APR 4 2000

SANDIA REPORT

SAND2000-0759
Unlimited Release
Printed March 2000

A Design Methodology for Unattended Monitoring Systems

J. D. Smith and Sharon M. DeLand

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

RECEIVED
APR 10 2000
OSTI

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, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent 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.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (703) 605-6000
Web site: http://www.ntis.gov/ordering.htm

Available to the public from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161
Microfiche copy: A01

DISCLAIMER

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

SAND2000-0759
Unlimited Release
Printed March 2000

A Design Methodology for Unattended Monitoring Systems

J. D. Smith and Sharon M. DeLand

Mission Analysis and Simulation Department
Sandia National Laboratories
Box 5800
Albuquerque, NM 87185-0977

Abstract

A methodology has been formulated to assist engineers in designing unattended monitoring systems that can be used to verify compliance with a variety of international agreements. In particular, this report describes how the methodology can be used to design unattended monitoring systems for detecting the diversion of nuclear materials from facilities. Through a sequence of activity-based studies, the methodology prompts the design engineer to address important issues of concern. These issues include definition of facility elements; identification of targets, threats, and potential pathways by which nuclear materials can be diverted; construction of target/threat-based scenarios that potentially challenge the system; and development of a monitoring-system design that specifically addresses these challenges. Importantly, the methodology provides a quantifiable way to assess the performance of the system design.

Acknowledgments

The authors wish to thank Tom Sellers and Darryl Drayer for suggesting this project and for their continuing support. We are grateful to Basil Steele, Mark Snell, and Sabina Jordan for several discussions about the physical protection methodology. We are thankful to Charlie Harmon for discussions about his broader methodology and how our approach fits within it. We also thank George Baldwin and Nicole Andrews for their comments on an earlier draft of this report. Any errors that remain are entirely those of the authors.

Finally, we wish to acknowledge the generous support of the Laboratory-Directed Research and Development Program, through which this project was funded.

Contents

Figures

Tables

Abbreviations and Acronyms

DBT	Design Basis Threat
DOE	Department of Energy
FMECA	Failure Modes, Effects, and Criticality Analysis
IAEA	International Atomic Energy Agency
MSAD	Monitoring System Analysis and Design
P_d	probability of detection
PPM	Physical Protection Methodology
PRA	Probabilistic Risk Assessment
SQ	significant quantity

This page intentionally blank.

A Design Methodology for Unattended Monitoring Systems

Introduction

An *unattended monitoring system* is an integrated set of sensors and data acquisition components used to monitor the status of high-value assets and processes. Typical sensors include breakbeams, motion sensors, radiation sensors, temperature sensors, video cameras, and other sensors applicable to monitoring conditions inside facilities or within well-defined regions. In most cases, the unattended monitoring system includes a communication link to allow data to be retrieved remotely by the user; it is possible, however, to collect data on-site and retrieve it periodically. Depending on the application, the purpose of the monitoring system may include detecting intrusion into a secured area, verification that known processes are occurring as expected, or detection of diversion of high-value assets.

Currently, there is no standard approach to guide design engineers tasked with developing unattended monitoring systems. Typically, an engineer visits the facility in which a monitoring system is to be installed, gathers information on the facility layout, and observes how the facility operates. Then, using engineering judgment and his knowledge of monitoring technologies, the engineer develops a system design. The effectiveness of the resulting design is highly dependent on the expertise of the engineer who developed it. Furthermore, because no systematic approach exists to assess quantitatively the effectiveness of a given design, even the most experienced engineer has difficulty choosing from among competing designs and optimizing a particular design.

Establishing a methodology for the design of unattended monitoring systems will lead to better monitoring systems that come as close as possible to achieving any specified monitoring objective. Such a methodology will ensure the engineer systematically considers the requirements for any proposed monitoring system and will help him assess how well the proposed monitoring system satisfies those requirements. A design methodology will also help the design engineer balance constraints on the monitoring system including cost, restrictions on the technology that can be used, and permissible impact on the facility and/or operations. Finally, a design methodology will help the design engineer capture any assumptions made in the analysis and design process and analyze their impact on overall performance.

The purpose of this report is to document our initial formulation of a methodology for the design of unattended monitoring systems. We refer to this methodology as the Monitoring System Analysis and Design (MSAD) methodology and recognize that the methodology outlined here is far from complete. Our approach is to adapt established system design methodologies in the areas of physical protection and probabilistic risk assessment to the problem of designing an unattended monitoring system for use in monitoring an international agreement.

To make the application of the methodology more concrete, we demonstrate how it can be applied to the design of an unattended monitoring system for a storage facility with the goal of detecting the diversion of nuclear materials from the facility. For this report, diversion is defined as the intentional, clandestine redirection of nuclear materials, purportedly intended for peaceful purposes such as energy or medical radioisotope production, in order for a host country to acquire nuclear weapons capability [1]. We assume that diversion of nuclear material at this storage facility requires removal of the material from the facility; in more complex facilities, removal of the material might not be necessary for diversion. The country in which the storage facility is located is a signatory to the Non-Proliferation Treaty. The facility is subject to international nuclear safeguards administered by the International Atomic Energy Agency (IAEA). The design engineer is a DOE national laboratory employee designing a monitoring system for use by the IAEA for use at the aforementioned storage facility.

Since detecting diversion necessarily focuses on detecting loss or redirection of nuclear materials, "The IAEA uses nuclear material accountancy as its basic measure for the safeguarding of declared material" [2]. Nuclear materials accounting establishes "the quantities of nuclear material present within defined areas and the changes in these quantities that take place within defined periods of time" [3]. Operator (host country) accounting information is compared to information from independent measurements by the IAEA to determine that material is properly accounted for. Containment and surveillance measures "to monitor access to the material are used to complement the information gathered from nuclear material accountancy" [2]. In particular, containment and surveillance can reduce the frequency of inventory-related measurements (item counting and non-destructive assay). Because Sandia specializes in containment and surveillance systems, rather than nuclear material accountancy, we focused on measures to monitor access to the material in our sample problem. We have not considered inclusion of nuclear material accountancy but a complete methodology for the design of unattended monitoring systems would need to address both accountancy and containment and surveillance measures.

The reader may be concerned that use of such a simple, specific example may limit the general applicability of the resulting methodology. Our intent was to use the example to illuminate the steps in the methodology and to begin to highlight areas where the methodology needs to be extended or modified. We believe the overall methodology is very general in nature since it is essentially a standard systems analysis methodology. However, more work needs to be done to show the methodology can be applied to other monitoring system design problems. While we have suggested some areas in the text where the methodology could be modified to apply to other problem domains, more complex design problems need to be analyzed in order to have a general methodology. Such analyses were beyond the scope of the current project.

Background

To determine what elements the methodology should contain, we reviewed methodologies in related areas. We first considered the physical protection methodology (PPM) developed by Sandia National Laboratories [4-12], which has been applied towards the physical protection of nuclear material. The monitoring goals for physical protection are, in general, quite different from those for detecting diversion of nuclear materials. Physical protection can often be couched as an *intrusion detection* problem with an emphasis on detecting each intrusion in time to apprehend the adversary before he can do significant damage through either theft or sabotage. Protecting against diversion focuses on detecting *loss or redirection of material* in time to prevent the host country from amassing enough material to acquire a nuclear weapon. Because the host country has a right to access the material for legitimate purposes, intrusion detection plays a limited role in detecting diversion of nuclear materials. Nonetheless, the monitoring system design problem is conceptually similar for physical protection and detecting diversion of nuclear materials; it is the monitoring system objectives and constraints that are different.

The second methodology we considered was Probabilistic Risk Assessment (PRA), which is commonly used in the evaluation of system safety [13-22]. While outwardly a different problem, the basic analytical approach has great general applicability. Indeed, PPM and PRA are closely related systems analysis methodologies. Both offered insights into the development of calculable models of facilities and processes, the establishment of measures of effectiveness for quantifying performance assessments, the identification of vulnerabilities or weak links in a system, and the use of an iterative approach for correcting such weaknesses.

Document Organization

This report provides a top-down view of the methodology, which consists of seven interrelated studies. In the next section, an overview of the entire approach is presented. Detailed descriptions of the seven studies follow, with a sample problem used across the studies to illustrate application of the methodology to the design of an unattended monitoring system capable of detecting the diversion of nuclear materials from a storage facility. In concluding remarks, other possible applications of the methodology are identified.

Overview of the Methodology

This section discusses the analyses and tools used in the methodology, introduces modeling conventions and terms, and describes the start-up requirements that must be met before the methodology can be used for the problem of interest.

The methodology is composed of seven interrelated analyses that are performed sequentially by the design engineer. The seven analyses are a combination of analyses used in the PPM and PRA. Figure 1 illustrates the flow of these analyses, highlighting the inputs to the methodology as well as the major outputs of each analysis.

We assume that the monitoring goals have been refined into quantitative *evaluation criteria* before the engineer begins to use the MSAD methodology. The evaluation criteria specify the level of performance the system design should achieve. Specifying achievable, quantifiable evaluation criteria from monitoring goals that are generally broad in scope is a significant undertaking. While we recognized its importance, identifying techniques to analyze the monitoring regime and goals was beyond the scope of the current project.

The basic approach in the methodology is to define a set of significant scenarios for the monitoring problem of interest and analyze those scenarios to determine key monitoring points and key monitoring parameters. The scenarios account for both the vulnerabilities in the facility and the capabilities of the threat. The design engineer uses the key monitoring points and parameters to select types of sensors and their location within the facility. The engineer then uses information collected during the course of the methodology to assess the overall performance of the monitoring system within the context of the facility and selected threat. The methodology stops with the creation of an acceptable conceptual design in which types of sensors, their performance requirements, and general locations are specified. There is considerable additional effort required to turn the conceptual design into a physical monitoring system that meets the performance requirements; this effort was also beyond the scope of the current project.

The outputs identified in Figure 1 are prepared by the design engineer and used at some subsequent point in the methodology but not necessarily in the next analysis in the sequence. The final output of the methodology is a system design that meets or exceeds the performance level specified by the evaluation criteria. As indicated in the figure, the design engineer may perform the analyses again if the system design does not meet the requisite performance level.

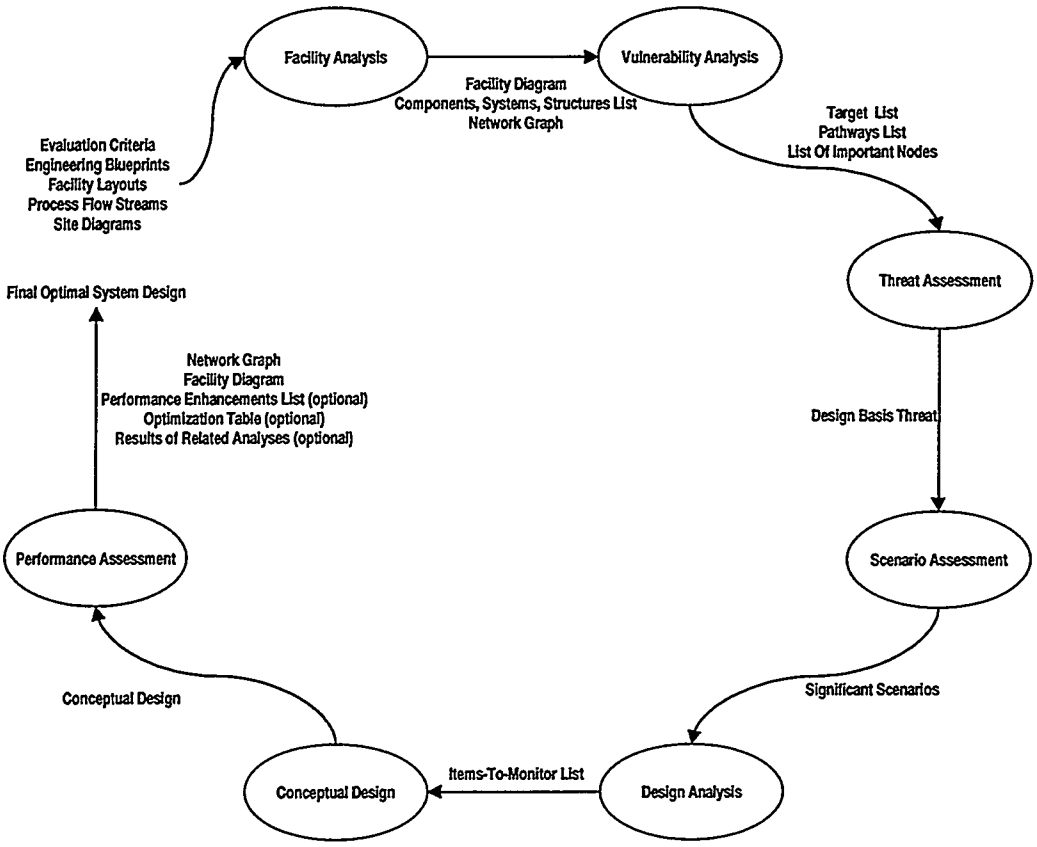


Figure 1. Overview of the Methodology

Methodology Analyses

Each analysis in the methodology addresses a particular aspect of developing the system design, as defined by the analysis' purpose in Table 1. To achieve its particular purpose, an analysis consists of one or more activities that are generally performed by the design engineer in sequence. Like analyses, individual activities also have their own inputs and outputs, but some outputs are only used within a particular analysis. Thus, the composite set of outputs for the methodology actually exceeds the outputs identified previously in Figure 1.

Tools

The methodology is mostly a paper-and-pencil exercise. Activities in some analyses require the use of a calculator. No software tools, however, are required.

Table 1. Purposes of the Analyses

Analysis	Purpose
Facility Analysis	To create a model of the facility that captures all of the possible routes by which the problem of interest (e.g., diversion of nuclear materials) could occur
Vulnerability Analysis	To identify the targets, the pathways by which potential threats could access these targets, and the characteristics of the pathways
Threat Assessment	To define the threats, map the threats to the targets, and determine the design basis threat (i.e., the threat the system will be designed to counter) for the monitoring system
Scenario Construction and Assessment	To develop significant scenarios by which the targets could be acquired by the design basis threat (and consequently other lesser threats)
Design Analysis	To define the initial characteristics of the monitoring system
Conceptual Design	To prepare a high-level design of the monitoring system, specifying both types of sensors to be used and their general location within the facility
Performance Assessment	To assess the performance of the proposed design and modify the design as needed to achieve the desired performance

Modeling Conventions and Terms

A major activity that occurs during the Facility Analysis is the construction of a topological model, called the *Network Graph*. This graph is then updated or referred to in subsequent analyses. The Network Graph thus may evolve across the set of analyses. A network graph is a well-known mathematical construct used to analyze pathways and networks. It is constructed with two types of elements: an arc and a node. A *node* is an ellipse that typically represents a location. An *arc* is a curved line that represents a path between two locations. A series of arcs and nodes that can be traversed from a target to the exterior of the facility is referred to as a *pathway*; for demonstration purposes in this report, we have alternately used the term *diversion pathway*. A *scenario* describes the traversal of a threat across a particular pathway.

Start-up Requirements

As mentioned previously, the MSAD methodology can be used to design unattended monitoring systems for various problems of interest. Accordingly, the goals, objectives, and evaluation criteria for the monitoring system need to be specified for the specific problem before the design engineer begins using this methodology. The evaluation criteria constitute the basis upon which the performance of the monitoring system design will be assessed and thus must be measurable and quantifiable. In this report, we have not described how one goes about defining specific goals, objectives, and evaluation criteria, but we have provided below the requirements upon which we applied the methodology to a specific problem of interest.

IMPORTANT: Please note that the evaluation criterion defined for the monitoring-system design illustrated in this report relates specifically to detecting diversion. If this methodology is used for a different problem, the design engineer will need to reformulate the goals, objectives, and/or evaluation criteria as necessary for that particular problem. Such changes may also impact the collection of certain data and the calculation of particular system performance measures based on that data within several analyses of the methodology.

Sample Problem Start-up Requirements

As described earlier, our implementation of the methodology in this report relates to the problem of detecting diversion of nuclear materials at a storage facility under international safeguards. We assume that this is a long-term storage facility and that the material may not be removed legitimately from the facility. In this context, the primary goal of the monitoring system is to provide assurance to the IAEA that the nuclear materials remain at the facility and have not been removed. The underlying assumption in monitoring system design is that the risk of detection can deter the host from diverting material. Therefore, the major objective in applying the methodology to the storage facility is to develop a monitoring system design that can detect the removal of nuclear materials from the facility and thus reduce the incentive to attempt diversion. Development of this design considers possible vulnerabilities in the facility and addresses ways to reduce the vulnerabilities to enhance the level of performance of the design.

We chose one overall metric to assess whether the system objective has been achieved; the metric is the risk of undetected diversion, measured in significant quantities (SQ) per annum. The SQ is a standard unit of measure used in the international safeguards community. It is, according to the IAEA, the approximate amount of plutonium-239 (8 kg) or highly enriched uranium-235 (25 kg) for which "taking into account any conversion process involved, the possibility of manufacturing a nuclear explosive device cannot be excluded." [23] The risk of undetected diversion depends on many closely related factors, including: the intent of the host to divert materials; the host country's willingness to risk being caught; the probability of detecting the diversion; and the difficulty of diverting the material including sheer physical effort, time, and cost.

Creating a detailed model for the risk of undetected diversion was beyond the scope of the present work. We will, instead, assert that it is possible to create such a model and look at how such a metric would be used in the methodology. In order to demonstrate how the methodology allows the design engineer to gather systematically the necessary information to calculate the performance metric, we will collect the information required for two of the factors listed above: "work" (the physical effort required to execute the diversion) and "probability of detection."

work – the amount of physical effort it takes for the threat to acquire the target; this factor is calculated for both individual arcs and complete pathways. It is based on the physical properties (i.e., material thickness and material yield strength) of elements constituting the facility.

probability of detection – the chance that a particular action or event will be observed and correctly identified. We will treat this factor as an attribute of a particular type of sensor.

Once the performance metric has been established, the design engineer must define one or more evaluation criteria, which set the bounds for minimum acceptable performance. In our case, we have (somewhat arbitrarily) set the evaluation criterion to 0.1 SQ/yr. This means that at most one-tenth of a significant quantity can be diverted per year without detection; consequently, it would take the host country 10 years to divert a significant quantity of material from this facility. In practice, the evaluation criteria would be negotiated between the customer (the IAEA in this case) and the design engineer based on what criteria both provide sufficient confidence that the monitoring objectives are being met and are achievable. It is possible the design engineer will discover during the design process that the evaluation criteria are not achievable. If this is the case, the evaluation criteria will need to be renegotiated and the monitoring approach itself may need to change.

Facility Analysis

The first step in the design methodology is Facility Analysis. The purpose of this analysis is to create a topological model of the facility. This model, called the Network Graph, should capture all of the possible pathways by which the problem of interest (e.g., diversion of nuclear materials) could occur. For the problem of diversion, these pathways are typically those along which nuclear materials may be moved, either normally or for the purposes of diversion. In subsequent studies in the methodology, these pathways are used to guide the selection and placement of sensors for the unattended monitoring system.

Activities

The design engineer will perform the following activities in the Facility Analysis study:

- Gather facility information
- Identify key facility elements
- Construct the facility model

Descriptions of these activities follow, with inputs and outputs for each activity highlighted.

Gather Facility Information

Inputs Engineering Blueprints, Facility Layouts, Process Flow Streams, Site Diagrams, Personnel Classification Lists, Evaluation Criteria

Output Facility Diagram (Recommended)

Description

The design engineer must first gather information that describes the physical characteristics of the facility, as well as the operations or processes that occur in the facility. For the problem of diversion, information about individuals who have access to the facility is also important. Examples of documents that provide this information are listed under inputs above. Note that the means by which the performance of the system design will be evaluated (i.e., the evaluation criteria) must also be available to guide the design engineer in deciding what information to gather. Because the evaluation criteria are considered a global input to the methodology, these criteria will not be identified as an input in subsequent studies in the methodology; however, the design engineer should reference the criteria wherever necessary.

Figure 2 shows the physical layout of a simple storage facility to which we will apply the MSAD methodology. The facility is not representative of any real facility, but is simply used here for illustrative purposes. The facility has one door and contains two sealed drum canisters, each containing unirradiated uranium dioxide ceramic fuel pellets; the pellets in one canister are 20% U-235 enriched and the pellets in the other are 10% U-235 enriched.

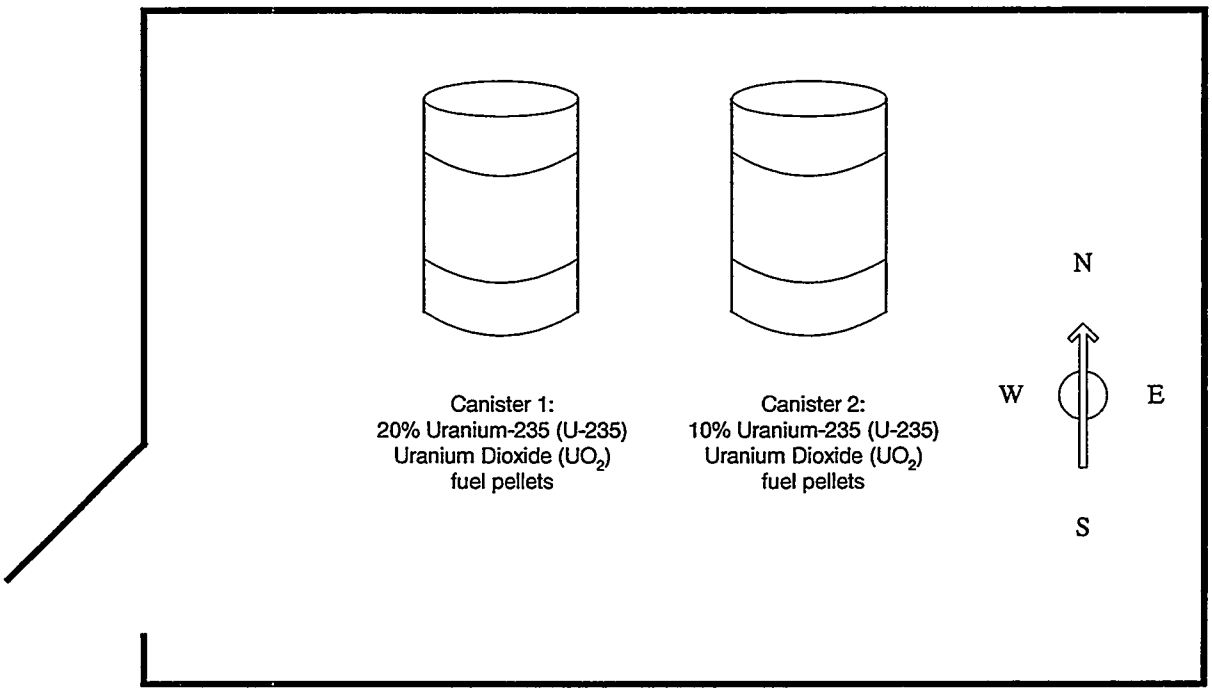


Figure 2. Facility Diagram of Sample Storage Facility

During this information-gathering activity, it may be useful for the design engineer to prepare a diagram similar to that shown in Figure 2 and update the diagram during subsequent studies in the methodology, as applicable.

Identify Key Facility Elements

Inputs Engineering Blueprints, Facility Layouts, Process Flow Streams, Site Diagrams

Output Components, Systems, and Structures List

Description

Using the physical and operational information gathered in the previous activity, the design engineer next prepares a list of the key elements at the facility. To construct this

list, we propose a simple classification scheme, whereby each element is classified as a component, system, or structure. In this scheme, the following general definitions apply:

component – a base element of a system

system – a regularly interacting or independent group of items forming a unified whole

structure – something that is constructed (e.g., a building)

An example of a component is a grapple for accessing fuel bundles in a cooling pond; an example of a system is a glove-box hot cell; and examples of structures are walls, doors, and large ventilation ducts. The level of detail captured at this point affects the completeness of the final analyses. However, if available facility information and/or resources are limited, the design engineer may wish to capture certain elements in aggregate form, and then, update the list in finer detail at a later date.

For the simple facility shown in Figure 2, we have classified the elements contained in the Components, Systems, and Structures List as follows:

- Structures: four walls, roof, floor, door
- Systems: two canisters ("storage systems")
- Components: cap and case of each canister

Construct the Facility Model

Input Components, Systems, and Structures List

Output Network Graph

Description

Once the components, systems, and structures have been developed, the design engineer can construct a topological model of the facility, the network graph. For the sample storage facility in this report, we have taken three-dimensional volumes (interior of magazine, interior of canister, exterior of magazine) as nodes and have used the boundaries between these volumes (walls, door, floor, ceiling, cap, case) as the arcs. While this approach may seem counterintuitive, the definitions of nodes and arcs worked well for our problem of interest (detection of diversion) because significantly more effort is required to breach the boundaries than to move from the door to the canister.

Figure 3 illustrates a Network Graph for the sample storage facility. Beginning at the top of the figure, one proceeds from the two nodes defining locations outside the storage facility along pathways defined by the various arcs to the interior, and then continues until the internal volumes are reached. Note that the interior coincidentally corresponds to the exterior of the two canisters. The four walls are differentiated arbitrarily as N, S, E, and W.

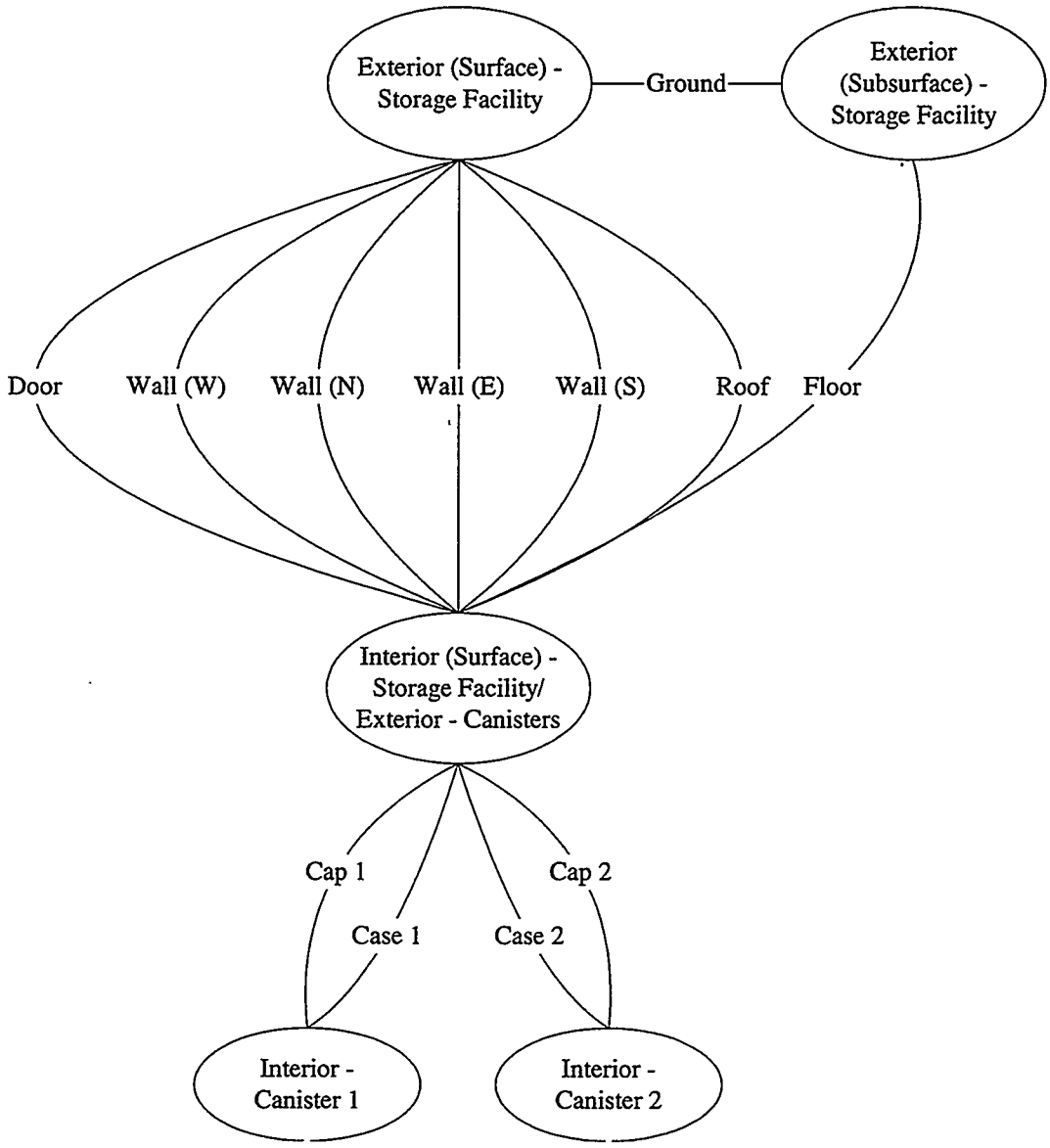


Figure 3. Network Graph of Sample Storage Facility

The Network Graph constructed during the Facility Analysis study will be used and modified throughout the subsequent studies in the methodology. As such, the design engineer may need or wish to add additional information to the graph before moving on to the next study in the methodology. The paragraphs below describe situations that may prompt the design engineer to further annotate the graph at this time.

Updating the Network Graph to Include an Existing Sensor System. For some applications, the facility of interest may include an existing sensor system that the design engineer wishes to incorporate within the new monitoring system design. In such a case, the design engineer should update the initial Network Graph to include the existing sensor system. There are two approaches. The first is to simply annotate the graph with a probability of detection appropriate for the sensor(s) monitoring each arc. This is the

approach that we will take in this paper. The second approach is to create new nodes representing the sensing volumes and new arcs representing the paths between them. The former approach is much simpler but may not accurately capture how well the sensor provides coverage of the path segment. The latter approach, while more complete, rapidly leads to a complicated Network Graph.

Updating the Network Graph to Capture Alternate Information. The design engineer may choose to capture alternate important information, such as process flow, on the Network Graph by using color or other means. As an example of using color to discriminate processes, green could be used to identify normal material flows, red could be used for potential diversion pathways, and perhaps a third color such as yellow could be used for instances where both the normal and diversion routes coincide. Other significant facility-specific information collected during the Facility Analysis study could be assigned at this time to the appropriate arc or node, or serve as input to a subsequent study in the methodology. Such information might include continuous versus discrete operations, personnel (operator, security and management) activities, and on-site inspection activities. Such information may affect choices made for the monitoring system. For example, required on-site inspections may be adequate to assess whether facility structures have been altered to permit diversion. In this case, achieving the required monitoring level may not require sensors on the diversion paths that require breaches of the facility structure.

Updating the Network Graph to Incorporate Future Facility Enhancements. The Network Graph may require some iterative refinement to achieve the level of detail and fidelity with the actual physical system necessary for some of the downstream analyses. A final aspect to be considered is the complete life cycle of the facility to ensure that no details have been overlooked in the Facility Analysis study. The design engineer should find out whether modifications to the actual facility or to operational procedures within the facility are anticipated. If so, then the design engineer should update the Network Graph to incorporate such changes. Failure to incorporate planned changes in the overall monitoring system design could have unforeseen effects. For example, additional and potentially vulnerable pathways could result from facility enhancements; and if not identified, these pathways could negatively impact the overall performance of the evolving system design.

Vulnerability Analysis

The second step in the design methodology is the Vulnerability Analysis. The primary purposes of this study are to identify targets in the facility and the pathways by which the targets can be accessed for the problem of interest. As part of this analysis, the characteristics of facility elements are also defined and insights into the strengths and weaknesses of the facility are gained.

Activities

The design engineer will perform the following activities in the Vulnerability Analysis study:

- Identify and rank potential targets
- Define start and end points of pathways
- List pathways
- Review and screen out untenable pathways
- Identify important nodes
- Perform a Failure Modes, Effects and Criticality Analysis (FMECA)
- Assign attributes to facility elements

Descriptions of these activities follow, with inputs and outputs for each activity highlighted.

Identify and Rank Potential Targets

Inputs Network Graph and, as applicable, any of the following: Process Flow Streams and Engineering Blueprints

Outputs Target List, Network Graph (Updated)

Description

Identifying and ranking potential targets in the facility may be considered part of a Threat Assessment. However, we found that the information on the targets was required in order to identify potential pathways so we have moved this activity to the Vulnerability Assessment.

For the problem of diversion, targets may include nuclear materials as well as certain equipment and systems. Determining whether or not nuclear materials are attractive targets is based both on the ease of acquisition and the ease with which the materials could be used in a nuclear weapons program. Failure to identify all of the potential targets could allow diversions to go undetected since the monitoring system will not be designed counter diversion of unidentified targets.

To identify the potential targets, the design engineer can use the Network Graph and information gathered during the facility analysis such as process flow streams and engineering blueprints. Once the targets have been identified, the design engineer should rank the targets based on the criterion of the targets' desirability to potential adversaries. After creating the ranked Target List, the design engineer should annotate the Network Graph to identify the target locations and corresponding amounts as applicable.

For the sample storage facility in this report, we have created a ranked Target List composed of two targets:

1. 141 kg UO_2 fuel pellets, 20% enrichment U-235
2. 141 kg UO_2 fuel pellets, 10% enrichment U-235

This ranking is based on the presumption that, from an adversarial point-of-view, it is more advantageous to divert higher quality material.

Define Start and End Points of Pathways

Inputs Network Graph, Target List

Output Pathway Points List

Description

In this activity, the design engineer uses the Network Graph and the Target List to define the start and end points of all possible pathways by which the identified targets can be accessed by the threats. For the sample storage facility in this report, the start points denote the locations of the targets, and the end points denote the locations at which one can assume diversion has occurred. On the Network Graph, both start and end points are defined as nodes.

For the sample storage facility, the Pathway Points List created in this activity consists of two start points and one end point:

Start points: interior of canister 1 and interior of canister 2
End point: exterior of the magazine

List Pathways

Inputs Network Graph, Pathway Points List

Outputs Pathways List, Network Graph (Updated)

Description

For this activity, the design engineer first prepares an initial list of all pathways. A pathway consists of all the arcs and nodes to be traversed between any start point and end point. Thus, for each start point in the Pathway Points List, the design engineer would examine the Network Graph to identify all possible pathways to the respective end

point(s). Each start point can thus, depending on the number of end points, result in several pathways.

For the sample storage facility in this report, we created a Pathways List composed of 28 individual pathways (see list below). Twenty-four of the pathways are described by two arcs, and four of the pathways are described by three arcs. All pathways begin with the target and end at the exterior surface of the facility.

1. Cap 1 - Door
2. Case 1 - Door
3. Cap 2 - Door
4. Case 2 - Door
5. Cap 1 - Wall (W)
6. Case 1 - Wall (W)
7. Cap 2 - Wall (W)
8. Case 2 - Wall (W)
9. Cap 1 - Wall (N)
10. Case 1 - Wall (N)
11. Cap 2 - Wall (N)
12. Case 2 - Wall (N)
13. Cap 1 - Wall (E)
14. Case 1 - Wall (E)
15. Cap 2 - Wall (E)
16. Case 2 - Wall (E)
17. Cap 1 - Wall (S)
18. Case 1 - Wall (S)
19. Cap 2 - Wall (S)
20. Case 2 - Wall (S)
21. Cap 1 - Roof
22. Case 1 - Roof
23. Cap 2 - Roof
24. Case 2 - Roof
25. Cap 1 - Floor - Ground
26. Case 2 - Floor - Ground
27. Cap 2 - Floor - Ground
28. Case 2 - Floor - Ground

Review and Screen Out Untenable Pathways

Once the initial list of pathways has been compiled, the design engineer should then evaluate the pathways to determine whether the pathways would be credible (or technically feasible) in scenarios for the problem of interest. For example, in the case of diversion, one might evaluate the credibility of the pathways by considering the size and form of the targets in relation to the characteristics of the structures (i.e., arcs) through which these targets would have to pass. Thus, if a particular pathway included a floor drain and a target was a solid material larger than the drain, then that pathway could be eliminated from the initial list of pathways.

The 28 pathways identified above for our sample problem are all credible pathways.

Identify Important Nodes

Input Network Graph

Outputs List of Important Nodes, Network Graph (Updated if desired)

Description

Using the Network Graph, the design engineer examines the nodes and identifies those that have many arcs coming into and/or going out of them. These nodes may become key monitoring locations later in the methodology. The design engineer may also wish to update the Network Graph to highlight the important nodes determined in this activity.

For the sample storage facility in this report, the List of Important Nodes contains a single item: Interior (Surface) - Storage Facility/ Exterior - Canisters, which is the central node in the Network Graph. We did not update the Network Graph, however, as a result of this activity due to the simplicity of the example facility.

Perform a Failure Modes, Effects, and Criticality Analysis (FMECA)

Input Components, Systems, and Structures List, Evaluation Criteria

Output FMECA Table

Description

This activity involves evaluating each of the key elements in the facility to determine a set of FMECA-related parameters with respect to the predefined evaluation criteria for the monitoring system. The key facility elements were specified in the *Components, Systems, and Structures List* constructed during the *Facility Analysis* study. The FMECA parameters are defined as follows:

Function	-	Class of the element as determined from the Components, Systems, and Structures List
Failure Mode	-	Mechanism by which the element can lose its ability to perform its desired function. There may be more than one failure mode for a given element.
Effect	-	Implication of the failure on the element's ability to perform its function
Criticality	-	Relative importance of the element with respect to the evaluation criteria

The level of detail necessary for the FMECA is directly proportional to the information available and the fidelity of the analysis. If a quantitative assessment is desired, very detailed information regarding the facility is necessary; and the function, failure, and effect analyses require a significant allocation of analytical resources. In many cases, however, a qualitative FMECA is sufficient.

A simple table can be constructed to capture the information obtained from this analysis, where the rows identify the facility elements and the columns, the FMECA parameters. For the sample storage facility in this report, we performed a simple qualitative FMECA and provide the results in Table 2. Each of the elements in the sample storage facility was individually analyzed. Examining the logic applied for the "door" in particular, the element is classified as a structure by function and it may fail or lose structural integrity by breach. The overall system effect with respect to diversion is to allow access to the canisters containing the nuclear materials, but the element is qualitatively assessed as "low" in criticality because of its common use in "normal" storage facility operations. It is in fact likely that the door element may be a constant source of noise in the acquired sensor response data, and, in turn, directly affects the design and implementation of the monitoring system.

Table 2. FMECA Table for Sample Storage Facility

Element	Function	Failure Mode	Effect	Criticality
Walls (4)	Structure	Breach	Access to canisters	Moderate
Roof	Structure	Breach	Access to canisters	Moderate
Floor	Structure	Breach	Access to canisters	Moderate
Door	Structure	Breach	Access to canisters	Low
Cap 1	Component	Breach	Access to target	High
Case 1	Component	Breach	Access to target	High
Cap 2	Component	Breach	Access to target	High
Case 2	Component	Breach	Access to target	High

Assign Attributes to Facility Elements

Inputs FMECA Table, Network Graph, Information about the Facility

Outputs FMECA Table (Updated), Network Graph (Updated)

Description

The design engineer now characterizes each of the facility elements using a set of common attributes which contribute to the overall performance of the monitoring system. We have already indicated that two factors that affect the risk of undetected diversion are the effort required to divert the material and the probability of detection. To keep the example simple, we have chosen to measure the effort required to divert the material using the quantity of work, defined as the product of yield strength and thickness, required to breach each element of the path. Thus the attributes we will use are material type, material thickness, and material yield strength. We also use the attribute of probability of detection when a sensor is monitoring a path segment. Design engineers who use different criteria to evaluate the performance of the monitoring system design than those we selected for the problem of diversion may need to define other attributes for this particular activity.

For this activity, the FMECA Table (prepared in the previous activity) and the Network Graph are used. In addition, the design engineer must obtain information that describes the physical characteristics of the elements. The documents gathered during the Facility Analysis may be useful, but additional information may also need to be collected. The elements to be characterized are those listed in the FMECA Table; these elements should also be represented as nodes or arcs on the Network Graph. We recommend first updating the FMECA Table to include the performance-related attributes and then transferring this information to the corresponding arcs (and nodes if applicable) of the Network Graph.

Table 3 shows an updated FMECA Table prepared to include characteristics of the attributes for the sample storage facility in this report. Because there was no existing monitoring system in the facility, the probablity of detection of all elements is equal to zero.

Figure 4 shows a fully updated Network Graph of the storage facility after all of the Vulnerability Analysis activities have been performed. First, we indicated the type of material located at the two canister nodes as described in the *Identify and Rank Potential Targets* activity. Second, we transferred the values assigned for the three physical attributes to the arcs as described above. Because the probablility of detection is zero for all such arcs, we did not transfer those values to the graph.

Table 3. FMECA Table with Performance-Related Attributes for Sample Storage Facility

Element	Function	Failure Mode	Effect	Criticality	Material Type	Material Thickness (cm)	Material Yield Strength ($kg\text{-}cm/s^2$) [24]	P_*
Walls (4)	Structure	Breach	Access to canisters	Moderate	concrete	30.5	$2x10^6$	0.0
Roof	Structure	Breach	Access to canisters	Moderate	concrete	30.5	$2x10^6$	0.0
Floor	Structure	Breach	Access to canisters	Moderate	concrete	30.5	$2x10^6$	0.0
Door	Structure	Breach	Access to canisters	Low	steel	0.635	$22x10^6$	0.0
Cap 1	Component	Breach	Access to target	High	steel	0.635	$22x10^6$	0.0
Case 1	Component	Breach	Access to target	High	steel	0.635	$22x10^6$	0.0
Cap 2	Component	Breach	Access to target	High	steel	0.635	$22x10^6$	0.0
Case	Component	Breach	Access to target	High	steel	0.635	$22x10^6$	0.0

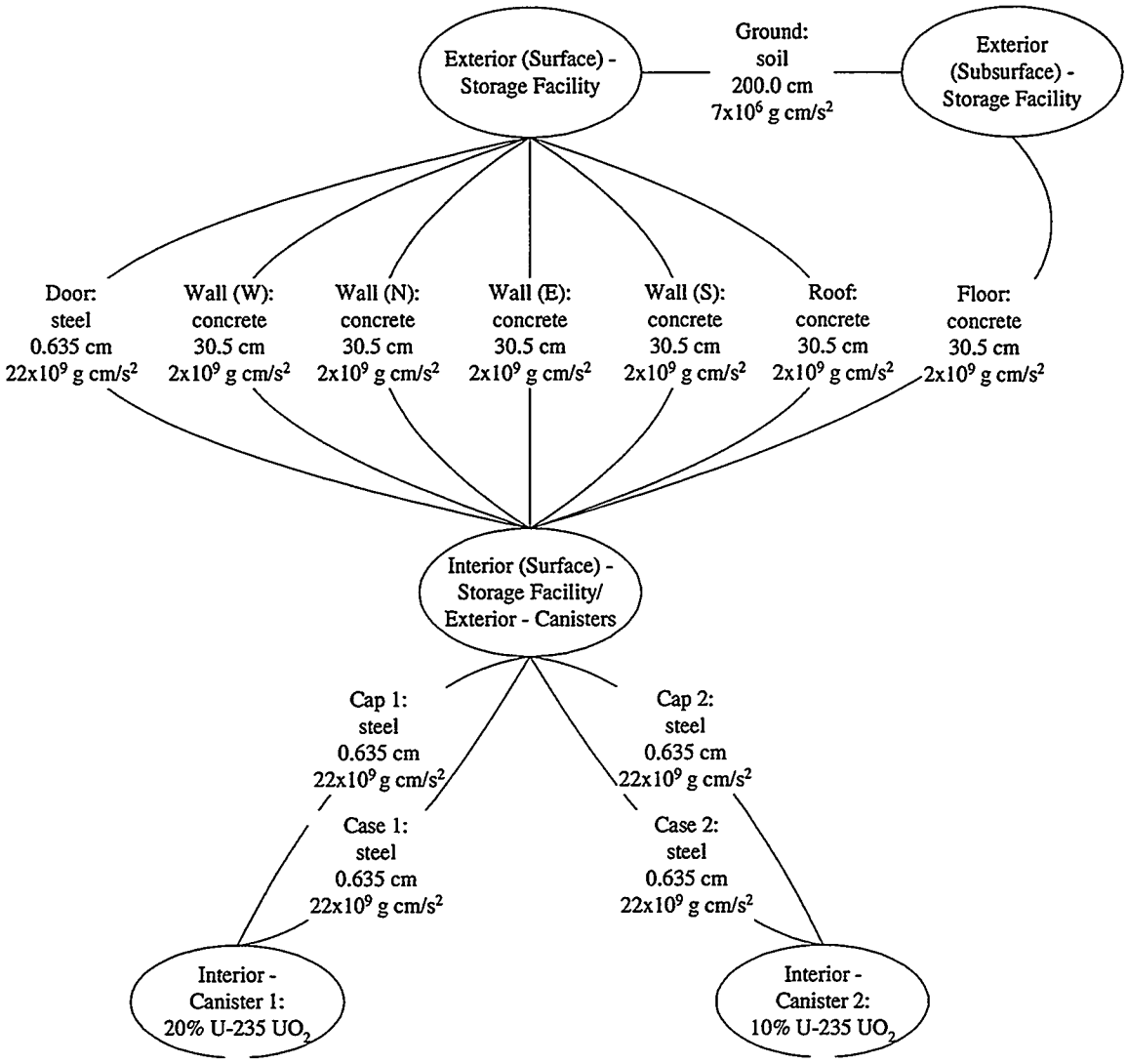


Figure 4. Network Graph of Sample Storage Facility Updated with Performance Attributes. Each arc is labeled with the material type, thickness, and yield strength.

Threat Assessment

Threat Assessment is the third analysis in the design methodology. Here, potential threats to the facility are identified and mapped to the facility targets. This mapping is used to select the threat level to which the unattended monitoring system will be designed.

Activities

The design engineer will perform the following activities in the Threat Assessment study:

- Define threats
- Develop frequency estimates
- Develop consequence estimates
- Compute risks
- Select the design basis threat (DBT)

Descriptions of these activities follow, with inputs and outputs for each activity highlighted.

Define Threats

Inputs Personnel Classification Lists (and/or other Threat-related Information), Target List

Output Threat List

Description

The design engineer begins the analysis by defining the potential threats to the facility. The definition of a threat in the MSAD methodology depends on the goals and objectives established for the monitoring system. Since the application of the methodology in this report focuses on detecting the diversion of nuclear materials, we have narrowed the definition of threat to include only personnel who have access to the facility. Applications of the methodology with wider scope might have a broader definition of a threat that could encompass events like earthquakes and power outages, as well as other people and/or objects that may or may not have access to the facility.

As part of the threat-definition process, we determined that a convenient way to categorize personnel-type threats is by job classification. Other classifications, of course, could be developed to fit one's particular application of the MSAD methodology. Using personnel classification lists gathered during the Facility Analysis study, we identified five classes of jobs as likely threats:

1. Managerial
2. Technical
3. Security Force
4. Clerical
5. Janitorial

Develop Frequency Estimates

Input Target List, Threat List

Output Frequency Estimates Table

Description

Up to this point in the methodology, the design engineer has independently identified targets in the facility and threats to the facility. In this activity, the targets and threats will be associated (or mapped) and estimates computed to determine the frequency at which the potential diversion could occur, based on access to the targets.

To perform this activity, the design engineer first constructs a table to map the targets to the threats. The rows in the table are the targets from the Target List, and the columns are the threats from the Threat List (or vice versa). After constructing the table, the design engineer needs to compute a frequency estimate for each target/threat pairing (i.e., cell in the table). Using the problem of diversion, the frequency estimate specifies how often the particular target could potentially be diverted by the particular threat based upon the number of expected threat accesses to the target per year. The number of accesses we used was based on the number of accesses required to support normal operations. For this example problem, we have assumed that the technical and managerial staffs have the highest number of accesses to the material while the janitorial staff has the lowest number of accesses.

The frequency estimates play an important role in determining what threats the monitoring system will be designed to protect against. Since the host has essentially unlimited access to the storage facility, diversion of the material may occur at any time – not just with normal accesses. Therefore, it is important that the design engineer have reliable information about the number of actual accesses to the material; the most likely source of this information is the monitoring system itself. Therefore, one of the first identified requirements for the monitoring system in our example problem is to count the number of accesses to the material. Furthermore, it would be useful if the monitoring system could distinguish between the type of staff accessing the material; this is a difficult problem and we will not attempt to address it in this paper.

For the sample storage facility in this report, Table 4 shows the frequency estimates for each target and threat combination. The threats are arranged in order of increasing frequency of access. We assumed each threat would attempt a diversion of some quantity of nuclear material with every entry into the facility.

Table 4. Diversion Attempt Frequency Estimates for the Sample Storage Facility

Target	Threat Classifications				
	Janitorial	Clerical	Security Force	Technical	Managerial
141 kg UO_2 20% U-235	2 attempts/yr	4 attempts/yr	12 attempts/yr	24 attempts/yr	48 attempts/yr
141 kg UO_2 10% U-235	2 attempts/yr	4 attempts/yr	12 attempts/yr	24 attempts/yr	48 attempts/yr

Develop Consequence Estimates

Input Target List, Threat List

Output Consequence Estimates Table

Description

Next, the design engineer estimates the consequence of each threat's actions against each target. The consequence is some measure of the (usually negative) outcome of a threat action against a target. The severity of the consequence usually varies with the capabilities of the threat. To perform this activity, the design engineer first constructs a table to map the targets to the threats. The rows in the table are the targets from the Target List, and the columns are the threats from the Threat List (or vice versa). After constructing the table, the design engineer fills in the table with a consequence estimate for each target/threat pairing (i.e., cell in the table).

In the case of diversion, we have chosen to measure the consequence in terms of significant quantities of material. We assume that this is a host-country engineered diversion of material and therefore, if a staff member of any category is participating in a diversion attempt, we assume they have enough training and resources to effectively carry out the diversion. We decided, therefore, that in the absence of any monitoring system, the consequence of any diversion attempt would be that all of the material would be diverted. Recall that for 20% or greater enrichment of the Uranium 235 isotope, 25 kg U-235 = 1 SQ. In our example, the canister containing the 20% enrichment material contains 1 SQ while the canister with the 10% enrichment material contains 0.5 SQ.

For the sample storage facility in this report, Table 5 shows the consequence estimates that were derived for the pairings of targets and threats.

Table 5. Consequence Estimates Table for Sample Storage Facility

Target	Threat Classifications				
	Janitorial	Clerical	Security Force	Technical	Managerial
141 kg UO_2 20% U-235	1.0 SQ	1.0 SQ	1.0 SQ	1.0 SQ	1.0 SQ
141 kg UO_2 10% U-235	0.5 SQ	0.5 SQ	0.5 SQ	0.5 SQ	0.5 SQ

Compute Risks

Input Frequency Estimates Table and Consequence Estimates Table

Output Risk Table

Description

Using the frequency and consequence estimates from the previous two activities, the design engineer now computes the risks associated with the particular target-threat combinations. Risk is generally defined as the product of the occurrence frequency and the associated consequence.

The computed risks should be compared to a pre-established risk tolerance criterion in order to assess which threat-target combinations need to be addressed in the design process. The risk tolerance criterion is usually a "rule of thumb" and is very domain specific. For example, in probabilistic risk assessments associated with safety of nuclear facilities, a commonly used risk criterion is 1×10^{-6} latent cancer fatalities/yr. In principle, threat-target combinations for which the risk is less than the risk tolerance level do not need to be addressed with a monitoring system.

We do not know if there is a commonly accepted risk criterion for diversion. Therefore, we have arbitrarily set one of 0.1 SQ/yr. This criterion is identical to our performance criterion because we happened to choose the risk of undetected diversion as our performance metric.

Table 6 shows the Risk Table we constructed for our sample storage facility to hold the new values computed in this activity. The risk values may appear strange to the reader since they are so high and imply an annual diversion that exceeds the amount of material in the facility. However, if the values are taken to be the rate at which the material could be diverted as opposed to the amount of material that could be diverted, they accurately represent the risk posed by the various threat-target pairs. All of the threat-target pairs exceed our risk tolerance. Therefore the monitoring system design must address all of the threat-target combinations.

Table 6. Risk Table for the Sample Storage Facility

Target	Threat Classifications				
	Janitorial	Clerical	Security Force	Technical	Managerial
141 kg UO_2 20% U-235	2 SQ/yr	4 SQ/yr	12 SQ/yr	24 SQ/yr	48 SQ/yr
141 kg UO_2 10% U-235	1 SQ/yr	2 SQ/yr	6 SQ/yr	12 SQ/yr	24 SQ/yr

Since the second target has half the enrichment of the first target and both targets are accessed with equal frequency, diversion of the second target poses half the risk that diversion of the first target poses.

Select the Design Basis Threat

Input Risk Table

Output Design Basis Threat

Description

The Design Basis Threat (DBT) is the level of threat to which the monitoring system will be designed. Generally, the DBT is the threat that poses the greatest risk. The presumption here is that by designing a monitoring system to protect against the DBT, the system should also be able to defeat all threats that pose less risk to the facility. An important assumption underlying the assertion that it is sufficient to consider the DBT alone is that the other threats use the same mechanisms to defeat the system but are less capable and thus less effective.

In some cases, it may not be possible to adequately protect against the selected design basis threat given other constraints (e.g., cost) on the monitoring system. In such cases, the design engineer may need to choose a lesser DBT in consultation with his customer.

For the sample storage facility in this report, we used the process described above to select the Managerial threat as the DBT. In the next step in the methodology, we will develop diversion scenarios. We will limit our diversion scenarios to those involving the managerial staff, but will develop scenarios for both targets since the risk associated with both targets exceeded our risk tolerance criterion.

Scenario Construction and Assessment

In the fourth step of the methodology, detailed scenarios are constructed and assessed. These scenarios characterize the conditions under which threats can acquire targets based on the objectives established of monitoring system design for the problem of interest. For diversion, the scenarios capture the ways that the targets can be removed from the facility along the various pathways (arcs and nodes) of the Network Graph.

Activity

The design engineer will perform one activity in the Scenario Construction and Assessment study:

- Develop significant scenarios

A description of this activity follows, with inputs and output highlighted.

Develop Significant Scenarios

Inputs Design Basis Threat (DBT), Risk Table, Pathways List, Network Graph

Output Significant Scenarios (as Text Descriptions and/or as Event Trees or Fault Trees)

Description

Beginning with the DBT-target combinations with a risk above the risk tolerance criterion identified in the Threat Assessment, the design engineer constructs an extensive set of scenarios by which the DBT can acquire the target(s) in question. The scenarios can be specified as text descriptions, and/or as event trees or fault trees. Event trees present the sequence of occurrences, whereas fault trees depict the chain of component failures. In developing the scenarios, the design engineer can use the Pathways List in conjunction with the Network Graph to follow the pathways to or from the target(s). The knowledge, skills and access to the facility of the DBT should be considered during the scenario-development activity.

When performing this activity, the design engineer can choose to develop scenarios for all of the pathways defined on the Pathways List or just some of the pathways from this list. The number of scenarios developed could be greater than or less than the number of pathways on the Pathways List.

After constructing the set of scenarios, the design engineer should assess the likelihood of occurrence and select those deemed most credible. The pruned set of scenarios is the output of this activity and referred to henceforth as *significant scenarios.*

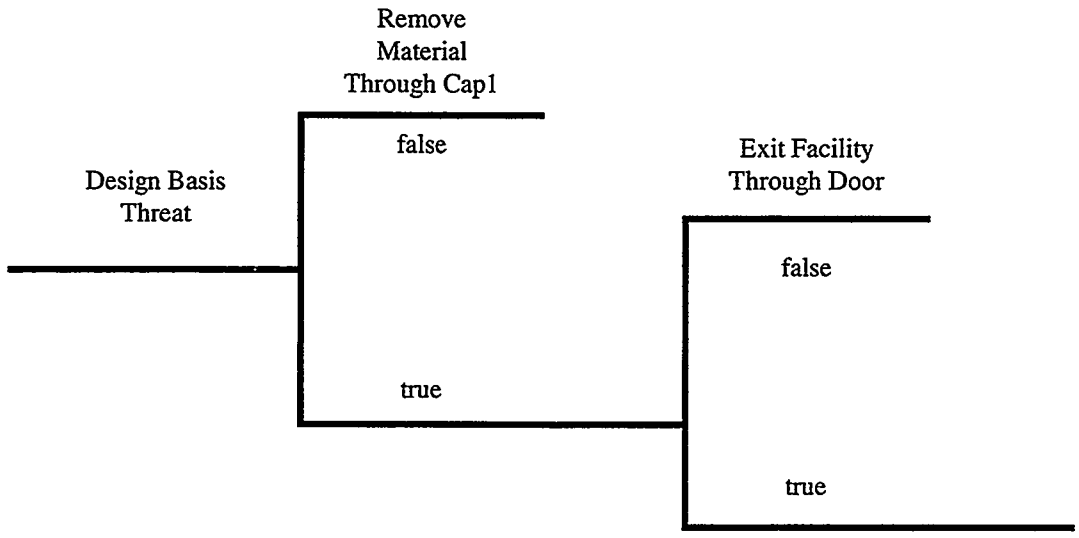
Figure 5 illustrates an event tree and a fault tree prepared for one sample diversion scenario (i.e., Cap 1 - Door, which is the first pathway on the Pathways List for our sample storage facility). The initial text description prepared for this scenario is as follows:

> The DBT takes off the cap from canister 1, removes the material, and exits the facility through the door. (This scenario assumes that the DBT has access at any time to the facility.)

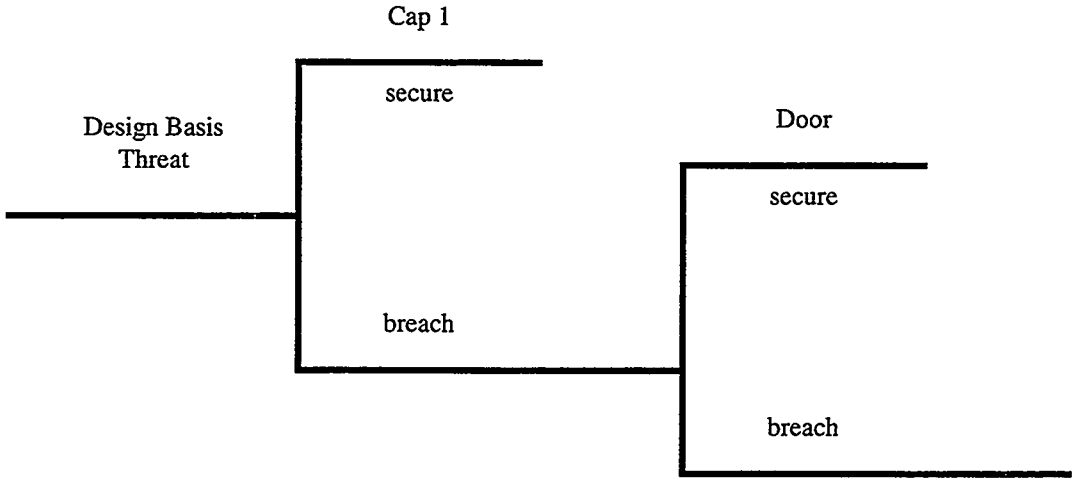
Note that for the sample storage facility in this report, we constructed one scenario for each of 28 pathways. To be conservative in our analysis, we assessed that all pathways provided a credible means of diversion and thus our output from this activity consisted of 28 significant scenarios.

There may be some question as to why we include scenarios in which a wall, ceiling, or floor has to be breached when our threat is on staff at the facility in question and would most likely go through the door. In the absence of a monitoring system, the door is clearly the most likely route for removing material and hence, one of the most obvious monitoring locations. However, focusing a monitoring system on just the most likely scenarios leaves it vulnerable to less likely, but still feasible, scenarios. We maintain the other scenarios to ensure that they are addressed by the design.

Our diversion scenarios begin with the threat already at the target and follow the threat as he removes the material from the facility. We did this for two reasons. First, we wished to focus on the diversion-detection aspects of our sample problem as opposed to the intrusion-detection (and hence physical security like) aspects of the problem. Thus, we focused the scenarios on the removal of the material. Secondly, the threat in our case is an insider and may be attempting the diversion as part of a normal access to the material. Thus, it was not clear to us where the threat should be located for the scenario development. As a result, none of our diversion scenarios considers the effort of approaching the material distinctly from the effort of removing the material. There is thus an implicit assumption that the threat uses the same path to arrive at the material and to exit with it.



Event Tree



Fault Tree

Figure 5. Event and Fault Trees Constructed for Sample Diversion Scenario.

Design Analysis

The fifth step in the methodology is Design Analysis. During this analysis, the critical items to monitor are identified and briefly characterized.

Activity

The design engineer will perform one activity in the Design Analysis study:

- Define initial monitoring system characteristics

A description of this activity follows, with inputs and output highlighted.

Define Initial Monitoring-System Characteristics

Inputs Significant Scenarios and, if applicable, any of the following: List of Important Nodes, Pathways List, Network Graph

Output Items-to-Monitor List

Description

Using the significant scenarios developed in the previous study and, if desired, other inputs that capture key elements or pathways in the facility, the design engineer first prepares a list of items to monitor for the new unattended monitoring system. These items generally are facility elements found in more than one of the scenarios (e.g., wall, target, door). In addition, important nodes identified during the Vulnerability Assessment study should also be included as items in the list.

Once the items have been identified, the design engineer characterizes each of the items. This characterization consists of two parts:

- Strategic Monitoring Regions – one or more regions where sensors should be placed to observe the item. Note that actual selection and final placement of the sensors occurs in the Conceptual and Physical Design Studies, with optimization occurring during the Performance Assessment study.

- Critical Measurement Parameters – type of data that the sensor(s) in the corresponding regions should collect to ensure that the item is being adequately monitored.

Following characterization of the items, the design engineer can capture all of the information easily in a single table such as that shown in Table 7, which was prepared for the sample storage facility. As can be seen, the items in the Items-To-Monitor column have been organized into three groups (i.e., target, facility, and monitoring system). The Strategic Monitoring Regions column lists all viable sensor locations to allow the design engineer flexibility in siting and implementing the monitoring system. Note that as the

overall design process is iterative in nature, any preliminary situating of sensors in the Design Analysis study is likely subject to modification in later iterations. It is generally preferable to specify the parameters to be measured in a generic way (e.g., mass or radiation). The typical critical-measurement parameters with respect to diversion fall into three major categories of containment, surveillance, and physical characteristics.

Finally, we note that once a monitoring system is implemented, it will also have to be assessed for vulnerability to tampering and spoofing. Potential candidate items to monitor for monitoring systems include sensors, transmission lines, data logger, and data storage and processing equipment. Critical measurement parameters for these monitoring system elements include data authenticity and tampering.

Table 7. Items-To-Monitor List

Items To Monitor	Strategic Monitoring Regions	Critical Measurement Parameters
Targets:		
20% U-235 enriched	142 kg UO_2, Canister 1	mass, radiation, temperature
10% U-235 enriched	142 kg UO_2, Canister 2	mass, radiation, temperature
Facility:		
Canister 1	Cap 1, Case 1	intrusion, motion
Canister 2	Cap 2, Case 2	intrusion, motion
Door	Door, Interior, Exterior	intrusion, motion
Wall (West)	Wall (W), Interior, Exterior	intrusion, motion
Wall (North)	Wall (N), Interior, Exterior	intrusion, motion
Wall (East)	Wall (E), Interior, Exterior	intrusion, motion
Wall (South)	Wall (S), Interior, Exterior	intrusion, motion
Roof	Roof, Interior, Exterior	intrusion, motion
Floor	Floor, Interior, Exterior	intrusion, motion
Monitoring System:		
none	--	--

Additional Considerations. As determined for the sample storage facility during the Threat Assessment study, the most likely adversary in a diversion scenario is an insider at the facility. This insider could surreptitiously remove a sizeable quantity of materials at one time or extract smaller less detectable amounts over an extended period. While specifying a knowledgeable, well-equipped insider having full support of the host country as the Design Basis Threat (DBT) is a logical choice, designing a system to defeat this threat may, in practice, be an unattainable goal. Alternately, the design engineer may consider how to best combine barriers, sensors, and procedures into the monitoring-system design in a cost-effective manner irrespective of the DBT. Further, during the Design Analysis study, it is important to also consider the impacts of implementing the monitoring system and ensuring compatibility with the operational, safety, and economic constraints of the facility. For the problem of diversion of nuclear materials, failure to address such considerations could result in the host country's rejection of the monitoring system as prohibitively intrusive upon operations or costly in terms of implementation and maintenance.

Conceptual Design

During this sixth step in the methodology, the conceptual design for the new unattended monitoring system is developed. The conceptual design describes the types of sensors to be used and their general location in the facility. This study includes activities for visually and mathematically representing the new system design.

Activities

The design engineer will perform the following activities in the Conceptual Design study:

- Assign sensors to arcs and nodes

Descriptions of these activities follow, with inputs and outputs for each activity highlighted.

Assign Sensors to Nodes and Arcs

Inputs Network Graph, Items-To-Monitor List, Facility Diagram

Outputs Network Graph (Updated), Facility Diagram (Updated), Items-To-Monitor List (Updated)

Description

During the Design Analysis, the design engineer identified the strategic regions on arcs and nodes where the sensors for the new monitoring system are to be located. Now, the design engineer annotates the arcs and nodes of the Network Graph to denote one or more types of sensor at each listed strategic monitoring region. This annotation process can be enhanced by also specifying any additional attributes that might be useful for future preparation of hardware specifications.

After the Network Graph has been annotated, the design engineer needs to identify the data acquisition or archival equipment that will connect the individual sensor elements into a unified system. These components can then be specified on the Items-To-Monitor List under the Monitoring System category. Next, the design engineer can update the original Facility Diagram (created in the Facility Analysis study) or create another Facility Diagram to visually represent the sensors and related computer-system components that will be a part of the new monitoring system.

For the sample storage facility, Figure 6 shows the Network Graph updated with the sensors and corresponding attributes. The sensor-related data is italicized. We placed a magnetic switch on the door and vibration sensors on the walls, roof, and ceiling to detect possible accesses to the facility. The probability of detection values used for the magnetic

switch and vibration sensors assumed an adversary with power tools [25]. We put an electronic scale under each canister to detect any disturbance of the canisters, particularly removal of the material. Finally, we selected two video cameras to observe access to the canisters as well as the data acquisition equipment for the monitoring system. The cameras are also used to observe tampering with each other. We used a conservative estimate of the accuracy of the scale (0.1 kg) and guessed a probability of detection of 0.99 for it.

Figure 7 presents a visual representation of the new unattended monitoring system for the sample storage facility.

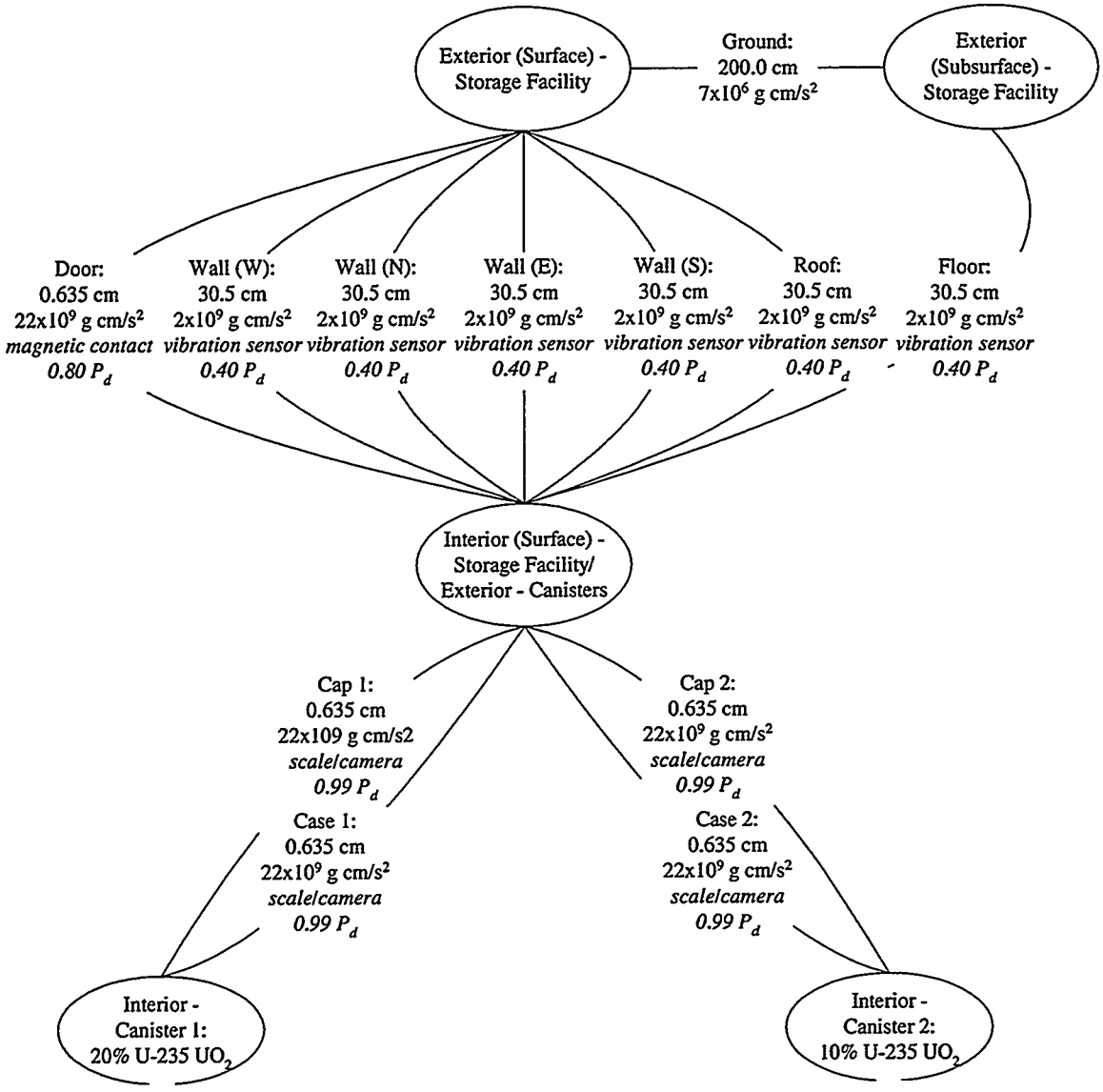


Figure 6. Network Graph of the Sample Storage Facility Updated with Sensor Data.

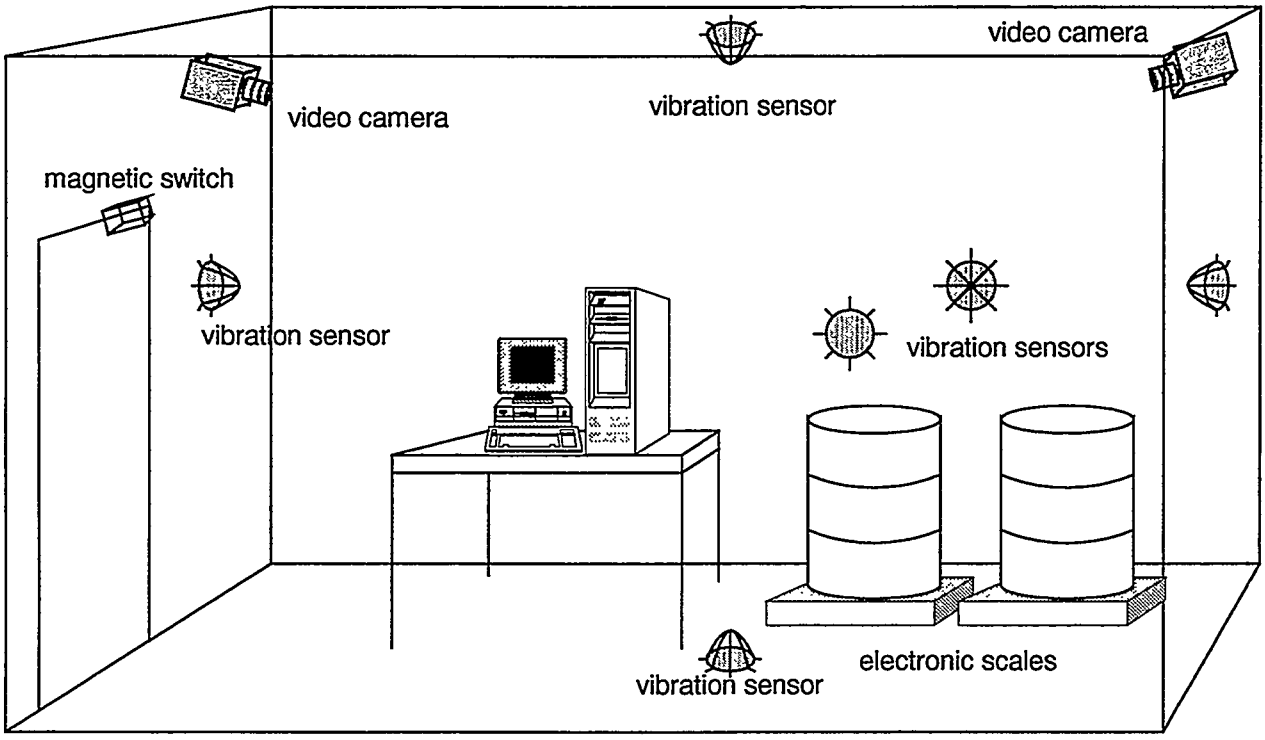


Figure 7. Facility Diagram Illustrating the Conceptual Design of the Unattended Monitoring System for the Sample Storage Facility.

Performance Assessment

The purpose of this step is to assess the performance of the proposed design and modify the design as needed to achieve the desired performance. Estimates of system performance are calculated and assessed relative to the pre-established evaluation criteria. Should the system be found deficient, an optimization analysis is performed to enhance the overall level of system performance. It should be noted that the measures by which we have chosen to evaluate system performance could differ in other applications. Consequently, certain parts of the study may have to be altered by the design engineer.

Activities

The design engineer will perform the following activities in the Performance Assessment study:

- Calculate performance estimates
- Assess system performance
- Perform optimization analysis

Descriptions of these activities follow, with inputs and outputs for each activity highlighted.

Calculate Performance Estimates

Inputs Network Graph

Output Performance Estimates Table

Description

This activity involves the calculation of numerical performance estimates for the set of pathways. The algorithm for computing an overall performance estimate depends on the performance metric chosen. In our case we chose risk of undetected diversion as the performance metric. We compute the risk for each pathway and set the overall system performance equal to the risk value associated with the pathway having the highest risk.

In a more complicated monitoring scenario, the number of paths may be quite large. In the work described in this report, we did not consider how to systematically reduce the number of pathways needed to compute the overall performance. However, we believe it is feasible for the design engineer to do so by examining how the overall performance metric depends on the contributing factors in his model.

In order to calculate the performance estimates, the design engineer creates a new table to store the results of the activity (see Table 8 for layout of rows and columns). The rows are the pathways and the columns are the factors that contribute to the performance metric, as well as the performance metric itself.

Next, the design engineer fills in the columns. For the example worked in this paper, the values in the Pathway ID column are the paths developed in the Vulnerability Analysis. For each path, we computed the work to forcibly breach all of the barriers along the path. The total work was the sum of the work on each element of the path, computed from the product of material thickness and material yield strength. The calculation of the overall P_d for each pathway was done two ways, depending on the path. For pathways involving the door, we used the probability of detection at the canister cap or case as the probability of detection for the entire path. This is because the material is normally accessed through the door and so a detection involving the door sensor alone is not sufficient to detect a diversion. For pathways not involving the door, we determined that we only needed detection by a single sensor in order to detect something suspicious occurred. Therefore, the probability of detection is given by 1 minus the probability of failure to detect, where the probability of failure to detect is the product of the failure to detect on each element of the pathway. For example, for Pathway 5 (Cap 1 – Wall (W)), the probability of detection is given by:

$$P_d = 1-(1-0.99)(1-0.40) = 0.994$$

Finally, the design engineer computes the risk of undetected diversion function for each pathway. As stated earlier, we did not develop a quantitative model for computing risk of undetected diversion but instead asserted that it was possible to do so. Therefore, in our Performance Estimates Table, we simply asserted values for the Risk of Undetected Diversion, assuming that the risk was highest for paths associated with lower probability of detection and less work.

Table 8 presents the results of the performance estimates calculated for diversion pathways of the sample storage facility.

Assess System Performance

Inputs Performance Estimates Table

Output None

Description

The design engineer should review the performance estimates for each pathway calculated in the previous activity to determine whether the system achieves the desired performance level according to the previously established evaluation criteria. For example, the desired performance level is achieved for the detection of diversion in our sample storage facility when the risk of undetected diversion for all diversion pathways is less than 0.1 SQ/yr (our single evaluation criterion). The risk of undetected diversion values in Table 8 are less than the predefined evaluation criteria, and so the conceptual system design is complete. The design engineer should subsequently refer to the section entitled "Related Analyses" at the end of this study.

Table 8. Performance Estimates Table for Sample Storage Facility

Pathway Identifier	Work (ergs)	Probability of Detection (P_d)	Risk of Undetected Diversion (SQ/yr.)
1. Cap 1 - Door	2.794E+10	0.99	2.0E-2
2. Case 1 - Door	2.794E+10	0.99	2.0E-2
3. Cap 2 – Door	2.794E+10	0.99	2.0E-2
4. Case 2 - Door	2.794E+10	0.99	2.0E-3
5. Cap 1 - Wall (W)	7.497E+10	0.994	1.0E-2
6. Case 1 - Wall (W)	7.497E+10	0.994	1.0E-2
7. Cap 2 - Wall (W)	7.497E+10	0.994	1.0E-2
8. Case 2 - Wall (W)	7.497E+10	0.994	1.0E-2
9. Cap 1 - Wall (N)	7.497E+10	0.994	1.0E-2
10. Case 1 - Wall (N)	7.497E+10	0.994	1.0E-2
11. Cap 2 - Wall (N)	7.497E+10	0.994	1.0E-2
12. Case 2 - Wall (N)	7.497E+10	0.994	1.0E-2
13. Cap 1 - Wall (E)	7.497E+10	0.994	1.0E-2
14. Case 1 - Wall (E)	7.497E+10	0.994	1.0E-2
15. Cap 2 - Wall (E)	7.497E+10	0.994	1.0E-2
16. Case 2 - Wall (E)	7.497E+10	0.994	1.0E-2
17. Cap 1 - Wall (S)	7.497E+10	0.994	1.0E-2
18. Case 1 - Wall (S)	7.497E+10	0.994	1.0E-2
19. Cap 2 - Wall (S)	7.497E+10	0.994	1.0E-2
20. Case 2 - Wall (S)	7.497E+10	0.994	1.0E-2
21. Cap 1 - Roof	7.497E+10	0.994	1.0E-2
22. Case 1 - Roof	7.497E+10	0.994	1.0E-2
23. Cap 2 - Roof	7.497E+10	0.994	1.0E-2
24. Case 2 - Roof	7.497E+10	0.994	1.0E-2
25. Cap 1 - Floor - Ground	7.637E+10	0.994	8.0E-3
26. Case 2 - Floor - Ground	7.637E+10	0.994	8.0E-3
27. Cap 2 - Floor - Ground	7.637E+10	0.994	8.0E-3
28. Case 2 - Floor - Ground	7.637E+10	0.994	8.0E-3

If, however, the risk of undetected diversion values had been larger than the predefined evaluation criteria, the system would have required optimization to bring the risk of undetected diversion values for all pathways down to the predefined performance level. The optimization process is explained below.

(if applicable) Perform Optimization Analysis

Inputs Based on Activity Part (See below)

Outputs Based on Activity Part (See below)

Description

The optimization-analysis activity involves redesigning or upgrading the current physical design of the system to overcome noted vulnerabilities by implementing countermeasures.

Using the Performance Estimates Table prepared in the previous activity, the design engineer needs to determine the most vulnerable pathway(s) of the network. The most vulnerable pathways are those pathways that fail to satisfy the performance criteria by the largest amount.

Next, the design engineer specifies precise ways by which the current system design can be modified to raise the overall performance level, focusing on the most vulnerable pathway(s). The enhancements that the engineer chooses depend on the performance criteria and any constraints imposed on the user by the customer or other impacted parties. In our example, the design engineer's customer is the monitoring agency. In such a situation, the design engineer will probably not be able to change the physical design of the facility but can modify his sensor selection, either by changing the chosen sensors or by adding new sensors, to improve the probability of detection.

Once the engineer has chosen specific performance enhancements, he updates the Network Graph to reflect the changes. He then needs to update the values for key factors, such as work and probability of detection, for each of the affected pathways. Finally, the engineer updates the performance measures (i.e., risk of undetected diversion in our problem) for each affected pathway.

Once the performance measures have been updated, the design engineer should assess whether the new values satisfy the evaluation criteria established for the monitoring system. If the results are satisfactory, no further design changes are required. However, if the performance measures do not meet the evaluation criteria, the design engineer should iterate on this optimization process.

Achievement of the previously established evaluation criteria for overall system performance marks completion of the system design. However, the design should be continuously reviewed and reanalyzed to maintain or increase system performance in response to component degradation and aging, modifications or upgrades to the facility or

monitoring system, and ever-increasing threats. As necessary, the design engineer may want to subject the new design to the rigors of the entire methodology once again, beginning at the Facility Analysis or some further study along the way.

Related Analyses

In addition to the calculation of numerical performance estimates, several other related analyses may also be conducted during the Performance Assessment study. A cost/benefit study can be used to examine the incremental system performance gained following the addition of each performance-enhancement measure. A normalized, relative financial outlay is assigned for implementation of each measure, and the overall system improvement or benefit is plotted versus the expenditure. The procedure permits trade-off studies to be performed, allowing assessment of alternate approaches or a series of related measures to achieve the same overall system performance. For example, it may be more cost effective to post several security guards rather than install video equipment to survey a large perimeter enclosure given that the same number of personnel would be required to observe the television monitors.

The design engineer can also use sensitivity analysis to determine critical parameters and uncertainty analysis to define error bounds surrounding the system performance estimates. In calculating the system performance measure of work for the sample storage facility, for example, material yield strength was a significantly more important material characteristic than material thickness, and was therefore a more critical parameter. However, materials characteristics including yield strength are derived experimentally and cited over a range of acceptable values, and uncertainty analysis may be performed to establish the appropriate ranges and associated error bounds of both physical data and derived results.

Conclusions

We presented a high-level methodology for the design of unattended monitoring systems, focusing on a system to detect diversion of nuclear materials from a storage facility. The methodology is composed of seven, interrelated analyses: Facility Analysis, Vulnerability Analysis, Threat Assessment, Scenario Assessment, Design Analysis, Conceptual Design, and Performance Assessment. The design of the monitoring system is iteratively improved until it meets a set of pre-established performance criteria.

The methodology presented here is based on other, well-established system analysis methodologies and hence we believe it can be adapted to other verification or compliance applications. In order to make this approach more generic, however, there needs to be more work on techniques for establishing evaluation criteria and associated performance metrics. We found that defining general-purpose evaluation criteria for verifying compliance with international agreements was a significant undertaking in itself. We finally focused on diversion of nuclear material in order to simplify the problem so that we could work out an overall approach for the design methodology. However, general guidelines for the development of evaluation criteria are critical for a general-purpose methodology. A poor choice in evaluation criteria could result in a monitoring system design that solves the wrong problem.

A second topic that needs further investigation is how to balance competing constraints. In reality, the design engineer has to balance constraints, such as cost and intrusiveness, imposed by either the monitoring agency or the host. While we noted points in the methodology where the constraints would affect design choices, we did not investigate general approaches to multiple constraint satisfaction.

A third area to be investigated is the development of guidelines for modeling facilities and monitoring systems with network graphs. We chose to look at a particularly simple example in order to illustrate the major steps of the methodology. However, real monitoring problems may involve more complex facilities and the monitoring of ongoing activities and processes. It is important to develop detailed guidelines for: the development of network-graph based facility models, the level of fidelity required in the facility models, the best approach for modeling the combination of the facility and the monitoring system, and approaches for modeling the monitoring of processes.

While many details of the methodology implementation still need to be worked out, the use of a structured framework such as that presented here offers significant benefits over current practice. In particular, this methodology assists the design engineer in systematically considering the requirements for any proposed monitoring system and helps him assess how well the proposed monitoring system satisfies those requirements. A design methodology also helps the design engineer capture any assumptions made in the analysis and design process and analyze their impact on overall performance. The

methodology presented in this report is a first step in developing such a systematic approach to the design of unattended monitoring systems.

References

1. United Nations, "Treaty on the Non-Proliferation of Nuclear Weapons" (1968). United Nations Treaty Series, Registration No. 10485, Vol. 729, United Nations, New York, March 05, 1970, pp. 169–175. See Article III. Also available at http://www.iaea.org/worldatom/Documents/legal/npttext.html

2. International Atomic Energy Agency, "Assurance of Non-Diversion of Nuclear Material," in *Against the Spread of Nuclear Weapons: IAEA Safeguards in the 1990s*, 93-04459, IAEA/PI/A38E, International Atomic Energy Agency, Vienna, December 1993. Also avilable at: http://ww.iaea.org/worldatom/inforesource/other/safeguards/pia3809.html

3. International Atomic Energy Agency, *IAEA Safeguards: An Introduction*, IAEA/SG/INF/3, IAEA, Vienna (1981) p. 20.

4. Chapman, L. D., Engi, D., and Grant, H., *Safeguards Network Analysis Procedures (SNAP)*, NUREG/CR-0725, US Nuclear Regulatory Commission, Washington, DC, January 1977.

5. Bennett, H. A., and Olascoaga, M. T., *Design Guidance and Evaluation Methodology for Fixed-Site Physical Protection Systems*, Volumes I and II, NUREG/CR-1198, US Nuclear Regulatory Commission, Washington, DC, March 1980.

6. Bennett, H. A., and Olascoaga, M. T., *An Evaluation Methodology Based On Physical Security Assessment Results – A Utility Theory Approach*, SAND78-0377, Sandia National Laboratories, Albuquerque, NM, March 1978.

7. Chapman, L. D., *Applications of Graph Theory Methods to Safeguards Problems*, SAND80-0835A, Sandia National Laboratories, Albuquerque, NM, March 1980.

8. Paulus, W. K., *Generic Physical Protection Logic Trees*, SAND79-1382, Sandia National Laboratories, Albuquerque, NM, April 1980.

9. Chapman, L. D. and Olascoaga, M. T., *Systematic Analysis Of A Physical Protection System*, SAND81-0446C, Sandia National Laboratories, Albuquerque, NM, June, 1981.

10. Chapman, L. D., *Characterisitcs Of Safeguards Models*, SAND81-2207A, Sandia National Laboratories, Albuquerque, NM, October 1981.

11. Williams, J. D., *Physical Protection System Design and Evaluation*, SAND97-0624A, Sandia National Laboratories, Albuquerque, NM, February 1997.

12. Basil Steele, private communication, October 1998. Excerpts provided from *The Physical Protection System Design Methodology Training Course,* The Fourteenth International Training Course, Sandia National Laboratories, Albuquerque, NM.

13. Hickman, J. W. et al., *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, NUREG/CR-2300 Volumes 1 and 2, US Nuclear Regulatory Commission, Washington, DC, January 1983.

14. Greenberg, H. R. and Cramer, J. J., eds., *Risk Assessment and Risk Managemennt for the Chemical Process Industry*, Van Nostrand Reinhold, New York, 1991.

15. McCormick, J. J., *Reliability and Risk Analysis: Methods and Nuclear Power Applications*, Academic Press, New York, 1981.

16. Roberts, N.H., Vesely, W.E., Haasl, D.F. and Goldberg, F.F., *Fault Tree Handbook*, NUREG-0492, US Nuclear Regulatory Commission, Washington, DC, 1981.

17. Varnado, G.B., Horton, W.H. and Lobner, P.R., *Modular Fault Tree Analysis Procedures Guide*, NUREG/CR-3268, Volumes 1 through 4, US Nuclear Regulatory Commission, Washington, DC, 1983.

18. Cramond, W. R. et al., *Probabilistic Risk Assessment Course Documentation*, NUREG/CR-4350, Volumes 1 through 7, US Nuclear Regulatory Commission,Washington, DC, 1985.

19. Jae, M. and Apostolakis, G. E., "The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies," *Nuclear Technology* **99**, pp142-157 (August 1992).

20. Ganter, J. H. and Smith, J. D., "MPATHav: A Software Package for Multiobjective Routing in Transportation Risk Assessment," Proceedings of the 11th International Conference on the Packaging and Transportation of Radioactive Materials (PATRAM '95), Volume I, Las Vegas, NV, December 3-8, 1995.

21. Wyss, G. D., Craft, R. L., Vandewart, R. L. and Funkhouser, D. R., *Recasting Risk Analysis Methods in Terms of Object-Oriented Modeling Techniques*, SAND98-1752C, Sandia National Laboratories, Albuquerque, NM, July 1998.

22. International Atomic Energy Agency, *Risk Analysis for the Protection of the Public in Radiation Accident*, IAEA Safety Series 21, STI/PUB/124, Vienna, Austria, 1967.

23. International Atomic Energy Agency, *IAEA Safeguards: Glossary, 1987 Edition*, IAEA/SG/INF/1 (Rev. 1), International Atomic Energy Agency, Vienna, 1987. P. 23.

24. Muvdi, B. B. and McNabb, J. W., *Engineering Mechanics of Materials*, Macmillan Publishing Ltd, London, England, 1981.

25. Ivan Waddoups, private communication, March 2000.

Distribution

1	MS	0425	A. C. Payne, Jr., 9815
1	MS	0977	W. R. Cook, 6524
1	MS	0977	J. M. Brabson, 6524
2	MS	0977	S. M. DeLand, 6524
3	MS	0977	J. D. Smith, 6524
1	MS	1140	J. K. Rice, 6500
1	MS	1213	D. E. Ellis, 5300
1	MS	1215	N. S. Andrews, 5313
1	MS	1215	W. E. Chambers, 5313
1	MS	1361	J. C. Matter, 5323
1	MS	1361	R. L. Martinez, 5323
1	MS	1363	L. S. Walker, 5335
1	MS	1371	D. D. Drayer, 5322
1	MS	1371	G. T. Baldwin, 5324
1	MS	1371	C. D. Harmon, 5391
1	MS	9201	M. Abrams, 8114
1	MS	9201	W. L. Hsu, 8112
1	MS	0188	D. L. Chavez, 4001, LDRD Office
1	MS	9018	Central Technical Files, 8940-2
2	MS	0899	Technical Library, 4916
1	MS	0614	Review & Approval Desk, 4912 For DOE/OSTI

This page intentionally blank.