SANDIA REPORT SAND82-0366 • Unlimited Release • UC-15

Printed March 1982

Comprehensive Safeguards Evaluation Methods and Societal Risk Analysis

J. Mark Richardson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

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.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: 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, nor any of their contractors, subcontractors, or 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, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors or subcontractors.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

NTIS price codes
Printed copy: A04
Microfiche copy: A01

SAND--82-0366

DE82 013273

Distribution Category
UC-15

SAND82-0366
Unlimited Release
Printed March 1982

COMPREHENSIVE SAFEGUARDS EVALUATION METHODS AND SOCIETAL RISK ANALYSIS

J. Mark Richardson
Systems Analysis and Technology Applications
Division 4416
Sandia National Laboratories
Albuquerque, NM 87185

DISCLAIMER

This book 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.

Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
for the
U.S. Department of Energy

3-4

ABSTRACT

Essential capabilities of an integrated evaluation methodology for analyzing safeguards systems are discussed. Such a methodology must be conceptually meaningful, technically defensible, discriminating and consistent. A decomposition of safeguards systems by function is mentioned as a possible starting point for methodology development.

The application of a societal risk equation to safeguards systems analysis is addressed. Conceptual problems with this approach are discussed. Technical difficulties in applying this equation to safeguards systems are illustrated through the use of confidence intervals, information content, hypothesis testing and ranking and selection procedures.

Acknowledgment

The author gratefully acknowledges the helpful assistance of Mark K. Snell, Division 1765, in the development of some of the material contained in this report. Valuable discussions were also held with Harold A. Bennett and Leon D. Chapman, Divison 4416.

Contents

Illustrations

1. INTRODUCTION

Safeguards systems at nuclear facilities consist of the physical protection, material control and material accounting systems. Therefore, a comprehensive methodology for evaluating vulnerabilities and upgrade options of a safeguards system should consider the interrelationships of these three systems. Such a technique is needed to represent existing capabilities as well as to quantify the impacts of specific system improvements.

As a way of approaching this methodology development, the concept of systems integration must be considered. A very general integration scheme would allow for consideration of the safeguards consequences arising from such systems as operations and safety. However, safeguards integration has generally come to mean the specification of and allowance for interactions among the physical protection, material control and material accounting systems at a nuclear facility. A comprehensive evaluation method should provide the framework for including system interactions at any level desired. The first major topic of this report is a general discussion of comprehensive evaluation methods for safeguards systems analysis and design.

One method of safeguards system evaluation that has been proposed uses the concept of societal risk as a measure of system effectiveness. The risk equation includes three terms: frequency of events, probability of events having consequences of public concern and a measure of the societal impact of the consequences. A risk approach has been used effectively to analyze safety systems and associated risk to the public. However, the application of risk analysis to safeguards is not as straightforward as its application to safety. The second subject of this report is a technical analysis of risk and its application to analysis of safeguards systems. Particular attention is given to the probabilistic assumptions in risk analysis, uncertainty in societal risk results and the use of risk as a decision-making tool in safeguards analysis and design.

2. EVALUATION METHODOLOGY

The desirability of developing a technique for evaluating overall safeguards performance is recognized and should be actively pursued. Several topics that must be considered in a comprehensive evaluation have been identified. These include problem definition, properties of evaluation methods, effective ways of decomposing the problem into manageable portions and the recognition of differences in integration and aggregation techniques.

The first problem which must be addressed is the scope of the effort. One possible type of integration involves strictly safeguards functions; i.e., physical protection, material control and material accounting. This approach would allow specification of trade-offs among safeguards options within a facility in order to optimize protection. A higher level of integration could be achieved by consideration of interactions among systems at a facility, such as safeguards, operations and safety. This level of integration would be extremely useful in design studies but of less use in vulnerability analyses. Therefore, the purpose of the integration methodology must be defined explicitly.

2.1 Necessary Properties

The development of a comprehensive methodology for assessing safeguards system performance would be useful for identifying vulnerabilities, as well as for specifying trade-offs, for example, in comparing the cost impact of upgrades to a facility or upgrades at different facilities. There are several properties which such an evaluation method should possess in order to be effective in determining appropriate trade-offs. The evaluation method should be

1. Conceptually meaningful. The method should be easily understood and logically related to the real system and its environment.
2. Technically defensible. The theoretical derivation of the methodology should be correct and understandable in order for the results to be accepted. Also, the information used in the method should be defensible and as far removed from arbitrary judgment as possible.
3. Discriminating. The methodology should be able to distinguish quantitatively the differences in various systems. It should aid a decision maker beyond his intuition and knowledge of the system.
4. Consistent. Independent analysis groups, using the same information, should reach similar upgrade or evaluation decisions. If their recommendations differ, it should be theoretically and practically possible to identify their different assumptions.

If these properties are included in an evaluation methodology, then a useful tool for analyzing, comparing and contrasting safeguards systems should result.

2.2 Threat Decomposition

Some consideration has been given to two methods of decomposing this problem into logical, connected parts. One decomposition can be accomplished by generating a set of specific threats that are believed to be credible at a certain facility. Another method is based on decomposing the facility safeguards system according to functions performed by safeguards components. Both methods are discussed below.

The threat decomposition method begins with a specification of adversary intent, such as sabotage or theft, and then proceeds to more detailed threat characteristics, such as specific adversary goals, adversary types, personnel and resources. Threat decomposition relies explicitly on the choice of a small, facility-specific number of threats chosen independently of the safeguards features at the facility. Figure 1 provides an example of a threat decomposition to the personnel level, resulting in 13 specific threats. Because it depends on a specific threat spectrum, this method probably cannot identify safeguards deficiencies other than those inherent in this set of threats. If intelligent adversaries are assumed, then a threat that is not considered in the site-specific threat spectrum and hence is not explicitly guarded against, could easily become the most likely to occur. Threat decomposition, because it begins with threat specification, could provide no information on vulnerabilities or capabilities beyond those addressing the analyst's *a priori* conception of credible threats.

Another shortcoming of threat decomposition is that it forces analysis of safeguards systems using scenario techniques in order to address the specific threats. Scenario techniques certainly play an important role in safeguards analysis, but they

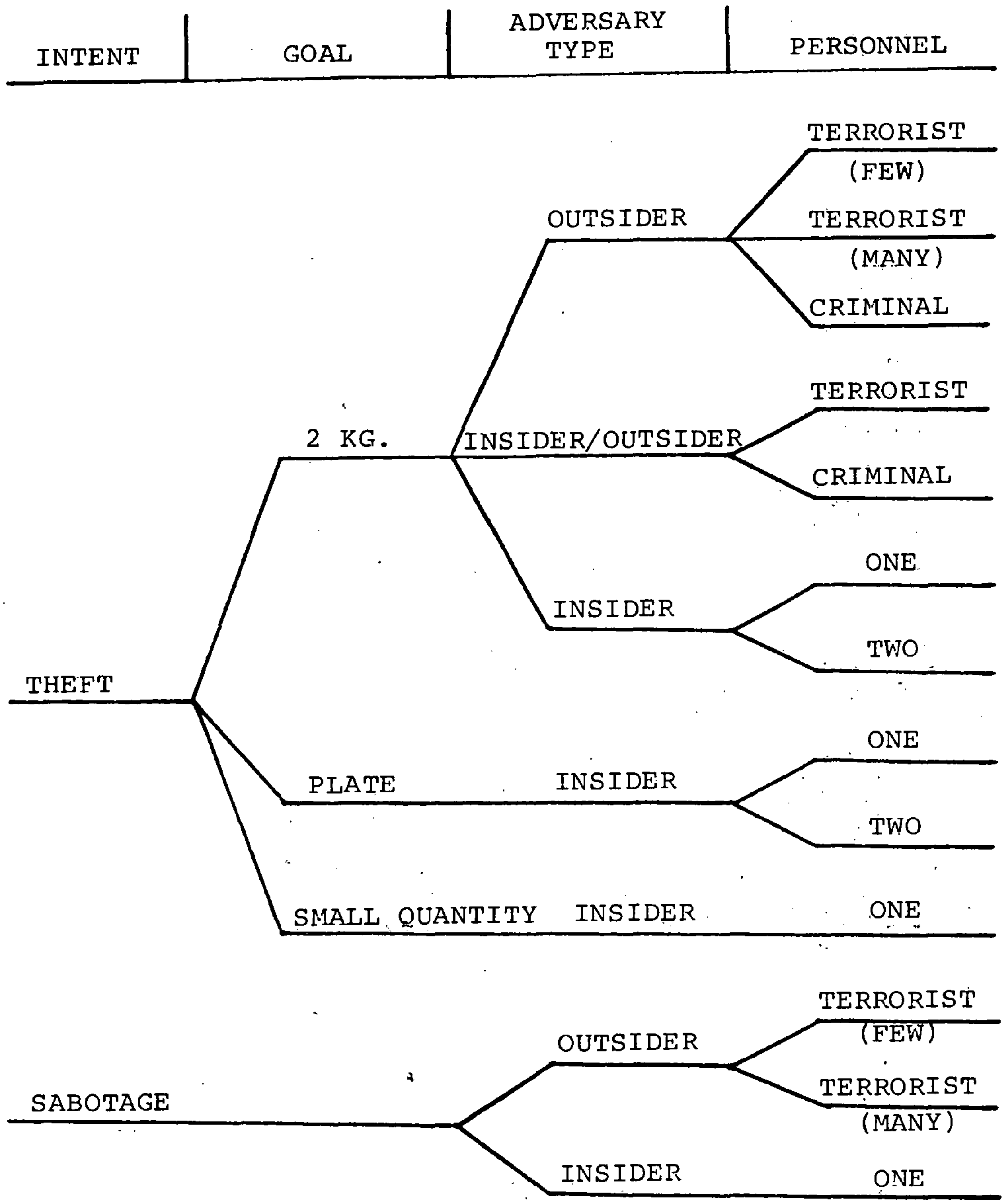


Figure 1. Threat Decomposition

present rather serious problems when used exclusively. The goal of performing a comprehensive analysis can never be attained by considering scenarios alone with no regard for the interactions between the safeguards systems and the threats. Because of the intractably large number of possible scenarios for any threat, some bounding technique must be employed that is as independent of arbitrary judgment as possible. Threat decomposition requires the analyst to bound the problem subjectively by making value judgments concerning what is thought to constitute a "representative" scenario. It is not clear how this scenario is to be chosen nor how it is to be determined that any one scenario includes all aspects of a threat. This method relies heavily on arbitrary judgment and thereby loses technical credibility because of the subjective choice of scenarios. For the reasons cited above, this type of analysis is conducive to neither reproducibility of results, internal consistency nor comprehensiveness.

2.3 Functional Decomposition

The threat spectrum must be factored into the evaluation, however. The capabilities of the safeguards system itself should be used to identify which types of threats are difficult to protect against and, therefore, must be further analyzed. This approach to the problem would decompose safeguards systems into the various functions performed by the system. Examples of functions could include interruption, neutralization, access denial, prevention of acquisition and prevention of removal. These terms, as well as other safeguards terms, are defined in the glossary. The decomposition would proceed to a detailed level, such as the component level. If elements of the material control and accounting system, such as paper transactions or accounting records, are considered as components, then all decompositions could be considered to extend to the component level. This method is logically compelling because the adversary interacts with the safeguards system at the component level, and the specifics of this interaction are what the analyst needs. Component performance can then be specified, and the capabilities of the system can be determined.

Figures 2a-2c show a decomposition based upon the subfunctions of sabotage prevention and prevention of theft and diversion. Sabotage is prevented by preventing access to or destruction of material or components. Theft can be prevented by prevention of access, acquisition or removal of material. The decomposition can proceed in a similar manner to the component level. In this manner, systems responsible for each safeguards component may be identified and evaluated. Figures 2a-2c identify the physical protection (PP), material control (MC) and material accounting (MA) systems and their responsibilities.

In the functional decomposition, the threat spectrum for a facility is factored into the problem at the component level by specification of component performance against postulated threats. This is a more general method than considering threats as the first step in the analysis because the problem can be bounded in an explicit, reproducible manner. Bounding is achieved by using realistic limits on component performance against adversary capabilities, thereby obviating the necessity of finding "representa-

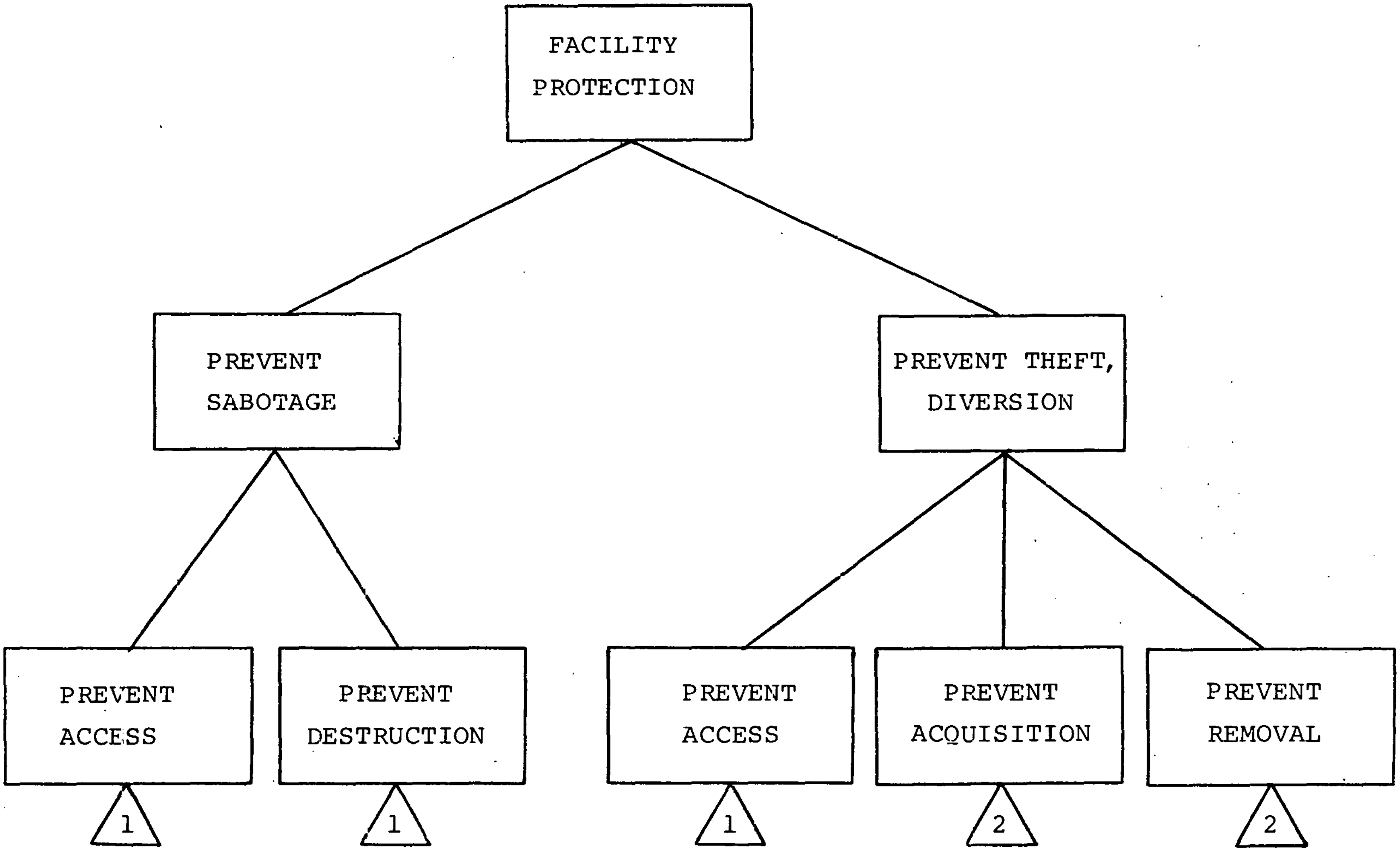


Figure 2a. Decomposition of System Functions

PP - Physical Protection

MC - Material Control

MA - Material Accounting

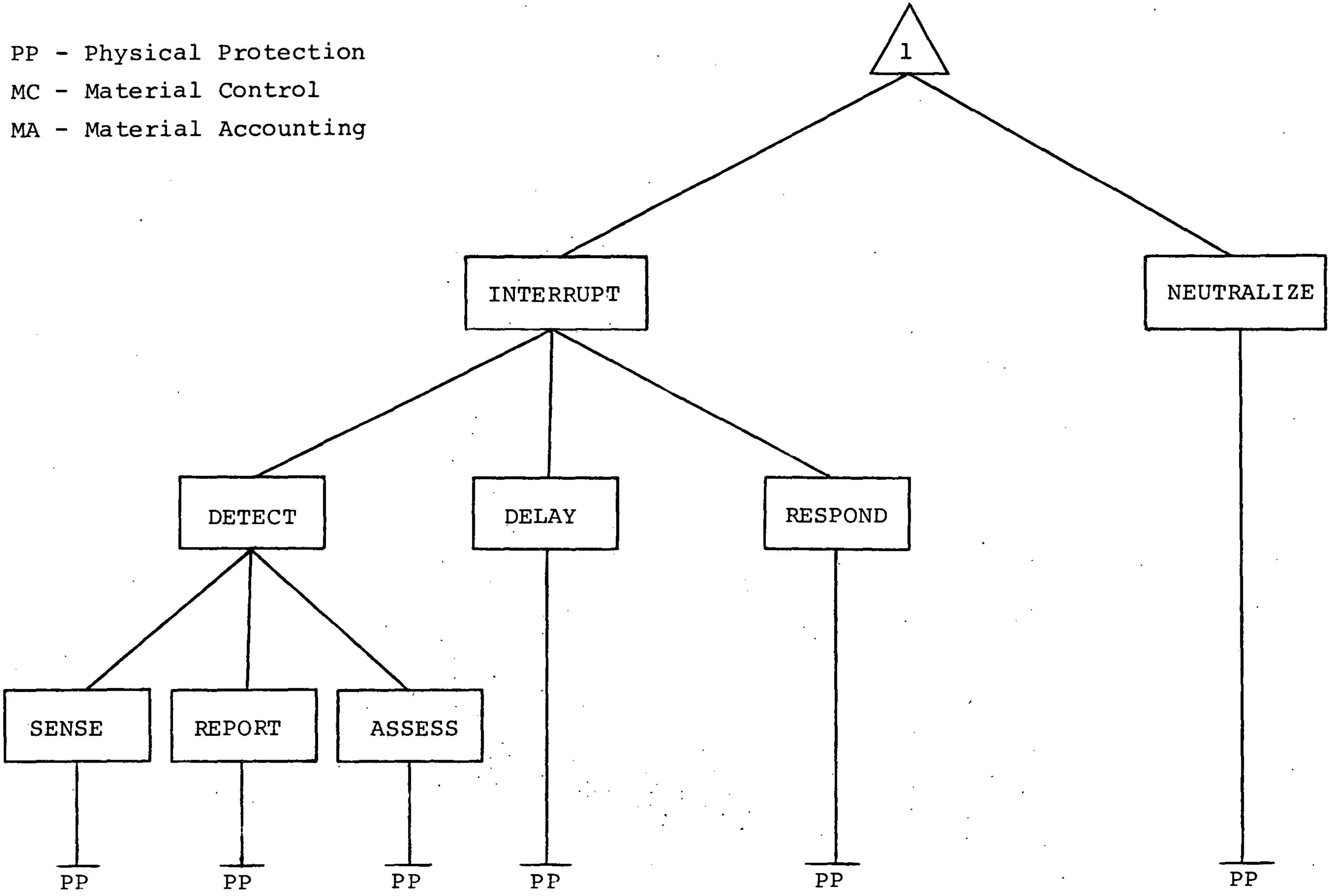


Figure 2b. Decomposition of System Functions (Continued)

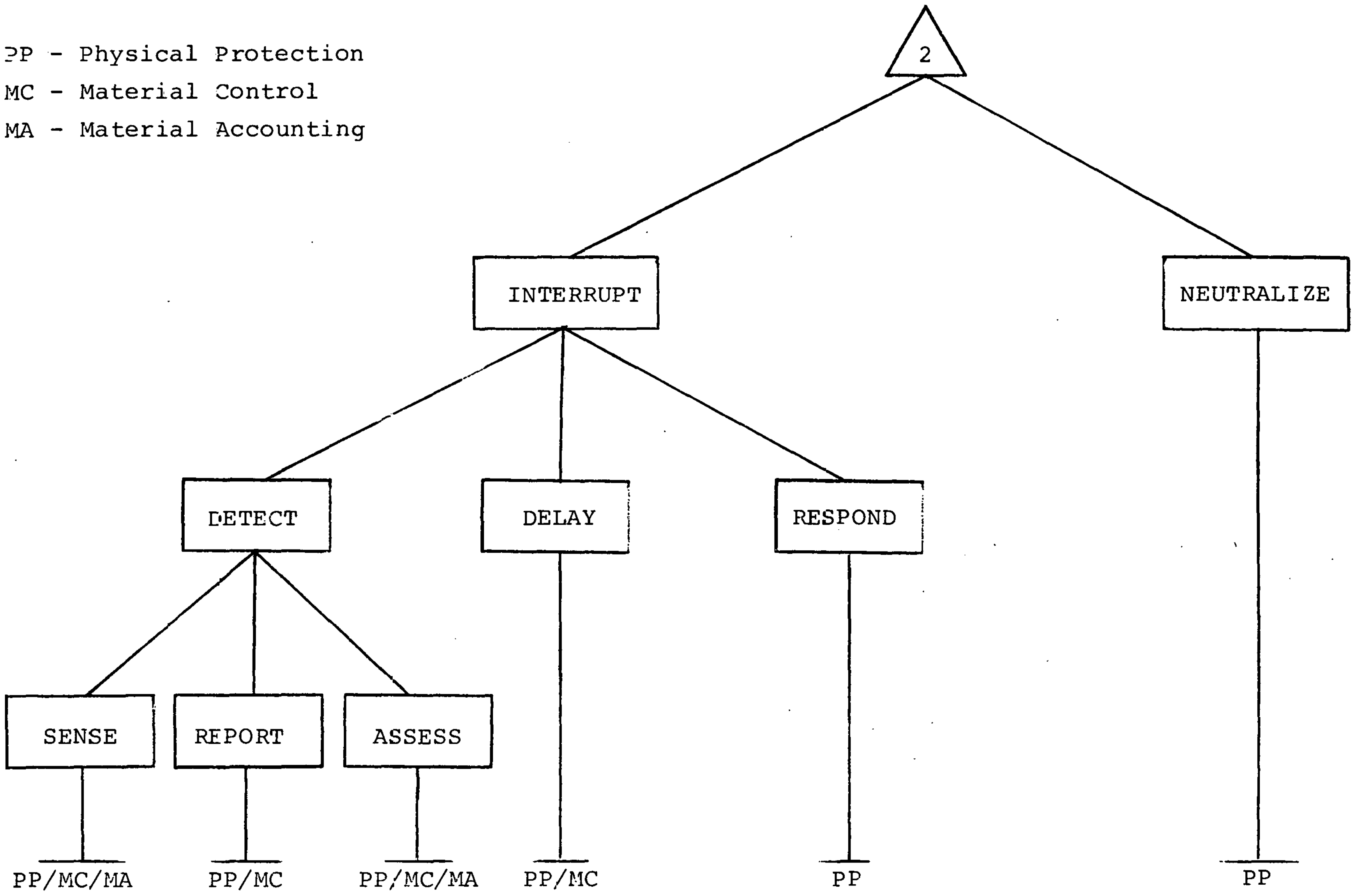


Figure 2c. Decomposition of System Functions (Continued)

tive" scenarios. Best-estimate analysis is easily performed, and sensitivity analysis can be done by varying component performance parameters. Note that all elements of a safeguards system, e.g., barriers, alarms, communication devices, guards, procedures, paper transactions, etc., can be considered as components with associated performance parameters. Such a functional decomposition could allow integration of safeguards systems with other facility systems.

It is impossible to specify an approach for the best evaluation methodology. Conceptually, it does appear that a functional decomposition provides a better starting point for evaluation than a threat decomposition. The best approach may very well be different from either of these. It is clear, however, that more work should be devoted to this problem.

An additional word is in order concerning integration versus aggregation of results for a safeguards analysis. An integrated evaluation scheme implies that system characteristics are meshed at a level as detailed as possible and that this interlocking is continued, where possible, until a coherent, manageable result is obtained. Thus, such a scheme should explicitly account for system interactions at detailed levels. This type of analysis may be contrasted with aggregation schemes, in which a combinatorial technique is used to produce a number for decision making. Aggregation may be employed at any level of the analysis but is often used as the last step of the analytic process. Information is lost in aggregation, but this loss may sometimes be justified, quite properly, by the increased ease in assimilating the results. A good integrated methodology would almost certainly require some type of aggregation as part of the analysis. It is felt, however, that an aggregation is not sufficient; some integration of system characteristics should be considered since a method of identifying and accounting for system interactions has not been developed.

3. SOCIETAL RISK ANALYSIS AND SAFEGUARDS

Risk analysis has proved its worth in several areas of application. In particular, the analysis of system safety has shown that risk analysis can be very useful. This utility is, of course, a direct consequence of the appropriateness of the application, as well as the existence of meaningful data for parameter specification and validation procedures. There is a relatively large body of data for component failure, and much work has been done on the modeling of physical consequences resulting from reactor accidents. Fault tree analysis can provide probabilistic data for a safety system. All these factors combine to provide a meaningful application of risk analysis to reactor safety studies.

3.1 The Risk Equation

The risk equation $R = F \cdot P \cdot C$, where F represents event frequency, P is the probability of the event having consequences of concern and C represents the consequences of the event, was presented as a method for studying the societal impacts of safeguards systems.[5] This so-called ERDA-7 risk equation could provide useful results if F, P, and C could be specified realistically. This section discusses the risk equation and its application to a comprehensive safeguards evaluation methodology in the context of thc four properties listed above.

In the use of this risk equation in safeguards analysis, the three terms have the following specific interpretations: F is a measure of the number of adversary attempts which may be directed against a facility (it may be an absolute or a relative magnitude), P represents the probability of a successful adversary attempt against a facility (it is a measure of the effectiveness of the facility safeguards system) and C is a measure of the consequences resulting from a successful adversary attempt.

3.2 Safeguards Application

In general, risk analysis is a conceptually meaningful way to study safeguards systems. It is related to how well the system responds to postulated threats and could, theoretically, be used to evaluate trade-offs. The ERDA-7 type risk approach has serious problems in its implementation, however. In fact, the author believes that the last three desirable properties for an evaluation methodology are not satisfied by this particular risk formulation.

3.2.1 Technical Considerations

The author feels that the ERDA-7 type risk framework is not technically defensible. The first objection is that the three terms in the risk equation are not independent, an implicit assumption of the method. The numbers assigned to frequency and probability are correlated because the adversary's perception of the probability of successful action influences the frequency of his attempts and the type of strategy to be used. Consequence numbers are correlated with attempt frequencies because the adversary's perception of possible consequences affects the likelihood of his attempting any aggressive action. Successful attempt probabilities are influenced by consequences through both the adversary's dedication to achieving a particular consequence and the safeguards system's dedication to preventing that particular consequence. Specification of the appropriate F, P and C, each of which depends dynamically on the others, appears to be an intractable problem.

In particular, the specification of F in safeguards applications is impossible. In safety studies, F represents component failure frequencies. These frequencies can be measured and/or approximated by experimental techniques and historical data. F can be specified realistically in this application because of the predictability of hardware performance. In safeguards applications, the frequency of events, e.g., sabotage attempts, is not predictable because the adversary is human and intelligent with unpredictable actions. Also, the adversary is influenced by a multitude of considerations. Thus, the analyst is forced to try to predetermine a strictly human decision with virtually no inputs. The current data base of incidents at nuclear installations is so small that no useful information can be obtained from it; nor is it clear that data for industrial sabotage and terrorist attacks is applicable to the nuclear industry. Even if such a data base did exist, the extrapolation of the data into the future would have little a priori validity, again because of the human element involved. For example, it is possible that a successful act against one facility would lead to a number of similar assaults at other facilities. The important point to make in this regard is that the frequency of attempts is not a random variable, although in the risk framework it is assumed to be random.

If the frequency term is considered to specify relative frequencies, the same problems are encountered. Suppose the relative frequency of threat 1 to threat 2 is to be used. Then, the the ratio F_1/F_2 is of interest. In order to assign a meaningful value to this ratio, meaningful information concerning F_1 and F_2 must be available, whether or not a value is explicitly assigned to these frequencies. Thus, specifying the relative frequency is plagued by the same problems as assigning individual values to frequencies.

Further problems arise when consequences are considered. Physical modeling has been done for radiation plume dispersal, health effects and damage resulting from release of radiation, such as from an act of sabotage. The result is a broad spectrum of consequences depending on the amount of release and its characteristics, meteorological conditions, population, evacuation procedures, medical facilites, etc. Choosing a number to represent such a broad range of consequences is at best a rough approximation, even though the potential health effects are the portion of consequence analysis that can be tied to physical laws.

Other questions in consequence analysis must address societal impacts of events. How can the effects of theft of special nuclear material be quantified? Even if the ultimate use of the material were known, which will not usually be the case, it is only possible subjectively to assign a consequence to the theft. Factors such as public opinion toward the nuclear industry and regulatory pressure resulting from nuclear incidents are also germane to consequence analysis. Prediction and quantification of these factors is little more than guesswork. It is concluded that the enumeration of accurate consequences is an exceedingly difficult problem.

3.2.2 Decision Making

It also appears that the ERDA-7 type risk analysis approach is not able to discriminate adequately between different systems. The uncertainty inherent in F, P and C as estimates of the true values limits the ability of this risk methodology to distinguish differences. This limitation of the risk equation will be illustrated, assuming for the first example a normal distribution of the variables and for the second example a lognormal distribution of the variables. Also, the information contained in the risk equation will be shown to be always less than the information in the probability term P. The information in P is obviously degraded by using the ERDA-7 type risk approach.

Confidence Intervals

Consider the following measured ranges for the risk parameters, assuming only one threat category:

$$F = 0.1 \pm 0.06$$

$$P_o = 0.8 \pm 0.2 \quad , \quad P_u = 0.3 \pm 0.2$$

$$C = 0.5 \pm 0.2$$

F may be interpreted as either an absolute or a relative event frequency. F and C have been chosen to lie within the interval from 0 to 1 in order to minimize the impacts of absolute magnitudes on the risk. P_o and P_u are the probabilities of adversary success against the original system and against the upgraded system, respectively. Note that each parameter is specified as a random variable.

The error bounds on these parameters are interpreted in the following way. Some measurement procedure, or analog of a measurement procedure, is used to obtain the F, P and C parameters. The errors indicate the standard deviation associated with the procedure. The underlying probability distribution is assumed normal in each case, although this is certainly not necessary for the following analysis. Normality may generally be assumed, however, for measurements and associated errors. Also note that the uncertainty in each case is a conservative assumption. In this example, F and C are assumed to be known with very good precision, given the arguments cited previously. In an actual application, these standard deviations would probably be much larger than the specified mean in each instance, perhaps by orders of magnitude.

Using standard error propagation techniques, described in Appendix A, the original risk is

$$R_o = 0.04 \pm 0.031 \ .$$

The risk associated with the upgraded system is given by

$$R_u = 0.015 \pm 0.015 \ .$$

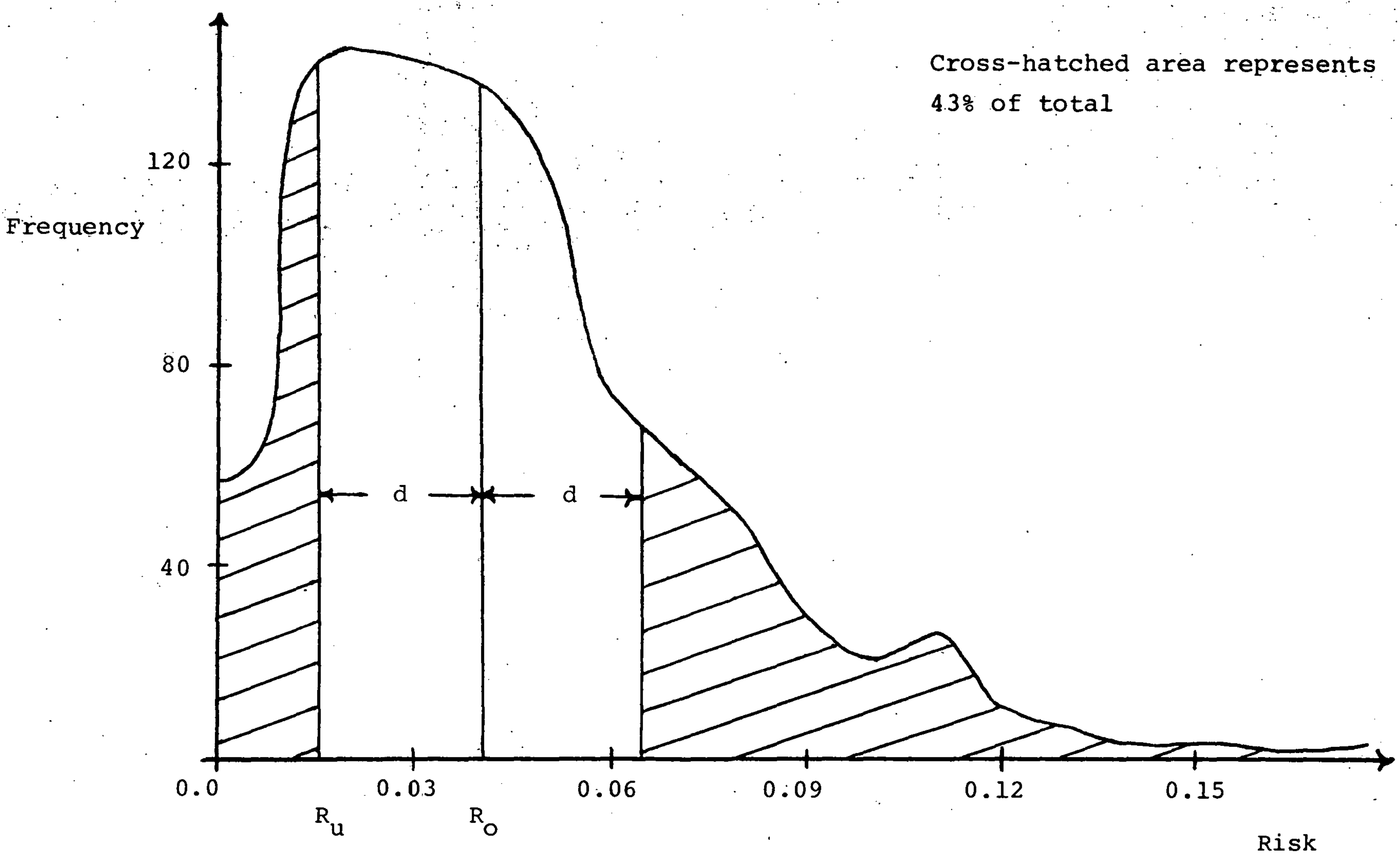
The question of interest is whether or not the difference between $E[R_o]$ and $E[R_u]$ is statistically significant and distinguishable by risk analysis.

Figure 3 shows the frequency distribution of the original risk, R_o. This distribution was obtained by a Monte Carlo simulation. One thousand random samples were chosen for each of the parameters F, P_o and C. These samples were drawn from the appropriate distribution for each parameter. The random samples were constrained to lie within the unit interval, another conservative assumption which decreases the variation in the resulting risk values. One thousand samples of R_o were thus obtained; Figure 3 gives the results.

The difference, $d = E[R_o - R_u]$, is also shown in Figure 3, and the interval of width 2d about $E[R_o]$ is indicated. The significance of this figure lies in the following. It can be asserted that $E[R_u]$ is significantly different from $E[R_o]$; however, from a statistical point of view, this assertion has a 43% probability of being incorrect, as indicated by the cross-hatched area in Figure 3. Another way of saying the same thing is that a random sample from the frequency distribution of R_o has a 43% chance of being farther away from $E[R_o]$ than $E[R_u]$ is away from $E[R_o]$. If a one-sided test is preferred, since $E[R_u]$ is less than $E[R_o]$, there is a 40% probability of a random sample R_o falling below $E[R_u]$.

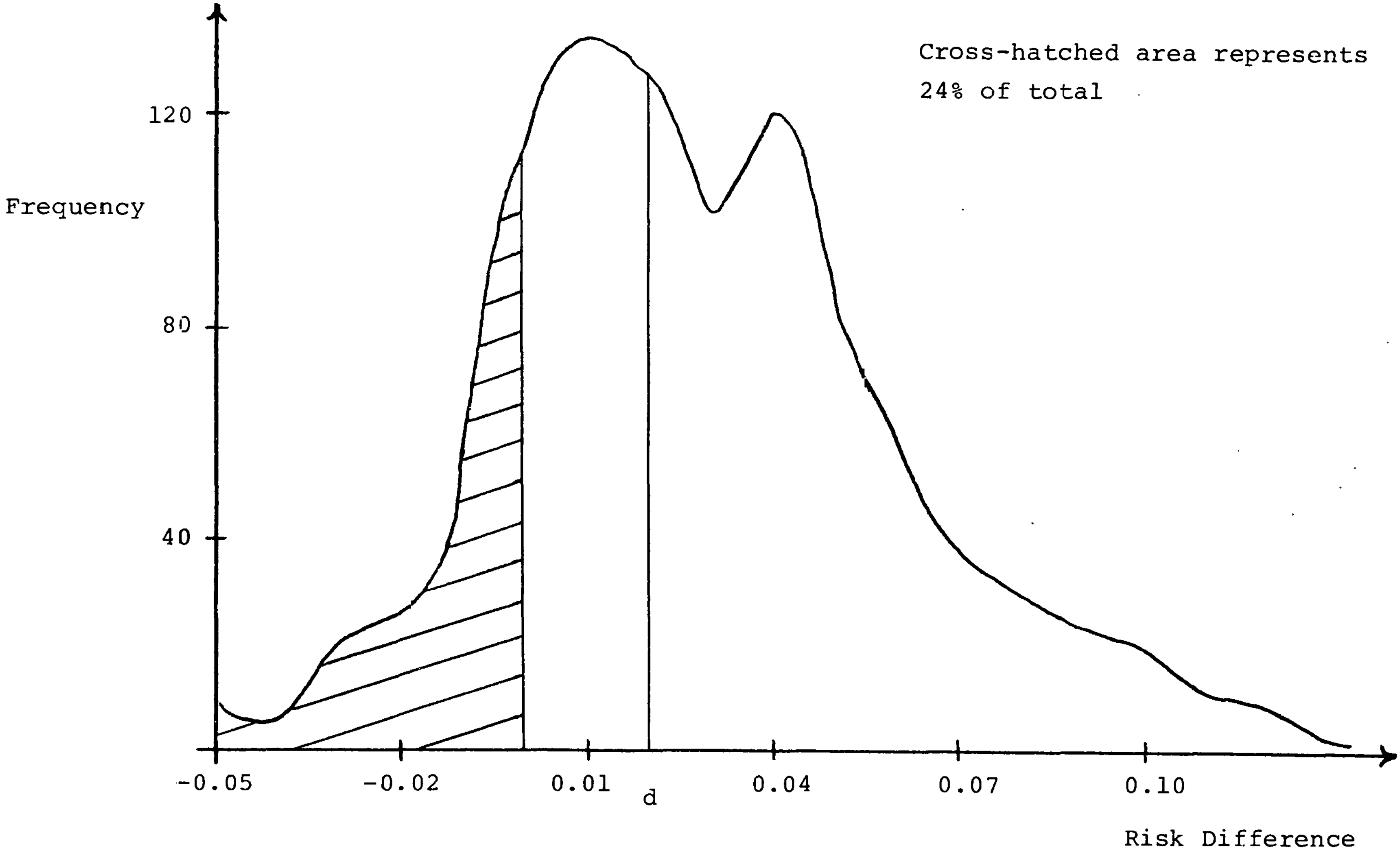
Figure 4 is the probability distribution function of the differences in sample values of the random variables R_o and R_u, again obtained from a Monte Carlo simulation. Assuming that the F and C terms have been estimated independently for R_o and R_u, the calculated value of the difference is

$$D = 0.025 \pm 0.034 .$$



Cross-hatched area represents 43% of total

FIGURE 3. Risk Frequency Distribution



Cross-hatched area represents 24% of total

FIGURE 4. Distribution of Risk Difference

If the mean value of the difference, d = E[D] = 0.025, is used as a binary decision variable, this figure shows that with a 24% probability, indicated by the cross-hatched area in the figure, the upgraded system would be evaluated as having a worse risk than the original system, i.e., 24% of the time the random variable $D = R_o - R_u < 0$, so that $R_u > R_o$. However, this difference will not be used only as a binary decision variable, i.e., for choosing one system over another, but also as a method for comparing several systems. Because of the large standard deviation associated with this difference, the use of this number and similar numbers from other systems in a comparison or ranking would lead to decisions with large probabilities of being erroneous. Figures 3 and 4 graphically illustrate the effects that errors can have in this risk analysis of safeguards. These uncertainties arise when comparing only two systems. The problems would be greatly compounded when considering several different systems. Recall also that conservative assumptions have been made at each step of this example.

Information Content

Another way of examining uncertainty in the risk equation is to consider its information content. In this context, the information content is considered to be measured by the ratio of the expected value to the standard deviation. This quantity may be heuristically compared to the signal-to-noise ratio in communication theory. Appendix B provides the derivation of the information content of the risk equation. A measure of uncertainty may be defined as the inverse of the information content. Figure 5

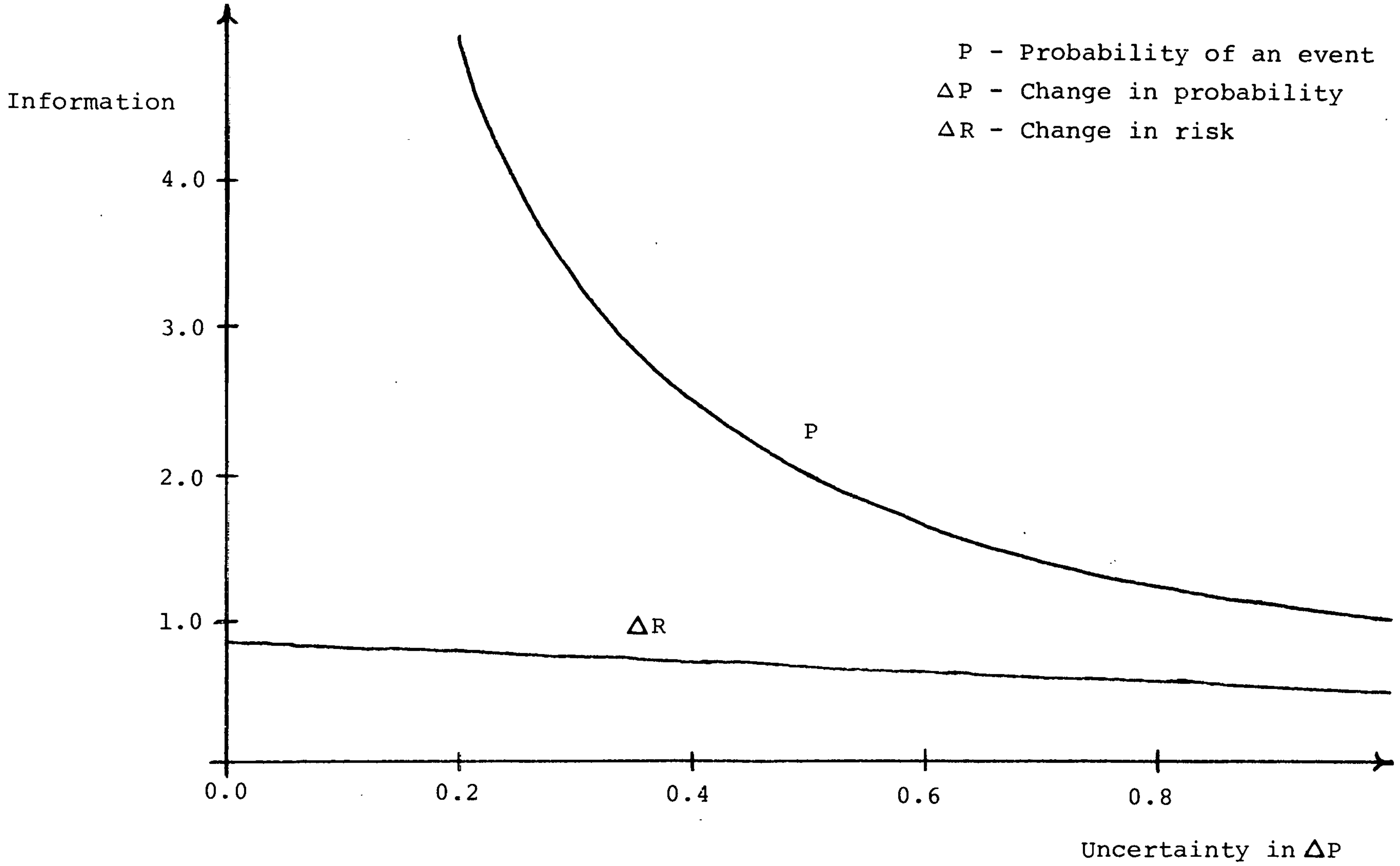


FIGURE 5. Information Content

shows the information in ΔR as a function of uncertainty in ΔP. The quantity ΔR is the difference in R_o and R_u resulting from the change ΔP from P_o to P_u, that is,

$$R = F \cdot \Delta P \cdot C \ .$$

Figure 5 shows plots for information content in both the risk equation and the P parameter as functions of uncertainty in ΔP. As uncertainty increases, information content decreases, as expected. Conversely, as uncertainty in ΔP approaches 0, corresponding to perfect knowledge of ΔP, information in ΔR approaches a finite value as a result of uncertainty in F and C. However, information in P approaches infinity, again indicating perfect knowledge. The most important point to notice is that there is always more information contained in P than in the ERDA-7 type risk equation. Therefore, the risk approach always degrades the information which it utilizes. For statistically meaningful changes in successful attempt probabilities from an original to an upgraded system, the uncertainty in ΔP will probably be on the order of 0.6 or less. This is the area of substantial information loss in using the risk equation. For this example, the uncertainty in ΔP is 0.4. Although chosen arbitrarily, the values for P_o and P_u that result in this value for ΔP are not unreasonable. However, even if uncertainty in ΔP were near 1.0 or even larger, the information content in the P parameter is still greater than that in the risk equation, and the problems with statistical significance are still encountered if risk is used as a decision tool.

Hypothesis Testing

As can be seen from the foregoing arguments, the merits of risk as an evaluation tool are heavily influenced by assumptions concerning the uncertainties in F, P and C. The usual cost-impact approach ignores uncertainties, assuming that measured or derived values are the true values. Consider another example that incorporates some of the measurement error concepts from the Reactor Safety Study (WASH-1400).[1] This study was performed on safety systems rather than safeguards systems, thus, probabilistic assumptions are justified, and error bounds are easier to specify. The example is based on lognormal probability distributions and uses the WASH-1400 assumption of order of magnitude error bounds on certain parameters.

The goal is to ascertain whether a given upgrade improves performance over the original system. The original and upgraded systems can be compared analytically by computing $E[D] = E[R_o - R_u]$ and examining the information content of this difference. The goal is to determine whether an upgrade improves system effectiveness by greater than q x 100% over the original system. In terms of standard hypothesis testing, the goal is to determine whether $r_o = r_u$ or whether $r_u \leq (1 - q)r_o$, where the lower case letters represent the true values. The numbers for this example were obtained from Reference 2, Table 9. Appendix C provides the details supporting the following conclusions.

A system effectiveness measure of q = 0.24, or 24% improvement, was derived by Al-Ayat and Judd.[2] Suppose that a Type I error of 25% is acceptable, i.e., 25% of the time an upgraded system will be judged better than the original system when in fact the risk associated with both systems is the same. Implementation of worthless upgrades would result from making a Type I error. As is shown in Appendix C, 67% of the time the 24% upgrade in systems effectiveness determined by Al-Ayat and Judd will be rejected as worthless. If, instead of the 25% value above, a Type I error of 10% is desired, then the 24% upgrade will be rejected 83% of the time.

Alternatively, suppose that the capability of detecting the 24% upgrade 80% of the time is desired. Then a 70% chance of making a Type I error occurs. In other words, 70% of the time worthless upgrades will be implemented. If only 50% detection of the actual upgrade is acceptable, then 38% of the time useless upgrades will be implemented.

This example is yet another graphic illustration of the uncertainties which plague the ERDA-7 type risk approach to safeguards. Drawing conclusions from this type of analysis will very likely result in wrong decisions. In fact, even determining the tradeoff between implementing statistically insignificant upgrades and not implementing meaningful upgrades is virtually impossible because of uncertainties.

Ranking and Selection

Another desirable attribute for an evaluation method is to be able to rank upgrades. Suppose that there are n feasible upgrades, U(1),...,U(n), and an analysis team would like to choose the upgrade with the lowest risk. Common ranking procedures that might be used for ranking the upgrades are weakened in much the same way as the hypothesis testing procedure when similar assumptions about uncertainty in F and C are made. To see this, compare two upgrades, 1 and 2. Assume upgrade 1 has the true higher risk so that $r_1 > r_2$. The analysts would evaluate the two upgrades and produce estimates R_1 and R_2. They would then compare the two estimates and choose the system with the lowest estimated risk. In this case, they would like to choose upgrade 2. This correct selection occurs if $R_1 > R_2$ or if $D = R_1 - R_2 > 0$. Thus, the probability of making the correct decision is

$$P(D > 0) = P(R_1 > R_2) \ . \tag{1}$$

Assume that F, P and C are independent lognormal random variables. Also assume that the better upgrade, 2, has at least a q x 100% effectiveness as compared to the inferior upgrade, 1. This constraint may be stated as

$$(1 - r_2/r_1) \geq q \ . \tag{2}$$

Using Eq. 2 and two threat categories, consider the following example:

	THREAT	
	1	2
Upgrade 1	p_{11}	p_{12}
Upgrade 2	p_{21}	p_{22}
Frequency of Attempt	f_1	f_2
Consequence	c_1	c_2

where p_{ij} = probability of adversary success against the facility with upgrade i when threat j occurs. Let $p_{11} = p_1$ and $p_{22} = p_2$, and suppose that $p_{12} = p_{21}$ and are negligible with respect to p_1 and p_2. This assumption is made for computational and notational convenience and does not materially affect the conclusions. Note that this example is easily extended to any number of threats and any number of upgrades.

The estimated parameters are related to the true parameter values by (see Appendix D, Eq. D1):

$$\begin{aligned} F_i &= f_i \cdot \exp(S_{f_i} X_i) \\ C_i &= c_i \cdot \exp(S_{c_i} Y_i) \\ P_{ij} &= p_{ij} \cdot \exp(S_{p_{ij}} Z_i) \end{aligned} \qquad (3)$$

where the X_i, Y_i and Z_i are independent standard normal random variables. Because of the assumptions concerning p_{12} and p_{21},

$$D \approx F_1C_1P_1 - F_2C_2P_2 \ .$$

From Eqs. 1 and 3, the probability of a correct decision is approximately

$$P(F_1C_1P_1 > F_2C_2P_2) \approx P[f_1c_1p_1 \cdot \exp(S_{f_1}X_1 + S_{c_1}Y_1 + S_{p_1}Z_1) > f_2c_2p_2 \cdot \exp(S_{f_2}X_2 + S_{c_2}Y_2 + S_{p_2}Z_2)] \ .$$

Taking the natural logarithm of this event does not change the probability, therefore

$$P[F_1C_1P_1 > F_2C_2P_2] \approx P[(S_{f_1}X_1 + S_{c_1}Y_1 + S_{p_1}Z_1) - (S_{f_2}X_2 + S_{c_2}Y_2 + S_{p_2}Z_2) > \ln(f_2c_2p_2/f_1c_1p_1)] . \tag{4}$$

The random variable on the left side of this equation is normal with zero mean and variance

$$S^2 = S_{f_1}^2 + S_{f_2}^2 + S_{c_1}^2 + S_{c_2}^2 + S_{p_1}^2 + S_{p_2}^2 . \tag{5}$$

Using Eq. 2 and a q x 100% effectiveness of upgrade 2 as compared to upgrade 1,

$$1 - \frac{f_2c_2p_2}{f_1c_1p_1} = q .$$

Thus,

$$p_2 = (1 - q) \cdot f_1c_1p_1/f_2c_2 . \tag{6}$$

The probability in Eq. 4 may now be rewritten as

$$P[SW > \ln(f_2c_2p_2/f_1c_1p_1)] \approx P[W > \frac{1}{S}\ln(1 - q)]$$
$$= 1 - G\left(\frac{\ln(1 - q)}{S}\right) \tag{7}$$

where W is a standard normal random variable, and G(x) is the standard normal cumulative distribution function.

Error factors for lognormal random variables are discussed in Appendix D. From the Appendix D discussion, Eq. 5 and the assumption that error factors for F and C are greater than some value, e, (see especially Appendix D, Eq. D2):

$$S^2 \geq \frac{4(\ln(e))^2}{(1.645)^2}$$

where 1.645 is the 95th percentile point for the standard normal distribution. The probability in Eq. 7 is bounded above, i.e.,

$$P[W > \frac{1}{S} \ln(1 - q)] < 1 - G\left(\frac{1.645}{2} \frac{\ln(1 - q)}{\ln(e)}\right)$$

With a bound on the error factor, e, of 10 and q = 0.25, corresponding to a 25% upgrade, the probability of making the correct decision with this risk procedure is

$$P(\text{correct decision}) \approx 1 - G(-0.103) = 0.54 .$$

In other words, a risk ranking procedure using the frequency and consequence error uncertainties in Appendix D would have only a 4% edge over flipping an unbiased coin for choosing a 25% upgrade.

As can be seen from these illustrations, the uncertainties associated with the risk equation limit its effective use as a decision-making aid. Even with conservative assumptions concerning errors, the uncertainties preclude accurate judgements based on the results. Furthermore, there may be a better decision variable subsumed in the risk equation, namely P. The use of successful attempt probabilities, P, is most likely not the answer to the problems posed by the development of a comprehensive safeguards evaluation method, but the argument can certainly be made that it is a more effective tool than the risk equation.

There are also problems with the consistency of the risk approach. Because of the lack of meaningful data and methodologies for specification of F and C as well as discrepancies which may arise in the calculation of P, different analysis groups would almost certainly arrive at different conclusions regarding comparisons of safeguards systems. The author feels that the major contributors to this probable inconsistency are the arbitrariness of specifying attempt frequencies, either absolute or relative, and the problems of specifying meaningful consequences. In general, the lack of a coherent methodology for parameter specification places severe constraints on the consistency of the risk analysis approach.

For the several reasons discussed in this section, it is believed that the application of the ERDA-7 type risk approach to safeguards systems is not feasible. In particular, the use of this risk equation as a safeguards analysis tool has serious technical drawbacks, is unable to discriminate effectively between different systems and is likely to be inconsistent in its application. Therefore, an entirely different approach is indicated for development of a comprehensive evaluation methodology.

4. CONCLUSIONS

A need exists for the development of a comprehensive evaluation methodology for analyzing safeguards systems. Such a methodology would also be valuable as a design aid. An acceptable evaluation technique must be conceptually meaningful, technically defensible, discriminating and consistent. Preliminary work indicates that a useful starting point for development is a functional decomposition of safeguards systems, proceeding to the component level, if possible. More work remains to be done, however, before the best method can be specified.

The ERDA-7 type risk approach has been examined in some detail in its application to safeguards systems analysis. This approach is inappropriate in safeguards work for many reasons. These include the problems of obtaining useful data, errors in assuming that attempt frequencies are random, dependence of terms in the risk equation, problems in performing a meaningful consequence analysis and uncertainties in the results of the risk analysis. For these reasons, it is concluded that the use of societal risk as a safeguards analysis tool will not be productive and, indeed, may likely result in wrong decisions being made and implemented.

GLOSSARY OF SELECTED TERMS IN SAFEGUARDS SYSTEMS MODELING

Access Control - A function which monitors and enables authorized movement of people and material through barriers and prevents unauthorized movement of people, special nuclear material, and contraband.

Access Privilege - Authorization to enter a protected area or to have access to a security system component or to a protected object.

Adversary - An individual or an organized group threatening health, safety, or national security through an intention to comment malevolent acts involving protected objects, e.g., nuclear weapons.

Alarm - A mechanism to warn or alert the guard force; generally consisting of some form of sensor and a device to communicate signals from the sensor to the security force.

Area - A space enclosed by a connected set of barriers and controlled openings.

Assessment (of an alarm) - Action by members of the security force, to determine whether an activated alarm indicates an actual threatening situation or is a false alarm, or to collect further information on the origin of an alarm signal.

Barrier - A material object or set of objects that separates, demarcates, or impedes passage.

Component (security-system component) - A mechanism that helps carry out one or more of the assigned functions of the security system, e.g., an alarm or a barrier.

Consequences - Losses to society caused by perpetration of an event, including death, injury, and property damage, as well as other types of losses to society.

Covert Activity - An activity that has not been recognized by the security system.

Critical Insiders - An insider, or some combination of a few insiders, that has high capability or the highest capability (based on access and control privileges) to carry out successfully an adversary action.

Critical Path - A penetration path that, by some measure, provides an adversary with a high probability (or the highest probability) of successful accomplishment of his goal.

Deceit (mode) - An action mode wherein the adversary seeks to overcome some element of the security system by misrepresentation or deception, e.g., by wearing a bogus uniform or using counterfeit identification.

Delay - An increase in the time required for completion of some activity.

Detection - A determination that an unauthorized action has occurred. Detection includes sensing, alarm, and assessment.

Deterministic (treatment of stochastic elements) - A type of mathematical treatment wherein any random elements in a system are not explicitly retained. They may be reflected in values chosen for certain parameters, e.g., mean values for stochastic variables.

Diversion - The removal of SNM from authorized locations, process lines, or transports for some unlawful use by persons who are authorized to possess the material.

Diversionary Activity - An adversary activity, the main objective of which is to divert the attention of the security system (or its capability to respond) from another, more important adversary action.

Events - Unauthorized acts involving nuclear materials or nuclear facilities which cause or threatened to cause damage to society.

Fault Tree Analysis - A technique that identifies those sequences of events that lead to some defined end event. The analysis reveals combinations of basic antecedent events that result in the outcome of interest.

Force (mode) - An action mode wherein the adversary employs overt aggressive activities--such as violence, compulsion, constraint, or the proximate threat of these--against people or things, in order to overcome some element of the security system.

Global Assessment - An evaluation of a security system that is, in some well-defined sense, comprehensive with respect to the entire range of adversary actions that are judged to threaten the protected facility. For example, a model might estimate the "worst-case" probability of success for a single group of up to 12 men (with defined capabilities) that might attempt to penetrate to a storage space and escape with SNM, along any path through the facility.

Insider - Someone with legitimate authorization to carry out some activity within the protected facility.

Interruption - A security system action that breaks into an adversary action sequence, leading at least to a delay or shift in adversary action, e.g., the arrival of a guard and the initiation of a combat engagement.

Material Accounting System - The personnel, equipment and procedures intended to provide information on the quantity and location of SNM within a facility for the purposes of inventory and production control, as well as detection of theft or long-term diversion.

Material Control System - The personnel, equipment and procedures intended to limit the opportunity for diversion of nuclear material, to initiate emergency material protection measures upon receipt of alarms and to provide information relevant to detection and assessment of anomalous conditions.

Monte Carlo Calculation - The statistical estimation of some quantity by repetitive execution of a series of calculations using an appropriately weighted random sampling of a parameter space.

Neutralization - Defeat of an adversary force by a secuitry system, in a combat engagement or by other means.

Outsider - A person that interacts with a facility without legitimate authorization, i.e., someone other than an insider.

Overt Activity - An activity that is recognized by the security system.

Path (adversary path) - A possible route for an adversary between specified points of interest at a protected facility, e.g., from a point at the perimeter to a target (protected asset) location, from the target to the perimeter, or both combined.

Pathfinding Procedure - A procedure that identifies adversary paths that meet certain criteria, e.g., the path from the facility perimeter to an interior target for which an adversary using stealth would have the highest probability of avoiding detection.

Performance Parameter - A numerical quantity, the value of which decribes the level of performance of a person, system, subsystem, piece of equipment, or component in relation to a specified objective or function.

Physical Protection System - The personnel, equipment and procedures intended to operate in real time to interrupt and neutralize unauthorized events.

Portal - A passageway through a barrier.

Response - The actions of a safeguards system after the detection and verification of an unauthorized event.

Response Time - The time required for a guard force to respond to a perceived threat to protected assets. This can include time for assessment of an alarm, for communication between guards, and for travel between different points in the facility. In the case of off-site response forces, it may include time for preparation and transportation.

Safeguards System - The total system intended to prevent unauthorized events involving nuclear materials or nuclear facilities. Often subdivided into the physical protection system, the material control system and the material accounting system.

Scenario-Oriented Model - A model that provides a capability to simulate the events of specific scenarios when provided with either a specified set of starting conditions and adversary objectives or a detailed specification of the main course of events.

Sensor - A device that responds to a physical stimulus (as sound, pressure, or a particular motion) and transmit a resulting impulse; generally a component of an alarm system.

Single Random Draw - Generation of a value for some quantity, such as a performance parameter or a binary decision variable, by a single random selection carried out in accord with an appropriate probability distribution function.

Stealth (mode) - Adversary action directed at overcoming elements of the physical protection system by escaping detection. Such actions may include evasion, covert violent actions, etc.

Subsystem (physical security subsystem) - A group of persons or devices (components) forming a unified whole that serve some common purpose as part of the security system, e.g., to detect intrusion through the perimeter fence using various sensors, power supplies, signal lines, signal amplifiers, an audible alarm unit, and a visual display unit.

Tampering - Covert alteration of some security system component or subsystem so as to weaken it or change it for the worse, e.g., the covert deactivation of an intrusion sensor.

Target - An object or location that must be reached by an adversary to accomplish his malevolent intentions.

Theft - The unlawful removal of SNM from a facility or transport by persons who are not authorized to possess the material.

Threat - All the attributes, actions, and strategies of a hypothesized single individual or group intent on malevolent action involving nuclear material.

Timely Detection - Detection of an adversary activity in time to have some chance to prevent the adversary from successful completion of his goal, e.g., the detection of an intrusion in time to permit interception of the adversaries before they reach their target.

Unauthorized Activity - In a protected facility, an action that is not an authorized procedure or that is done by a person that is not authorized to do it.

Validation - As applied to a security system evaluation model, the collection of evidence that the results of the model's calculations are true, probable, or valid indications of the security system's ability to accomplish its objectives.

REFERENCES

1. WASH-1400: Reactor Safety Study - An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, NUREG-75/014 (Washington: U.S. Government Printing Office).

2. Al-Ayat, R. and B. Judd, "Illustrative Application of an Integrated Evaluation Framework for Nuclear Safeguards Systems," Draft Report (Lawrence: Lawrence Livermore National Laboratory, May 27, 1981).

3. HTGR Accident Initiation and Progression Analysis Status Report, Vol. II, "AIPA Risk Assessment Methodology," GA-A13617, UC-77 (Washington: General Atomic, October 1975).

4. Aitchison, J. and J. A. Brown, The Lognormal Distribution with Special References to Its Uses in Economics, (Cambridge: Cambridge University Press).

5. Bennett, C. A., W. M. Murphey and T. S. Sherr, Societal Risk Approach to Safeguards Design and Evaluation, ERDA-7 (Washington: U.S. Government Printing Office).

Appendix A

Standard Deviation of Product of Three Terms

Suppose three quantities are given by

$$x \pm a$$

$$y \pm b$$

$$z \pm c\ .$$

Then, the standard deviation of the product, denoted by

$$xyz \pm d\ ,$$

can be calculated from the relation

$$\left(\frac{d}{xyz}\right)^2 = \left(\frac{a}{x}\right)^2 + \left(\frac{b}{y}\right)^2 + \left(\frac{c}{z}\right)^2 .$$

Appendix B

Risk Analysis: Information Content

Given the equation

$$R = F \cdot P \cdot C \ ,$$

where F, P and C are specified as

$$F \pm f$$

$$P \pm p$$

$$C \pm c \ ,$$

we are interested in the information content of

$$\begin{aligned} \Delta R &= R_o - R_u \\ &= F \cdot P_o \cdot C - F \cdot P_u \cdot C \\ &= F \cdot \Delta P \cdot C \ . \end{aligned}$$

Define the information content to be the ratio of the expected value of a parameter to its standard deviation. The quantity of interest is then

$$\frac{\Delta R}{\sigma \Delta R} \ .$$

Recalling that $Var(x) = E(x^2) \mid E^2(x)$,

$$\frac{\Delta R}{\sigma \Delta R} = \frac{E(F \cdot \Delta P \cdot C)}{\sqrt{Var(\Delta R)}}$$

$$= \frac{E(F\cdot\Delta P\cdot C)}{\sqrt{E(F^2 \cdot \Delta P^2 \cdot C^2) - E^2(F\cdot\Delta P\cdot C)}}$$

$$= \frac{1}{\sqrt{\frac{E(F^2)}{E^2(F)} \cdot \frac{E(\Delta P^2)}{E^2(\Delta P)} \cdot \frac{E(C^2)}{E^2(C)} - 1}}$$

$$= \frac{1}{\sqrt{\frac{F^2 + f^2}{F^2} \cdot \frac{\Delta P^2 + \Delta p^2}{\Delta P^2} \cdot \frac{C^2 + c^2}{C^2} - 1}}$$

$$= \frac{1}{\sqrt{\left(\frac{f^2}{F^2} + 1\right)\cdot\left(\frac{\Delta p^2}{\Delta P^2} + 1\right)\cdot\left(\frac{c^2}{C^2} + 1\right) - 1}} \cdot$$

Appendix C

Risk Analysis: Hypothesis Testing

The example presented in this appendix incorporates some of the measurement error concepts described in Reference 1. The study suggests that certain hardware components have order-of-magnitude error bounds on their availabilities. The example illustrates that similar uncertainty concerning F and C terms seriously degrades the discriminatory power of an evaluation tool using societal risk. Note that these error bounds are based on hardware. The actual uncertainty associated with F and C in the safeguards application would certainly be greater.

An important role for an evaluation scheme is to ascertain whether a certain upgrade improves system performance. The method should allow the analyst to determine whether performance is actually improved or if the proposed upgraded system has virtually the same risk as the original system. Upgrades generally consist of adding safeguard features to a facility so that risk will be reduced; however, an expensive upgrade that leads to a very small percentage decrease in risk may not be cost-effective. It is imperative, therefore, that the method allow consideration of whether a substantial decrease in risk has occurred or whether the new system has essentially the same risk. This problem can be placed within the framework of statistical hypothesis testing. In this framework, there are two situations, or states of nature, that concern the analyst:

1. The original system risk is the same as the upgraded system risk, i.e., $r_o = r_u$, and
2. The upgraded system risk is more than q x 100% lower than the original system risk, i.e., $r_u \leq (1 - q)r_o$.

Lower case letters represent true values, while capital letters represent estimates of the true values. The following decision table illustrates the situation.

		TRUE STATE	
		$r_o = r_u$	$r_u \leq (1 - q)r_o$
ANALYST'S DECISION	$r_o = r_u$	Correct	Type II Error
	$r_u \leq (1 - q)r_o$	Type I Error	Correct

If the analyst concludes that the risks are equal, when in fact they are, he has made a correct choice; if he concludes that they differ when in fact they do not, he has made a Type I error. In this context, the Type I error corresponds to determining that a marginal upgrade is valuable. Alternatively, it may be true that the upgraded system is in fact q x 100% better; in this case, if the analyst concludes that the risks are equal, he has made a Type II error. A Type II error corresponds to determining that an effective upgrade is insignificant in terms of system performance. Both of these errors must be considered in an evaluation. There is generally a trade-off between the two; in this application of risk analysis, the trade-off results in no confidence in any decision.

Assume that the goal is to determine whether a system upgrade improves effectiveness by at least q x 100% over the original system. Stated as a hypothesis test, the goal is to determine whether $r_o = r_u$ or whether $r_u \le (1 - q)r_o$. Assuming that $R_o - R_u = D$ is normally distributed, standard theory suggests that no significant improvement has been accomplished unless

$$D \ge Z(a) \times S(D) , \qquad (C1)$$

where S(D) is the standard deviation of the difference, Z(a) is the (1 - a) x 100 percentile point of the standard normal distribution function, designated G(x), and a is an acceptable Type I error.

The power function of this test is defined as the probability of correctly rejecting the hypothesis of equal risks and is useful for determining how well the test given by Eq. C4 performs when an effective upgrade has been achieved. The power function is given by

$$1 - G(Z(a) - E[D]/S(D))$$

where G(x) is the cumulative normal distribution function, e.g., G(2) = 0.977.

The higher the power function, the greater the probability that evaluators will not discard a desirable upgrade as being worthless. Conversely, the higher the Type I error, the higher the probability that a worthless upgrade ($r_o = r_u$) will be judged to have a better than q x 100% reduction in risk. As an example, the numbers in Reference 2, Table 9, are used. It is shown in Appendix D that using reasonable assumptions from the Reactor Safety Study,[1]

$$E[D]/S(D) \approx 0.305 ,$$

with q = 0.24. Using this ratio, the following table is determined.

Z(a)	Type I Error	Power
0.0	0.5	0.620
0.25	0.401	0.526
0.5	0.308	0.422
0.75	0.227	0.328
1.0	0.159	0.243
1.25	0.1056	0.172
1.5	0.067	0.116

The proper trade-off between Type I error and power is indeterminate because of uncertainties. To achieve a Type I error of 25% requires lowering the power to approximately 0.33. In other words, 67% of the time, the upgraded system in Reference 2, Table 9, will be rejected as an ineffective upgrade. On the other hand, if the power is fixed at 0.5, a Type I error of approximately 0.38 results. In other words, useless safeguards systems would be judged to be effective 38% of the time.

Appendix D

Risk Analysis: Rankinq and Selection

The effect of uncertainty on societal risk analysis is explored in this appendix using data from Reference 2, Table 9. Assume that the F, P and C terms in R are lognormally distributed. Upper case letters indicate estimated values, while lower case letters indicate the true values. For a variate, say F,

$$F = \exp(X) \ ,$$

where X is a normal random variate with mean, u, and standard deviation, s. The mean value, u, is determined by assuming that the true value, f, is the median of the F distribution, i.e.,

$$u = \ln(f) \ .$$

Thus, F has the form

$$F = f \exp(sW) \ , \qquad \text{(D1)}$$

where W is a standard normal random variate and the standard deviation, s, is defined in terms of an error factor, e, given by

$$e = \exp(Z(a) \times s) \ ,$$

so

$$s = \ln(e)/Z(a) \ ,$$

where Z(a) is the (1 - a) x 100th percentile point of the standard normal distribution. Reference 1 uses a = 0.05 as does General Atomic in an illustration of Risk Assessment Methodology.[3] The error factor has the following significance. If the error factor for f is 10, then

$$P(0.1 \times f \leq F \leq 10 \times f) \geq 1 - 2a \ .$$

For simplicity, assume that the F and C terms collectively have an error factor, e, while the probability terms have a common error factor, e(p). The frequency and consequence terms can be thought of as coming from expert analysis; therefore, their error factors will be similar; probability terms are results of various evaluation codes, modified by expert opinion, so that they would have a different error factor. Define

$$\begin{aligned} s &= \ln(e)/Z(0.05) \\ s(p) &= \ln(e(p))/Z(0.05) \ , \end{aligned} \qquad \text{(D2)}$$

where s is the common standard deviation for the normal variates used in the F and C terms, while s(p) is the common standard deviation for the normal variates used in the P terms. Assume that the F, C and P terms are independent random variables.

In Reference 2, Table 9, the facility risk with no safeguards, designated the Reference Risk r_o, is compared to the facility risk with safeguards, designated the Existing Risk r_u. Assuming the values in Reference 2, Table 9, are the true but unknown values for the facility, the safeguards system reduces societal risk by 24%.

The mean and standard deviation of the difference $D = R_o - R_u$ are derived below in order to arrive at a conservative upper bound on E[D]/S(D) in terms of the error factor, e. This bound is used for the analysis in Appendix C. The difference in risk is

$$D = \sum_{i=1}^{14} F_iC_iP_{io} - \sum_{i=1}^{14} F_iC_iP_{iu}$$

$$= \sum_{i=1}^{14} F_iC_i(1 - P_{iu}) ,$$

since $P_{io} = 1$ for every i as a result of the assumption of no safeguards in the original system. Let $P_{iu} = P_i$ and $p_{iu} = p_i$ for notational convenience.

The product F_iC_i is a lognormal random variable where the exponentiated normal random variable has mean $\ln(f_ic_i)$ and variance $2s^2$ (see Reference 4, Theorem 2.2). To simplify notation, let $a_i = f_ic_i$, $A_i = F_iC_i$, $B_i = (1 - P_i)$ and $b_i = (1 - p_i)$. Then

$$D = \sum A_iB_i \ .$$

The following result allows the calculation of the expected value of each term. If $Y = \exp(X)$ and $X \sim N(u,s^2)$, then $E[Y] = \exp(u + s^2/2)$ (see Reference 2, page 8). Thus,

$$\begin{aligned} E[A_iB_i] &= E[A_i]E[B_i] \\ &= (a_i \exp(2s^2/2)) \cdot (1 - p_i) \cdot \exp(s^2(p)/2) \\ &\leq f_ic_i(1 - p_i) \cdot \exp(s^2) \\ &= a_ib_iQ , \end{aligned}$$

where

$$Q = \exp(s^2) \ .$$

Therefore, d, the expected value of D, is bounded above by

$$d \le Q \Sigma f_i c_i (1 - p_i) = Q(r_o - r_u) \ . \qquad (D3)$$

The variance of D, $S^2(D)$, is the sum of the variance of the individual terms A_iB_i, i.e.,

$$\mathrm{Var}(D) = \Sigma \ \mathrm{Var}(A_iB_i) \ .$$

The variance of the product A_iB_i can be simplified to

$$\begin{aligned} \mathrm{Var}(AB) &= E[(AB)^2] - E^2[AB] \\ &= E[A^2]E[B^2] - E^2[A]E^2[B] \\ &= (\mathrm{Var}(A) + E^2[A]) \cdot (\mathrm{Var}(B) + E^2[B]) - E^2[A]E^2[B] \ . \qquad (D4) \end{aligned}$$

Eq. D4 reduces to

$$\mathrm{Var}(AB) = \mathrm{Var}(A) \cdot E[B^2] + E^2[A] \cdot \mathrm{Var}(B) \ .$$

The analysis in this appendix focuses on the uncertainty in F_i and C_i, combined in the A_i term, so that the variance of A_iB_i can be bounded below by

$$\mathrm{Var}(A_iB_i) \ge \mathrm{Var}(A_i)E[B_i{}^2] \ . \qquad (D5)$$

The variance of A_i is (see Reference 3, Eq. 2.8)

$$\begin{aligned} \mathrm{Var}(A_i) &= E^2[A_i] \cdot (\exp(2s^2) - 1) \\ &= a_i{}^2Q^2(Q^2 - 1) \ . \end{aligned}$$

The variance of D is bounded below by

$$\begin{aligned} \mathrm{Var}(D) &\geq \sum \mathrm{Var}(A_i)E[B_i{}^2] \\ &= Q^2(Q^2 - 1)\sum a_i{}^2 \; E[(1 - P_i)^2] \;. \end{aligned}$$

Let $M = Q^2(Q^2 - 1)$, so that

$$\mathrm{Var}(D) \geq M \cdot \sum a_i{}^2 E[(1 - P_i)^2] \;.$$

This summation can be expanded considering that the jth moment of the lognormal random variable is $\exp(ju + j^2s^2/2)$ (see Reference 4, page 8). Then

$$\begin{aligned} &\mathrm{Var}(D) \geq M \cdot \sum a_i{}^2(1 - 2E[P_i] + E[P_i{}^2]) \\ = M \cdot &(a_i{}^2 - 2\exp(s^2(p)/2) \sum a_i{}^2 p_i + \exp(2s^2(p)) \sum a_i{}^2 p_i{}^2) \;. \end{aligned} \tag{D6}$$

$s^2(p)$ is unknown; however, if the variable $v = \exp(s^2(p)/2)$, the sums in Eq. D6 become a fourth-order polynomial in v that can be plotted as a function of v. For this example, the function is

$$479v^4 - 1148v + 701 \;.$$

This function is a strictly-increasing function of v for v 1, so that

$$\begin{aligned} \mathrm{Var}(D) &\geq M \cdot (\sum a_i{}^2 - 2\sum a_i{}^2 p_i + \sum a_i{}^2 p_i{}^2) \\ &= M \cdot \sum a_i{}^2 \,(1 - p_i)^2 \;. \end{aligned} \tag{D7}$$

The ratio $E[D]/S(D)$ is then bounded above by

$$E[D]/S(D) \leq \frac{Q(r_o - r_u)}{S(D)}$$

$$\leq \frac{Q(r_o - r_u)}{\sqrt{M}\,\sqrt{\sum a_i{}^2(1 - p_i)^2}}$$

The first inequality is a result of Eq. D1, while the second follows from Eq. D7. The relationship between Q and M allows us to write

$$E[D]/S(D) \le \frac{1}{\sqrt{Q^2 - 1}} \cdot \frac{r_o - r_u}{\sqrt{\sum a_i{}^2(1 - p_i)^2}}$$

Using the values of Reference 2, Table 9, we obtain

$$E[D]/S(D) = 2.14/\sqrt{Q^2 - 1} \; . \tag{D8}$$

Reference 1 includes error factors of 3 and 10 in its discussion of error propagation (see Reference 1, Appendix II). The latter factor of 10 is used for some components (see also Reference 1, Appendix III); it is highly questionable whether human judgment concerning f_i and c_i could be more accurate. Therefore, for an error factor of 10, the bound in Eq. D8 is 0.305, i.e.,

$$E[D]/S(D) = 0.305 \; .$$

Distribution:

TID-4500 UC-15 (336 copies)

U. S. Nuclear Regulatory Commission
Division of Facility Operations
MS 5650 NL
Washington, DC 20555
Attn: John Telford
Jerry Ennis (2)

U. S. Nuclear Regulatory Commission
Division of Safeguards, MS-881
7915 Eastern Ave.
Silver Spring, MD 20910
Attn: R. Erickson
L. Evans
R. Dube
T. Allen
E. Quinn
T. Sherr

Lawrence Livermore National Laboratory
P. O. Box 818
Livermore, CA 94550
Attn: A. Poggio

Larry Harris
Science Applications, Inc.
1200 Prospect
La Jolla, CA 92038

U. S. Department of Energy
Office of Safeguards & Security
MS A-21016
Washington, DC 20545
Attn: Tom Isaacs
S. C. T. McDowell
Glenn Hammond
Magal Rao
Nick Ovuka
Don Emon
Art Katz
Nelson Marsh

1700	W. C. Myrc
1710	V. E. Blake, Jr.
1714	W. F. Hartman
1720	C. H. Mauney
1730	M. L. Kramm
1750	T. A. Sellers

Do Not Microfilm

Distribution Cont:

1759	D. L. Mangan
1760	J. Jacobs
1760A	J. M. de Montmollin
1765	D. S. Miyoshi
1765	M. K. Snell
1768	C. E. Olson
4400	A. W. Snyder
4410	D. J. McCloskey
4414	G. B. Varnado
4416	L. D. Chapman
4416	K. G. Adams
4416	J. A. Allensworth
4416	H. A. Bennett
4416	L. M. Grady
4416	C. P. Harlan
4416	R. D. Jones
4416	J. M. Richardson (3)
4416	B. J. Roscoe
4416	S. L. K. Rountree
4416	D. W. Sasser
3154-3	C. H. Dalin (25) (for DOE/TIC)
3141	L. J. Erickson
3145	W. R. Dameron
3151	W. L. Garner (3)

Org.	Bldg.	Name	Rec'd by	Org.	Bldg.	Name	Rec'd by

Sandia National Laboratories