NUREG/CR-2551
SAND82-0332
RS
Printed April 1982

Rank Ordering of Vital Areas Within Nuclear Power Plants

BEST AVAILABLE COPY

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

TOTAL PAGES: 38

Includes all Paginated and Non-Paginated Pages

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

SF2900QA(8-81)

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, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2551
SAND82-0332

RANK ORDERING OF VITAL AREAS WITHIN NUCLEAR POWER PLANTS

J. Mark Richardson

Date Published: April 1982

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

Prepared for
Division of Facility Operations, Safeguards Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1060

ABSTRACT

The conceptual development of a methodology for rank ordering vital areas within nuclear power plants based upon times associated with sabotage events and their consequences is discussed. The important time parameters in the analysis include the time required to detect the perpetration of sabotage, the time required to repair or mitigate the consequences of the sabotage and the total time available to perform these functions before it is too late to reverse the damage. These time interval parameters are incorporated into an interruption analysis importance measure that provides information on the ability of the protection systems to cope with the results of the sabotage. A consequence analysis that considers categories of release characteristics is the next step in the ranking scheme. Results of the interruption and consequence analyses are combined to attain a risk index associated with each vital area. The final ranking can be used to order upgrade priorities and to allocate scarce protection resources effectively.

EXECUTIVE SUMMARY

Currently, the criterion used to differentiate vital areas at nuclear power plants is the classification of Type I or Type II, where Type I indicates a vital area in which it is possible to induce a release of radioactivity by having access to that area alone and a Type II vital area is one in which it is not possible to produce a radioactive release by having access solely to that area. A greater knowledge of vital area importance could be achieved with a ranking scheme that indicates relative criticality in terms of the possibility and consequences of radiological release. Such a ranking could provide important information and guidance concerning the effects of maintenance and test activities on the importance of vital areas, the structuring of security force responses and the efficient allocation of scarce protection resources.

This report presents the conceptual development of a rank ordering methodology for vital areas at nuclear power plants. The methodology considers the interrelationships among important parameters that affect the security of vital equipment and the effects of these interrelationships on radiological release. These parameters are combined into an importance measure that provides graphical information on the relative criticality of the vital areas. These results are combined with a consequence analysis that considers categories of radiological release characteristics. A risk index associated with each vital area can be determined from these analyses and used to order priorities for upgrading protection as well as for allocating existing protection resources more effectively.

CONTENTS

Section		Page
1	INTRODUCTION	11
2	METHODOLOGY	12
	2.1 Parameters for Ranking	17
	2.2 Interruption Analysis	20
	2.3 Importance Measures	21
	2.3.1. Critical Detection Time	22
	2.3.2 Relative Detection Time	27
3	RISK INDEX ANALYSIS	30
4	CONCLUSIONS AND RECOMMENDATIONS	34
REFERENCES		46

ILLUSTRATIONS

Figure		
1	Sabotage Protection Time Line	13
2	Structure for Rank Ordering	15
3	Operational Systems Time Line	16
4	Comparison of Recovery Time, Detection Probability and Response Time Rankings	19
5	Last Point for Occurrence of Detection	23
6	Importance Measure, $Q \cdot Dt$	25
7	Relative Detection Time Importance Measure	28
8	Risk Index Analysis Time Line	31
9	Ranking Methodology	32

RANK ORDERING OF VITAL AREAS WITHIN NUCLEAR POWER PLANTS

1. INTRODUCTION

At the present time, vital areas at nuclear facilities are classified as either Type I or Type II vital areas. A Type I vital area is an area from which a significant radiological release from the facility could be achieved by access to that vital area alone. A Type II vital area is a location which must be visited in combination with one or more other vital areas in order for radiological release to be achieved. The Type I/Type II designation has served as the basis for safeguards guidelines and makes a useful and important distinction among vital areas. However, this criterion does not provide a great deal of information about the relative importance of individual vital areas. This information can be gained by the development of a ranking scheme that incorporates more detail than the Type I/Type II designation. Such a ranking scheme could provide many advantages over the Type I/Type II classification scheme. A ranking would indicate the relative importance of the vital areas in terms of the possibility and consequences of radiological release. A vital area whose compromise would result in a relatively rapid release would be ranked as more important than one from which a rapid release could not be achieved. Also, a combination of Type II vital areas could be more critical than a Type I area, especially in considering insiders, and a ranking method could indicate that circumstance.

Once a rank ordering scheme has been established, security force response could be structured to protect the vital areas that are most critical in terms of rapid consequences of component or system compromise. This capability would be especially helpful since the number of vital areas to be protected usually exceeds the number of security officers available to respond[1]. The development of safeguards priorities during repair and maintenance activities would also be aided by a vital area ranking scheme. For example, a single Type II area could temporarily become extremely important during maintenance or repair that involved especially critical components. A ranking that includes pertinent outage information could indicate the crucial importance of an area at a particular time that, at other times, is not critically important. The Maintainability Analysis Procedure(MAP)[2] could be used in conjunction with a vital area ranking to examine the consequences and impacts of scheduled maintenance and repair.

Ranking methods have been applied previously to nuclear power plants at the reactor systems level. A simple ranking based on number of occurrences of

reactor scrams and forced outages was performed by Combustion Engineering, Inc. as part of a safety and availability study[3]. Science Applications, Inc. performed a systems ranking as part of a study concerning sabotage by insiders[4]. These examples illustrate both the potential and current usefulness of ranking procedures.

This report describes the development of a methodology that would be adequate for structuring a comparative ranking of vital areas. Section 2 discusses the identification of those critical parameters that bear on the importance of vital equipment. These parameters include detection time, the time required for repair or mitigation and the total time available to preclude radiological release given sabotage success. These parameters are used as importance measures and combined into an analysis of the facility capabilities for interrupting the sabotage effects sequence before the release of radioactive material. A comparative analysis is performed on the relative merits of rankings based on individual parameters versus combined parameters, with the latter shown to be preferable.

Importance measures are formed using combinations of the most important time parameters. Two such measures are discussed in detail in Section 2. The first measure is structured to show the various relationships among repair time, recovery time and detection time. The second combined importance measure illustrates the particular requirements on sabotage detection capabilities for vital areas.

The insights and results from the interruption analysis are combined with an analysis of sabotage consequences in Section 3 to provide a risk index associated with each vital area. The individual rankings from the interruption and consequence analyses are used to gain an understanding of the relative importance of each vital area to the security of the facility. This risk index can then be used in ordering priorities for upgrades or in allocating scarce protection resources in more effective ways.

Section 4 presents the conclusions of this study and discusses recommenda- for further work in this area.

2. METHODOLOGY

The conceptual basis for developing a ranking method for vital areas is the time history of system response to loss of specified components or systems. The time line provides dynamic input to evaluate the criticality of specific components or systems. The interactions and interdependence of the appropriate time intervals make the time-dependent analysis especially relevant to the ranking problem. Figure 1 presents a generic time line that illustrates the interactions of protection systems.

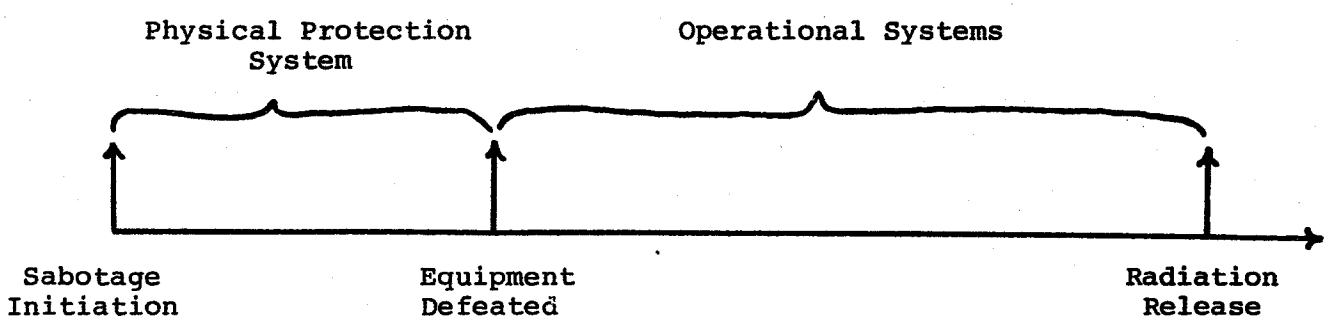

Figure 1. Sabotage Protection Time Line

As Figure 1 indicates, two possible methods exist for dealing with sabotage. At least conceptually, the first opportunity for interacting with a saboteur is through the physical protection system (PPS). The effective time for the PPS to operate is the interval from initiation of sabotage to the completion of the sabotage activity. The actual length of this time interval could be quite small or relatively large as compared to the time interval associated with operational systems response. The length of the PPS time interval as well as the relative importance of the PPS in the time history depends upon the particular threat involved in the analysis. For example, outsiders may be much more likely to interact with the PPS than would insiders.

Once a sabotage act has been completed, protection from radiological release must be provided by the operating and safety systems, referred to here as the "operational" systems. This response could include virtually all personnel at the site. The primary events associated with a response by operational systems are the detection of sabotage and the repair or mitigation of the consequences of the sabotage. The terminal event in the operational system time interval is considered to be the possible release of radioactive material.

A method for analyzing the interactions between the PPS and the operational systems is depicted in Figure 2. The analysis begins with the specification of the reactor components or systems of interest. The capabilities of the operational systems to protect this equipment are analyzed, and whether or not these systems provide adequate protection is determined. If adequate pretection is not provided by the operational systems, then the PPS must be analyzed in order to determine whether it can provide the necessary protection. This method considers the most cost-effective approach first because, if they are adequate, the existing operational systems can provide protection more economically than the PPS.

Figure 3 shows the relevant events and time parameters associated with the operating and safety systems in the operational systems time line. These include demand for the sabotaged equipment, detection of the sabotage, repair of the damaged equipment and the critical recovery point for the particular system. The critical recovery point is that time after which no actions will prevent release of radioactive material. Thus, it is the limiting time for effective occurrence of all other events.

The order of the events is not fixed, of course. For different acts of sabotage on different systems or components, some events may not occur and others may change places in the temporal sequence. For example, the repair event may not occur at all in a particular sequence. The effects of the sabotage may have to be handled by employing other systems rather than by repairing the sabotaged one. In effect this means simply that the repair event occurs after the critical recovery point and thus is not an option in the protection

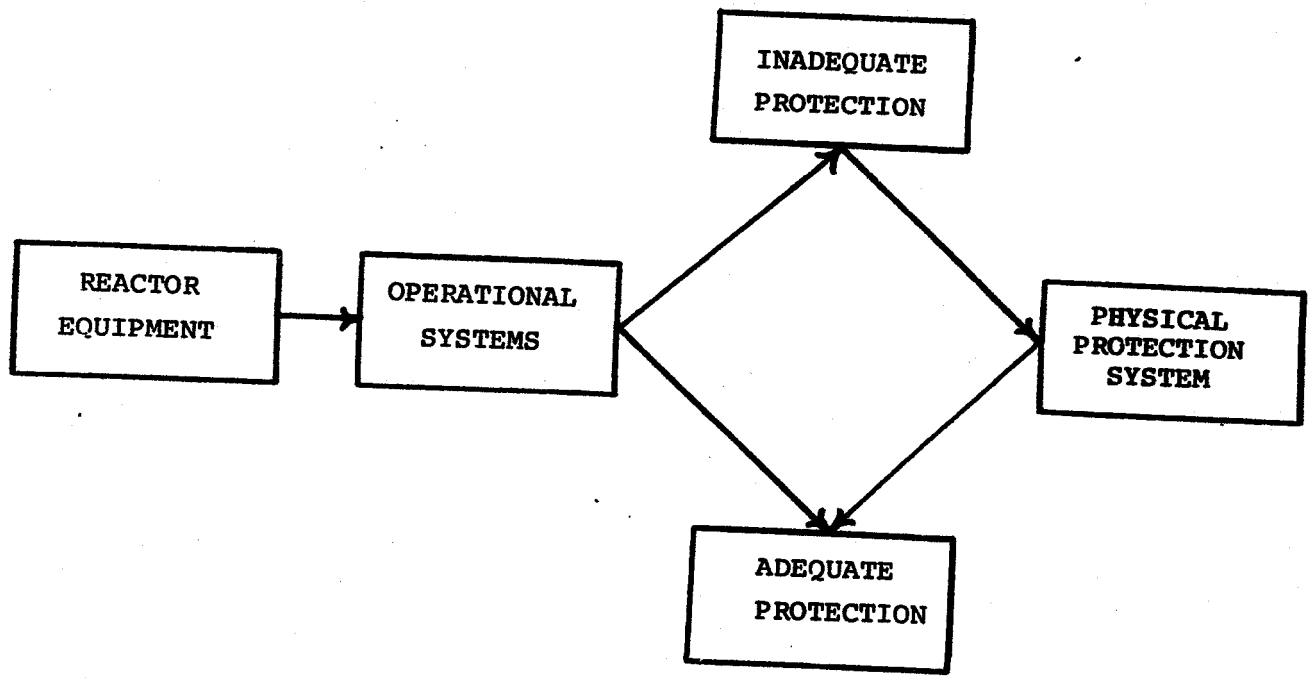

Figure 2. Structure for Rank Ordering

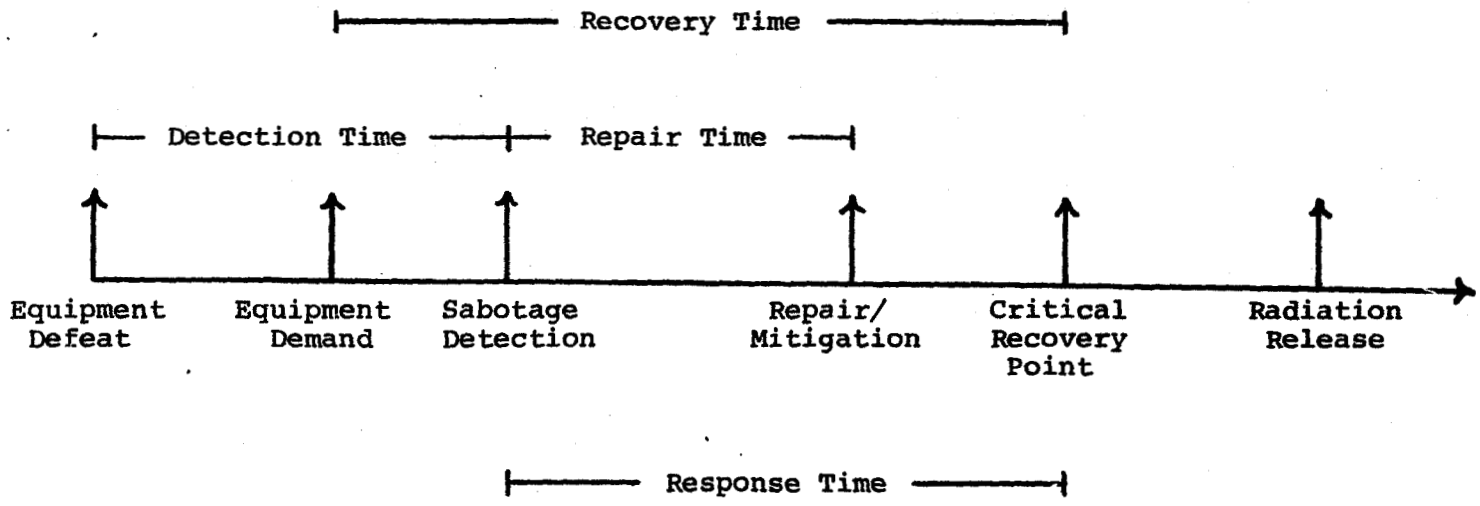

Figure 3. Operational Systems Time Line

scheme. As another example, if standby or non-operating equipment is compromised, sabotage detection could occur before demand for the sabotaged equipment. Ideally, this would always be the case.

The time from demand to the critical recovery point is designated the recovery time. It is obvious that the longer the time interval, termed the response time, between an event such as sabotage detection and the critical recovery point, the better chance the operational systems have for an effective response. This fact has some important consequences for developing ranking methods.

The time interval between sabotage detection and repair or mitigation will be relatively constant for a given type of component or system which is damaged to the extent that it must be replaced or another type of component or system must be used to perform its function. Consequently, the important critical events are the detection of sabotage and the demand for the sabotaged equipment. In the instance of sabotage of operating equipment, demand occurs at the same instant as sabotage completion. The operator then tries to ascertain the reason for loss of the capability associated with the sabotaged equipment. When the reason is determined, the detection event is considered to have occurred. Alternately, if the sabotage is perpetrated on components or systems that are in a standby or back-up mode, then an actual time interval exists between sabotage completion and the demand event during which time detection may occur. Hence, maintenance and safety check activities could play an important part in detecting sabotage of standby equipment.

2.1 Parameters for Ranking

Based on the time line for response of the operational systems until radiological release, three potential methods for rank ordering vital areas can be identified. These are based upon recovery time, response time and the probability of detection of sabotage.

The first method is based on recovery time and is concerned with the time from demand to the critical recovery point. The advantage of such a method is that the recovery time parameter includes the total time during which it is possible to ameliorate the effects of sabotage. This would provide a ranking in which the least time for recovery would indicate the most critical vital area. However, recovery time ranking would not explicitly consider the various factors included in the relative ease of repair or mitigation associated with a particular vital area. For example, if a long recovery time were associated with a vital area, this area may still be critical because of a long repair or mitigation time for dealing with the effects of sabotage. Therefore, recovery time is probably not a sufficiently robust parameter on which to base a ranking method.

The second method which could be used as the basis for structuring a ranking method is based on response time, the time from sabotage detection to the critical recovery point. As in the case of recovery time, a long response time is desirable since it would provide a comparatively longer repair or mitigation time, which is also desirable. The important event in a response time analysis is the detection event. The earlier detection can be accomplished, the more time is available for repair. It is evident that a close relationship exists between recovery time and response time and that it reflects the relationship between the demand and detection events. Ideally, the detection event should occur before the demand event, in order to provide a longer response time than recovery time. Because of these interactions, as well as the failure of a response time analysis to consider explicitly repair or mitigation times, a ranking method based on response time alone would also be inadequate.

A third possibility for developing a ranking method involves the use of probability of detection of sabotage. In such a ranking method, a component or system with a low probability of sabotage detection would be considered more critical than one with a high probability of detection. This type of ranking method would provide useful information on the relative ability to determine the status of components or systems. However, importance of equipment is not considered, nor is criticality in terms of repair or mitigation of sabotage consequences. Although sabotage detection is an interesting parameter in the time sequence, it is inadequate to serve as a complete basis for rank ordering of vital areas.

Figure 4 illustrates the inadequacy of any one of these parameters by itself to serve as the basis for a rank ordering scheme. In the example in Figure 4, each of the three parameters discussed is used as the basis for ranking three vital areas (1, 2 and 3) with completely dissimilar results, i.e., totally different ranks are assigned to the same vital area. The ranking based on minimum recovery time provides the order from most critical to least critical vital area and results in the rank order of 1,2,3. Similarly, the rank order based on minimum detection probability is 3,2,1. Minimum response time ranking gives the order 2,1,3. Each method indicates a different vital area as being the most critical to power plant safety. Thus, although these parameters provide useful information for ranking, when each is considered by itself, the results are contradictory. The next section discusses a ranking method which combines several important parameters in order to minimize the possibility of discrepancies while retaining the information provided by each.

VITAL AREA 1	VITAL AREA 2	VITAL AREA 3
RECOVERY TIME = 2 HR	RECOVERY TIME = 12 HR	RECOVERY TIME = 2 DAYS
DETECTION PR = .95	DETECTION PR = .6	DETECTION PR = .2
RESPONSE TIME = 4 HR	RESPONSE TIME = 2 HR	RESPONSE TIME = 1.5 DAYS

VITAL AREA RANKINGS

MIN (RECOVERY TIME) - 1, 2, 3
MIN (DETECTION PROB) - 3, 2, 1
MIN (RESPONSE TIME) - 2, 1, 3

INTERRUPTION ANALYSIS - 1, 3, 2

Figure 4. Comparison of Recovery Time, Detection Probability and Response Time Rankings

2.2 Interruption Analysis

A more comprehensive and meaningful analysis of vital areas can be performed by combining the pertinent parameters into an interruption analysis. The interruption analysis described here has as its purpose the determination of the relative ability of the protection systems at a nuclear power plant to break into a sequence of events which has been initiated by a saboteur. The sequence of events will be similar to that shown in Figure 3 and the analysis is performed in a relative manner by ranking vital areas with respect to other vital areas. This type of analysis retains the benefits of each of these parameters while incorporating the insights gained from considering interrelationships among them. A combined analysis reflects the importance of interactions and relationships among components and systems rather than individual numerical values. For example, a relatively short recovery time may not be of great consequence if the associated repair time is even shorter than the recovery time. Similarly, a high probability of detection may not be an indication of relative security of a component or system if damage to that equipment is not reparable. Even a cursory look at these interdependencies illustrates the importance of considering how the relevant time parameters interact with one another.

Repair time, the time interval from detection of sabotage to completion of the repair or mitigation activity, is included explicitly in the interruption analysis. Detection time, the interval from component defeat to sabotage detection, is also included. As with the other parameters, these time intervals are more important for their relative length than for their absolute magnitude. Detection probability is thought to be the least important parameter for several reasons. It is very difficult to measure, or even to approximate, and would thus lend undue uncertainty to the analysis. The other parameters are time intervals and are therefore intrinsically commensurable. This explicitly probabilistic quantity also lacks the inherent relationship to the other parameters which characterizes the time intervals. The interruption analysis will be primarily based on the times associated with sabotage detection, component repair or mitigation, response and recovery.

The detection time interval should be as short as possible. In the case of sabotage of operating equipment, the effects of the sabotage will likely be known almost immediately. Repair or mitigation activities would be rapidly instituted, probably even before it is determined that sabotage was the actual cause of the disturbance. In this case then, the sabotage detection event does not necessarily occur the instant repair or mitigation begins. For operating equipment, component demand, which is coincident with defeat of the operating equipment, is the determining event. However, the occurrence of the demand and the sabotage detection events are crucial in the analysis of sabotage of

standby or non-operating equipment. If maintenance or testing activities can determine that equipment has been tampered with, then the equipment demand event may not occur at all. The important point to notice is that the recovery time can be effectively extended indefinitely if the demand event does not occur. That is, without occurrence of the demand event, the critical recovery point would never occur and the rest of the sequence would be forestalled because of an essentially infinite recovery time. Refer to Figure 3 for clarification of these relationships.

If the demand event does occur, then prior occurrence of the detection event ensures a relatively longer time available for repair or mitigation. Unless detection occurs before demand, the repair or mitigation time must be shorter than the recovery time to preclude the sequence extending beyond the critical recovery point. Similarly, the response time is lengthened resulting in higher probabilities of covering for the damaged components, perhaps by changing the operating mode of the facility. Detection time should be as short as possible while realizing that the zero detection time associated with simultaneous occurrence of the defeat and detection events is not necessarily optimal except in the case of sabotage of equipment in operation.

A second look at the example of Figure 4 from the perspective of the interruption analysis reveals that consideration of recovery time, detection probability and response time in combination results in a different, and more accurate, importance ranking than the ranking based on single parameters. The most critical vital area is 1, even though a high detection probability is associated with this area, because response time is twice as long as recovery time. Vital area 3 ranks second in importance, even though it has a very low probability of detection, because it has a relatively long recovery time. Vital area 2 is the least critical of the three because the response time is short in comparison to the recovery time. Although this example is rather contrived and omits important considerations such as repair or mitigation time, it does illustrate the type of interactions that should be included in a sabotage time sequence interruption analysis.

Importance measures assigned to the components of interest in an interruption analysis allow the formulation of a ranking procedure. These measures are structured in such a way that decisions concerning protection or upgrade choices can be made. The next section discusses importance measures based on the time interval parameters.

2.3 Importance Measures

Importance measures provide the analyst and, ultimately, the decision-maker with insight into the critical interrelationships of the system under study.

Consequently, the most crucial of the system characteristics should be included in the derived measure. These system characteristics and properties must be combined not only logically but also in such a way that the analyst can learn about non-obvious relationships and draw conclusions of practical significance. The importance measures discussed here for vital area ranking utilize time intervals and so they are logically consistent. They also provide general guidance on required protection levels and possibilities for upgrading the protection of vital equipment. These importance measures utilize combinations of the pertinent parameters as a basis for the rank ordering methodology and they provide a criticality ranking based on the region in which the numerical value associated with each vital area lies.

2.3.1 Critical Detection Time

The first combined importance measure for rank ordering is formed from the repair time, recovery time and detection time parameters. These quantities are chosen because of their inherent importance in providing protection to the nuclear facility and the relationships which exist among them. The repair time is used because it is one of the limiting parameters that indicates the potential ability of a facility's protection systems to ameliorate the consequences of sabotage. This interval must allow not only for the possibility of repair of damaged equipment but also for the substitution of other operational equipment for the compromised components. This time span serves as a hard constraint on the last point at which the detection event must occur in order to allow for recovery before the critical recovery point is reached. Figure 5 illustrates the effect of this constraint. Detection must occur in time to allow repair or mitigation to take place. Otherwise, the critical recovery point is reached before repair or mitigation can be completed. The minimum time required to effect a repair or to mitigate the consequences of sabotage of a given type of equipment is relatively constant. The problems associated with shortening this minimum repair time argue for the necessity of detection at the earliest time in order to provide a longer time for accomplishing the repair or mitigation.

Recovery time is included in the importance measure because it identifies the maximum time available for handling the immediate consequences of sabotage in an acceptable manner. The recovery time serves as a hard constraint on the total time available to perform both the sabotage detection and the repair or mitigation of sabotage consequences. The recovery time is thought to be fairly constant for the loss of given equipment, so the parameter which can vary the most in the importance measure is the detection time.

Detection time is the time interval from defeat of vital equipment to the actual ascertainment that sabotage has been perpetrated on the particular equip-

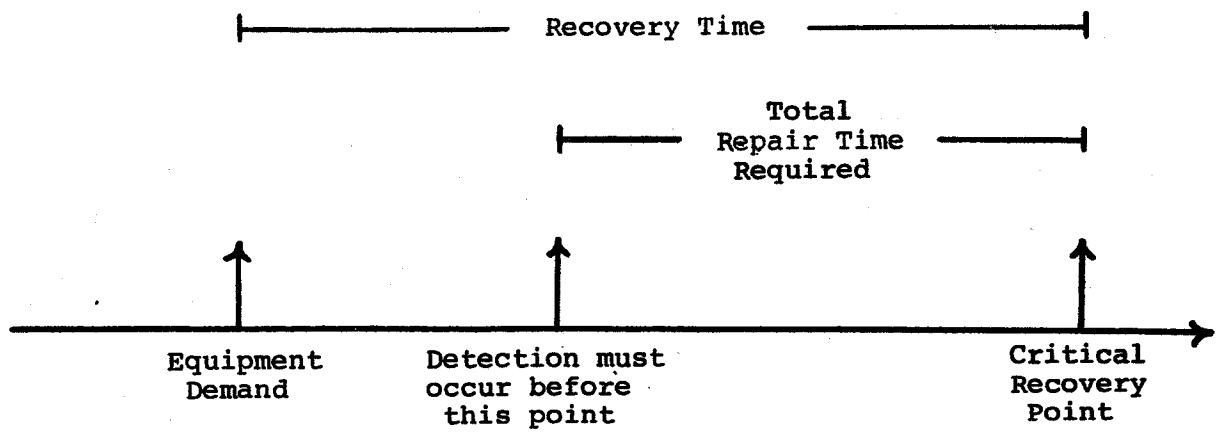

Figure 5. Last Point for Occurrence of Detection

ment. Because of the flexibility that exists for facility personnel and operating components to determine that sabotage has been performed, this time interval is likely to be the one with the greatest capability of affecting the importance measure. The detection time referred to here specifically excludes detection by the PPS, unless that detection occurs after defeat of the equipment; thus, the detection event of interest at this point is that performed by the operational systems.

Two primary capabilities exist for shortening the detection time. The first is the installation of operational control elements (OCEs)[5]. These OCEs are intended to act as sensors for individual components that serve as indicators of the operational status of the components. For example, an OCE on a valve could indicate whether the valve is open or closed as opposed to simply providing the more usual information on the status of controllers or actuators. OCEs are susceptible to sabotage, and their cost would be prohibitive if used in a general protection scheme. For protection of particularly important components, however, OCEs represent a potentially significant method of meaningfully reducing detection time. The second capability for decreasing detection time involves increasing the frequency of maintenance and testing activities which would decrease detection time for sabotage of equipment in a standby or safety mode. The purpose of increased maintenance and testing, in terms of the sabotage time sequence analysis, is to try to ensure that the detection event occurs before the demand event, thereby preventing reliance on damaged equipment for safety functions. Of course, there is a cost associated with increasing maintenance and test schedules that must be evaluated in light of decreased detection time and the increased protection afforded.

The first importance measure, IM, formed from the time interval parameters is given by

$$\begin{aligned} IM &= (Rp/Rc) \cdot Dt \\ &= Q \cdot Dt \end{aligned}$$

where Rp designates repair time, Rc designates recovery time and Dt represents the detection time. Q is used for notational convenience and represents the quotient Rp/Rc.

Figure 6 is a graph representing the relationship between detection time and the importance measure. The measure effectively divides the plane into three regions which are used for determining the importance of the vital area and equipment. Note that Q is used as a varying parameter in the measure. The graph in Figure 6 illustrates the critical importance of detection time in the interruption analysis and also the relatively constant nature of the repair and recovery times. The ratio of repair to recovery time can be determined and

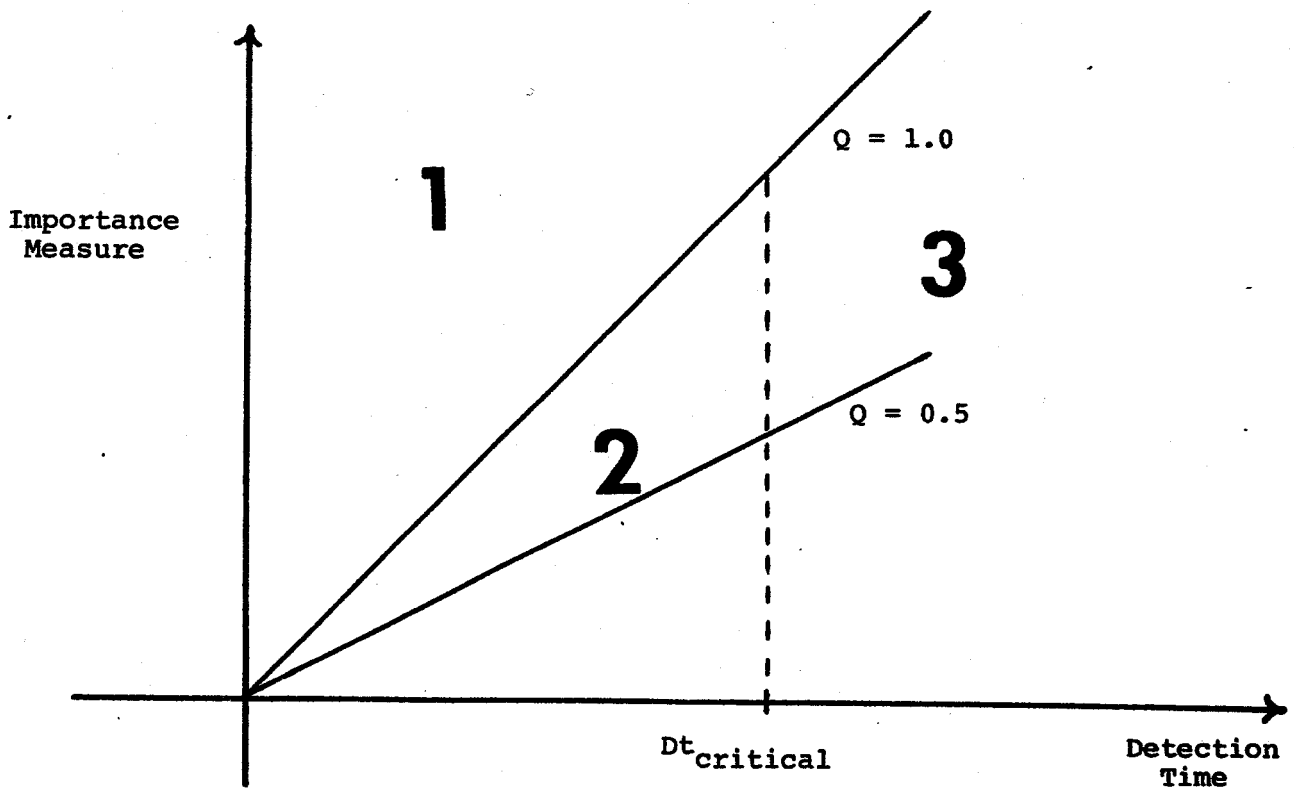

Figure 6. Importance Measure, Q·Dt

and is modeled by the family of curves in Figure 6. The effect of detection time on the importance measure can then be easily visualized.

The point marked $Dt_{critical}$ in Figure 6 represents the point at which the sum of detection time and repair time is equal to the recovery time. That is, it is the point after which sufficient time is not available to effect a repair or to mitigate the consequences of sabotage even if detection occurs. The importance measure thus falls into one of three regions on the graph in Figure 6. Region 1 is that area in which $Q > 1$, indicating that repair time is greater than recovery time. The second region is that area in which $Q < 1$ and $Dt < Dt_{critical}$ and the third region is that for which $Q < 1$ and $Dt > Dt_{crititial}$. Each region implies different conclusions to be reached about the importance measures that lie within that region and about the associated vital equipment.

Suppose that the measure for some vital equipment lies within region 1, i.e., $Q > 1$. The importance measure shows that this equipment is especially critical because the repair time for that equipment exceeds the total time available for recovery. The detection time is not a significant factor. This situation for equipment of vital importance is unacceptable, and there are two broad options for dealing with it. One option is to require the PPS to provide adequate protection, e.g., through such methods as barrier erection or entry control. The PPS option should be considered if it is determined that the operational systems cannot provide the required protection, either because of technological or financial constraints. The other option is implemented by the operational systems in the plant and consists of decreasing the repair time sufficiently for $Q < 1$. This could entail having more personnel on hand at all times, having repair equipment and parts on hand or making novel use of existing equipment. If the recovery time is shorter than about 2 hours, it is felt that no repair or mitigation would be possible because of the short time available. The recovery time arising from the loss of specific vital equipment is not amenable to significant increase through action by the operational systems. The PPS option and the option of decreasing repair time are the important alternatives for dealing with equipment whose importance measure lies within region 1.

Consider next the implications for equipment whose importance measure lies within region 2. This region is bounded above by the line $Q = 1$ and on the right by $Dt_{critical}$. It is the region for which the existing operational system appears adequate to handle the sabotage event. Within this region, a low value for Q and a low value for $Dt_{critical}$ are desirable. Tha is, for a given ratio of repair time to recovery time, a short detection time is best to allow maximum time for repair or mitigation. Similarly, for a given detection time, a low ratio of repair time to recovery time is preferable.

If an importance measure lies within region 3, then upgrades to the protection level of that vital equipment must be made. In order to shift the importance measure from region 3 to region 2, a decrease in detection time is required. This decrease could be accomplished technologically by either the installation of OCEs or entry controls, or it could be accomplished procedurally by increased maintenance or testing activity. Region 3 requires an enhanced detection capability by the facility. Along with a decrease in detection time, a decrease in Q could also be effected, as discussed above. In instances of a high Q value coupled with detection time greater than $Dt_{critical}$, Q would have to be decreased to prevent the importance measure from shifting to region 1.

The structure of this importance measure provides insight into the interrelationships among the time interval parameters. Indeed, based on insights gained from this measure, a slightly different importance measure can be formulated that incorporates the same relationships but is designed to accentuate the importance of the relative lengths of the time intervals. This new measure is presented in the next section.

2.3.2 Relative Detection Time

In the second combined importance measure, recovery time is used as the basis for the time interval relationships. Recovery time for the particular vital equipment under consideration is assigned the value of unity. The detection and repair times for that equipment are then related to the recovery time as a ratio of intervals. To illustrate, suppose that Q = Rp/Rc = 0.7. Thus, repair time requires 7/10 of the total time which is available for recovery. This implies that detection must be accomplished in a maximum of 3/10 of the total time available for recovery. The advantage of this importance measure is that repair time and detection time are explicitly related to the total time available to perform these functions.

Figure 7 presents the graph associated with this importance measure. In this graph, the abscissa is the proportion of recovery time available to perform the detection function. Hence, the maximum detection time in the figure is unity. Information concerning repair time and recovery time is contained in the parabola. The straight lines are again parametrized on the value of Q. Thus, for Q = 0.5, repair or mitigation requires half the time available for recovery. The intersection of the line Q = 0.5 with the parabola occurs at a relative detection time of 0.5, i.e., the detection event must occur within one-half the total time available for recovery. Similarly, a line with Q = 0.25 would intersect the parabola at a detection time equal to 0.75, indicating a relatively longer time for performance of the detection function.

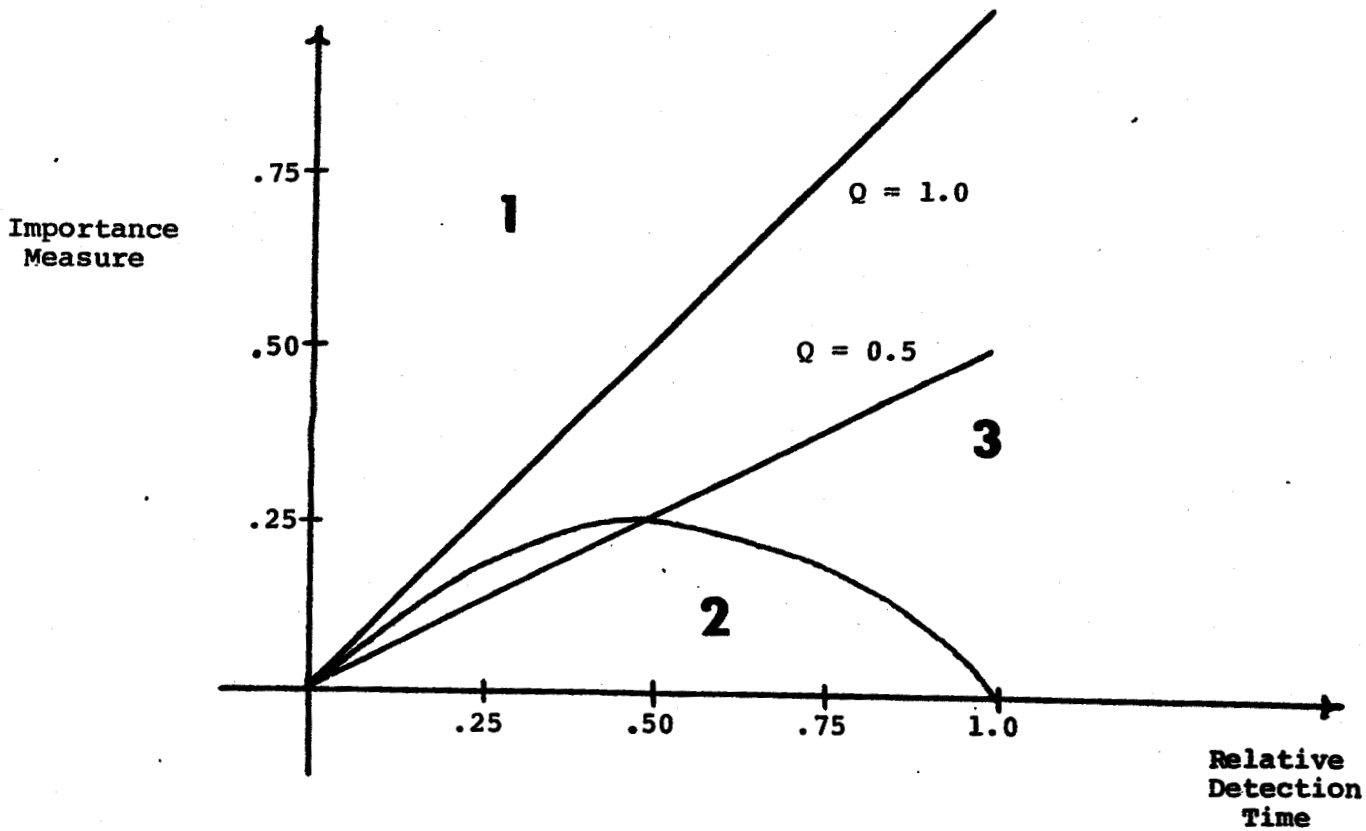

Figure 7. Relative Detection Time Importance Measure

Notice also that, as Q approaches zero, meaning either that repair time is very short or that recovery time is very long, the intersection of the line parametrized by Q with the parabola approaches a detection time of unity. This circumstance is consistent because detection time could then approach the total time available for recovery. On the other hand, if Q is greater than or equal to unity, then the parametrized line intersects the parabola only at a detection time of zero since repair or mitigation requires at least all of the total time available for recovery. Therefore, no time is available for the detection function. The parabola thus divides the graph into areas in which different protection strategies are required.

If the importance measure lies within region 1, where $Q > 1$, the PPS must provide added protection or else the repair time must be shortened. However, if the option to shorten repair time is chosen, it is not sufficient merely to ensure that $Q < 1$. The detection time must also be sufficiently short to be practicable with the shortened repair time. If it is not, then the importance measure is shifted into region 3 and not into the required region 2. If the importance measure lies within region 3, detection time is too long for the associated ratio of repair time to recovery time. To shift the measure to region 2 requires that the detection time be decreased, thereby shifting the importance measure along the appropriate Q-parametrized line into region 2. Alternately, the value of Q could be decreased, thereby shifting the importance measure vertically down into region 2. Of course, a combination of these upgrades may prove to be the most practical.

Region 2 is the area within which the importance measures for vital equipment must lie in order to ensure adequate protection of the facility. The important point about the relative detection time importance measure illustrated in Figure 7 is that, given a value for Q, it is immediately apparent what is the maximum allowable time to perform the detection function. Of course, it is desirable for the actual importance measure to have a numerically small value, corresponding to both a low Q-value and a shorter detection time relative to recovery time. As expected, if either the Q-value or relative detection time is comparatively large, then the other value must be small in order to maintain the importance measure within the parabola.

The interruption analysis discussed in this section is an important step in developing a general ranking procedure for vital areas or equipment. In the next section, this type of analysis is included in a conceptual scheme for ranking that includes both operational and physical protection systems, an interruption analysis, upgrade choices, a consequence analysis and the synthesis of these considerations into a ranking procedure.

3. RISK INDEX ANALYSIS

The major components of the conceptual rank ordering methodology are the interruption analysis and an analysis of consequences. These two analyses are combined as described below into a risk index to provide the final ranking. The interruption analysis, as discussed above, has two major segments: the protection afforded by the PPS and by the operational systems. The consequence analysis is concerned with the characteristics of the particular radioactive release resulting from sabotage of particular vital equipment. It does not take into consideration atmospheric modeling, population modeling or effects modeling and hence cannot be considered exhaustive. However, a more complete modeling of consequences is not warranted by the demands of the rank ordering.

Figure 8 shows the temporal relationships among the segments of the interruption analysis and the consequence analysis. For the purposes of ranking, the time line sequence must be extended beyond the radioactive release event. Thus, the analysis for the vital equipment begins with initiation of sabotage, extends through the defeat of the equipment and beyond the radioactive dispersal to consideration of the particular characteristics of the radioactive material released. The consequence analysis is important because the severity of the ultimate consequences of sabotage has an important bearing on the level of protection to be afforded vital equipment. Thus, the relationships among repair, recovery and detection times are not necessarily sufficient to rank vital equipment and areas in the most meaningful way.

A methodology for ranking vital equipment and areas is shown in Figure 9. The first step is to perform an interruption analysis on the vital areas and equipment within the facility (see Section 2.2). Importance measures incorporating repair times, recovery times and detection times would be determined. This critical information could conceivably be obtained from several sources, and quite likely all these sources would need to be utilized. For example, time parameter information can be obtained from dynamic models. These models, which attempt to depict the consequences of loss of vital equipment by analytical computer codes, would be particularly useful in determining estimates of recovery time. An associated potential source of information concerning the interactions of plant operating systems and the effects of sabotage is time-gated fault trees[4]. These are typical sabotage trees with the added feature of time gates added at appropriate places in the trees. These fault trees would provide very useful information on time intervals associated with events in the sabotage sequence analysis.

Another source of information would be questionnaires. These questionnaires would be used to gather information on operating procedures, repair capabilities, availability of extra equipment, possibilities for novel use of exist-

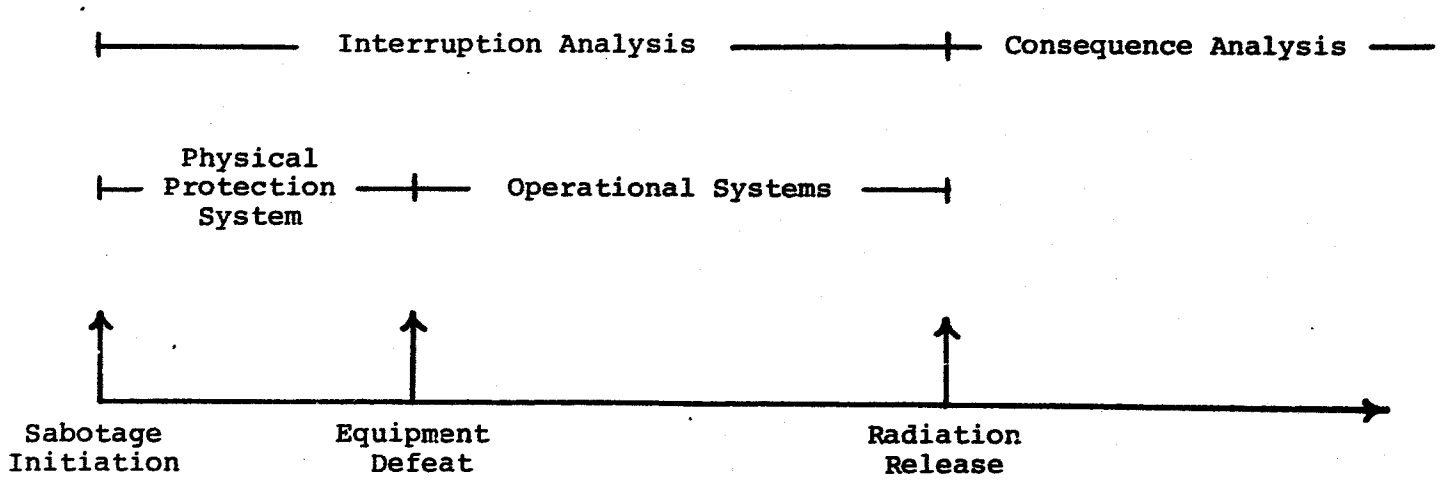

Figure 8. Risk Index Analysis Time Line

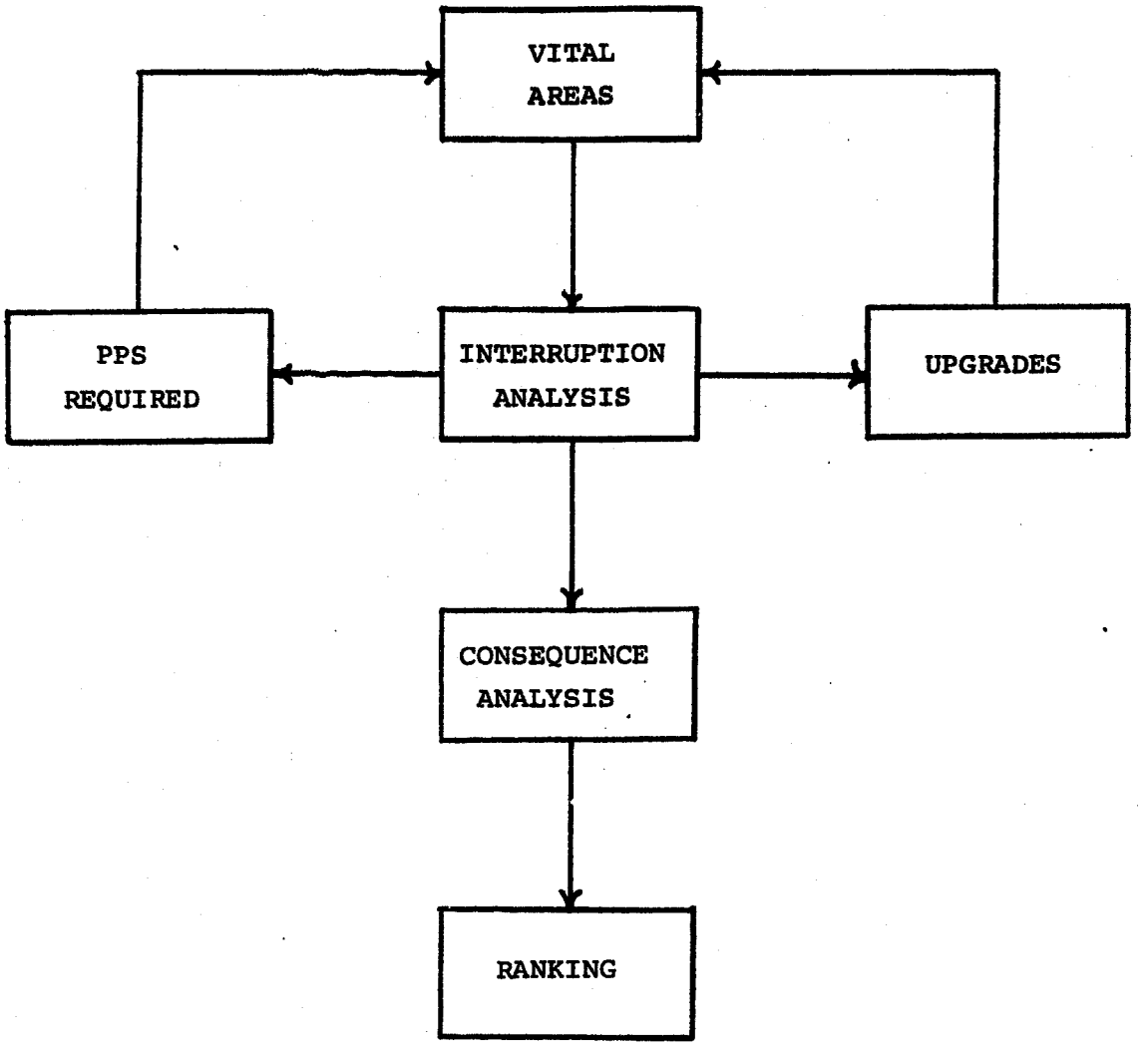

Figure 9. Ranking Methodology

ing equipment, etc. This information would be especially useful in determining realistic estimates of repair times and detection times.

The results of the interruption analysis would be used to make a decision on whether or not particular vital equipment is adequately protected. If the value of the importance measure obtained from the interruption analysis lies in region 2 of the graph in Figure 6 or Figure 7, then the ranking procedure may continue to the consequence analysis as indicated in Figure 9. However, if the measure lies in regions 1 or 3, then consideration must be given to improved protection strategies. If it is determined from the interruption analysis that a higher protection level is necessary, then upgrades could be considered along with the feasibility of requiring the PPS to provide enhanced protection. After these decisions have been made, then the upgraded equipment and areas are again considered from the point of view of the interruption analysis. This procedure is continued until an adequate level of protection is attained, indicated by the value of the importance measure lying in region 2. These iterations are an essential part of the methodology and must be performed with cost/benefit trade-offs in mind.

The next step in the procedure is the consequence analysis. The proposed consequence analysis is not all-inclusive. For the purpose of rank ordering vital areas and equipment, an analysis which includes such information as atmospheric dispersion, plume modeling, health effects, property damate, etc. is not necessary. The important information is the general consequences of radiological release, e.g., the types and quantities of radioactive material which spread beyond the boundaries of the plant. A sufficient consequence analysis could be performed by consideration of release categories arising from sabotage activities. The Reactor Safety Study[6], Appendix VI, lists release categories associated with hypothetical accidents at power reactors. This type of consequence analysis would be useful in the ranking methodology. These factors provide enough detail to serve as input to the ranking without being so cumbersome as to be prohibitive in either data gathering and extrapolation or manpower requirements.

The final step in the methodology is the ranking itself. The most important direct inputs to the ranking are the results of the interruption analysis and the consequence analysis. The result of each of the interruption and consequence analyses will be an importance ranking based on the respective criteria of importance to release possibilities and importance of release characteristics. Each vital area and associated equipment will have a ranking based both on interruption and consequence modeling. Therefore, the analyst will have a good indication of the overall importance of each particular vital area by the final step of this methodology. Indeed, it may not be mandatory to combine explicitly and and numerically the results of the interruption and consequence analyses in order to have a meaningful ranking.

If, at this point, having a single numerical value attached to each vital area and associated operating equipment is desired, then a simple scheme would be preferable in order not to obscure the information in the interruption and consequence rankings. A simple weighted sum of the individual rankings could be used to provide an overall ranking for each area. This would allow the analyst or the ultimate decision-maker to weight the individual rankings in whatever manner was felt to be most appropriate. The interruption analysis is the more detailed and important of the two inputs and might be weighted somewhat more heavily than the results of the consequence analysis. The final ranking could then be used to order priorities for upgrades or to allocate existing protection resources more effectively.

4. CONCLUSIONS AND RECOMMENDATIONS

This report has presented the conceptual development necessary for structuring a rank ordering methodology for vital areas at nuclear reactor facilities. The methodology considers first the interrelationships among important parameters affecting the security of vital equipment and their effect on radiological release beyond the boundaries of the facility. These parameters are combined into an importance measure that provides graphical information on the relative criticality of the vital areas. The results of this interruption analysis provide general guidance on required protection levels for the vital areas and point out effective ways of improving protection.

The results of the interruption analysis are then combined with a consequence analysis that considers categories of radiological release characteristics. An exhaustive consequence analysis, including atmospheric, population and effects modeling, need not be perfomed for an effective ranking. The individual rankings from these two separate analyses may then be combined explicitly, if desired, in order to produce a risk index number associated with each vital area. This risk index could then be used to order priorities for upgrading protection as well as for allocating existing protection resources more effectively.

A greater effort would be required to perform the interruption analysis than the consequence analysis since the effort and expertise required in gaining adequate knowledge to estimate accurately the time parameters involved is much greater than that required to estimate rather broad categories of release characteristics. The interruption analysis would likely require the use of dynamic, computer-based models, questionnaires circulated to experts and the use, and possible development, of time-gated fault trees. To utilize these sources of information would require a non-trivial amount of resources. The benefits which could be realized include a much greater knowledge of the impor-

tance of vital areas relative to each other and of the most effective ways of allocating new or existing protection resources.

In order to provide a clear illustration of the advantages of a rank ordering scheme over the present Type I/Type II designation, two subsequent analyses should be performed. The first study is needed to specify explicitly the required data and the most efficient methods of obtaining the data. This study would involve the development of questionnaires for quizzing experts in power plant operations, determination of the applicability of using computer-based models of power plant dynamics and the investigation of fault trees for discovering the consequences of sabotage. Structuring the most efficient methods of gathering the requisite information is important to the practical applicability of the rank ordering methodology.

The second study would involve the application of the vital area rank ordering scheme to a nuclear power plant which has already had a Type I/Type II vital area analysis performed. The results would indicate the costs and the benefits from a detailed rank ordering as opposed to a Type I/Type II specification. The rank ordering would help to show the weaknesses in the current protection strategies and the areas in which allocations for upgrades could be used most effectively. This analysis would serve too as an illustration of the applicability of the proposed data gathering techniques.

REFERENCES

1. S. L. K. Rountree, Security Officer Response Strategies (SECURORS), SAND82-0410, Sandia National Laboratories, Albuquerque, NM, March 1982.

2. D. Engi, Maintainability Analysis Procedure (MAP), NUREG/ CR-1786, SAND80-2497, Sandia National Laboratories, Albuqurque, NM, December 1981.

3. Component Failures at Pressurized Water Reactors, ALO-74 (Windsor: Combustion Engineering Inc., October 1980).

4. L. A. Goldman and P. Lobner, Protection Against Unauthorized Activities by Plant Personnel (Task 2) -- System Ranking, SAI01581-337LJ (La Jolla: Science Applications Inc., September 1981). [Draft].

5. P. Lobner et al., Light-Water Reactor Operations Control Analysis (U), SAI/LJ 79:1112.1 (La Jolla: Science Applications Inc., September 1979), (CNSI).

6. 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, October 1975).

DISTRIBUTION:

U.S. NRC Distribution Contractor (CDSI)
7300 Pearl Street
Bethesda, MD 20014
280 copies for RS
25 copies for NTIS

Author selected distribution - 6 copies
(List available from author.)

400	C. Winter
1000	G. A. Fowler
1230	W. L. Stevens, Attn: R. E. Smith, 1233
1700	W. C. Myre
1710	V. E. Blake, Attn: M. R. Madsen, 1714
1716	R. L. Wilde,
1720	C. H. Mauney, Attn: J. W. Kane, 1721
1730	M. L. Kramm, Attn: W. N. Caudle, 1734
1750	T. A. Sellers, Attn: D. L. Mangan, 1759
1752	M. J. Eaton
1754	I. G. Waddoups,
1760	J. Jacobs, Attn: J. M. deMontmollin, 1760A J. D. Williams, 1769
1762	H. E. Hansen
1762	R. W. Mottern
1768	C. E. Olson, Attn: G. A. Kinemond, 1768
1765	D. S. Miyoshi
4400	A. W. Snyder
4410	D. J. McCloskey
4414	G. B. Varnado
4416	L. D. Chapman (5)
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 (5)
4416	B. J. Roscoe
4416	S. L. K. Rountree
4416	D. W. Sasser
5000	J. K. Galt
8214	M. A. Pound
3141	L. J. Erickson (5)
3151	W. L. Garner (3)