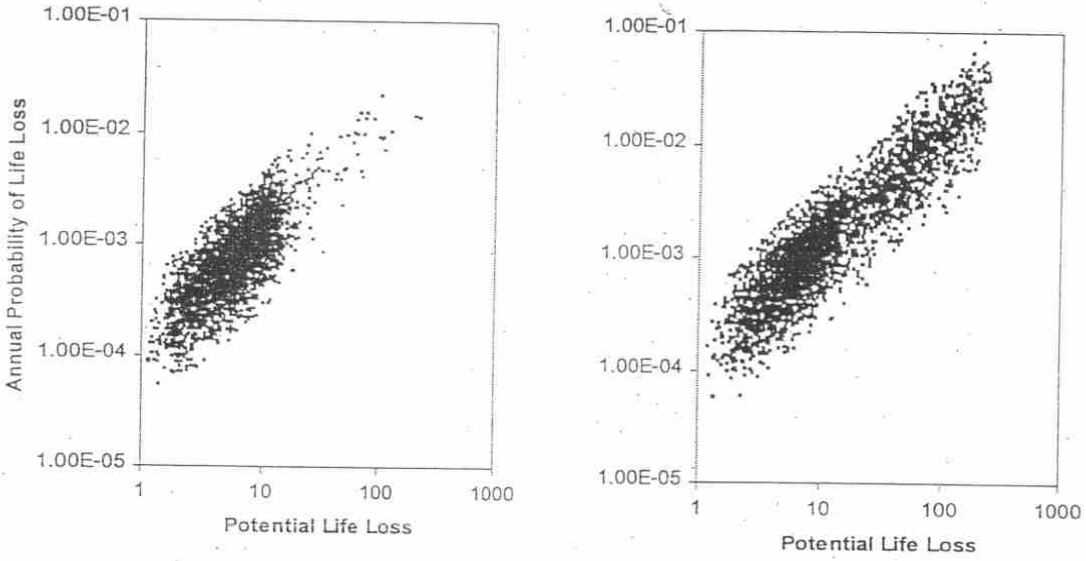
A.) Wager Involving Monetary Value



B.) Event Tree Involving Loss of Life

Expected Value

Figure 5



Tier 1 Plots for
Different Risk Combinations

Figure 6