CONF-9509220--2

SAND95-2012C

Process of System Design and Analysis

Byron Gardner
Nuclear Security Systems Center
Sandia National Laboratories
Albuquerque, NM 87185, USA

Abstract. The design of an effective physical protection system includes the determination of the physical protection system objectives, the initial design of a physical protection system, the evaluation of the design, and, probably, a redesign or refinement of the system. To develop the objectives, the designer must begin by gathering information about facility operations and conditions, such as a comprehensive description of the facility, operating states, and the physical protection requirements. The designer then needs to define the threat. This involves considering factors about potential adversaries: class of adversary, adversary's capabilities, and range of adversary's tactics. Next, the designer should identify targets. Determination of whether or not nuclear materials are attractive targets is based mainly on the ease or difficulty of acquisition and desirability of the material. The designer now knows the objectives of the physical protection system, that is, "what to protect against whom." The next step is to design the system by determining how best to combine such elements as fences, vaults, sensors, procedures, communication devices, and protective force personnel to meet the objectives of the system. Once a physical protection system is designed, it must be analyzed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to assure protection rather than regarding each feature separately. Due to the complexity of protection systems, an evaluation usually requires modeling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a reevaluation conducted.

Introduction

The design of an effective physical protection system (PPS) requires a methodical approach in which the designer weighs the objectives of the PPS against available resources, and then evaluates the proposed design. Without this kind of careful assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. For example, it would probably be unwise to protect a facility's employee cafeteria with the same level of protection as the facility's fuel storage area. However, maximum security at a facility's main entrance would be wasted if entry were also possible through an unguarded cafeteria loading dock.

The process of designing and analyzing a PPS is described in the remainder of this session.

Determine Physical Protection System Objectives

The first step in the development of a PPS design is to determine the objectives of the protection system. To formulate these objectives, the designer must (1) characterize (understand) the facility operations and conditions, (2) define the threat, and (3) identify the targets.

Facility operations and conditions characterization requires developing a thorough description of the facility itself (the location of the site boundary, building location, building interior floor plans, and access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features.

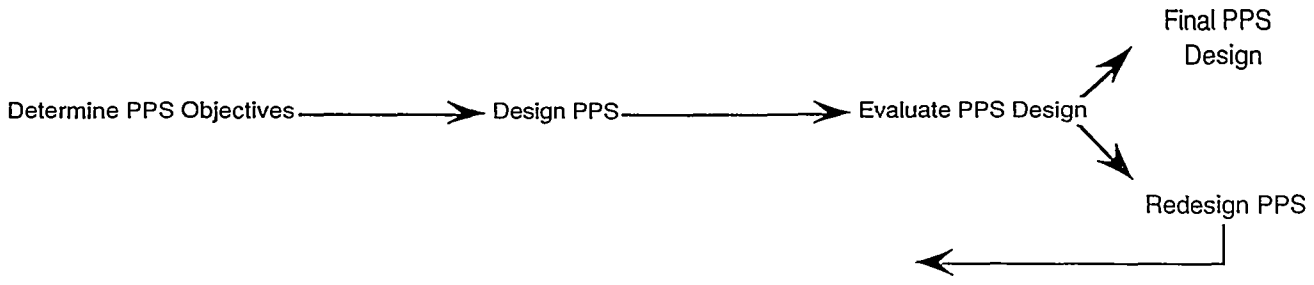


Figure 1. Design and Analysis Cycle

Next, a threat definition for the facility must be made. Information must be collected to answer three questions about the adversary:

(1) What class of adversary is to be considered?

(2) What is the range of the adversary's tactics?

(3) What are the adversary's capabilities?

Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is the attempt to defeat the detection system and enter the facility covertly.

Important capabilities for the adversary include his knowledge of the PPS, his level of motivation, any skills that would be useful in the attack, the speed with which the attack is carried out, and his ability to carry tools and weapons. Since it is not generally possible to test and evaluate all possible capabilities of an unknown adversary, the designer and analyst must make assumptions. These assumptions can be based on published information about human performance and the tested vulnerabilities of physical protection elements.

Finally, target identification should be performed for the facility. In most nuclear facilities, nuclear materials appear in several different physical and chemical forms. The attractiveness of these materials as theft or sabotage targets depends greatly on their form, since the form of the material determines its ease of acquisition by the potential thief, as well as the ease of subsequent malevolent use. In light water reactors, for example, nuclear material appears in four forms: fuel assemblies, solid wastes, liquid wastes, and gaseous wastes. These materials rank differently in terms of their attractiveness to a potential saboteur or thief.

In a nuclear reactor, the greatest concern in the design of a PPS is to prevent radioactive release from the reactor that may be caused by sabotage. Vital areas (those areas within a reactor complex that contain equipment, systems, devices, or material whose failure, destruction, or misuse could result in a radiological release endangering the public) are of particular concern. For example, the containment building that houses the reactor, the steam generators, and the primary coolant loops will always be designated a vital area. Many other locations containing machinery and safety systems designed to decrease the severity of accidental damage to nuclear facilities may also require designation as vital areas. As severity of damage decreases, we reach the point of "acceptable risk" below which we are willing to endure damage because additional protection is not worth the cost.

Given the information obtained through facility characterization, threat definition, and target identification, the designer can determine the protection objectives of the PPS. An example of a protection objective might be to "interrupt a well-equipped, criminal adversary before he can remove nuclear material from a vault."

Design a Physical Protection System

The next step in the process is to determine how best to combine such elements as fences, vaults, sensors, procedures, communication devices, and protective force personnel into a PPS that can achieve the protection objectives. The resulting PPS design should meet these objectives within the operational, safety, and economic constraints of the facility. The primary functions of a PPS are detection of an adversary, delay of that adversary, and response by the security inspectors (guard force).

Certain general guidelines should be observed during the PPS design. A PPS system is generally better if detection is as far from the target as possible, and delays are near the target. In addition, there is close association between detection (exterior or interior) and assessment. The designer should be aware that "detection without assessment is not detection." Another close association is the relationship between response and response force communications. A response force cannot respond unless it receives a secure communication call for a response.

These and many other particular features of PPS components help to ensure that the designer takes advantage of the strengths of each piece of equipment and uses equipment in combinations that complement each other and protect any weaknesses.

Evaluate the Physical Protection System Design

Analysis and evaluation of the PPS design begins with a review and thorough understanding of the protection objectives the designed system must meet. This can be done simply by checking for required features of a PPS, such as intrusion detection, entry control, access delay, response communications, and a protective force. However, a PPS design based on required features cannot be expected to lead to a high performance system unless those features, when

used together, are sufficient to assure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a PPS.

An existing PPS at an operational facility cannot normally be fully tested as a system. The nature of the protected nuclear facilities and materials prevents tests involving simulated adversary teams that penetrate barriers or steal nuclear material and protective forces that carry out the response functions. Since direct system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates by the application of system modeling techniques.

The end result of this phase of the design and analysis process is a system vulnerability assessment. Analysis of the PPS design will either find that the design effectively achieved the protection objectives or it will identify weaknesses. If the protection objectives are achieved, then the design and analysis process is completed. However, the PPS should be analyzed periodically to ensure that the original protection objectives remain valid and that the protection system continues to meet them.

Redesign of the Physical Protection System

As mentioned above, the result of the analysis phase is a system vulnerability assessment. If the PPS is found ineffective, vulnerabilities in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial protection system design to correct the noted vulnerabilities. It is possible that the PPS objectives also need to be reevaluated. An analysis of the redesigned system is performed. This cycle continues until the results indicate that the PPS meets the protection objectives.

Specifics of U.S. DOE Physical Protection System (PPS) Design

Requirements contained in DOE Orders are used as a baseline for DOE PPS design. The key orders used are the 5630 Series "Safeguards and Security" and 6430.1A "General Design Criteria." These orders are accessed by using the

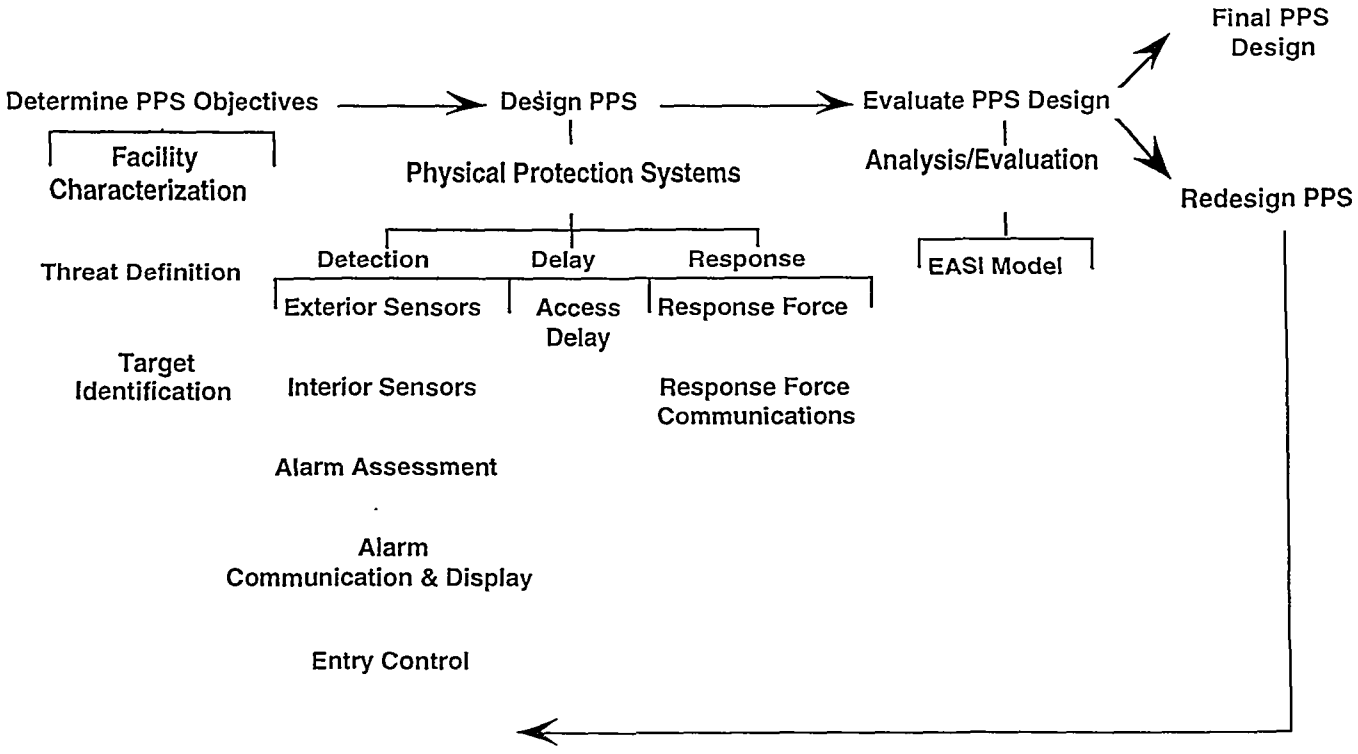


Figure 2. Design and Evaluation Process Outline (DEPO)

World Wide Web (Internet) U.S. Department of Energy, home page, DOE Orders, file name, VM1.HQADMIN.DOE.GOV:70/11/doemenu1. These orders provide a solid framework for designing and implementing safeguards and security systems that will be highly effective in defending nuclear materials against a broad range of threats. Effective protection against both insider and outsider adversaries is achievable if PPS systems are designed in accordance with these orders.

The exact characteristics of the DOE Design Basis Threat Policy (DBTP) are classified. However, the DBTP covers terrorists, criminals, ant-nuclear extremists, disgruntled employees, and psychotics. Careful attention is given to key adversary attributes when designing a PPS. The key elements that significantly affect safeguards and security system performance are numbers of adversaries, motivations, types of weaponry and explosives, willingness to use violence, and technical sophistication. The DOE DBTP covers these elements in great detail. The US uses the DBTP as the cornerstone for designing and evaluating the performance of safeguards and security systems.

A good example of an unclassified threat policy can be found in the U.S. Code of Federal Regulations, Title 10, Part 73, Subsection 73.1. This section describes the design basis threat assumed for U.S. power reactors under the control of the U.S. Nuclear Regulatory Commission. This threat policy has all of the important attributes necessary for a sound physical protection system design.

The U.S. DOE DBTP is sometimes modified to incorporate concerns over regional or international groups that are identified during threat assessments. Periodically a group is identified that might target U.S. nuclear facilities. In these cases the DBTP is amended to reflect the increased concern over terrorist attributes of a particular group. However, the design basis threat policy is never diminished as a result of these assessments.

Target identification for DOE special nuclear materials against theft is done by utilizing the "Graded Safeguards Table" found in DOE Order 5633.3C. See Attachment A. This table is used to prioritize the importance of nuclear materials in the DOE inventory. Highly sophisticated physical protection and safeguards systems are used to secure materials identified as Category I or Category II. Less stringent protection systems safeguard Category III and Category IV materials. The consequence values for theft of these materials, used in risk evaluations, are listed in consequence tables found in the DOE "Site Safeguards and Planning Guide." See Attachment B. Note the U.S. DOE Graded Safeguards Table is somewhat different from the IAEA INFCIRC/225/Rev.3 "Categorization of Nuclear Material Against Theft or Diversion." See Attachment C. However, DOE requirements for protection of Category I and II nuclear materials are much more stringent than those called for in INFCIRC/225/Rev. 3.

Another target identification activity that DOE facilities must accomplish is the identification of radiological sabotage targets. These are targets, that if dispersed into the environment, would cause significant detrimental impact to the health and safety of the public and the environment. Typical targets include reactors and various isotopes of plutonium. In order to identify radiological sabotage targets, nuclear materials are examined to determine their susceptibility to dispersion. If a material has high potential for a credible dispersion scenario, the consequences of this dispersion are categorized by using the consequence table found in the DOE Site Safeguards and Security Planning Guide. See Attachment D. Nuclear materials with high consequence values are provided very high levels of protection against sabotage.

A very valuable tool for determining the impact of dispersion of a nuclear material is the HOTSPOT Health Physics Code. This code, developed by Lawrence Livermore National Laboratory (LLNL), is a very valuable screening tool for determining radiological sabotage targets. The code has been authorized for release in the Former Soviet Union. The user's manual has been translated into Russian. The U.S. contact for distribution of this code is Steven Homann, LLNL, phone number 510-423-4962, E-mail address shomann@llnl.gov.

Once a new PPS has been designed or an upgrade has been designed for an existing system, a vulnerability analysis is conducted. This is a systematic way of ensuring the design would meet an acceptable level of performance against adversaries identified in the DBTP. It is important to note that this vulnerability analysis focuses on performance of the PPS and not simply compliance with regulations.

DOE facilities use the ASSESS Code "Analytical System and Software for Evaluating Safeguards and Security" as the primary software and methodology for conducting vulnerability assessment on PPS systems. This code developed jointly by Sandia National Laboratories and Lawrence Livermore National Laboratory, analyzes effectiveness of the PPS against a broad range of insider and outsider threats. This code has been authorized for release in the Russian federation. A number of ASSESS training classes have been presented at Russian Institutes. Please contact Jack Blasy at LLNL, phone number 510-422-3014, E-mail (Jack.Blasy@quickmail.llnl.gov) or Byron Gardner, at SNL, phone number 505-844-5300, E-mail (bhgardn@somnet.sandia.gov), for information concerning these classes.

In addition to the use of the ASSESS code, DOE requires whole system performance tests, limited scope performance tests, and initial data verifications to be conducted prior to acceptance of the final design for a PPS. Performance testing allows for another perspective to be used in evaluating the effectiveness of the PPS. The DOE

methodology for conducting vulnerability assessments is shown in Attachment E.

After a vulnerability assessment has been completed, a risk assessment and cost benefit analysis are conducted. The cost benefit analysis shows which upgrades or designs are most cost effective in reducing the risk to the target. The formulas for DOE conditional risk evaluations are shown in Attachment F. The consequence values used in these formulas are obtained from those discussed in Attachments B and D. The exact quantitative levels of risk that are acceptable to the DOE are classified. However, highly attractive materials must be protected to a level that provides a very low risk rating.

Summary

A recommended process for the design and analysis of a PPS was presented in general terms for international applications. Additionally, a detailed description for how the U.S. Department of Energy designs a PPS was also presented. Contacts for future U.S. and Russian Federation cooperation on PPS design and vulnerability analysis are included in this paper.

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

ATTACHMENT A

U.S. - Categorization of Nuclear Material for Protection Against Theft / Diversion

Material Type	Attractiveness Level	Plutonium / U 233 (Quantities in Kilograms)				Contained U 235 (Quantities in Kilograms)				Other Nuclear Materials
		1	2	3	4	1	2	3	4	4
Weapons	A	All Quantities	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Pure Products	B	≥ 2	≥ 0.4 > 2	≥ 0.2 > 0.4	< 0.2	≥ 5	≥ 1 > 5	≥ 0.4 > 1	< 0.4	N/A
High - Grade Material	C	≥ 6	≥ 2 > 6	≥ 0.4 > 2	< 0.4	≥ 20	≥ 6 > 20	≥ 2 > 6	< 2	N/A
Low - Grade Material	D	N/A	≥ 16	≥ 3 > 16	< 3	N/A	≥ 50	≥ 8 > 50	< 8	N/A
All Other Materials	E	N/A	N/A	N/A	Reportable Quantities	N/A	N/A	N/A	Reportable Quantities	Reportable Quantities

WEAPONS
- Assembled weapons and test devices

PURE PRODUCTS
- Pits, major components, buttons, ingots, recastable, metals
- Directly convertible materials (a)

HIGH GRADE MATERIAL
- Oxides, carbides, etc.
- Solutions, e.g. nitrates (≥ 25 g/l)
- Fuel elements and assemblies,
- Alloys and mixtures
- UF_4 or UF_6 (≥ 50% u-235)

LOW GRADE MATERIAL
- Solutions; (1-25 g/l)
- Process residues requiring extensive reprocessing
- Moderately radioactive materials
- UF_4 or UF_6 (≥ 20% <50% U_{235})
- PU_{238} (except waste)

ALL OTHER MATERIALS
- Highly irradiated forms
- Solutions (≥ 1 g/l), uranium containing < 20% U_{235} (any form or quantity

8/7/95JAL

CONSEQUENCE VALUE TABLE FOR THEFT/DIVERSION OF SPECIAL NUCLEAR MATERIAL

Consequence Value	Nuclear Material Description
1.0	**WEAPONS -** • Assembled weapons and test devices
0.8	**CATEGORY 1 - QUANTITY - PURE PRODUCTS** • Pits, major components, buttons, ingots, recastable, metals • Directly convertible materials (1)
0.7	**CATEGORY 1 - QUANTITY - SIMPLE COMPOUNDS** • Oxides, carbides, etc.
0.6	**CATEGROY 1 QUANTITY - HIGH GRADE MATERIAL** • Solutions, e.g. nitrates ($\geq$ 25 g/l) • Fuel elements and assemblies, alloys and mixtures • UF_4 or UF_6 ($\geq$ 50% u-235)
0.4	**CATEGORY 2 QUANTITY** • Pure Products • High Grade Material • Low Grade Material Solutions; e.g. nitrates (1`-25 g/l) Recyclable materials Process residues Moderately radioactive materials (2) PU_{238} UF_4 or UF_6 ($\geq$ 20% <50% U_{235})
0.2	**CATEGORY 3 QUANTITY** • Pure Products • High Grade Material • Low Grade Material
0.1	**CATEGORY 4 QUANTITY** • Pure Products • High Grade Material • Low Grade Material • All other materials containing SNM Highly radioactive forms (b) Solutions, Uranium containing less than 20% U_{235}

ATTACHMENT C

INFCIRC/225/Rev.3 Categorization of Nuclear Material for Protection Against Theft / Diversion

MATERIAL	FORM	CATEGORY 1	CATEGORY 2	CATEGORY 3[3]
Plutonium [1]	Unirradiated [2]	≥ 2 kg	< 2kg ≥ 500 grams	≤ 500 grams > 15 grams
Uranium - 235	Unirradiated [2] --enriched ≥20% ^{235}U --enriched 10 > 20% ^{235}U --enriched but < 10%	≥ 5 kg	< 5kg ≥ 1 kg ≥ 10 kg	≤ 1 kg > 15 grams < 10 kg ≥ 1 kg ≥ 10 kg
Uranium 233	Unirradiated [2]	> 2 kg	< 2kg ≥ 500 grams	< 500 grams ≥ 15 grams
Irradiated Fuel *			Depleted or natural uranium, thorium or low-enriched fuel (≤ 10% fissile content)[4/5]	

* Based upon international transport considerations. The State may assign a different category for domestic use, storage, and transport taking all relevant factors.

1. All plutonium except that with isotopic concentration exceeding 80% in plutonium-238

2. Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr (100 rads/hr) at one meter unshielded.

3. Quantities not falling in Category 3 and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudence management practice.

4. Although this level of protection is recommended, it would be open States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

5. Other fuel which by virtue of its original fissile material content is classified as Category 1 or 2 before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100 rads/hr) at one meter unshielded.

8/7/95JAL

CONSEQUENCE VALUE TABLE FOR RADIOLOGICAL SABOTAGE OF SPECIAL NUCLEAR MATERIAL

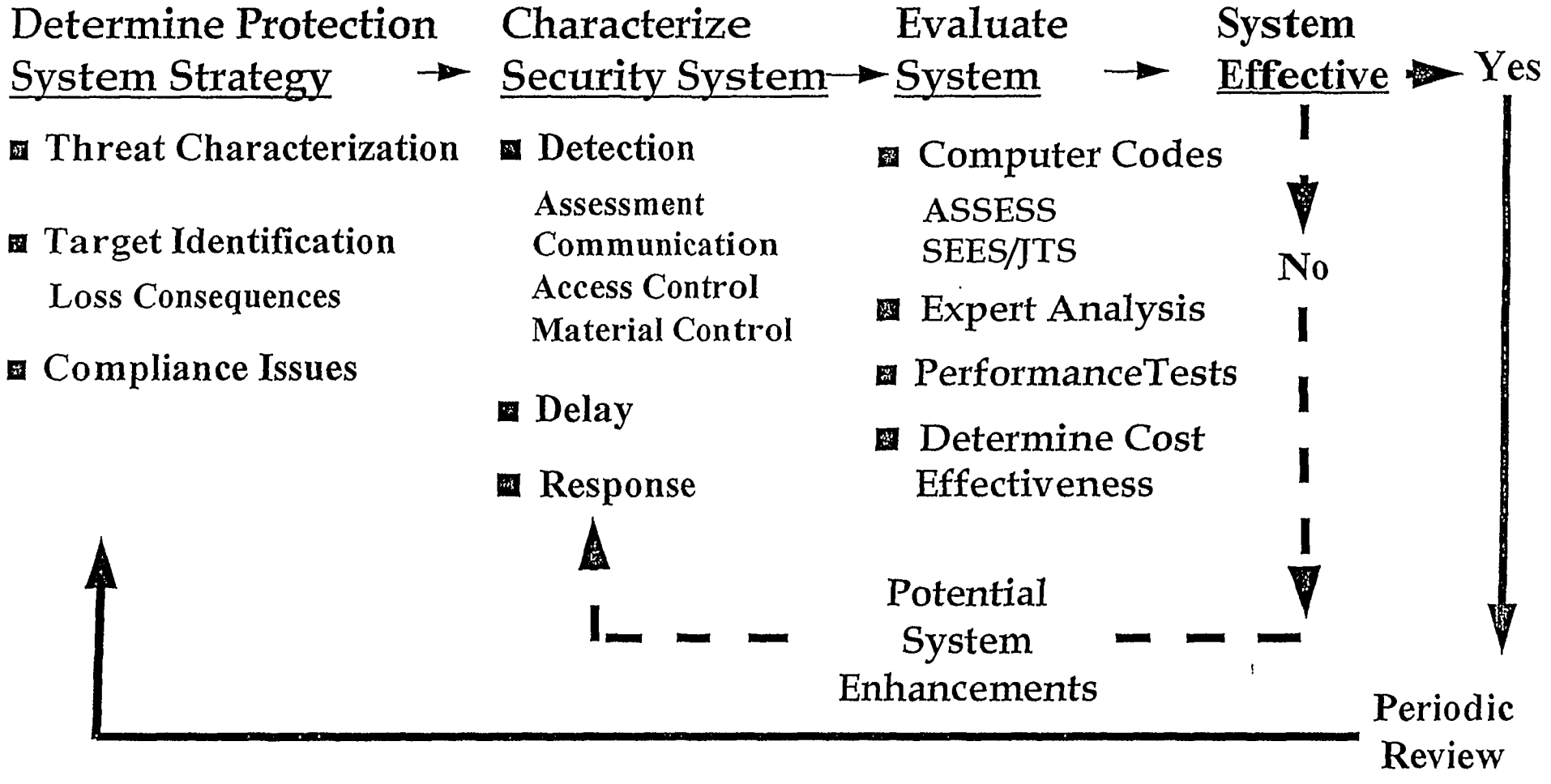
CONSEQUENCE VALUE	RADIOLOGICAL RELEASE AT THE SITE BOUNDARY RELATIVE TO THE DOSE CRITERIA OF 10 CFR 100 *
1.0	$\geq$ 250 REM WHOLE BODY / 3000 REM THYROID
0.5	125 REM WHOLE BODY / 1500 REM THYROID
0.2	50 REM WHOLE BODY / 600 REM THYROID
0.1	25 REM WHOLE BODY / 300 REM THYROID
0.01	$\leq$ 2.5 REM WHOLE BODY / 30 REM THYROID

For values of radiological releases that fall between the values given in the table,interpolate the table to determine theappropriate consequence value.

*10CFR 100 An individual located at any point on the site boundary would not receive a whole body dose in excess of 25 rem or a total radiation dose in excess of 300 rem to the thyroid from idoine exposure during a period from the onset of the postulated fission product release until two hours after onset.

ATTACHMENT E

Methodology for Analysis of Security System Effectiveness



Conditional Risk Equations

Vulnerability analysis must establish the value for physical protection system effectiveness (P_E) and sufficient documentation must be recorded to justify the results. The analysis should provide system effectiveness results for three kinds of threat events:

- Theft and Diversion of Weapons and Weapons Components, and Special Nuclear Materials (SNM)
- Radiological and/or Toxicological Sabotage
- Industrial Sabotage

These events must be analyzed to allow for involvement of both outsider and insider threats.

Against outsiders and the active, violent insider, the P_E is determined by the product of the Probability of Interruption, P_I , and the probability of Neutralization. P_N :

$$P_E = P_I \times P_N$$

Against the active, non-violent, and passive insider, the P_E is determined by the Probability of Detection (P_D).

$$P_E = P_D$$

The probability of system failure ($P_{\text{System Failure}}$) is determined by subtracting P_E from unity, or 1.0.

$$P_{\text{System Failure}} = 1 - P_E \quad \text{or} \quad 1 - [P_I \times P_N]$$

The risk ratings associated with these events are obtained from the product of $P_{\text{System Failure}}$ and the consequence (**C**) of the adversary's act. The probability of an adversary attack (P_A) is assumed to be 1.0.

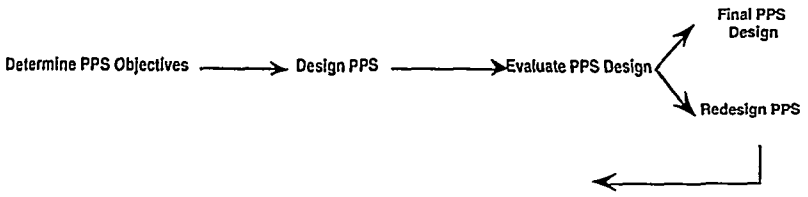
Outsiders and active, violent insiders

$$R = P_A \times P_{\text{System Failure}} \times C \qquad R = P_A \times [1 - (P_I \times P_N)] \times C$$

Active, non-violent, and passive insiders

$$R = P_A \times P_{\text{System Failure}} \times C \qquad R = P_A \times [1 - (P_D)] \times C)$$

Design and Analysis Cycle



2/1

Physical Protection System Objectives

Understand what to protect and from whom:

- Characterize the facility
- Define the threat
- Identify the targets

2/2

Facility Characterization

Characterize the facility in terms of

- Site boundary
- Buildings
- Room locations
- Access points
- Processes within the facility
- Operating conditions (working hours, off-hours, potential emergencies)
- Existing physical protection features

2/3

Threat Definition

Using all information sources determine:

- Classes of adversaries
  - Outsiders
  - Insiders
  - Outsiders in collusion with insiders
- Range of adversary tactics
  - Stealth
  - Force
  - Deceit
- Capabilities of adversaries
  - Knowledge
  - Motivation
  - Skills
  - Weapons and tools

2/4

Target Identification

Determine the possible targets for the following actions:

- Radiological sabotage
  - Identify vital areas to protect
- Theft of nuclear material
  - Identify location of nuclear material to protect

2/5

Initial Physical Protection System Design

Design the physical protection system by:

- Combining physical protection components into a system within a facility's constraints
- Using components that complement each other and correct for weakness
- Placing detection toward the perimeter and delay toward the target

2/6

Evaluation of Physical Protection System Design

Evaluate the physical protection system by:

- Checking for required features
- Using modeling techniques (preferred method)

2/7

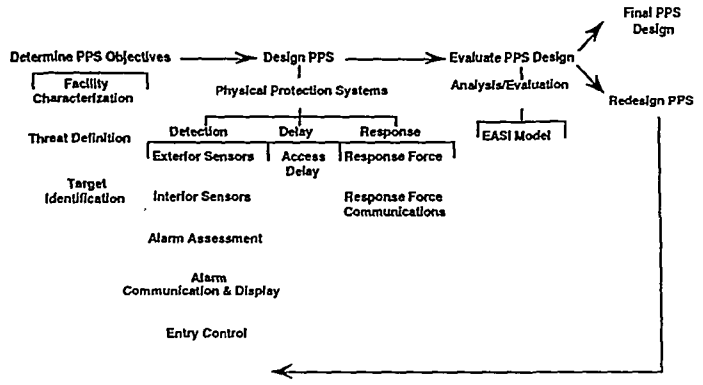
Redesign or Upgrade of Physical Protection System

As a result of the analysis:

- Identify vulnerabilities in the PPS
- Redesign system to correct noted vulnerabilities
- Reevaluate to verify vulnerability is corrected

2/8

Design and Evaluation Process Outline (DEPO)



2/9