NUREG-0335

SAFEGUARDS SYSTEMS CONCEPTS FOR NUCLEAR MATERIAL TRANSPORTATION

Final Report

System Development Corporation
for
U. S. Nuclear Regulatory Commission

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Nuclear Regulatory Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, nor assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, nor represents that its use would not infringe privately owned rights.

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy $9.50 ; Microfiche $3.00

The price of this document for requesters outside of the North American Continent can be obtained from the National Technical Information Service.

NUREG-0335
NRC-13

SAFEGUARDS SYSTEMS CONCEPTS FOR NUCLEAR MATERIAL TRANSPORTATION

Final Report

O. C. Baldonado
M. Kevany
D. Rodney
D. Pitts
M. Mazur
P. Stephens
V. Olcutt

Manuscript Completed: April 1977
Date Published: September 1977

System Development Corporation
7929 Westpark Drive
McLean, VA 22101
TM-WD-7900/003/00

Prepared for
Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Under Contract No. AT(49-24)-0333

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

CHAPTER 1

INTRODUCTION AND OVERVIEW

1.0 INTRODUCTION AND OVERVIEW

1.1 Overview of the Project

The Office of Nuclear Regulatory Research of the Nuclear Regulatory Commission (NRC) commissioned a project to develop integrated system concepts for the safeguard of nuclear materials against malevolent action during interfacility transport. This report describes the conduct and findings of the project. It addresses potential threats by terrorists and others to interface with nuclear materials in transit. It also recommends measures which can be taken to reduce both the likelihood of such threats and the probability of success if carried out.

The study was divided into three major portions:

- The development of adversary action sequences.
- The assessment of the vulnerability of the transport of nuclear materials to adversary actions.
- The development of conceptual safeguards system design requirements to reduce vulnerabilities.

The development of conceptual design requirements is significant. It means that licensees would have more flexibility in meeting NRC regulations since there would be a variety of specific measures from which to choose in order to meet those regulations. But it also means that NRC must develop and implement evaluation techniques in order to assess licensee compliance with the requirements.

It was recognized from the beginning that this SDC study is just one of many in this important subject area. It was also recognized that within the time and resource limits of the present contract, it was not possible to achieve the same level of broad and detailed analysis as some of the other studies. However, this did not inhibit the project team from taking a "fresh" approach to the problem. While information from other studies was reviewed, there was no intention to rely on their findings or recommendations.

1.2 Overview of the Report

Chapter 1 provides an introduction to the objectives and scope of the study. It describes the problem of transporting nuclear materials, the adversary threat, the safeguards strategies available to combat that threat, and the governmental interfaces involved in dealing with it.

Chapter 2 outlines the methodology which was developed and followed in the conduct of the study. It describes how data was acquired, how adversary action sequences were developed, how vulnerability assessments were conducted, and how conceptual design requirements were developed.

Chapter 3 describes the adversary action sequences in detail. It also classifies the adversaries by a number of attributes.

Chapter 4 describes the conduct and findings of a first order vulnerability assessment of generic safeguards systems to representative adversary action sequences.

Chapter 5 describes the recommended safeguards system design requirements.

Chapter 6 deals with an evaluation of the impact of the recommended design requirements on society in general and on the nuclear power industry in particular.

1.3 Scope of the Study

Considerable debate continues on the role of nuclear fuel in the nation's energy system. However, it appears that it must play a vital role especially toward the end of the century. As the nuclear industry grows, there will be an increasing stress on safe shipment of nuclear materials between facilities. The increased emphasis will be based not only on the amounts of materials to be shipped but also on the shift to materials of a more strategically significant nature. These Strategic Special Nuclear Materials (SSNM) include plutonium, uranium 233, and uranium 235 at 20% enrichment. The new fuels will presumably be more attractive to terrorists and other potential adversaries, and so, additional safeguards in the shipment of materials will be required.

It is important at the outset to emphasize that this report is quite limited in scope. Its findings and recommendations relate to the transportation of nuclear materials only. It is not a policy study on the overall issues involved in the nuclear fuel cycle, such as the question of whether or not nuclear materials are unsafe either in transit or at fixed facilities. The study was based on the following assumptions:

- that demand for energy, including nuclear energy, will continue to increase. Therefore, the concepts that have been advanced in this report are based on the assumption that the number of shipments will grow from relatively few to several thousand each year.

- that the general economic, social, and political conditions that have existed in the U.S. since World War II will continue to prevail into the twenty-first century. (Because of the risk that this assumption may be somewhat optimistic, there is discussion of the impact of radically changing conditions on the commercial nuclear industry in Chapter 6 of this report.)

- that the nuclear materials transportation sequence begins once a decision to transport has been made. The transportation process ends in one of three ways. It may end at the point at which the SSNM is transferred from the shipper to the recipient. It may end at the point at which SSNM is stolen and removed to a safe haven (from this point responsibility shifts to the law enforcement and emergency preparedness agency). The transportation process may also end if it is interrupted by sabotage and/or SSNM dispersal en route.

- that the adversary is capable of having a maximum quantity of forces and resources to devote against a transportation shipment. It is assumed that no adversary group will contain more than 15 dedicated members of whom no more than two are insiders, either directly employed by the nuclear power industry or a transportation carrier. Obviously, there is nothing magic about the number 15. An attack with an unlimited number of participants could take place, although some research has suggested that there are a number of factors such as lack of cohesiveness that would mitigate against a large group size. In any case, a group of more than 15 members would virtually constitute an army that only the U.S. military would be able to confront.

The scope of the study was limited by the following boundaries:

- Only shipments of nuclear material within the continental U.S. have been addressed.

- Four modes of transport have been considered: rail, truck, barge, and airplane.

- Emphasis has been placed on Strategic Special Nuclear Material (SSNM) rather than on other types of nuclear material such as high-level waste.

- Theft, rather than sabotage, was viewed as the primary action against which to protect.

- "Hot pursuit" of stolen SSNM was examined, but recovery of SSNM was considered an alternative strategy outside the focus of this study.

1.4 Overview of the Transportation Safeguards Problem

The requirement of safeguard systems for transport of nuclear materials is based on the fact that certain nuclear material to be used in the fuel cycle may be used for malevolent purposes, including the construction of an explosive device, or the dispersion of materials which are hazardous to the public's health. Briefly, the plans for the future nuclear fuel cycle show plutonium (PU) and highly enriched uranium (U_{235}) being utilized. It is estimated that as little as five kilograms of plutonium could be used by persons with some education and training in physics to construct a nuclear device capable of an explosion with the destructive force of approximately 20,000 tons of TNT. Present estimates project about 150 shipments of these strategic materials by 1980.

Safeguards for nuclear materials in transit are at least as important as safeguards for nuclear materials at fixed sites -- in some ways more important. While being transported, nuclear material has a higher probability of being attacked for the following reasons:

- A greater number of people are involved in the transportation sequence and have access to the SSNM at both the origin and destination points of the shipment.
- The SSNM is in a moving vehicle that is a relatively easy target for adversaries.
- Only the vehicle compartment and the SSNM container obstruct potential adversaries while there are many more physical obstructions in a fixed facility.
- It is easier to divert material that is being moved.

Thus, it is evident that nuclear material may be more vulnerable during the transportation process than it is at fixed facilities.

The transport of SSNM will take place between four types of facilities spread throughout the country. The shipments will have the following origins and destinations throughout the nuclear fuel cycle (Figure 1-1):

- Fuel fabrication plant to nuclear reactor (power generator).
- Nuclear reactor to fuel reprocessing plant.

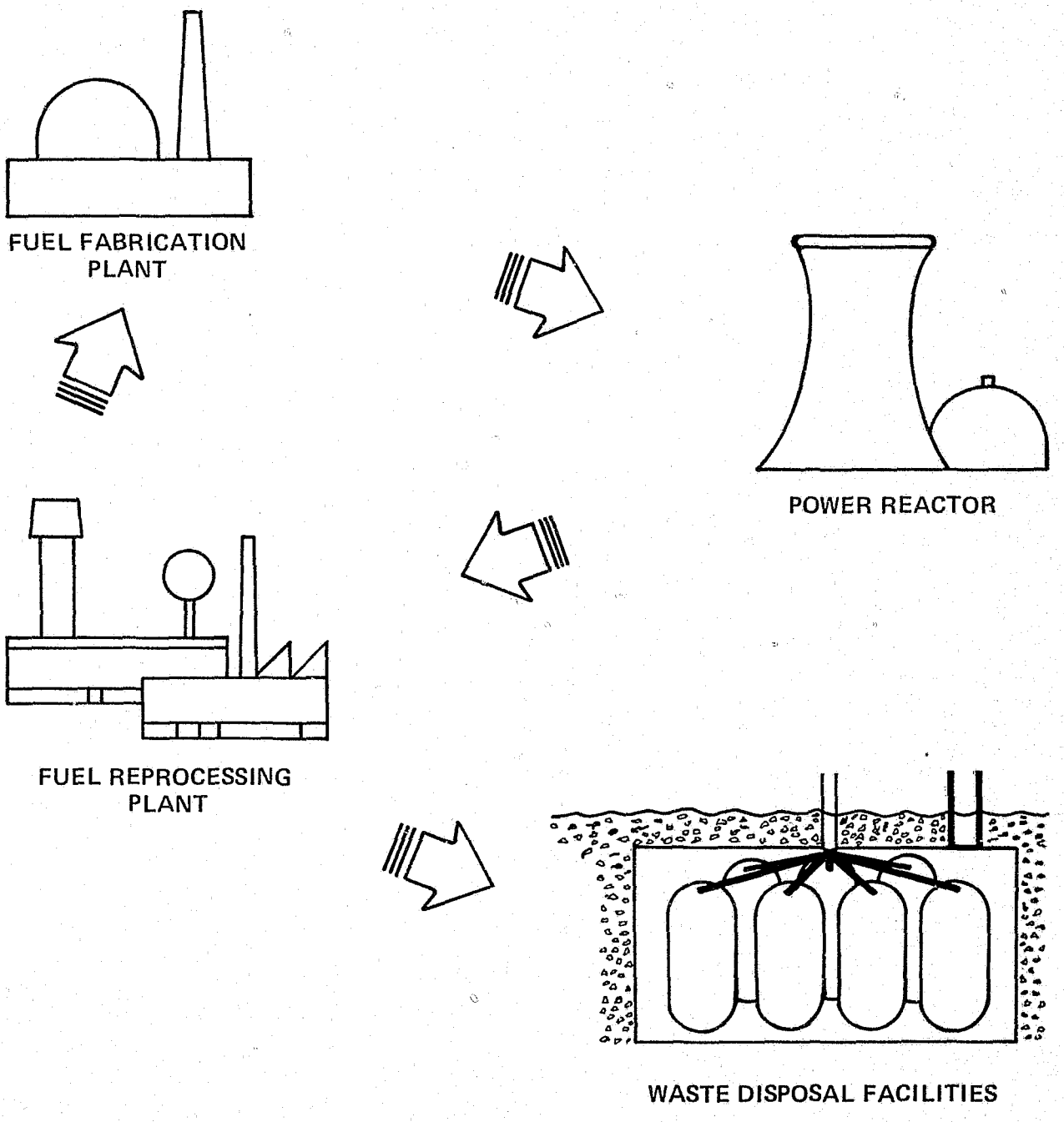

FIGURE 1-1: NUCLEAR FUEL CYCLE
ORIGINS AND DESTINATIONS OF SSNM SHIPMENTS

- Fuel reprocessing plant to fuel fabrication plant.
- Fuel reprocessing plant to waste storage facility.

As depicted in Figure 1-2, the transport sequence includes eleven stages, all of which must be provided with safeguards against diversion or attack.

1.5 Overview of the Threat

There is no doubt that terrorism is becoming an increasingly important weapon in the arsenal of those who wish to force their demands upon society. While terrorists typically do not wish to harm large numbers of people, they often threaten to, in order to have their demands taken seriously. Governmental negotiators must take the threat to use force as seriously as the use of force itself in order to protect innocent lives. A terrorist group would have few means more effective to threaten the lives of innocent people than the theft of SSNM. Thus, the possibility of theft or diversion of SSNM must be considered one of the most serious potential dangers to society, especially if the material is used to construct and threaten detonation of a nuclear device.

1.6 Overview of Safeguards Issues

In order to protect SSNM in transit from malevolent action, it is necessary to provide safeguard measures in an integrated manner. These measures, implemented by the various organizations involved in an SSNM shipment, will reduce the vulnerability of the shipment to a level which is compatible with the national safeguard objective. It is the role of NRC to set safeguards system design requirements, and it is in support of this role that the present study was undertaken.

In conceptualizing safeguards systems, several issues must be considered. The level of safeguards required will be based on the anticipated level of threat. Since no successful attack has been conducted on a nuclear material shipment, there is no empirical data specifically related to this threat, and so the level to be planned for must be based on analytical studies. Two factors are important to this analysis. The first has to do with the probability that an attack will take place. The second factor concerns the magnitude of damage which could occur if a malevolent adversary action is successful and a nuclear device is detonated. Since no such attack has yet taken place, estimation of the probability is extremely difficult. Extremely high casualty and damage estimates abound in the press, but there is no doubt

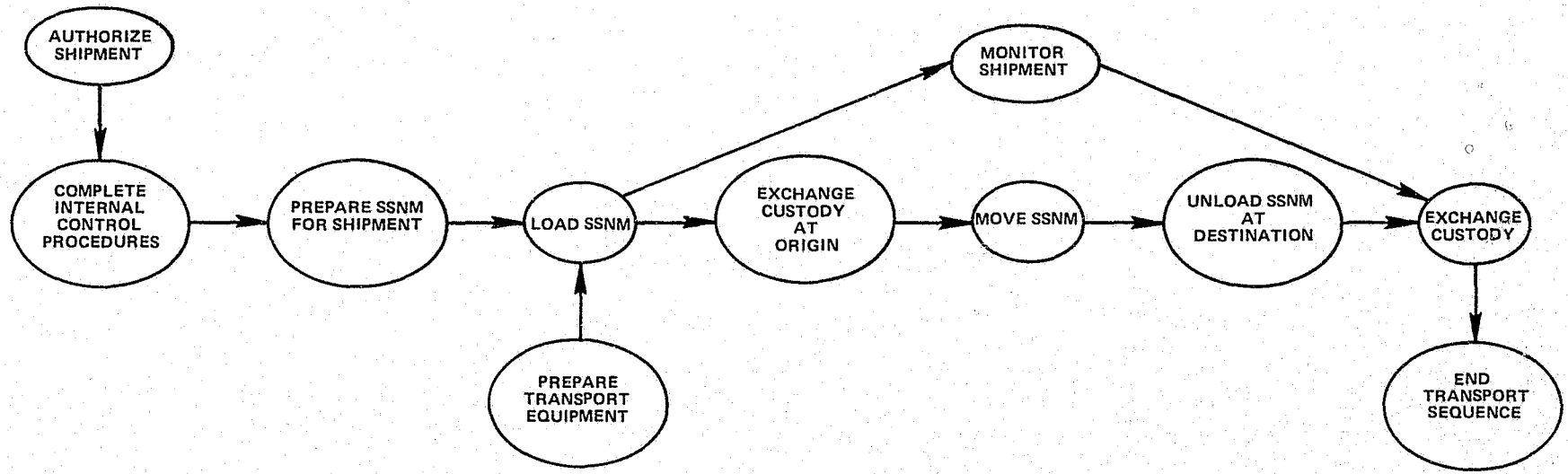

FIGURE 1-2: OVERVIEW OF THE SSNM TRANSPORT SEQUENCE

that even a rudimentary nuclear device detonated at the proper place and time could be an enormous catastrophe. Because of this potential, the level of safeguards required is significantly higher than is warranted by the probability of occurrence. But the level of safeguards cannot be considered in the context of the nuclear industry alone. The present political atmosphere is extremely sensitive to the impact of proposed government regulations and actions on civil liberties. The impact of such measures as intelligence gathering, use of sophisticated weapons, and provision for more effective guard forces would be subject to careful scrutiny in the present political climate. On the other hand, the level of terrorist activity in the U.S. currently is low. If such activity should increase and pose a larger threat to society, the attitude toward proposed safeguard measures might change significantly.

The size of the nuclear transport industry in the future is also an important issue. At present, the transport of SSNM is very limited. It does require some special protection but the number of shipments is very few and disruption and inconvenience is minor. The industry at its present size cannot afford, or justify, many safeguard measures to significantly decrease the level of vulnerability. If the nuclear industry grows as projected, however, the increase in shipments will justify a completely different approach than that taken at present. Rather than participating in the general transportation network, the nuclear industry could afford a specialized transport system of its own, justifying specialized equipment, dedicated employees, and other improved safeguards measures.

1.7 Safeguards Strategies

When the safeguards issue is examined through the eyes of experts in the security and law enforcement fields, strong intelligence gathering, firepower, and physical protection strategies tend to be emphasized. Defense is seen as the primary need. However, if the issue is viewed from the perspective of those involved in the nuclear transport industry, powerful defense strategies are seen as an unwanted economic burden and a serious imposition on the business operations of the individuals and firms in the private sector. From their perspective, the safeguard emphasis should be on a strategy of improved communication between shipment and support agencies, and an effective technique for the location and recovery of materials if they should be diverted.

The safeguards strategy selected must balance the often competing objectives of these different elements of the overall system. Each component is important to evaluate. Obviously, the system must reduce the vulnerability of the SSNM to malevolent action. However, the level of vulnerability which may be achieved must be limited by the cost to society of the safeguards measures. The economic and social costs of the system must be reasonable in terms of the benefits provided and the economic realities of

the nuclear fuel cycle. The ease with which the system may be implemented must also be considered. Dependence on a yet undeveloped technology would be unreasonable. From the perspective of NRC's regulatory role, it must also be possible to evaluate the implementation of system components.

To minimize the impact on civil liberties, a strategy of heavy dependence on physical protection devices could be adopted. Under this option, rather than using techniques which may affect the civil liberties of those in the nuclear industry or the population in general (extensive intelligence gathering, background investigations, numerous armed guards, etc.), mechanical techniques and physical devices (heavy containers, sophisticated seals and locks, immobilization devices, etc.) would be emphasized. These latter protective measures are primarily passive in nature, having little or no effect on anyone other than a person attempting to gain unauthorized access to or control over SSNM. However, complete reliance on this strategy leaves the shipment vulnerable to some types of attack, such as deceit where an attacker is an insider with access to information, keys, codes, etc.

The various options for safeguards systems may be divided into the following strategies:

- Self-sufficient convoy based on large numbers of well-trained, well-armed guards.
- Self-sufficient shipment based on very strong physical defense equipment (extremely large containers, sophisticated locks, immobilization mechanisms, foam, etc.).
- Avoidance of contact en route through use of air shipment.
- Avoidance of contact en route through use of complete camouflage of shipment.
- Shipment of very small quantities – less than those required for an explosive device.
- Minimal shipment defense with reliance on response forces.
- Minimal shipment defense with reliance on effective recovery techniques.
- Elimination of transport through co-location.

An effective safeguards systems will probably be based on combinations of elements of some or all of these above strategies, especially in the near term, where no one strategy will be completely effective.

An integrated safeguards system, in order to be extensive enough to protect against all possible situations, should include four basic classes of safeguard functions.*

- Deterrence -- Convince potential attackers that an attack is useless prior to their undertaking it or that continuation is useless if the attack has begun. This is accomplished by publicizing information on the invulnerability of the shipment, the difficulty of conducting an attack, the difficulty of utilizing SSNM, and the consequences to be faced upon failure. It may also include the infiltration of an adversary organization and planting information to deter or prevent planned action.

- Detection -- Establish procedures and employ persons and equipment which will allow the responsible parties to recognize an attempt by an adversary to conduct an action against a shipment, or the possibility that an action may be taken or has been taken (completed). The detection of an attack includes not only the simple fact that an attack is identified, but also the notification of appropriate response mechanisms with the information necessary for reaction. This detection is based on the evaluation of indicating signals and the distinction between a malevolent act and an innocent occurrence. Examples of these indicating signals are the violation of control procedures and the triggering of detection devices.

  As with deterrence, detection may occur prior to attack (e.g., detection of suspicious persons around a plant), and may result in avoiding the attack, either through the arrest or discouragement of the potential attackers, or by modifying defenses to ward off the attack (e.g., assigning additional guards or rescheduling shipment). Detection may also occur during the attack and may be used to activate defense forces or techniques to defeat the action.

- Defense -- Interrupt the adversary action sequence during the actual attack by either passive or active means. Passive mechanisms include barriers which the adversary must penetrate in order to obtain the SSNM, such as immobilization devices, locks, seals, and foam. Killing or apprehending the adversary are active means of stopping the attack.

- Consequence Reduction -- Establish and implement procedures that will reduce the severity of the effect of an SSNM theft or dispersal on society, either before or after any given malevolent act occurs. These procedures may be directly related to the recovery of the stolen

*See ERDA-7. Societal Risk Approach to Safeguards Design and Evaluation

material or may deal with the after-effects of a completed adversary action sequence (e.g., detonating a nuclear device, blackmail, dispersal of the material, etc.).

1.8 Organizational Relationships to Transportation Safeguards

According to the terms of the Energy Reorganization Act of 1974, the Nuclear Regulatory Commission (NRC) is responsible for the regulation of the commercial nuclear industry. The Atomic Research Commission (AEC) which was responsible for both the regulation of the nuclear industry and the promotion of energy development was abolished. NRC's sole objective is regulation, safeguards, and safety in the commercial nuclear industry, while energy development is the responsibility of the Energy Research and Development Administration. The terms of the Act provide that NRC assume more of a regulatory responsibility for the safeguard of peacetime nuclear power than its predecessor the Atomic Energy Commission.

The basic function of the NRC -- to regulate the commercial nuclear industry and minimize hazards -- involves interfacing with a number of other governmental and commercial organizations. These interfaces may be summarized as follows:

- Licensees are responsible for protecting the materials they use or transport and for providing physical protection (including guards) of those materials. NRC assures they do this, as a condition of their license.

- State and LLEA's are not under NRC authority but are assumed willing and able to provide a response force in the event of a nuclear emergency. NRC encourages them to assume this responsibility and requires licensees to interface with them.

- NRC is responsible for developing contingency plans for dealing with blackmail threats and possible sabotage. But the FBI investigates possible sabotage or subversion threats.

- The U.S. Department of Transportation is responsible for the direct regulation of carriers in order to protect the public from risks to health and safety.

- State and local governments also regulate various aspects of nuclear material transport in the interest of public health and safety.

These organizational relationships are graphically illustrated in Figure 1-3. Thus, it is apparent that a number of agencies are involved. Should an adversary action be attempted, agency interfaces will

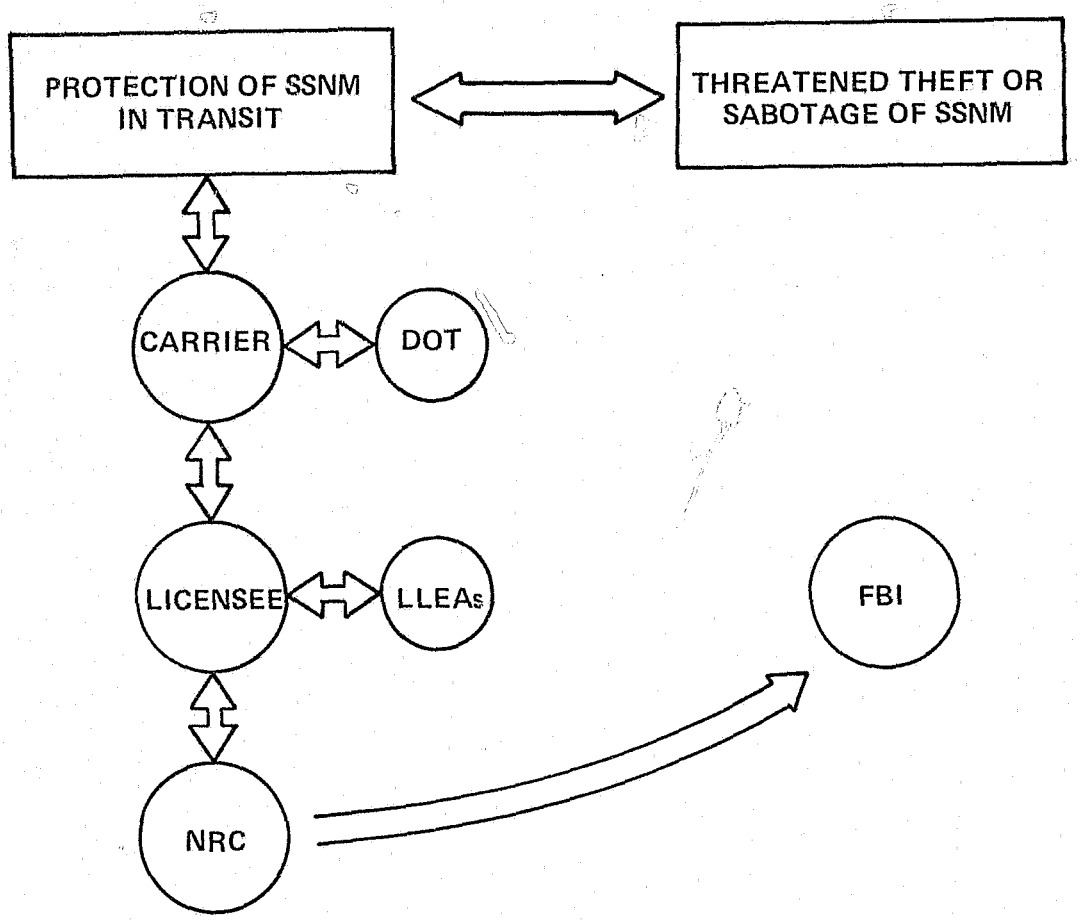

FIGURE 1-3: ORGANIZATIONAL RELATIONSHIPS IN SSNM TRANSPORTATION

evolve in the following manner. The FBI will be responsible for identifying the characteristics of possible adversaries, evaluating their objectives, identifying their resources, investigating actual or potential actions and apprehending those involved. NRC will develop the contingency plans necessary for dealing with conceivable threats. The licensees and the carriers under DOT regulations must be prepared to deal with an actual theft attempt. State law enforcement officials and LLEA's will respond to calls for assistance if the guard force accompanying a shipment is unable to thwart a theft attempt. The licensee must communicate into LLEA's en route.

This division of responsibility between NRC and DOT could cause confusion and at a minimum obscures responsibility and authority. NRC is responsible only for regulating the licensee whereas DOT is responsible for regulating the carrier. It is true that each licensee must make plans with the carrier to protect SSNM in transit, but the carrier is nevertheless not directly bound by NRC regulations.

The parameters of NRC's responsibilities for operations beyond regulation are somewhat difficult to specify. NRC is clearly responsible for regulating the industry which in itself is charged by NRC with a large number of safeguards requirements; but where industry responsibility ends and NRC responsibility or the responsibility of other federal agencies begins is not always clear. For example, the regulations state that licensees are not required to protect facilities or shipments against "an enemy of the United States whether foreign government or other person," but the regulations do not define exactly what an enemy of the United States is, and clearly it is a highly subjective judgment as to what constitutes an enemy.

In the course of this report, various ideas will be advanced which, if acted upon, would involve a change in these relationships toward more interagency involvement and more communication between NRC and the industry.

CHAPTER 2

STUDY METHODOLOGY

2.0 STUDY METHODOLOGY

2.1 Overview

The technical effort of the project was divided into three formal subtasks:

- Development of Adversary Action Sequences.
- Performance of a Generic Vulnerability Assessment.
- Development of Integrated Safeguards System Design Requirements.

The interrelationship among these three subtasks and supporting activities is shown in Figure 2-1.

Throughout the conduct of the study, the methodology was refined and modified based on the insights gained from the performance of each subtask and supporting activity.

2.2 Analysis of Adversary Actions

Since it is the threat of an adversary action to carry out a malevolent act that generates the requirement for safeguards, an analysis to understand these actions was a prerequisite to the development of effective safeguard system concepts. This analysis provided not only an understanding of the nature of adversary actions, but also information for use in vulnerability assessment.

The analysis provided information on who might attack an SSNM shipment, how well prepared they might be to carry out an attack, and what actions they might take in conducting the attack. A particular concern was the generation of information to support estimations of both the probability of an attack and its success should it take place. It was postulated that the probability of attack is based on the nature of the adversary group, its motives, and its perception of how successful the attack will be. It was further postulated that the adversary's perception of its potential for success is based on its motivation, the capabilities and resources it can acquire, and its perception of the capabilities of the safeguards system that must be defeated.

The analysis involved an investigation and classification of the characteristics of potential adversaries, the capabilities and resources they might possess, and the actions they might take. Only three end results of these actions were considered (these being the only reasons seen for attacking SSNM in transit):

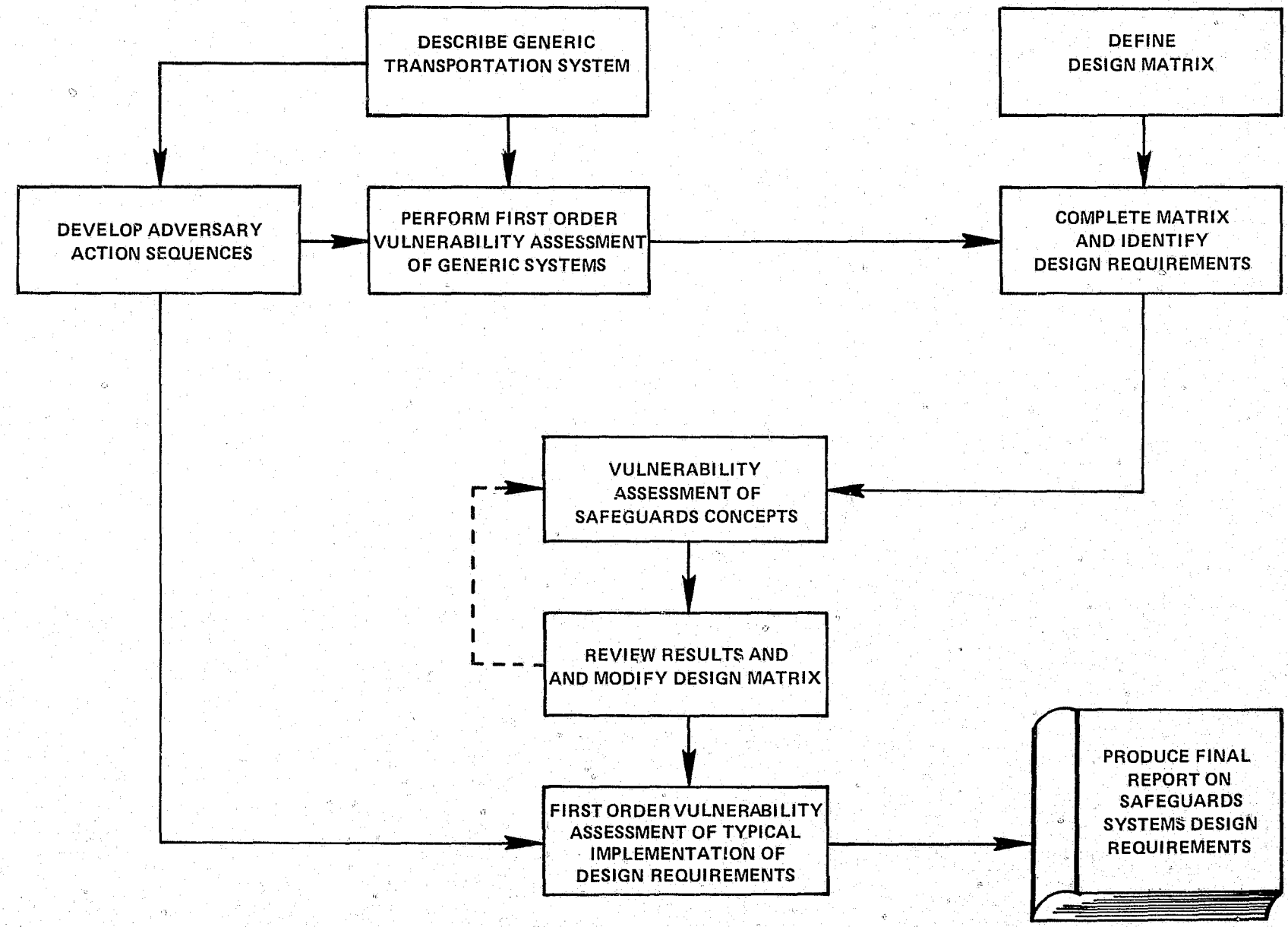

FIGURE 2-1: PROJECT WORK FLOW

- Diversion of SSNM to an adversary safe haven.
- Dispersion of radioactive material at the attack site.
- Sabotage of the SSNM shipment without removal or dispersion.

Clearly, a very large number of possible adversary action sequences (AAS) to achieve these ends could be generated. It would not be feasible during the time allotted for the study to consider the impact of every possible AAS on a safeguard system. Consequently, the study team developed a classification system that permitted groups of actions to be tested against the safeguard system simultaneously.

The classification system finally adopted grouped the AAS by certain attributes. The attributes chosen were those that had an impact on vulnerability. For example, all AAS could have been grouped according to the day of the week on which they occur; but since "Day of Occurrence" had no discernible effect on vulnerability, it was not used as a grouping attribute. On the other hand, the size of the adversary group did have an effect, so "Number of Personnel" was a valid attribute upon which to group or classify the AAS. (In this case, the grouping consisted of three classes: Class 1, 1-6 people; Class 2, 7-12 people; Class 3, 13 or more people. The groupings for other attributes are given in Chapter 3.)

The results of the adversary actions development were used to provide information for the vulnerability assessments conducted in the subsequent subtasks. The sequences themselves were incorporated in vulnerability matrices and the supporting data were used in the estimation of vulnerability values in the matrices. A complete description of this effort is presented in Chapter 3.

2.3 Vulnerability Assessment of the Generic SSNM Transport System

As a starting point for the analysis of safeguards system vulnerability, first order assessments were conducted based on a set of adversary actions sequences and the various safeguard systems considered in this study.

The methodology of the generic vulnerability assessment provides an interface between the various adversary action classes and the protective mechanisms that comprise the safeguards systems under consideration.

Define a protective mechanism (PM), as an obstacle to be overcome by an adversary if he is to succeed. The entire safeguard system can then be considered to be made up of several individual PM's. PM's to be considered as part of the safeguard systems include guards, barriers, security and administration procedures, etc.

Vulnerability of the system may be defined as the probability of a system being unable to thwart the successful completion of an adversary action. It is necessary to think of each adversary action in terms of its probability of successful completion, V. Thus, the intelligent adversary will carry out a set of actions that, from this viewpoint, have maximum V. (The consequences are assumed to be constant.) Any change in the set of adversary actions that leads to an improvement in the plan will translate into a change in the probability or an increase in V.

A safeguards system is viewed as a means to reduce V. The perfect system is one that results in a zero completion probability. Any improvement in a safeguards system should result in a corresponding decrease in V.

There are two parts to the methodology of the generic vulnerability assessment. The first part concerns the assessment of the vulnerability of a safeguards subsystem to a particular adversary action class. The other part describes how the vulnerabilities of the system to the different adversary action classes are combined to obtain the overall safeguards system vulnerability. Each part is considered below in turn.

2.3.1 Vulnerability of a Safeguards System to An Adversary Action Class

The safeguards system is composed of protective mechanisms, $PM_1, PM_2, \ldots, PM_n$. Each protective mechanism poses a barrier to the adversary that must be overcome for him to succeed.

Define $V_j(PM_k)$ as the vulnerability of the kth protective mechanism, PM_k, to adversary class S_j. Therefore, the vulnerability of each of the protective mechanisms, assuming n of them, will be designated by $V_j(PM_1), V_j(PM_2), \ldots, V_j(PM_k) \ldots, V_j(PM_n)$. Assuming independence of the protective mechanisms, the entire system vulnerability to the particular S_j is:

$$V_j = \prod_{k=1}^{n} V_j(PM_k)$$

Any protective mechanism that is not included in the analysis, or is not germane to a particular adversary action class, will have a vulnerability equal to 1. If one PM_1 is perfect against the class S_j, then $V_j(PM_1) = 0$, and hence $V_j = 0$ for this case.

The technique of individually assessing the vulnerabilities of the individual protective mechanisms was followed under the assumption that it is much easier to deal with one safeguards system component at a time.

It may also be of interest to note that, as far as the methodology is concerned, S_j could also represent a particular step in a particular adversary action sequence. Then, $V_j(PM_k)$ can be interpreted to be the vulnerability of the PM_k to the particular step S_j. In this manner, the same methodology can be applied to assess the vulnerability of the safeguards systems to a specific adversary action sequence instead of to a class of adversary action sequences.

2.3.2 Overall Safeguards System Vulnerability

The overall safeguards system vulnerability is derived by combining the vulnerabilities of the system to a set of adversary action classes. Before this can be done, it is necessary to consider the frequency distribution of adversary action classes, because the importance of an adversary action class is dependent on both the chance of success and the frequency of the occurrence.

The vulnerability V_j of the system to the particular adversary action class S_j is weighted by the frequency number, $P(S_j)$. Thus, $P(S_j)V_j$ is the weighted vulnerability, and the vulnerability of the entire system to the entire set of adversary actions is given by V:

$$V = \prod_{j=1}^{m} P(S_j)V_j \qquad (2.2)$$

As an example, suppose one has three classes of adversaries, S_1, S_2, S_3:

S_1: Low level threat; guns, pistols, rifles for weapons.

S_2: Medium level threat; automatic firearms for weapons.

S_3: High level threat; rockets for weapons.

Assume that the relative frequencies for $P(S_1)$, $P(S_2)$, and $P(S_3)$ are .94, .04, and .02 respectively. See Table 2-1 for the vulnerability numbers.

By using equation (2-2),

TABLE 2-1: "ARMS" CLASSIFICATION OF ADVERSARY ACTIONS

ADVERSARY ACTION CLASSES	RELATIVE FREQUENCY $P(S_k)$	VULNERABILITY V_k	WEIGHTED VULNERABILITY $P(S_k)V_k$
Low Threat Level: Guns, Pistols, Rifles	.94	1.0×10^{-6}	9.4×10^{-7}
Medium Threat Level: Automatic Weapons	.04	2.0×10^{-5}	8.0×10^{-7}
High Threat Level: Rockets	.02	3.0×10^{-4}	6.0×10^{-6}

$$V = \sum_{j=1}^{3} P(S_j)V_j$$

$$= 9.0 \times 10^{-7} + 8.0 \times 10^{-7} + 6.0 + 10^{-6}$$

$$= 7.74 + 10^{-6}$$

Note that, although a medium level attack has greater chance of success than a low level attack, the low level attack poses the greater threat when the relative frequencies are taken into account.

There are two reasons for obtaining the overall vulnerability from the weighted vulnerabilities. First, it gives a measure of the vulnerability of the safeguards system. This facilitates an assessment of whether the safeguards system provides adequate protection against adversary actions. Second, it provides a check and balance on the accuracy of the assessment of vulnerabilities, when it is considered in conjunction with a vulnerability assessment under a different classification of adversary actions.

The methodology for vulnerability assessment was facilitated by the use of a set of matrices. A separate matrix was generated for each case to be evaluated. In the horizontal rows, the adversary action class is identified along with the $P(S_k)$ and values for the vulnerability of each PM to the action class. The vertical columns list the individual PM's. For each action class the V_k and $P(S_k)V_k$ are also computed and displayed. Table 2-2 provides an example of a completed matrix typical of those obtained in the generic vulnerability analysis.

The data values for the $P(S_k)$ were computed on the basis of data acquired on similar malevolent acts committed by adversary groups similar to the class being evaluated. This was done because there have been very few malevolent acts perpetrated against the nuclear power industry; consequently, it was impossible to attain a reasonable data base from investigations into past incidents identical in type to those considered in this project. In trying to form the desired frequency distributions, therefore, the project team investigated incidents of a similar nature, such as bank robberies, hijackings, bombings, etc. A BDM report, Analysis of Group Size, gave a comprehensive analysis of the number of persons engaged in all forms of malevolent acts. A distribution of the number of persons who would be involved in an attack against the transport of SSNM was estimated on the basis of the statistics in the BDM report; these were used in the general vulnerability analysis. Such estimates, however, must be treated with caution, because the safeguards in operation at the time have an impact on the adversary group that is considering attack.

TABLE 2-2: ADVERSARY ACTION – SAFEGUARDS INTERACTION MATRIX NO. N

DEDICATION CLASSIFICATION – PROTECTIVE SYSTEM X

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS											
NO.	$P(S_k)$	DEDICATION	PM1	PM2	PM3	PM4	PM5	PM6	PM7	PM8	PM9	PM10	V_k	$P(S_k)V_k$
1	.75	Low: Casual	.9	.15	.4	.5	.1	.01	.75	.8	.1	.1	1.62×10^{-7}	1.22×10^{-7}
2	.2	Medium: Sustained Discomfort and Injury	.9	.3	.6	.5	.2	.05	.8	.9	.6	.2	7.00×10^{-5}	1.40×10^{-5}
3	.05	High: Willing to Accept Loss of Life	.9	.4	.7	.5	.8	.1	.8	.9	.7	.4	2.03×10^{-3}	1.02×10^{-4}

SAFEGUARDS SYSTEM VULNERABILITY $= \sum_{k=1}^{3} P(S_k)V_k$

$= 1.22 \times 10^{-7} + 1.40 \times 10^{-5} + 1.02 \times 10^{-4}$

$= 1.16 \times 10^{-4}$

Other techniques for obtaining needed information were considered. For example, a technique commonly applied when empirical data are not available is the use of simulation. However, this was rejected since the complex interrelationships among relevant variables were not known, and a mere random generation of vulnerability probabilities was considered inadequate. The technique that was determined to be most valid in view of the difficulty in obtaining reliable and thorough empirical data was the Delphi technique. Accordingly, this technique was used for generating the necessary vulnerability probabilities in the Generic Vulnerability Analysis and the vulnerability analysis of a typical implementation of the design requirements. Use of this technique made it possible to consider the numerous variables related to each probability value and generate a single value.

The Delphi technique uses a group of persons, in this case a panel of experts in the security and safeguards field, and provides a dynamic procedure for forming consensus in the estimation of values. It is particularly useful in a situation such as the one faced in this study where complex relationships must be analyzed and quantitative values determined. Each expert can consider these relationships and develop a value based on his perception of the situation (adversary action–protective mechanism confrontation) and his experience with similar situations. The varying opinions of individual experts are then reduced to a single consensus through successive evaluations based on the feedback of information from each evaluation. The participants are asked not only to assign values but also to provide a rationale for them. This information is analyzed by the project staff and provided to participants at each successive stage until consensus is reached. In this application of the technique, this communication framework was also used as a learning experience from which insight was gained for improvement of the safeguards system concepts.

The Delphi technique was used in the generic vulnerability assessment, in which a panel of experts skilled in relevant fields was convened. A set of adversary action sequences was provided to each member along with a description of each protective mechanism in the generic safeguards system. Each member was asked to estimate the individual PM vulnerability values and enter them in a matrix. The project staff then reviewed the scores and developed a set of questions for each panel member concerning assigned values that had significant variance or appeared extreme. These questions were explored with each panel member individually, and an opportunity for adjusting the values was given. These values were then discussed in a group session in which a final opportunity for value adjustment was given. These final values were then analyzed by the project staff and a consensus value was computed.

In addition, the panel was asked to evaluate overall protective mechanisms and to discuss the relative merits of each. The panel was also asked to comment on the significant aspects of the adversary action sequences.

The methodological decision to consider PM's as independent rather than interdependent facilitated the vulnerability analysis described above. It also provided an important benefit that aided the study considerably, because it showed which PM's were highly vulnerable and which were highly invulnerable. If PM's had been considered as interdependent, it would not have been possible to assess the vulnerability and, therefore, the significance of each PM. The fact that it was possible to assess individual PM's facilitated the development of the design requirements, which of necessity had also to be conceptualized in terms of a number of independent requirements.

The application of the methodology is described in Chapter 4.

2.3.3 An Example

The matrix shown in Table 2-2 is typical of those obtained in the generic vulnerability analysis. It demonstrates the results of a hypothetical vulnerability assessment of a Protective System X against a Dedication classification of adversary actions. The following points are made:

- This is the nth interaction matrix.
- Three levels of dedication were considered: low, medium, and high threat levels.
- The relative frequencies of occurrences of such attacks were determined to be .75, .2, and .05 respectively.
- Protective System X consisted of ten protective mechanisms.
- The numbers under each PM_1 were the assessed vulnerabilities of the particular protective mechanism against the various attacks.
- The vulnerabilities of the safeguards system to the low, medium, and high threat level attacks were 1.62×10^{-7}, 7.00×10^{-5}, and 2.03×10^{-3} respectively.
- The threats posed to the system by the different levels of attack (here, relative frequency of occurrence is taken into account) were 1.22×10^{-7}, 1.40×10^{-5}, and 1.02×10^{-4}.
- The overall safeguards system vulnerability was 1.16×10^{-4}.

The following conclusions can be drawn:

- "Dedication" is an important characteristic of adversary actions because changes in dedication are reflected in alterations in vulnerability. (A low vulnerability corresponds to a low level of dedication, etc.)

- The division into three levels of dedication is worthwhile because each threat level has a different vulnerability. Thus, no two levels of dedication represent the same threat.

- Protective System X is a reasonably well-designed safeguards system because the majority of protective mechanisms provide significant defenses. (It is only PM_1, PM_2, and PM_8 that are ineffective.)

2.4 Development of Design Requirements

To conduct the development activity, it was necessary to conceptualize design requirements for potential safeguards that would provide protection against each form of attack for each stage in the transport sequence. Subsequently, these requirements were evaluated in terms of their effectiveness and reasonableness. They were then combined into subsystems, the vulnerability of which was assessed. Finally, the impact of each requirement on the transport of nuclear fuel and on society was evaluated. The development activity took the information generated from the previous subtasks as major inputs. The adversary action sequence analysis provided information on the types of threats to be protected against, and the generic vulnerability assessment provided information on the effectiveness of the various safeguards measures. In addition, a literature review provided information on the wide range of safeguards measures being used or considered in the nuclear industry and others requiring security.

The method used in developing the safeguards system design requirements was based on the use of information such as that shown in Tables 2-2 and 2-4. The tables provided a structure for identifying design requirements, ensuring that safeguards were identified for each aspect of the transport sequence, and helping to determine the relationships among system elements.

The primary design chart is in matrix form. One axis describes the transport sequence: pre-transport, loading and unloading, in-transit, and post-diversion. The other axis is comprised of the safeguards systems functions of deterrence, detection, defense, and consequence reduction. Both axes are described in greater detail on the chart. Strategies were entered into each cell of the matrix to indicate approaches to safeguards that would fulfill the safeguarding function for the part of the transport sequence corresponding to that particular cell. Filling all cells in the matrix with one or more strategies

ensured that all safeguards functions were considered for all the sequences in the transport of materials. Table 2-3 portrays the matrix, with a few sample strategies entered in appropriate cells.

When all strategies had been determined, they were translated into objectives, which, in turn, were translated into design requirements that, when implemented, would fulfill the objectives. The process is shown in Table 2-4.

A set of forms like that in Table 2-4 was completed for each mode of transport and for each type of attack (force, stealth, deceit). The design requirements were then organized and combined into subsystems based upon a commonality of objectives. The subsystems were in turn integrated into safeguards systems. It was then possible to conduct a first order vulnerability assessment on the systems and to evaluate their impact on the nuclear fuel cycle and on society.

2.5 Vulnerability Assessment of Design Requirements

The vulnerability assessment of the design requirements was accomplished in a different fashion from that used in the generic vulnerability assessment. The significant point that needs to be understood is that the recommendations that are made are for design requirements for system concepts, not for safeguards systems themselves.

It is plainly not possible to quantify the vulnerability of a concept. For example, it is impossible to quantify the vulnerability of the concept of an armed escort. The detail needed to do this would involve the refinement of the concept to that of a specification or protective measure, rather than a design requirement. For example, how many guards should there be? What kinds of weapons should they carry? Thus, in order to evaluate the efficiency of safeguards concepts, it would be necessary to study all the possible safeguards systems that could be developed from the safeguards concepts. Such a task was infeasible and impractical.

A two-staged approach was taken. In the first stage, a panel of experts was convened; in a structured discussion, they described improvements in the design requirements needed to achieve a specified level of vulnerability. Each design requirement was analyzed from many perspectives, and the following questions were put to the panel:

- Does the design requirement under consideration offer a reasonable amount of protection when the effort that would be required to implement it is considered?

TABLE 2-4: STRATEGY, OBJECTIVES, AND DESIGN REQUIREMENTS

STRATEGY (Examples Only)	OBJECTIVE (Examples Only)	DESIGN REQUIREMENT (Examples Only)
Minimize transport distances	To lessen the chance of the material being acted upon while on the road	Co-locate or make the facilities close to one another
Minimize transport time	To lessen the chance of materials being acted upon	Increase vehicle speed Ship during low traffic hours
Keep transport origin/destination/ routing secret	To keep the enemy uninformed	Secret procedures and shipping schedules
Intelligence gathering along transport route	To obtain advance information to uncover potential adversary actions so special precautions can be taken	Interface with intelligence gathering agencies
Haul an escort/monitoring system	To keep materials under guard and their location known at all times	Escort/surveillance/communication system installed
Use transport containers/vehicles that are difficult to move	To impose a difficult equipment requirement on the adversary, thereby increasing the probability of detection	Proper design of containers and vehicles
Random scheduling of movements	To lessen the chance of materials being acted upon	Random number generation techniques for schedules

- What level of implementation of a design requirement is necessary for an adequate safeguards system?
- Are there any interrelationships between the design requirement under consideration and the others? If so, what are they?
- Are there any omissions in the design requirements in this Conceptual Safeguards Subsystem?
- How can an adversary overcome this Conceptual Safeguards Subsystem?
- Are there any deficiencies in the design requirements as a whole? As a corollary to this – is there a credible way for an adversary to steal SSNM in the transportation cycle?

Various safeguards philosophies were also considered. For example, the panel discussed whether reliance should be placed on a strong escort force rather than on a response force capability, and vice versa.

The panel also discussed the various impacts that the safeguards would have on the nuclear power industry and on society at large. There is a full discussion on these impacts in Chapter 6.

The method of detailed discussions with acknowledged experts can be criticized, because of the lack of precise quantifiable results. However, because of the nature of the problem, the state of the art, and the desire to make realistic recommendations, the Delphi approach appears both sound and valid. A safeguards study involves a large number of sociological considerations. As a consequence, it cannot be hoped to obtain vulnerabilities in the same manner that they are obtained in safety studies in nuclear power plants. More precise quantifiable analysis may be possible; however, it would necessarily be more complex than simple calculations involving probabilities. Safeguards have many interrelationships. To effectively understand the interrelationships involved in safeguards, more sophisticated multivariate techniques, such as Principal Components Analysis, would need to be used. Even so, there would be some unknowns that would make an accurate assessment of absolute frequencies extremely difficult. The revolutionary techniques of Catastrophe Theory as expounded by Rene Thom in "Stabilite Structurelle et Morphogenese" may offer one way of approaching this problem. However, such highly detailed and complicated techniques were beyond the scope of this study.

In the second stage of vulnerability analysis, an assessment was carried out using the methodology of the Generic Vulnerability Analysis. To facilitate this, a typical implementation of the recommended

design requirements was used along with previously developed adversary action sequences. The results were used to confirm the finding of the first stage assessment.

CHAPTER 3

ADVERSARY ACTION SEQUENCES

3.0 ADVERSARY ACTION SEQUENCES

3.1 Characterization of Adversaries

The potential adversaries were characterized in terms of the probability of their attempting malevolent action against an SSNM shipment and the potential for their success in such an attack.

As assessment of the likelihood of an attempted adversary attack is a complex matter. There are many factors involved, including the political and economic climate, the safeguards in operation, and the background and resources of potential adversaries. For the purposes of this study the primary characteristics selected for describing adversaries were: type objectives to be accomplished by the action; and the use to be made of the SSNM following a successful attack. The information and insights obtained from these descriptions played a key role in the estimations of frequencies of attacks, which are detailed in Chapter 4, Generic Vulnerability Analysis.

There are three major types of adversaries as described in Table 3-1. Examples of the motivation of each type are shown in Table 3-2.

Major adversary objectives include:

- Revenge
- Personal Gain
- Political or Sociological Gain

The adversaries may also be classified by the use to which they intend to put the SSNM. This classification includes:

- Detonation of a Nuclear Device
- Dispersion
- Blackmail (Political or Financial)
- Sale to Third Party
- Sabotage

TABLE 3-1: TYPES OF ADVERSARIES

CRIMINAL	DISSIDENT	DEMENTED
Individual	Individual	Individual
Ad Hoc	Employee	Sociopathic
Professional Criminal	Separatists (Domestic)	
	Revolutionaries (Domestic)	
	Reactionaries	
	Violent Issue-Oriented	
	Anarchists	
	Separatists (Foreign)	
	Revolutionaries (Foreign)	

TABLE 3-2: ADVERSARY TYPE BY MOTIVATION

CRIMINALS	DISSIDENTS	DEMENTED
• those who obtain SSNM – in order to resell it to the owner – in order to sell it to another buyer including a foreign nation – in order to hold it for a reward – in order to extort payment under threat of malevolent use	• those who seek political gain through the acquisition of SSNM such as release of political comrades • those who seek other kinds of gain based upon their value system	• those who seek attention or publicity • those who want to destroy the nuclear industry at any cost • those whose behavior is irrational or antisocial • those insiders who are "angry" at the system

Using the above classifications, analyses were performed of the range of potential adversaries who might attempt an attack on an SSNM shipment. Those classes of adversaries found inportant in this context were described for utilization in the vulnerability analyses. In addition, estimates were made of the probabilities of attack based on data from other forms of malevolent action by groups with similar characteristics.

3.2 Adversary Capabilities and Resources

The capability of an adversary group to successfully execute an action sequence was determined to relate most essentially to the resources and approach taken by the adversary. Table 3-3 lists the characteristics relevant to estimation of success. These attributes classify the various elements of resources and capability which a given adversary may possess. Each may have a separate value. For the purposes of this study, each was subdivided into three or four values based on a high, medium, or low level of resources as described in Table 3-3. The value of each attribute will also affect the composition of any action sequences which are to be developed. A very large number of possible combinations of these characteristics is possible.

The information required from previous analysis was studied and descriptive information for each attribute was generated. This information was used in selecting the sequences to be developed and in describing each sequence. The relationships among the attributes were evaluated and the potential number of combinations was reduced significantly to those which would be meaningful in the planned vulnerability assessment.

In theory, all the attributes discussed in Sections 3.1 and 3.2 could vary independently, and thus, potentially give rise to millions of different action classes. However, in reality a great many possibilities can be ruled out. For example, if the nuclear expertise (within "Knowledge and Experience") is low, then the fabrication of a bomb is not viable. Therefore, our initial approach was to reduce this total to a reasonable number of adversary actions which were determined to be feasible (see Appendix A).

In addition, those attributes which would prove most useful as control elements in the assessment were identified. For each class within these, an adversary action sequence was produced.

3.3 Action Sequence

To provide a basis for the vulnerability assessments of the safeguards systems, it was necessary to develop adversary action sequences. Each sequence is based on achieving some final action or end event and includes a series of steps necessary to achieve that event.

TABLE 3-3: RESOURCE CHARACTERISTICS OF ADVERSARY

NUMBER OF PERSONNEL		
a.	Low Threat Level	1–6
b.	Medium Threat Level	7–12
c.	High Threat Level	13 +
ARMS		
a.	Low Threat Level	Guns, Pistols, Rifles
b.	Medium Threat Level	Automatic Weapons
c.	High Threat Level	Rockets, Bazookas, Mortars
INTELLIGENCE AID/INFORMATION		
a.	Low Threat Level	Casual Observations
b.q	Medium Threat Level	Extensive Observations
c.	Medium-High Threat Level	Infiltration in Non-Sensitive Position
d.	High Threat Level	Infiltration in Sensitive Position
KNOWLEDGE AND EXPERIENCE		
a.	Low Threat Level	Casual
b.	Medium Threat Level	Literative Search; Explosive Capability
c.	High Threat Level	Detailed Understanding of Security Systems; Combat Experience; Nuclear and Explosives Expertise
DEDICATION		
a.	Low Threat Level	Casual
b.	Medium Threat Level	Sustained Discomfort and Injury
c.	High Threat Level	Willing to Accept Loss of Life
ORGANIZATION, PLANNING, TRAINING, AND SECURITY		
a.	Low Threat Level	Casual
b.	Medium Threat Level	Substantial: Overall Tactical Planning; Well Organized
c.	High Threat Level	Extensive: Detailed Planning; Disciplined Organization; Extensive Training; Safe Haven Prepared
MONEY		
a.	Low Threat Level	0–$5,000
b.	Medium Threat Level	$5,000–$100,000
c.	High Threat Level	$100,000 +
TRANSPORTATION		
a.	Low Threat Level	Station Wagon, Pick-up Truck
b.	Medium Threat Level	Cars, Vans, Light Trucks
c.	High Threat Level	Light Planes, Heavy Duty Trucks
EQUIPMENT		
a.	Low Threat Level	Hand Tools
b.	Medium Threat Level	Power Tools, Explosives
c.	High Threat Level	Heavy Duty Fork Lift, Radiation Protection

As stated in Section 3.2, three end events were considered in the study. The description of the transport sequence to be attacked also influenced the action sequence. Based on each of these events and the transport sequence, a logical set of actions leading to their accomplishment was generated.

To reduce the number of adversary action sequences to be developed, the initial set of sequences was analyzed and a generic sequence was developed, consisting of a basic set of actions which might be followed to achieve any desired event. A list of steps in the sequence is depicted in Table 3-4. The generic sequence was then used as a framework for the development of specific sequences for use in the vulnerability assessments.

The development of the sample sequences had to be performed from the viewpoint of the adversary and had to match the transport system to be attacked. The attack mode chosen by the adversary will depend upon the resources and attributes at his disposal and be influenced by his perception of the probability of success. The latter will also bear heavily upon whether he will even attempt to implement the plan for any given set of circumstances.

An adversary will try to optimize his potential to mount a credible threat by using the following methods:

Maximize	Minimize
Dedication and Motivation	Number of Personnel Involved
Intelligence Information	Number of Thefts
Planning, Organization, Training	Complexity of Plan
Security	Intelligence Indicators

These issues were taken into consideration in the development of adversary action sequences. The transport system used was important in determining the adversary action sequence. In the case of the vulnerability assessment of the generic transport system, the safeguards system focused primarily on defense against a force attack and so the sequences follow this mode. In the latter assessment, stealth and deceit were also considered.

Examples of the sample sequences utilized in the study are to be found in Appendix C. Those developed for the generic vulnerability assessment consisted of the following classes:

TABLE 3-4: GENERIC ADVERSARY ACTION SEQUENCE

ESTABLISH OBJECTIVES

Revenge
Personal Gain
Political/Sociological

DETERMINE INTENDED SSNM USE

Detonation of a Nuclear Device
Dispersion
Political Blackmail
Financial Blackmail
Sale to Third Party

SELECT THE TARGET

Toxicity/Radioactivity/Quantity of SSNM
Plutonium, Uranium, or Mixed Oxides
Penetration Point in Transport Cycle: Reprocessing–Storage–Fuel Fabrication–Power Plant–Reprocessing

FORMULATE ATTACK PLAN

Define Requisite Resources and Attributes
Select Operational Mode (force, stealth, deceit, or combinations thereof)
Define Acceptable Degree of Personal Risk
Establish Specific Responsibilities and Sequence of Activity (timing, resource utilization, facility location and preparation, training, contingency actions, intelligence gathering)

ACQUIRE RESOURCES

Insiders/Outsiders (specific talents, knowledge, training)
Specialized Equipment/Facilities
Money
Arms

PRACTICE AND TRAINING

IMPLEMENT THEFT

Intercept Shipment
Overcome Safeguards
Acquire SSNM
Make Getaway

FULFILL INTENDED USE OF SSNM

(With the possible exception of fabrication of a missile device, it is reasonable to assume that an adversary with the resources to accomplish theft of SSNM, has the capability of accomplishing his objectives.)

- Number of Personnel
- Intelligence Aid/Information
- Efficiency (a composite of Knowledge and Experience, Dedication, and Organization, Planning, Training, and Security)

The first two classifications highlight changes in the "Force" and "Force/Deceit" modes of attack, respectively. The third classification was created by the Delphi panel in the generic vulnerability analysis. These adversary action classes reflected the experts' perceptions of the weaknesses in the safeguards systems. A synopsis of one of these adversary actions is shown in Table 3-5.

For the vulnerability assessment of the recommended system design requirements, the classes of adversary action sequences utilized were based on the mode of attack (force, stealth, deceit) rather than on the classes used in the generic assessment. It was decided that the mode of attack was the single best parameter for assessing vulnerability. The sequences developed were described in a standard format and these descriptions were incorporated in the package of information provided to each panel member during the assessment.

TABLE 3-5: REPRESENTATIVE ADVERSARY ACTION – LOW THREAT – LEVEL – NUMBER OF PERSONNEL CLASSIFICATION

Transport Mode	Highway
Adversary Type	Dissident
Objective	Political/Sociological
Intended SSNM Use	Detonation
Number of Personnel	Low Threat Level – 4 People
Arms	Pistols, Rifles, Automatic Weapons
Intelligence Aid/Information	Extensive Surveillance
Experience and Knowledge	Some Combat Experience and Nuclear Expertise
Dedication	Willing to Accept Sustained Discomfort and Injury
Organization, Planning, Training, and Security	Substantial
Mode of Attack	Force/Deceit
Attack Plan	Extensive surveillance determines schedule of plutonium oxide shipment. Traffic is diverted from shipment. A crash is faked to block road in front of convoy. The adversaries approach convoy with "Police" car and attack convoy personnel. Truck doors are blown open and the SSNM is removed by hoist into van. Adversaries drive off.

CHAPTER 4

GENERIC VULNERABILITY ANALYSIS

4.0 GENERIC VULNERABILITY ANALYSIS

4.1 Information Generation

The first requirement of this portion of the effort was the definition of the generic SSNM transport sequence. A literature review and analysis of Federal regulations was made. To provide insight into the significance of variation in safeguards measures, it was decided to utilize three levels of safeguards systems. The three levels selected were:

- Existing NRC Regulations
- Current Transport Practice
- Heavily Protected Shipment

Descriptions of the three systems were developed in terms of the protective mechanisms (PM) comprising the system. This information was also used in the development of adversary action sequences in that subtask. Descriptive material on the three generic systems is provided in Table 4-1, and a complete description is found in Appendix C.

Three classes of adversary actions were also used:

- Number of Personnel
- Intelligence Aid/Information
- Efficiency

The adversary action sequences for each of these classes developed in the previous subtask were used. Table 4-2 provides a summary of the characteristics of each, and Appendix C includes a complete description of each adversary action.

For each classification, the key characteristic was varied in each adversary action while the remainder of the characteristics varied little from sequence to sequence. This set of sequences and safeguards provided a broad range of alternatives for evaluation.

The data describing vulnerability values were then generated. Since these data were not available from the literature search or other sources, the Delphi technique was used to generate them.

TABLE 4-1: SAFEGUARDS SYSTEMS A, B, AND C

PM	SAFEGUARDS SYSTEM A	SAFEGUARDS SYSTEM B	SAFEGUARDS SYSTEM C
PM1—Vehicle Velocity	No unnecessary intermediate stops	Same as A	Non-stop, no detour; routes checked out shortly before convoy passes through
PM2—Presence of the crew in the truck cab	Two unarmed crew members	Two trained crew members armed with M-16's	Two trained crew members in truck cab with handguns and automatic firearms
PM3—Presence of an armed escort	One escort car with two armed guards	Two escort cars with two armed guards in each car	Five escort vehicles with approximately 14 armed and trained crew members
PM4—LLEA response force	Normal routine LLEA operating	Same as A	Same as B, but convoy has radio link with LLEA
PM5—Specially designed truck	Truck walls one inch thick — doors have reinforced locks	Same as A – Also truck has immobilization devices, bulletproof cab, alarm system to release foam barrier around SSNM	Truck is a 5-axle semi trailer with inner armored container, access denial system, immobilization system and deterrent control system
PM6—Container weight, lock and temper seal	SSNM is locked and sealed in heavy (500 lb.) containers	Same as A	SSNM is locked and sealed in containers weighing not less than 2000 lbs.
PM7—Minimal transit time	Plan routes to minimize transit time. If 1 hour, only the driver need be in the truck cab.	Same as A.	Distances travelled vary from 50 to 150 miles.
PM8—Convoy camouflage	Ordinary in appearance but marked with identifying numbers or letters. Escort car is ordinary in appearance.	Same as A.	None
PM9—Natural wariness of unusual activities	Catch all protective mechanisms to maintain alertness	Same as A	Same as A and B
PM10—Personnel screening		Background checks and psychological tests for relevant personnel	Screen all personnel concerned with convoy
PM11—Hardware Security		Truck and escort cars kept in secure facility	Same as B
PM12—Convoy information security		Six options for schedule/routing. Decision made one week before.	Same as B

TABLE 4-2: SUMMARY OF ADVERSARY ACTION SEQUENCE CHARACTERISTICS

CLASSIFICATION	CLASSES	TYPE	MODE	USE
Number of Personnel	Low – 4 People	Dissident	Force/deceit	Detonation
	Medium – 8 People	Dissident	Force/deceit	Detonation
	High – 20 People			
Intelligence-Information	Low – Casual Observers	Demented	Deceit/force	Financial blackmail
	Medium – Detailed Surveillance	Demented	Deceit/force	Financial blackmail
	Medium/High – Insider in non-sensitive position	Demented	Deceit/force	Financial blackmail
	High – Insider in sensitive position	Demented	Deceit	Financial blackmail
Efficiency	Low – Little experience, training, and dedication	Demented	Force/deceit	Sabotage
	Medium – Reasonable experience, training, and dedication	Dissident	Force	Political blackmail
	High – Extensive training, planning, and experience	Dissident	Force	Detonation

A package of materials was produced for each panel member describing each safeguards system and its protective mechanisms and each of the adversary action sequences. Also included was a set of matrices to be completed in the Delphi session. The panel was convened, introduced to the project, and briefed on the Delphi session and what they would be expected to do over a 2-day period.

For the first two adversary action classifications, the panel of experts of the Delphi session was provided with representative action sequences. For the final classification, the panel was requested to construct the representative adversary action sequences themselves, having formed their own perceptions of how the safeguards systems could be best attacked.

In compliance with the methodology, the Delphi panel assessed the vulnerabilities of the safeguards systems against the various adversary actions and entered scores (their estimates of the vulnerability) of safeguards systems to the various adversary actions on the forms provided. They were instructed to give a value from 0 to 1, where 0 indicated complete defeat of the adversary and 1 indicated no PM impact on the adversary. Initially, each panel member gave an individual assessment for each cell (see Table 4-2). The results were reviewed by the staff and individual meetings were held to explore the scores assigned. Scores were adjusted if necessary in these individual meetings. A panel-staff discussion followed, in which differences were reconciled and a joint opinion was expressed. A structured discussion of issues noted by the staff during the Delphi session was also held with the panel. Information on these discussions was recorded for use in the development of design requirements. The data from the session were analyzed and composite values computed. Table 4-3 provides an example of the completed assessment matrices.

The three safeguards systems, the representative adversary actions, and the panel's vulnerability assessments are described in detail in Appendix C.

4.2 Conclusions of the Panel

The Delphi panel expressed many views and formed numerous conclusions during the Generic Vulnerability Assessment. The statements below describe comments and opinions that pertain to the various protective mechanisms considered in the Delphi session.

- Unless a convoy operates on a non-stop, no detour basis, together with route reconnaisance, etc., there is little difficulty in bringing the convoy to a halt and, consequently, the motion of the truck offers little protection.

TABLE 4-3: ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX NO. 5

INTELLIGENCE AID/INFORMATION CLASSIFICATION–PROTECTIVE SYSTEM B

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS														
NO.	$P(S_k)$	INTELLIGENCE AID/ INFORMATION	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security		V_k	$P(S_k)V_k$
2A	.40	Low – Casual Observations	.5	.4	.15	.7	.1	.95	.6	.8	.6	1.0	1.0	1.0		5.7×10^{-4}	2.3×10^{-4}
2B	.50	Medium – Extensive	.5	.4	.15	.7	.1	.95	.65	.85	.45	1.0	1.0	1.0		5.0×10^{-4}	2.5×10^{-4}
2C	.80	Medium High -- Insider in Non-sensitive Position	.55	.4	.1	.7	.1	.95	.65	.85	.4	.3	.3	.4		1.2×10^{-6}	9.3×10^{-8}
2D	.02	High – Insider in Sensitive Position	.8	.9	.25	.75	.99	.95	.9	.9	.4	.2	.3	.4		9.9×10^{-4}	2.0×10^{-5}

SAFEGUARDS SYSTEM VULNERABILITY

$$= \sum_{k=1}^{4} P(S_k)V_k$$

$$= 2.3 \times 10^{-4} + 2.5 \times 10^{-4} + 9.3 \times 10^{-8} + 2.0 \times 10^{-5}$$

$$= 5.0 \times 10^{-4}$$

- The protection supplied by the truck crew and the armed escort is proportional to their sophistication, the arms they carry, and the number of them that are present.

- The Local Law Enforcement Agency (LLEA) gives very little protection unless a well-trained response force is on alert while the convoy is in progress and there is an excellent communications system between the convoy and this force.

- The truck and container afford very good protection if they have effective immobilization and impenetrability devices.

- Transit time and camouflage are not very important. (Note that these conclusions were reached under an assumption of daylight travel.)

- Personnel security, hardware security, and schedule security offer good protection, where they are relevant, and are vital parts of a safeguards system.

- The catch-all protective mechanism "Natural Wariness" is quite effective. (This indicates that security awareness training, etc., is necessary in nuclear transport.)

4.3 Overall Assessment of Safeguards Systems Vulnerabilities

After the panel members had made their assessments of the vulnerabilities of the protective mechanisms that comprise the safeguards system, the following question was posed to them: "What are your assessments of the overall vulnerability of the safeguards systems to the various adversary actions?" Their composite views are listed in Appendix C and summarized in Table 4-4. The responses show a much higher vulnerability when compared with the vulnerabilities computed from the individual PM assessments.

Several explanations can be given for this phenomenon.

- In evaluating very small vulnerabilities, most people see little difference between 10^{-3} and 10^{-6}; thus, the assessment of 10^{-3} by the panel really represents the same impression as an assessment of 10^{-6} and is better expressed by saying the vulnerability is negligible.

- The panel gave vulnerabilities of .5 to each of three protective mechanisms. When asked to form an overall view, they carried over the impression of "fifty-fifty" likelihood of overcoming

TABLE 4-4: COMPARISON OF OVERALL VULNERABILITIES FOUND BY COMPUTATION AND PANEL ASSESSMENT

ADVERSARY ATTRIBUTE	SYSTEM A	SYSTEM B	SYSTEM C
Number of Personnel			
Computed	1.4×10^{-1}	1.6×10^{-3}	3.4×10^{-8}
Panel Estimate	6.2×10^{-2}	2.6×10^{-2}	5.8×10^{-4}
Intelligence Aid/Information			
Computed	2.0×10^{-1}	5.0×10^{-4}	5.1×10^{-8}
Panel Estimate	3.5×10^{-2}	5.0×10^{-3}	3.4×10^{-4}
Efficiency			
Computed	3.1×10^{-1}	2.2×10^{-2}	1.8×10^{-5}
Panel Estimate	6.4×10^{-1}	3.0×10^{-1}	7.6×10^{-3}

the defenses and, consequently, also gave a .5 vulnerability to the three protective mechanisms as a whole.

- The methodology leads to inaccuracies because of its reliance on the independence of protective mechanisms. The panelists, appreciating the fact that the various safeguards are interrelated and interdependent, formed impressions of safeguards systems vulnerability that took these factors into account.

From discussions with the panelists, it is clear that all of these explanations have some validity. From a methodological point of view, the last explanation is most important. It reinforces the previous comments concerning the interdependence of protective mechanisms and highlights the difficulty of obtaining accurate measures of vulnerability. See Appendix B.

4.4 Findings

The conclusions of the panel expressed earlier are not repeated here. This section is based on a study of the results of the Delphi session and the vulnerability assessments described in detail in Appendix C.

The first conclusion is that Safeguards System A (see Table 4-1 for system definitions) offers inadequate defense against the types of threats considered. Safeguards System B offers considerably more defense against all forms of attack, though it is still quite credible for an adversary to succeed. It is only in Safeguards System C that credible adversary action could be defeated with reasonable certainty.

In comparing the Number of Personnel and Intelligence Aid/Information classifications, it can be seen that the safeguards systems vulnerabilities do not differ widely for each of the three safeguards systems. This supports the view that the selected adversary actions are indeed representative and the overall impressions of the safeguards systems vulnerabilities are reasonable.

The assessed vulnerabilities for the Efficiency classification against Safeguards Systems B and C are somewhat different from those of the other classification. There are several pertinent comments that can be made here. First, the similarity of the results for Safeguards System A against all three classifications may be reasonably explained by the overall weaknesses of System A. Because of the relative ease with which any adversary could overcome the safeguards, there is not much difference between the results when any of the adversary attributes is considered.

The dissimilarities between the estimated vulnerabilities for the Efficiency and other classifications of adversary actions are explained by the attack purpose of Representative Adversary Action No. 3A (see Appendix C). The purpose of the adversary, in this attack, is to cause dispersion of plutonium oxide at the scene of the attack. Action 3A was used to test the study assumption that the safeguards against theft would also offer protection against sabotage. The Delphi panel, while agreeing with this view, identified sabotage attempt as a major threat. Consequently, when they constructed representative adversary actions, they designed such an incident and this adversary action was analyzed.

The consideration of a sabotage attack confirmed two assumptions. It did show that there was defense against such attacks, but it also showed that the vulnerability was significantly higher than attacks from more formidable adversaries whose purpose is theft of SSNM.

At a more detailed level, the following points were expressed by the panel:

- Training has a large impact on the efficiency and strength of the defenses.
- Security clearances are effective provided they are at a sufficiently high level. A routine check with local police departments for criminal records is not sufficient.
- A helicopter escort was viewed as a very useful defense in as much as it could coordinate the convoy, survey the surrounding area, sound an alarm, and keep the SSNM under observation until a response force arrived.
- The actual frequency of shipments would have a significant impact on defenses in at least two ways. First, if shipments occurred frequently, there would be little difficulty in an adversary locating a convoy. Second, frequent shipments make it more difficult for LLEA's to provide adequate protection.
- Secrecy is very important. People should receive information on a need-to-know basis, and all decisions, etc., should be made at as late a date as possible.

One of the major problem areas is the lack of data concerning absolute frequencies of attacks on SSNM shipments and relative frequencies of various kinds of attack. This matter was discussed with the panel and the following views were expressed.

- No one has any substantial knowledge concerning absolute frequency of attacks.

- The actual population size/distribution of criminals, dissidents and demented groups has a large bearing on the above frequencies.

- The visible strength of the safeguards system acts as a deterrent. As the strength of the defenses increases in the perception of the adversary, so will his reluctance to attack increase. As a consequence, there will be relatively fewer low sophistication/strength attacks against an improved safeguards system.

- A majority of attacks will take the form of harassment, with the purpose of causing adverse publicity to the nuclear power industry.

The panel pointed out some deficiencies in the methodology:

- If a PM is extremely effective, it might force the adversary to attack the system in a different fashion, thus bypassing this effective safeguard. Thus, one must be careful with the interpretation of the results.

  For example, if schedule security within the plant is extremely tight, the adversary may be forced to rely on external surveillance to determine the convoy route. Thus, schedule security is inapplicable in the vulnerability analysis, but it is certainly effective.

- The latitude in interpretation of the Representative Adversary Actions, which was necessary when evaluating them against different safeguards systems, caused wide variations in assessed vulnerabilities. The panel members assessed the representative adversary actions in different ways, and, consequently, they formed different opinions of the vulnerabilities.

As a final comment on the safeguards systems, Table 4-5 shows the results of the panel's comparison of the protective mechanisms vis-a-vis their importance.

The panel also expressed opinions concerning adversary attributes.

- There are only a small number of highly sophisticated adversary groups in existence.

- It is unlikely that a low resource group would stage an attack. Some intelligence information would always be available and an ineffective attack strategy would not get beyond the planning stage.

TABLE 4-5: IMPORTANCE OF PROTECTIVE MECHANISMS

RANK ORDERING AS TO IMPORTANCE WITH 1 BEING FIRST	PROTECTIVE MECHANISM	IMPORTANCE ON A SCALE OF 1—10, WITH 10 BEING MOST IMPORTANT
1	Truck Crew (armed, trained)	9
2	Armed Escort (trained)	9
3	Truck (protective, alarms)	8
4	Natural Wariness	8
5	LLEA (aware, prepared)	7
6	Personnel Screening	7
7	Hardware Security	6
8	Schedule Security	5
9	Container (500—2000 lbs.)	5
10	Vehicle Velocity	3

- A politically motivated attack with the purpose of holding an SSNM convoy for ransom, or for onsite dispersion, etc., is more likely than an attempt to construct an explosive device.

- Although terrorist groups are making gradual advances in the use of technology, the majority of them have only a low technical capability.

- There is less chance of an adversary infiltrating the nuclear power industry than attacking it. Only a few groups have the capabilities to attempt penetration.

The panel expressed views on the relative importance of adversary resources and attributes as shown in Table 4-6. For purposes of comparison, the resources and attributes were assumed to be at the same threat level. The experts expressed more definitive opinions as the threat level increased. For example, in comparing "Dedication" and "Arms" at a low threat level, it was not evident that "Dedication" was a more important attribute. However, at a high threat level, "Dedication" was definitely perceived to be more significant by the panel of experts.

The low rating for "Money" does not imply that this is an insignificant resource to an adversary. It simply means that the other resources are more important to him than money. This is not illogical because most things that can be obtained with money (including personnel services) can also be obtained through theft or blackmail. However, the adversaries will incur an additional risk if they choose to steal or to blackmail rather than obtain equipment or services legitimately.

Finally, a few other issues were discussed that are of interest. The following opinions were expressed:

- An intelligence network is a useful defense. It should involve coordination with other government agencies for the purposes of gathering information.

- One must consider the possibility of any employee being subverted; no one is sacrosanct.

- The vulnerability assessments express a intuitive feeling of the panel. It would be more accurate to give a range of vulnerability rather than a particular value.

- There is little value in making comparisons between the vulnerabilities with the objective of identifying the major threats. If any adversary action poses a credible threat, then it must be addressed and defended against.

TABLE 4-6: IMPORTANCE OF ADVERSARY ATTRIBUTES

RANK ORDERING AS TO IMPORTANCE WITH 1 BEING FIRST	ADVERSARY ATTRIBUTES	IMPORTANCE ON A SCALE OF 1–10, WITH 10 BEING MOST IMPORTANT
1	Intelligence Aid/Information	9
2	Dedication	9
3	Organization, Planning, Training, and Security	7
4	Knowledge, Experience	7
5	Number of Personnel	6
6	Arms	6
7	Transportation	4
8	Equipment	4
9	Money	1

CHAPTER 5

RECOMMENDATIONS FOR SAFEGUARDS SYSTEMS DESIGN REQUIREMENTS

5.0 RECOMMENDATIONS FOR SAFEGUARDS SYSTEMS DESIGN REQUIREMENTS

5.1 Overview

This chapter describes the main thrust of this study, namely, the development of conceptual safeguards system design requirements.

The activities performed in this portion of the study included:

- Identification of design strategies and objectives
- Development of safeguards system design requirements
- First order vulnerability assessment of design requirements
- Development of recommendations for safeguards systems

Basic safeguards strategies were examined to reduce the system vulnerability. In addition to minimizing vulnerability, constraints of reasonable cost, simple operation, and proper integration were considered in the development effort.

5.2 Safeguards Strategies

Safeguards strategies were considered in the development of design requirements basic. The range of safeguards to be developed included all elements in the transport sequence and provided all safeguards functions (deter, defect, etc.). There are numerous points in the SSNM transport sequence at which an attack may take place. In general, the adversary has the choice of attack point and so the safeguards system must be prepared to deal with an adversary action at all times. In addition, strategies such as redundancy or defense in depth were employed to achieve an acceptable level of capability.

Strategies for allocating safeguards resources or selecting emphasis among functions were also considered. For example, one might decide that a strong defense is sufficient and put few resources into detection or recovery. One might also consider a strategy based on a single tactic such as limiting SSNM shipments to small quantities below that required for construction of an explosive device (an unacceptable strategy because of the extremely large number of shipments required to support a viable nuclear fuel cycle). However, because no single tactic has proven completely effective, the realities of system implementation, the adversary's advantage in selecting place and type of attack and necessity

for defense in-depth, a balance of resource allocation and function emphasis remains the most viable strategy.

The level of resources to be applied is dependent upon the level of vulnerability to be achieved, the acceptable level of impact on the transport system and society and the perceived level of threat. One might develop a strategy employing one level of resources during times of social and economic stability while the safeguards system includes plans for the increase of safeguard capabilities if the stability deteriorates and the probability of adversary action increases. As an alternative to this the system may require at all times a level of capability required to meet maximum level of potential threat.

One might divide the overall safeguards system into several times phases.

- Prevent Attack
- Abort Attack
- Defend
- Delay
- Recover
- Mitigate Effects

These phases are not mutually exclusive but rather represent stages in the continuing protection of an SSNM shipment. They are similar to the safeguard functions of deterrence, detection, defense, and mitigation but are divided along a time sequence and each may include elements of one or more functions. Within each phase there may be one or more strategies for achieving success in safeguarding SSNM shipments.

The prevention of an attack may be achieved through deterrence measures which would discourage would-be adversaries, through secrecy procedures which limit the adversary's knowledge of the shipment or through minimizing the exposure of a shipment to potential action.

Abortion of potential actions may be accomplished through an effective intelligence system, employee alertness, or infiltration of adversary groups. This will help to detect potential actions before they occur and also stimulate action to apprehend adversaries or even change shipment plans.

Potential attacks may be avoided through security measures which deny access or through early detection leading to evasive action.

Defense of SSNM during transport is achieved through detection of the attack and defeat of the adversaries in the encounter with the use of some balance of guard forces, protective equipment, weapons, tactics and procedures, or with the use of equipment which denies access.

By use of guard force tactics, devices, and communication with a responding force, an attack may be delayed until response forces arrive. Recovery may be achieved through tactics for sealing off the area, use of additional response forces, and tracking devices.

Finally, the damaging consequences to successful adversary action may be reduced through selection of routes in low population areas and warning and evacuating the population of a hazard ones.

5.3 The Transportation Mode

The mode of transport to be utilized is of significance in conceptualizing a safeguards system. Each mode has certain advantages and disadvantages.

Each mode of transportation or a combination of modes has properties that can be examined and trade-off between benefits and limitations can be analyzed. Nuclear material belongs to a special commodity class that has a high ratio of dollar value per pound of the commodity weight. Traditionally, the shippers of these special classes have not regarded high transportation cost as a determining consideration. They have preferred top level service because of the high product value.

The following is a brief summary of the advantages and disadvantages of each of the four transportation modes (road, rail, air, and water). It is not intended to be an exhaustive analysis of the subject.

5.3.1 Road Transport

Advantages

- Road transport offers the greatest flexibility in the movement of SSNM, including the ability to transport to the scattered facilities and to avoid certain geographic areas.
- All nuclear facilities throughout the country can be reached by road.

- While road vehicles are vulnerable to adversary actions, adequate guards and escorts can reduce this vulnerability.
- Special vehicles and SSNM containers may also be used to reduce the vulnerability.
- The cost of road transport is reasonable. It is particularly cost effective in the near future when the number of SSNM shipments will be relatively low.
- There is little requirement for special equipment, other than the vehicle and containers themselves which may be built from components already available.
- Direct shipment service may be used without the need for transferring the cargo.
- Road transport is faster than the other surface modes.
- The coordination of the response force is fairly easy to attain.
- The response force can generally arrive at the attack scene with few problems.

Disadvantages:

- Highway shipment has a relatively high manpower requirement.
- The danger of attack to SSNM on the road increases with the length of the trip.
- There is a higher possibility of problems for highway travel due to fatigue of the drivers, needed repairs, and more difficult communication.
- Unavoidable remote areas must be passed through.
- Removal of containers from the attack scene may be relatively easy.

5.3.2 Rail Transport

Advantages:

- Because of the capability of carrying a heavy load and the wide size of the carrier, large secure containers may be used to increase the access time needed by the adversary to acquire the SSNM.

- Use of extremely large containers can limit adversary's capability to remove containers.
- Rail shipment is best for short distances, and well-guarded or special routes.
- The railroad is well-suited for transportation of heavy casks that contain high level wates. Because the casks are bulky and are of excessive weight, only railroad equipment can handle them.

Disadvantages:

- Railroads are limited to a few alternate routes, which are specific and well-known, and the majority of these routes pass through remote areas.
- Trains run on a familiar twenty-four hour schedule and they often keep accurately to a schedule that is easily obtainable.
- The placement of guards on the train and along the route is extremely limited.
- The escort force for rail shipment is readily identifiable, lack lateral movement to take cover during attack, and can be separated from the attack scene easily.
- Response force access to the attack site is restricted.
- The transfer points of railroad yards are poorly guarded, and easily accessible.
- The railroad service is totally depersonalized, established to handle mostly low level cost per ton commodities.
- Even with great improvement in present practices, including a dedicated train, special rolling stock, and better management, the inherent disadvantages and operational routines and inevitable interface with the presently existing railroad system would greatly handicap railroad effectiveness for the transport of SSNM.

5.3.3 Air Transport

Advantages:

- The shipment would be virtually invulnerable to force type attack while in the air.

- Use of escort aircraft or ground tracking may be used to reduce vulnerability to deceit diversion.
- Air routes may be varied frequently.
- If Short Take Off-Landing (STOL) helicopters or Lighter Train Air Vehicles (LTAV) are used, the SSNM may be picked up and delivered at the facility.
- This mode would require less expenditures on escort and protective reaction forces.
- Considering all cost factors, the "real" comparative cost of air transport, assuming effective safeguards are required, may be much lower than is generally realized.
- The hazard of crash causing radioactive release can be reduced by use of aircraft with relatively low crash speeds and by selecting routes which avoid populated areas.
- The LTAV has certain advantages such as: a reduced vulnerability to sabotage and diversion, a greater capacity for large shipments, high visibility, ease of tracking, ease of interception due to low velocity, and less hazardous accidents.

Disadvantages:

- The limited number of persons involved would make the system particularly vulnerable should outside infiltration occur.
- The rapid speed increases the probability of escape if diversion occurs though exposure time would be reduced.
- Use of conventional aircraft will require the additional use of trucks and intermode transfer to move SSNM from plant to airport.
- Air transport is generally expensive.
- A container which can withstand the impact of an air crash without releasing a radioactive hazard has not yet been developed.
- STOL have a limited flight range and payload capability.

- The STOL option would require acquisition and securing of take-off and landing space adjacent to nuclear facilities, a potentially high cost.

- LTAV require greater landing area and are not easily maneuverable for transferral of goods.

5.3.4 Water Transport

Representative candidates for waterway service are bulk and raw materials of low cost per ton values, rather than low-bulk/high value materials such as SSNM. Waterway transportation is probably the least effective mode, and is highly vulnerable to attack.

Advantages:

- The amount of time needed by the adversary to acquire the SSNM might be increased by the capability of the barge to carry extremely heavy and bulky containers.

- Delay time for adversary access to the SSNM can be created by sinking the SSNM containers.

- Waterway shipment is useful for short trips, well-guarded or special routes, and for transport of spent fuel.

- A barge can carry a large complement of guards and protective equipment.

- Water transport is very inexpensive.

Disadvantages:

- The accessability of this mode is limited to navigable rivers, lakes, or coastal waterways, and current and planned nuclear facilities are typically not located adjacent to such waterways.

- Waterways may be limited seasonly.

- Transferral of shipment to and from truck will be necessary in most cases, a very vulnerable operation.

- Traveling distances are usually several times longer by water than they would be by rail or road.
- Travel velocity is very slow, averaging five miles per hour, considering the slow velocity of tows, the necessity of multiple locking, and the slow speed of other waterway participants.
- Shipments are particularly vulnerable when passing through locks.
- Ports are another vulnerable point in that they are at present open and accessible to anyone, and they are inadequately equipped to handle SSNM shipments.
- There are unavoidable remote areas that the shipment will pass through.
- If a deceit attack occurs, the barge and attack group will be easily able to establish contact without obvious deviation from the route or schedule.

The recommendation of this study is the use of road transport in the near future and air transport at a later time when the number of shipments reaches a level to justify it, and when the present safety problems have been solved. There is a discussion of the air mode option as the long term solution later in this chapter.

5.4 Design Structure

In Section 2.4, Development of Design Requirements, we discussed the methodology used in the identification of the design requirements. This involved the use of two sets of matrices, one to identify strategies for safeguards and the other to obtain design requirements from the strategies.

The purpose of the strategy matrix (Table 5-1) was to ensure that a strategy was identified to perform each safeguard function at each stage in the transport sequence. One strategy matrix was developed for each mode of transport. The matrices were analyzed and reduced to a single comprehensive set of safeguards strategies.

A matrix translating each strategy into design requirements was produced from the strategy matrices for each transport mode. In this matrix an objective to be achieved by each strategy was determined and then design requirements which would achieve each objective were specified. Each of these matrices was also analyzed and reduced to a single comprehensive set of design requirements covering all functions for all elements of the transport sequence. (Table 5-2 provides a sample of this matrix.)

TABLE 5-1: SAFEGUARDS STRATEGIES FOR TRANSPORT SEQUENCE SEGMENTS

FUNCTION / TRANSPORT SEQUENCE	DETERRENCE	DETECTION OF: UNUSUAL ACTIVITIES	DETECTION OF: PROCEDURE VIOLATION	DETECTION OF: ADVERSARY ATTACK	DEFENSE: PROCEDURAL DEFENSES	DEFENSE: PHYSICAL PROTECTION	DEFENSE: REACTION DEFENSES	CONSEQUENCES REDUCTION
PRE-TRANSPORT								
PREVIOUS SHIPMENTS								
PLAN SHIPMENT					MINIMIZE ACCESIBILITY TO ATTACK			
PROCESS ADMIN.					INSURE INTEGRITY OFSSNM PERSONNEL & EQUIPMENT			
PREPARE MATERIAL		MAINTAIN INTELLIGENCE SYSTEM		N.A.		PROTECT SSNM EQUIPMENT & INFORMATION	ALTER SCHEDULE	
PREPARE TRANSPORT		ENGAGE HELP OF GENERAL PUBLIC			HAVE REDUNDANCY IN SAFEGUARDS			
PREPARE PROTECTION	MAINTAIN GOOD STAFF MANAGEMENT & RELATIONS							
LOADING UNLOADING	PUBLICIZE STRENGTH OF SAFEGUARDS LEGAL PENALTIES, & HARD-LINE	SURVEILLANCE	UTILIZE CHECK & DOUBLE CHECK PROCEDURES,		SECRECY ENDEAVOR TO MAINTAIN HIGH		CHECK-OUT UNUSUAL ACTIVITIES	MAKE SSNM EASILY TRACEABLE
LOAD UNLOAD VEHICLE	GOVERNMENTAL RESPONSE TO BLACKMAIL THREATS		INSTALL ALARM SYSTEMS		EFFICIENCY OF SAFEGUARDS			DENATURE SSNM
TRANSFER CUSTODY								
TERMINATE SHIPMENT	DESIGN DEFENSES TO APPEAR INVULNERABLE							
IN-TRANSIT					CONTINGENCY PLANNING			
INITIATION					MINIMIZE ACCESSIBILITY TO ATTACK			
OPERATION		DAYLIGHT TRAVEL		SURVEILLANCE, DAYLIGHT TRAVEL,	MAINTAIN CONTACT WITH CONVOY HQ. AND/OR RESPONSE FORCE	PROTECT PERSONNEL	RE-ROUTE CONVOY	
INTERMEDIATE STOPS				INSTALL ALARM SYSTEMS			OBTAIN AID FROM RESPONSE	
TRANSFER POINTS					INSURE INTEGRITY OF SSNM PERSONNEL & EQUIPMENT		FORCE WITHSTAND AN ATTACK	
ARRIVAL								
POST DIVERSION	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	RESPOND TO SSNM THEFT IN A COORDINATED FASHION

TABLE 5-2: STRATEGY, OBJECTIVE, DESIGN REQUIREMENT MATRIX
(SAMPLE PAGE)

STRATEGY	OBJECTIVE	DESIGN REQUIREMENT
Publicize strength of Safeguards, Legal Penalties, and Hardline Governmental Response to Blackmail Threats	Deter attacks through minimizing an adversary's perception of his chances of success and the consequences of failure.	Develop and conduct a continuing mass media and industry-wide program highlighting the generic Safeguards (stressing the insurmountable obstacle an adversary must overcome), the legal consequences faced by potential adversaries, the success to date of Safeguards, the dynamic nature of Safeguards (i.e., its continuous state of review and evolution so as to meet the demands of changing conditions), and the unequivocal intent to use deadly force to prevent theft. Give wide publicity to the apprehension and incarceration of any other terrorists intercepted during activities that are relevant to the generic Safeguards features. Advertise a hardline governmental position vis-a-vis response to blackmail of any kind, i.e., no capitulation to nuclear threats.
Design Defenses to appear invulnerable	Deter attacks through minimizing an adversary's perception of his chances of success	Where Safeguards features are exposed to public view, have them appear as formidable as is possible, e.g., the safe/secure trailer and tractor, escort guards well-armed and highly professional in deportment, etc. Project an image of alertness, efficiency, and impregnability.
Maintain good staff management and relations	To ensure personnel	Attract capable personnel by means of attractive salaries, benefit plans, and working conditions/requirements.

From the set of objectives identified in this matrix it was possible to identify common objectives. The next step was to group the design requirements associated with each objective into safeguards subsystems. A safeguards subsystem is a set of one or more design requirements which have a common objective.

The safeguards subsystems and design requirements were then described in a manner which would facilitate further analysis including vulnerability assessment and impact evaluation.

The panel of experts was convened and asked to evaluate the design requirements and adjust each requirement until an acceptable level of vulnerability against a specified level of adversary action was achieved. During this meeting, considerable evaluation of the reasonableness and impact of the design requirements was undertaken leading to further adjustments in the recommended design requirements. The final set of subsystems and design requirements was then evaluated by a second panel and a first order vulnerability assessment was completed.

The final set of recommended safeguards subsystems and design requirements are described in the following section.

5.4.1 Recommended Subsystems

The recommendations include two basic approaches. The first, which would be amenable to early implementation is based on the use of road transport and includes design requirements which will provide a level of safeguards vulnerability which is acceptable within the overall national safeguards objective. The second utilizes the air transport mode and provides an even greater level of security; however, certain technical problems must be solved and the number of SSNM shipments must increase before this would become a viable option. As will be noted later, several of the design requirements will require additional development or modification in authority or law before implementation. However, it is felt that the noted changes are reasonable. No recommendations are made which are thought to be "blue sky," that is dependent on a significant technological breakthrough or major change in our legal and constitutional system.

As described in the matrices presented above, the recommended systems meet the requirements for deterrence, detection, defense, and recovery/mitigation. They also include necessary attributes of redundancy (defense in depth), flexibility, and reasonableness of implementation.

The first (road) system is based on a balanced approach of procedures, guard forces, physical protection, and response capability. The second (air) emphasizes avoidance of contact with potential adversaries and so has limited guard force, physical protection, and response capability.

The recommended safeguards system design requirements are divided into eleven subsystems, each addressing an important objective in the overall system. The eleven interrelated and interdependent subsystems are:

1. Deterrence
2. Intelligence Management
3. Personnel Management
4. Authorization Procedures
5. Information Control
6. Physical Security of Transport System Facilities
7. Continuous Surveillance of SSNM during Transit
8. Defense Techniques
9. Recovery Capability
10. Use-Denial Techniques
11. Safeguards System Verification

The eleven are integrated to provide mutual support in forming the conceptual safeguards system. They provide protection at all stages in the transport sequence from the decision to ship, through physical transport, to acceptance at the destination including any intermediate stages such as transfer points.

While it is assumed that a licensee will be required to design a transport safeguard system which meets or exceeds the design requirements specified, it should be noted that not all design requirements fall solely on the licensee. Some, such as the intelligence gathering or material accounting, may be performed by a central national organization, probably a part of the federal government. Others, such as

a local response force may be within the responsibility of a local jurisdiction. The licensee will, however, be expected to identify the interrelationships among the organizations involved in a specific detailed plan and must make whatever arrangements are necessary, such as agreements with local authorities, for implementation.

Each subsystem is described in the following section in terms of its objective(s), the design requirements necessary to achieve the objective(s), the organizations involved in implementation, and a brief description of the significant points.

Appendix C provides a description of the performance parameters necessary for evaluating implementation and a more detailed narrative description of each design requirement.

Subsystem No. 1 – Deterrence:

Objective: To influence a potential adversary's perception of transport system vulnerability; to discourage potential adversary actions.

Design Requirements:

- A program for publicizing the fact that the transport safeguards represent an insurmountable obstacle.
- A program for publicizing the consequences to be faced by potential adversaries.
- A program for publicizing a hardline position regarding negotiations of any type with an adversary.
- A program for projecting an image of alertness, efficiency, and impregnability for any safeguards features which are visible to the public.
- Special legal penalties for attacks on nuclear shipments.

Organizations Involved: Licensees, NRC, industry associations.

Discussion: This subsystem is aimed at discouraging potential adversaries from attempting a malevolent act against an SSNM shipment. It would attempt to provide an image of the safeguards system as invulnerable, the SSNM of little value to an adversary, and the risk to an adversary in attempting an action as very great. It would also provide information which might

influence an adversary to discontinue an action once attempted because of the formidable nature of the safeguards measures.

This overall deterrence program should be developed and coordinated by the NRC. General information should be disseminated from the central source. Each licensee would be required to provide local support for the program by providing information and disseminating it on a local scale.

Subsystem No. 2 – Intelligence Management:

Objective: To obtain information on potential adversary actions so that action may be taken to counter them; to provide a source of information for the monitoring and upgrading of safeguards system performance.

Design Requirements:

- Development and operation of a central intelligence gathering and analysis program dealing with potential threats to the nuclear industry (this design requirement should cover fixed facilities as well as the transport sequence).
- Development of procedures for response to identified potential threats or conspiracies.
- Program of rewards for information on potential adversary actions.

Organizations Involved: Federal Government, licensee, local and state governments.

Discussion: It will be possible to discover and halt some potential adversary actions by obtaining and analyzing information on indications such actions might take place. At present, law enforcement agencies are obtaining information on persons and groups which have the potential for conducting an action against an SSNM shipment. The recommended subsystem would provide a mechanism for the acquisition and organization of relevant data and for analysis specifically directed at identifying threats of malevolent action against SSNM. It would require the designation of a control agency responsible for the intelligence function, the definition of procedures for routing appropriate data to the designated agency and the identification of what data are appropriate and what sources they may be obtained from. Techniques for analyzing the data and performing threat assessment would be a part of the system as would procedures for alerting appropriate response elements to take action on identified threats.

Subsystem No. 3 – Personnel Management:

Objective: To ensure personnel reliability for safeguards purposes, in particular, and sensitive elements of the nuclear industry in general; to create an atmosphere of security consciousness, perpetuate it, and develop the ability to act quickly, decisively, and appropriately.

Design Requirements:

- A program to employ capable personnel through attractive salaries, benefits, and working conditions.
- A program for careful selection and periodic review of high quality personnel.
- A program for training of personnel in safeguard system concepts and operation of safeguard measures.
- Clear definition of authorities, responsibilities, and relationships among all personnel and organizations.
- Personnel policies and procedures which provide proper incentive for good performance.

Organizations Involved: Federal Government, licensee, state and local governments.

Discussion: One of the most critical elements in the effectiveness of the overall safeguards system will be the personnel involved in its implementation. Virtually all design requirements or system components will be dependent on the actions of the personnel involved. As indicated in the vulnerability assessments conducted in this study, many potentially effective safeguard measures are vulnerable to subversion by personnel. For these reasons, it will be necessary to implement a strong personnel management subsystem which will ensure the reliability of the persons operating the transport system.

Subsystem No. 4 – Authorization Procedures:

Objective: To achieve control over authorized transport of SSNM; to deny access to SSNM through deceitful methods for misrepresenting authorization.

CONTINUED

1 OF 3

Design Requirements:

- Development of a comprehensive set of internal control procedures defining SSNM accountability.
- System for central-third party control over appropriate transportation authorization information.
- Procedures for SSNM custody exchange among parties.
- Use of paired authorization/verification throughout safeguards procedures.

Organizations Involved: Licensee, transport organization, central monitor organization.

Discussion: To reduce the possibility of unauthorized acquisition of SSNM through deceit or the weakening of one or more safeguard measures, a set of internal control procedures must be implemented.

A set of detailed procedures for all facets of the operation that involve access to or movement of SSNM should be produced describing accountability, authorization actions, and documentation required for internal control.

Subsystem No. 5 – Information Control:

Objectives: To maintain secrecy and security in the generation and use of critical transport information.

Design Requirements:

- Program for maintaining security over critical information on SSNM shipment.
- Program for generating secret shipment schedules.
- Program for secret route selection accounting for route vulnerability and response force availability.
- Program for selection of transport personnel for shipments.
- Program for use of secret, coded radio transmission of information during shipment.

Organizations Involved: Licensee, NRC.

Discussion: The effectiveness of the overall safeguards system can be enhanced by a strategy of securing certain information from potential adversaries and of random or specially selected schedules, staffing, and routing.

Both overt and covert adversary actions can be affected by this strategy. Deceitful operations become more difficult if access to information on where, when, and what SSNM will be shipped is restricted. Certain safeguard measures will be less vulnerable to tampering, subversion, or sabotage if knowledge of their existence and operation is limited. The placement of infiltrators or bribing of employees becomes less valuable if each person has limited access and individual selection for participation in a shipment is random or varies with each shipment. In addition, overt attack will be more difficult if the time of shipment and route to be followed are not known or easily obtained by the adversary.

Subsystem No. 6 – Physical Security of Transport System Facilities:

Objectives: To ensure that no facilities or equipment involved in SSNM transport can be tampered with, subverted, or sabotaged; to limit access to SSNM transport facilities to authorized personnel; to provide physical restraints on access to SSNM.

Design Requirements:

- A program of physical devices and procedures providing security for SSNM transportation equipment storage areas.
- A similar program for intermodal transfer points.
- A similar program for loading/unloading areas.
- Access control measures and procedures.
- Use of sealed, inpenetrable containers for SSNM shipment.
- Minimization of stops en route during SSNM transport.
- Program for establishment of physical security during unscheduled stops.

Organizations Involved: Licensee, transport operator.

Discussion: SSNM may be most vulnerable to an adversary action when it is outside of its normal position in a fixed facility but not actually in movement. This would include loading and unloading operations, intermediate transfer points or stops (for refueling, etc.).

To reduce vulnerability at these locations it will be necessary to provide a system of barriers, access control points, detection devices, and personnel to achieve an acceptable of security and limit access. SSNM loading/unloading areas should be dedicated and not shared with other forms of cargo.

Subsystem No. 7 — Continuous Monitoring of SSNM during Transit:

Objectives: To maintain continuous level of knowledge of the status of the SSNM and its transport system during movement of material.

Design Requirements:

- Program of procedures and devices to provide surveillance of the loading/unloading areas.
- Program of procedures and devices to provide visual, mechanical, and/or electronic surveillance of SSNM from within the convoy during transport.
- A similar program for surveillance from a remote, central control facility.
- Equipment and procedures for intra-convoy and control facility (HQ) communication throughout transport sequence.

Organizations Involved: Licensee, transport operator, central control organization.

Discussion: In order to detect adversary actions at the earliest possible moment, it will be necessary to maintain surveillance of SSNM at all stages during transport. Continuous remote and/or on-site surveillance should be provided of the SSNM and of safeguard related equipment and operations to minimize the opportunity for theft or tampering. A well-planned and designed system of surveillance should be developed which covers all important points at required times and with appropriate back-up in the event of malfunction. It may include personnel, equipment, and devices (such as closed circuit TV, sensors, intrusion devices, and communications gear),

tactics (foot patrols, escorts, etc.), and procedures for conducting surveillance and response to detected unusual conditions.

Subsystem No. 8 – Defense Techniques:

Objectives: To detect and defeat any adversary action launched against an SSNM shipment; to apprehend, drive off, or otherwise stop adversaries; to thwart an adversary's attempt to take possession of SSNM.

Design Requirements:

- Provision of necessary guard and escort forces to accompany all SSNM shipments positioned appropriately to provide maximum protection.
- Provision of guard and escort forces with appropriate weapons to resist attack.
- Provision of guard and escort forces with appropriate physical protection and equipment to resist attack.
- Program of encounter tactics and contingency plans to guide the guard force in successfully defending the SSNM shipment against attack.
- Use of transport equipment and SSNM containers which are adequate to deny removal of SSNM from the authorized transport sequence.
- Program for crisis management during adversary action defining organization, responsibilities, and resources.

Organizations Involved: Licensee, transport operator, LLEA.

Discussion: Defeat of a forceful adversary will be dependent on a defense force consisting of armed, trained guards, equipment, tactics, and an adequate response force. A decision in implementing these safeguards measures must be made between reliance on a remote response force or utilization of a self-sufficient convoy guard force.

Subsystem No. 9 – Recovery Capability:

Objectives: To recover and return to authorized control any SSNM which has been acquired in an unauthorized manner.

Design Requirements:

- Program of procedures, tactics, responsibilities, and equipment to be used to recover SSNM diverted from the authorized transport sequence.
- Devices and equipment attached to SSNM which will assist in relocation and recovery of SSNM.
- Program for notification of appropriate persons and organizations that SSNM has been diverted, dispersed, or sabotaged.

Organizations Involved: NRC, LLEA, FBI.

Discussion: In the case that an adversary is successful in acquiring or sabotaging SSNM during transport, the safeguards system must be capable of recovering the SSNM or of minimizing the impact of an act of sabotage or the dispersion of hazardous materials. The responsibility of the transport safeguards system extends only to the immediate recovery period including the notification of agencies to carry out clean-up, evacuation, or other emergency in the event of a sabotage or dispersion.

Tactics must be developed for immediate action to seal off the area surrounding an attack on an SSNM shipment. This action should be initiated at the first alert simultaneous to response force action. Devices which will emit radio signals or other location indication information should also be imbedded in the SSNM containers.

Subsystem No. 10 — Use-Denial:

Objectives: To mitigate the possible effects of a successful malevolent action against an SSNM shipment.

Design Requirements:

- Procedures for denaturing of SSNM to inhibit the manufacture of a nuclear bomb.
- Realignment of nuclear industry to take into account the denaturing of SSNM.

Performance Parameters:

- Procedures to check the efficiency of the denaturing.
- Procedures to validate the ability to denature.

Organizations Involved: NRC, licensee.

Discussion: This subsystem attempts to minimize the change of a nuclear explosion following a successful theft of SSNM. Materials can be added to the SSNM that inhibit its use in a fissile device. This use-denial technique allows for more time to recover stolen SSNM by increasing the time and resources needed by the adversary to make denatured SSNM "useful" to him.

The most effective way of denaturing plutonium is through chemical dilution, either dilution on command (at the time the adversary action occurs) or pre-dilution (at the reprocessing plant).

Subsystem No. 11 – Safeguards System Verification:

Objectives: To ensure that all elements of the safeguards system are in effect and operating to encourage all parties in the safeguards system to maintain a high level of system effectiveness.

Design Requirements:

- A program for evaluation of safeguard system plans.
- A program for periodic procedure/equipment tests.
- A program for check out of equipment/procedures prior to each shipment.
- A program for periodic audit by NRC of all safeguards system components.

Organizations Involved: Licensee, NRC, transport operator.

Discussion: To ensure that all safeguards systems design requirements will be achieved and that the safeguards measure equipment, personnel, and procedures will function properly when called upon, tests and evaluations must be performed prior to implementation, periodically following implementation and prior to each shipment.

5.5 Modifications and Developments Required

Many of the recommended safeguards system design requirements may be implemented directly without any further research, development, or modification of laws or regulations. For these requirements it will be necessary to design the specific implementation techniques, acquire the necessary resources from available sources and implement the measures. For others, it will be necessary to develop improved technological capability or an infrastructure must be developed before implementation of specific safeguard measures can proceed. It is recommended that NRC take the lead in seeing that the required activities are carried out even though some are beyond the bounds of present NRC authority.

The following is a discussion of the recommended developments:

- Specific legal penalties for interference in the nuclear fuel cycle. Existing laws concerned with theft or destruction of shipments of conventional materials may not be adequate to protect SSNM. Existing laws are essentially concerned with private property and the value of materials. Because of the magnitude of the hazard which can be created by an action against a nuclear shipment, the necessary legal changes should be enacted to facilitate the arrest and prosecution of adversaries who conduct or conspire to conduct actions against an SSNM shipment. Also particularly severe penalties should be attached to these violations. Suggested modifications may include automatic federal involvement even if an intrastate shipment is involved, the right to use deadly force and the severe penalty for conviction.

- Intelligence gathering related to a nuclear theft. While several agencies and organizations are monitoring various elements of the nuclear theft threat, there is no central program for acquiring and analyzing all relevent information and for providing threat assessment notification for appropriate response. An analysis should be made of the requirements for intelligence information, uses of the information, constraints on its acquisition and use, procedures for threat analysis and procedures for reaction to threat. Also the appropriate organization to conduct these activities should be identified and a plan for implementation developed.

- Central third party monitoring of shipment information. An organization should be identified to function as a third party SSNM shipment information monitor. The types of information to be monitored, procedures for exchanging information, security procedures and techniques, reaction responsibilities, and financing arrangements should be defined. A

plan for implementation and operation should then be developed, the necessary resources acquired and operation established.

- Sealed, impenetrable containers. An ongoing program of developing improved SSNM containers and techniques for tamper-proof sealing is continuing. While the "perfect" system may never be found there remains the need for a highly effective, economical container. The development of such a device is an appropriate role for the federal government to undertake.

- Procedures and devices for continual remote surveillance of SSNM shipments. Rather than a piecemeal implementation involving numerous approaches to remote surveillance from a control center, a single, effective system should be developed. It should include the necessary communications and detection devices, coding techniques, and procedures for operations and establishment of a control center (possibly in conjunction with the intelligence center, the third party information center.

- Centralized guard/response force training program. A central program for training SSNM transport guards and response forces should be developed. The program should include training and practice in security procedures, legal authority and responsibility, operation of safeguard devices, encounter tactics, and weapons training. The necessary lessons, training materials and programs should be developed and conducted by a central organization to assure a uniform standard of personnel capability.

- Special SSNM transport equipment. The ongoing program of developing specialized equipment for the safe, secure transport of SSNM should be continued at the national level.

- Legal controls on use of weapons. There is a need to modify federal, state, and local laws regulating the use of firearms. One issue to be clarified is the problem of state by state permission required for guard forces. The other is the authority to shoot to kill. This issue is discussed in more detail in Chapter 6.

- Response forces. At present there is complete dependence on local law enforcement agencies to provide required response forces. Several problems exist with this approach. Response to an attack on an SSNM shipment may represent a very special case beyond the typical capabilities of LLEA. Therefore, special arrangements, procedures, equipment,

tactics, and training must be developed and implemented along the routes of SSNM shipments before reliance on LLEA response can be justified. In addition, in some areas of the country, adequate LLEA's do not exist within an acceptable distance from potential attack points along an SSNM route. A contingency capability must be developed before SSNM shipments can be made through these areas without a self-sufficient guard force.

5.6 Air Transport – A Long Term Solution

The use of aircraft for the transportation of SSNM offers many advantages in the long term. The capitalization required to institute such a system is precluded at the present time by the small number of shipments being made. In the future, however, assuming current projections, there may be sufficient SSNM shipments to justify this expenditure.

Air transport is primarily concerned with medium to long distance trips. Short journeys will most likely be made by road.

The primary advantage of air transport is the fact that it severely restricts accessibility, thus making it difficult for an adversary to intercept shipment. While it is in the air, it will be virtually invulnerable to a force type attack, and the speed of air travel would greatly reduce exposure time. It will be more vulnerable during loading and unloading periods, and the immediate take-off and landing times.

The ideal way to minimize these vulnerabilities would be to use Short Take-Off/Landing aircraft (STOL) on airstrips installed within the nuclear facilities. This option poses practical problems such as cost and feasibility of installing airstrips at all nuclear facilities. It would be easier to implement a system in which the SSNM is transported to an airport, loaded onto a plane in a secure area, flown to another airport, unloaded in a secure area, and then transported to the destination. The means of transportation to and from the airport could be by truck or helicopter.

The use of a helicopter involves all the same advantages and disadvantages of other aircraft, and so it is not described separately. The disadvantages peculiar to a helicopter include low range and low altitude flying. This low range capability is not a problem for the transport of SSNM between nuclear facilities and airports. However, low altitude flying poses serious problems for the tracking of helicopters on radar screens. By use of constant radio communications and signalling devices as described in the design requirements, this problem can be alleviated.

Other advantages of air travel include flexibility in routing, avoidance of population centers, and reduction of resources necessary for the development of elaborate escort and response forces.

From a vulnerability point of view, the major drawback to air transport is the difficulty in recovering an air shipment of SSNM, if it is diverted. The major threat to air shipment is from a deceit-type attack. Therefore, design requirements specially suited for air travel are needed (these are described in detail at the end of this section). The main thrust of these design requirements is to ensure adherence to the scheduled flight plan.

Other design requirements should be unique to air transport. Personnel involved with SSNM transport must receive more intensive screening than those concerned with road transit, but fewer personnel are involved in air travel. Even more intensive monitoring of the position of the SSNM is indicated along with multiple independent checks. Radar tracking and escort aircraft are possibilities for monitoring, though escort planes would be very expensive. Recovery capabilities should include all those used for road transport, plus equipment specially designed for the tracking and relocation of aircraft. Evidently, a response force in this case poses feasibility problems. To intercept a diverted aircraft while in flight will, require an alert response force. The armed forces offer the only practical air response force and an investigation into the possibility of USAF involvement is recommended.

Problems concerning the air mode include cost, safety, and legal issues. The cost of air transport is usually high. Even with the savings on manpower and equipment, as described above, there still may be a net increase in expenditure. In the safety realm, there is an obvious safety hazard — until a container which can withstand the impact of an air crash can be designed. Such a container seems within current technological capabilities. Use of aircraft with relatively low crash speeds and avoidance of flying over population centers also eases this problem. Legislation is needed to change current limitations on the use of aircraft for the transportation of SSNM. The safeguards described earlier with respect to road transport offer protection for all the phases of road transport including transfer points that occur in a truck-aircraft-truck transport sequence. (Transfer points in a helicopter-aircraft-helicopter sequence are similarly covered.)

With respect to the recommended design requirements, the majority of the safeguards subsystems are unaffected by a change from road to air transport, at the conceptual level. At the implementation level, minor differences may occur due to the practical variation between the transport modes. The unchanged subsystems are:

- Safeguards Subsystem No. 1 — Deterrence
- Safeguards Subsystem No. 2 — Intelligence Management
- Safeguards Subsystem No. 4 — Authorization Procedures
- Safeguards Subsystem No. 5 — Information Control
- Safeguards Subsystem No. 6 — Physical Security of Transport System Facilities
- Safeguards Subsystem No. 10 — Consequence Reduction
- Safeguards Subsystem No. 11 — Safeguards System Verification

As mentioned above, Safeguards Subsystem No. 3, Personnel Management, needs alteration to take into account the greater reliance one must place on the honesty of air personnel. This requires a different interpretation of what is meant by reliable personnel, in the design requirement. To achieve this, personnel screening must be more extensive to reduce the danger of subversion.

The requirements for the remaining three safeguards subsystems, No. 7, Continuous Monitoring of SSNM During Transit; No. 8, Defense Techniques; and No. 9, Recovery Capability, are altered dramatically, with a change to air transport. More monitoring of the SSNM and recovery are required capability and significantly less defense techniques are needed. Three new safeguards subsystems, replacing the above subsystems, have been designed for air transport. They are now described.

Safeguards Subsystem No. 7 (Air) — Continuous Monitoring of SSNM During Transit

Objective: To maintain continuous level of knowledge of the status of SSNM and its transport system during movement of material.

Design Requirements:

- Program of procedures and devices to provide surveillance of the loading/unloading areas.
- Program of procedures and devices to provide within the convoy visual, mechanical and or electronic surveillance of SSNM during transport.

- Radar tracking to monitor position of aircraft and ensure strict adherence to pre-assigned flight plan.

- Equipment and procedures for communication between the aircraft and control facility (HQ) throughout transport sequence.

- Program of procedures to confirm take-off and landing with independent third party (Airport control tower, possibly).

Organizations Involved: Licensee, NRC, Transport Operator, FAA.

Discussion: While in the air, the crew should monitor and report status and remote surveillance should be maintained through use of radar tracking. During take-off and landing procedures for confirmation of status should be utilized.

Safeguards System No. 8 (Air) – Defense Techniques

Objective: To detect and avoid or defeat any adversary action launched against an SSNM shipment; to apprehend, drive off, or otherwise stop adversaries; to thwart an adversary's attempt to take possession of SSNM.

Design Requirements:

- Provision of armed guards to accompany all SSNM shipments.

- Program of encounter tactics and contingency plans to guide the guards and aircraft crew in successfully defending the SSNM shipment against attack.

- Use of transport equipment and SSNM containers which are adequate to deny removal of SSNM from the authorized transport sequence.

- Program for crisis management during adversary action defining organization, responsibilities, and reserves.

- Program for organizing, preparing, positioning, and alerting response force adequate to defeat a substantial adversary attack, involving liaison with USAF.

Discussion: The possibility of a forceful attack while in the air is rather remote. During take-off and landing, such an attack is more credible, though the protection given to the airport by Subsystem No. 6, Physical Security of Transport System Facilities, should diminish this threat.

A deceitful type attack poses a greater threat. However, by using trained armed guards, as well as the air crew, this threat is severely hampered. Also, by using specially constructed storage compartments and SSNM containers which inhibit acquisition of SSNM, the task of removing any radioactive materials is made much more difficult.

Safeguards Subsystem No. 9 (Air) – Recovery Capability

Objective: To recover and return to authorized control any SSNM which has been acquired in an unauthorized manner.

Design Requirements:

- Program of procedures, tactics, responsibilities and equipment to be used to recover SSNM diverted from the authorized transport sequence. Liaison with USAF to facilitate this recovery.
- Devices and equipment attached to SSNM and aircraft which will assist in relocation and recovery of SSNM.
- Program for notification of appropriate persons and organizations that SSNM has been diverted, dispensed, or sabotaged.

Organizations Involved: NRC, Licensee, LLEA, USAF.

Discussion: In the case that an adversary is successful in acquiring or sabotaging SSNM during transport, the safeguards system must be capable of recovering the SSNM or of minimizing the impact of an act of sabotage or the dispersion of hazardous materials. The responsibility of the transport safeguards system extends only to the immediate recovery period including the notification of agencies to carry out clean-up, evacuation, or other emergency actions in the event of sabotage or dispersion.

5.7 System Integration

Since safeguards mechanisms are essentially interdependent rather than dependent, it is vital that they act to support, rather than obstruct, each other. In other words, it is necessary that safeguards mechanisms be functionally integrated in a logical and effective system. Such a process of system integration involves the study of how safeguards mechanisms interact with each other in order to ensure that the safeguards system is fulfilling its essential function.

To be fully effective a system integration approach requires an examination of the safeguards mechanisms in the context of the particular situation in which they would be implemented. In this study, the particular situation is the transportation of SSNM.

For example, a safeguards mechanism relating to personnel management would involve the reliability and caliber of personnel so that transportation equipment is properly guarded and serviced. A safeguards mechanism relating to the need for reliable equipment would complement the first safeguards mechanism. The two mechanisms would act in support of each other. However, a safeguards mechanism suggesting comouflaged SSNM convoys would contradict a safeguards mechanism to provide machine gun replacements on top of all vehicles. These two mechanisms would not act in support of each other and, therefore, the effectiveness of the entire safeguards system would be damaged if they were implemented, even though they might be effective safeguards when examined independently. Thus, the need for a systems integration approach to safeguards system design is imperative.

A system integration approach, although necessary, is not always straightforward. For example, a guard may be more efficient if he perceives the entire safeguards system to be effective and secure. He may not act efficiently if he views the system as unreliable and ineffective. An examination of such possible variables as there is a complicated matter involving many different analysis inputs.

Figure 5-1 provides a rather basic view of the fundamental interrelationships involved in the system that the SDC project team has developed. The complexities involved in these relationships were discussed and analyzed by the Delphi panel to ensure that the system proposed was fully integrated.

During this analysis, the project team and panel were particularly sensitive to a number of factors which impacted the integration of the proposed system.

The most basic concern was to ensure that security was provided for the entire transportation system. The defenses had to protect against all possible malevolent acts. There could be no gaps between the

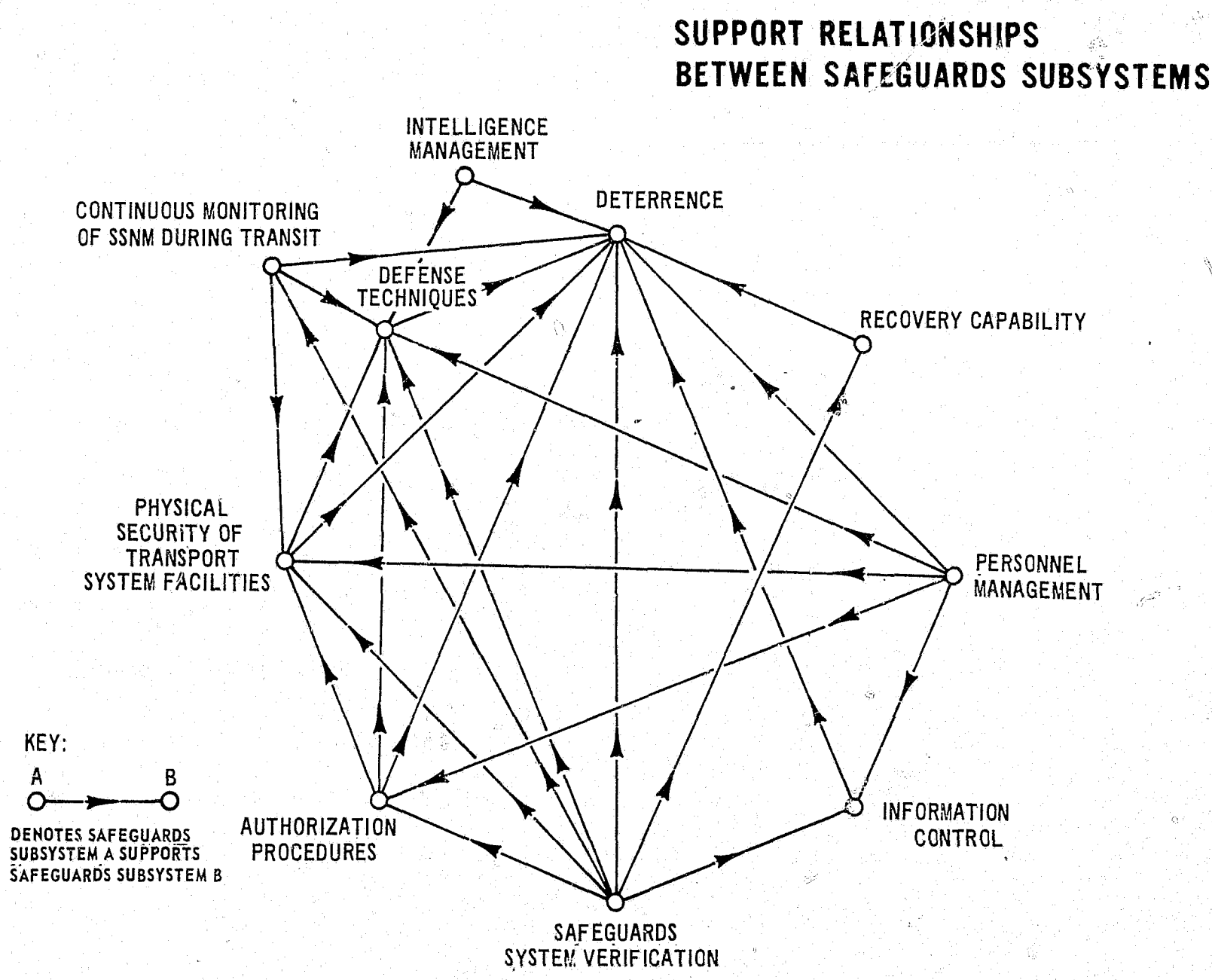

FIGURE 5-1: SUPPORT RELATIONSHIPS BETWEEN SAFEGUARDS SUBSYSTEMS

between the various safeguards. The interfaces between the safeguards needed to be studied and a certain amount of overlap needed to be provided between the design requirements to guarantee that there were no "holes" in the defenses. The method used in the development of design requirements (Section 5.1) fulfilled this purpose. Because all aspects of security for every part of the transport system were considered, it was possible to maximize protection.

The second factor considered was the susceptability of the system to a so-called "common mode" failure, where the failure of one part of the system impairs the functioning of other parts of the system. For example, an armed guard may detect an assailant, sound an alarm, and withstand an attack, but if the guard is quickly overcome, this has a negative effect on each of the above three measures.

Another factor examined was the situation where only one safeguards measure needs to be overcome before a malevolent act can be successfully completed. By having redundant defenses, this undesirable situation can be avoided. If these layers of protection are also made independent of one another, then the possibility of a "common mode" failure is greatly diminished.

Parts of a safeguards system, such as the people in the convoy have several functions. This allows for failures in security to take place. However, protection against such an eventuality is possible and was provided in the recommended design requirements. For example, the notion of a third party check on procedures, which was introduced in Safeguards Subsystem No. 4, Authorization Procedures, is a safeguard to provide in-depth assurance of the reliability of personnel. The design requirements mentioned in the critical Safeguards Subsystem No. 8, Defense Techniques, provide layers of redundancy. The armed escort, response force, impenetrable truck, etc., all provide many barriers that an adversary must surmount.

5.8 First Order Vulnerability Assessment of an Implementation of the Design Requirements

In order to confirm that the recommended design requirements represent adequate safeguards, a first order vulnerability assessment was carried out on a typical implementation of the safeguards. The methodology was the same as that used for the Generic Vulnerability Analysis. A different Delphi panel was used for the purposes of this assessment than was used for the evaluation of the design requirements. Only formidable adversaries were considered. Three different adversary actions were considered, each representing a possible attack by a group of 15 well-trained and equipped men, including two insiders. The adversary actions represented differing modes of attack: Force, Deceit, and a combination Force, Stealth, Deceit attack.

No adversary will come up against all the design requirements. Consequently, in an assessment of the vulnerabilities of the design requirements to an adversary action, many of the design requirements would be non-applicable. Therefore, the assessment of vulnerability was carried out on the various Safeguards Subsystems, as opposed to the individual design requirements.

The assessment was conducted in the following manner. If an adversary considered an attack at an intermodal transfer point, then in Safeguards Subsystem No. 6, Physical Security of Transport System Facilities, the design requirement that relates to transfer points came under investigation, and the vulnerability of the implementation of that requirement was assessed. If the rest of the design requirements were irrelevant to the adversary action under examination then this assessment became the vulnerability assessment of Safeguards Subsystem No. 6. If other design requirements within this subsystem were relevant, then similar vulnerability assessments were carried out on them. A composite vulnerability assessment of the entire subsystem was then formed. Composite assessments are shown in Table 5-3.

The information obtained from an assessment of Safeguards Subsystem No. 1, Deterrence is different from that of the other subsystems. No longer is the discussion concerned with vulnerabilities. Instead, effectiveness is the focus. A deterrence program does not have to be overcome before a malevolent. Consequently, the assessment of Subsystem No 1 should be interpreted as a measure of effectiveness where 0 represents the best possible deterrence system and 1 represents the worst. As before, the other assessments are of vulnerability, where 0 represents invulnerability and 1 represents total vulnerability. In the calculation of the system vulnerabilities, the assessment of Subsystem No 1 was disregarded. Its effect, as with all deterrent measures, is reflected in changes in the frequencies of attacks, which were considered earlier in this study.

In trying to draw conclusions from Table 5-3, it is essential to realize that these figures only have meaning in a relative sense. It is possible, however, to compare these results with those of the Generic Vulnerability Analysis. Such a comparison does indeed show that there has been a substantial improvement in protection.

TABLE 5-3:

ADVERSARY ACTION–SAFEGUARDS SYSTEM INTERACTION MATRIX
COMPOSITE VALUES FORMIDABLE ADVERSARIES
VS. U.S. RECOMMENDED SAFEGUARDS

ADVERSARY ACTION CLASSES | **PROTECTIVE MECHANISMS**

	Deterrence		Intellegence Management	Personnel Management	Authorization Procedures	Information Control	Physical Security of Transport System Facility	Continuous Monitoring of SNM during Transit	Defense Techniques	Recovery Capability	Safeguards System Verification				V_k
Force	.2		.2	.3	.4	.2	.3	.3	.01	.3	.3				4×10^{-7}
Deceit	.4		.2	.2	.1	.3	.4	.3	.1	.4	.3				2×10^{-6}
Combination: Force, Stealth, and Deceit	.3		.2	.3	.3	.2	.3	.3	.05	.3	.3				1.5×10^{-6}

CHAPTER 6

THE SOCIAL, ECONOMIC, AND POLITICAL COST OF SAFEGUARDS

6.0 THE SOCIAL, ECONOMIC, AND POLITICAL COST OF SAFEGUARDS

6.1 Overview

Any proposed safeguards system, if it is to be effective, will involve some cost to society, not only in economic terms, but also in social and political terms. It is difficult to assess the degree to which these costs are acceptable. The problem is compounded by the fact that what is acceptable in today's political environment may not be acceptable in a changed political environment. For example, with relatively little public alarm at the present time over the supply of energy, the public might properly be expected to be very concerned with, for example, the civil liberties implications of particular safeguards measures. But if the supply of energy were suddenly to become much more uncertain (as for example under oil embargo conditions), the public might be much less concerned with those same civil liberties implications, deeming it much more important to develop, relatively unrestricted, all available sources of domestic energy. Therefore, an ideal safeguards system should be dynamic and readily adaptable to the fluctuating political environment and concerns of the general public.

This chapter describes the social, economic, and political impacts of a safeguards system, including a discussion of the processes and factors involved in the acceptance or rejection of various safeguards.

It is not exhaustive, nor are all the various ramifications of each factor considered. The following list of factors, representing the minimum concerns which should be addressed before particular safeguards requirements are recommended, was developed.

- Civil Liberties – freedom of association and discussion, privacy rights, etc.
- Social Environment – air, water, land biotic.
- Political Environment – effect on nuclear debate, congressional reaction, etc.
- Legal Area – effect on communications, statutes, regulations, industrial standards, etc., both ERDA and NRC's emergency response capability.
- Energy System – effect on fuel cycle configuration, supply and demand, etc.
- Effective operation of the transportation system.
- Public Safety and Health – increased accident risk, release of effluents, etc.

CHAPTER 6

THE SOCIAL, ECONOMIC, AND POLITICAL COST OF SAFEGUARDS

6.0 THE SOCIAL, ECONOMIC, AND POLITICAL COST OF SAFEGUARDS

6.1 Overview

Any proposed safeguards system, if it is to be effective, will involve some cost to society, not only in economic terms, but also in social and political terms. It is difficult to assess the degree to which these costs are acceptable. The problem is compounded by the fact that what is acceptable in today's political environment may not be acceptable in a changed political environment. For example, with relatively little public alarm at the present time over the supply of energy, the public might properly be expected to be very concerned with, for example, the civil liberties implications of particular safeguards measures. But if the supply of energy were suddenly to become much more uncertain (as for example under oil embargo conditions), the public might be much less concerned with those same civil liberties implications, deeming it much more important to develop, relatively unrestricted, all available sources of domestic energy. Therefore, an ideal safeguards system should be dynamic and readily adaptable to the fluctuating political environment and concerns of the general public.

This chapter describes the social, economic, and political impacts of a safeguards system, including a discussion of the processes and factors involved in the acceptance or rejection of various safeguards.

It is not exhaustive, nor are all the various ramifications of each factor considered. The following list of factors, representing the minimum concerns which should be addressed before particular safeguards requirements are recommended, was developed.

- Civil Liberties – freedom of association and discussion, privacy rights, etc.
- Social Environment – air, water, land biotic.
- Political Environment – effect on nuclear debate, congressional reaction, etc.
- Legal Area – effect on communications, statutes, regulations, industrial standards, etc., both ERDA and NRC's emergency response capability.
- Energy System -- effect on fuel cycle configuration, supply and demand, etc.
- Effective operation of the transportation system.
- Public Safety and Health – increased accident risk, release of effluents, etc.

- Cost – direct (more power needed), government costs (more guards), indirect costs (cost of measures on other segments of society).

6.2 Scope of Impact Study

The scope of this contract did not allow for a thorough, systematic evaluation of each safeguards requirement against each of the above factors. However, it was possible to carry out a limited examination of the impacts caused by nuclear safeguards, and the conclusions of this research influenced the recommendations of this report.

Every design requirement developed during this study, was considered with regard to each of the factors listed above. The design requirements were included in the recommendations only if they did not grossly impact, in an adverse way, any of the listed considerations. The criteria for such judgments were the perceptions of what is publicly and governmentally acceptable at the present time, substantiated where possible with available objective data.

Many of the proposed safeguards requirements are extensions of activities in which government is already engaged. The project team was less concerned about such requirements than those which are totally new and more difficult for the public to accept. There are some requirements recommended that do have a high social, economic, or political cost. In those cases, only those that were considered to be vital safeguards concepts, essential to any well-designed safeguards system, were included. At the same time, we have tried to increase their acceptability by suggesting ways in which their impact may be minimized.

The project team also endeavored to keep in mind the distinction between the impact of the design and implementation of safeguards requirements, as opposed to their impact if they are actually employed to defeat an adversary action. A primary objective of an effective safeguards system is to deter a successful adversary action. But it might be necessary to fully activate all measures including engagement in gun battles, if the system was tested. Certainly, critics of safeguards measures and the nuclear power industry will consider the impact of the use of safeguards systems as well as their effect as a purely deterrent measure. Consequently, it was necessary to consider the impact of design requirements under actual sabotage or theft attempt conditions.

It is important to stress that a safeguards system should undergo a thorough impact evaluation prior to implementation. The difficulty in performing of such an evaluation was underscored in a draft

final report to the Office of Special Studies of NRC.* The report concluded that not all safeguards requirements could be quantified in terms of dollar cost. The approach taken was to divide the impacts into two groups: those to which a dollar cost could be assigned; and those to which no dollar cost could be assigned. For the latter, Brookhaven National Laboratory attempted a point scale. Each safeguards requirement would be assigned points, so that the overall cost of each measure could be evaluated. The major issue is whether it is possible to devise a satisfactory conversion model so that impacts, however measured, may be compared. Moreover, Brookhaven concluded that a satisfactory point scale could not be devised to measure all impacts. The necessity of conducting a thorough impact evaluation of the effects of safeguards requirements underscores the urgency of further research in this area.

6.3 Civil Liberties

Probably the most sensitive impact of the recommended safeguards requirements is on civil liberties. A number of the design requirements are likely to cause concern in this area. Most important among these are the requirements for security checks, for monitoring groups likely to commit nuclear-related crimes, and for the creation of an integrated central analysis organization to deal with all nuclear related intelligence data.

6.3.1 Personnel Clearances

It is recognized that these requirements may cause some problems in the area of civil liberties. It would mean an expansion of those jobs requiring security clearances and consequent discrimination against those citizens whose personal qualifications do not meet the high standards required. The civil liberties implications are viewed as extremely serious but mitigated by a number of factors. First, the principle of security clearances for a wide range of jobs both within and outside government is already accepted. The security requirement would not introduce anything new; it would merely increase the number of jobs subject to existing security procedures. Second, effects of security clearance procedures on individual privacy are minimized by the fact that they would not be employed without individual consent. Third, the security procedures used might be arranged in such a way as to minimize the impact on both First and Fourth Amendment rights. Participants at a conference on the Impact of Intensified Nuclear Safeguards on Civil Liberties held in October, 1975, felt, for

*Evaluation of the Impact of Safeguards Measures by Brookhaven National Laboratory.

example, that background investigations might be more objectional than psychological testing. This was because the former looked to associations and political beliefs while the latter attempted to measure emotional stability. However, these tests raise problems of validity and reliability. The conference found that the careful searching of employees when starting and leaving the job was a very effective security measure, widely employed in private industry, and not particularly objectionable. Electronic monitoring may be even less objectionable. The precise mix is obviously something to be determined later. The above discussion is referenced, however, in order to indicate that although security clearance procedures have obvious impact on civil liberties, the risks can be minimized.

There are some practical issues that need to be considered if personnel screening is to be extended in the commercial industry as it exists today. The presence of unions means that management alone will not have full decision-making power over such issues as hiring and firing, work schedules, in-service training, rest stops and manning. Management would also be restrained by State "right to work" laws, where they exist, and also by the necessity for equal employment opportunities. The form of any personnel screening system will therefore have to take these very important realities into account.

Moreover, the cost of thorough personnel screening is not inexpensive. A full field background check can cost anywhere from $5,000 to $10,000 per employee. There are also practical difficulties involved in undertaking such thorough checks within the framework of a commercial nuclear power industry which does not operate under government contracts.

All the above factors may pose obstacles to the creation of an effective security system within the industry. The panel of experts which convened at SDC in late January considered the security safeguard as critical. Since personnel were potentially the weakest link in the system, they believed thorough and extensive security screening throughout the industry was essential.

It should be noted that the realities of current industry, make it difficult to limit some of the effects of the recommendations. For example, existing private transporters of SSNM (currently, there are four major corporations and a number of small independents) also transport a wide range of other products that need protection. To restrict some of the guards to transportation of SSNM and isolate the training that we recommend accordingly would be impracticable given the existing nature of the industry. However, it would be equally unfair and impracticable to screen all guards whether they were carrying SSNM or not.

Further, the labor unions would, most likely, not accept differential wage scales for those employees carrying SSNM and those who were carrying other materials, and assignment rotations would be opposed if they were implemented for personnel with differing job classification levels. For these reasons, the labor unions would fight the requirement vigorously, and there would be an obvious impact on the nuclear debate generally.

The effect on the political environment of this requirement is less easy to predict. There is no doubt but that critics of nuclear power will see any recommendation for an expansion os security clearance procedures, particularly into the private commercial industry, as further evidence of the erosion of freedom and individual rights. The fact, however, that such procedures are already in existence for a wide range of jobs is likely to blunt this criticism.

6.3.2 Rewards

The safeguards requirement for substantial incentives/rewards for the detection and proper handling of irregularities caused some controversy among the Delphi panel members. The basic idea seems sound enough, but has obvious capacity for abuse – particularly in the areas of over-zealous employees conducting "fishing trips" which may damage employee morale, and employees with grudges using security issues as a mode of revenge. The ground rules for this requirement and the security issues to which it applies would have to be delineated very carefully. One of our consultants remarked that "bounty hunting" would not be an attractive addition to the industry framework.

A limited law dealing with rewards in the nuclear area is already on the books. Public Law 93-37 rewards people who assist government in the apprehension of anybody involved in nuclear theft or illegal nuclear manufacturing. Provision is made for reward payments up to $500,000 under this Act.

6.3.3 Intelligence

The requirement for gathering intelligence on suspected criminal groups would have to be implemented in such a way that civil liberties are protected. It would be important, for example, for the FBI to monitor only those groups that are likely to engage in such activities. Groups with a history of political dissent which had not broken the law must have their rights to freely dissent protected. The form of the monitoring, possible authorization for wiretaps, etc., are obviously delicate procedures that must be carefully worked out in the light of civil liberties implications.

The value of centrally gathered and disseminated intelligence on adversaries is apparent, but the legal and administrative problems involved may be problematic. Should the central intelligence unit be operated by NRC, by the private commercial industry, or by the FBI? Each option has advantages and drawbacks.

NRC, as its name implies, is charged with a regulatory responsibility. To expand its areas of operation into intelligence gathering, processing, and dissemination raises questions as to the legality of such an expansion of responsibility as well as its political acceptability.

The private commercial nuclear industry would, in all probability, be reluctant to accept the responsibility for an intelligence gathering unit. Moreover, such a privately operated unit may cause more public concern than one operated by a Federal Agency with the opportunity for Congressional oversight and review. The FBI is basically charged with domestic intelligence gathering, but granting the FBI this new function would essentially minimize NRC control and involve the agency in controversy if the FBI pursues its new assignment too enthusiastically.

It is evident from the above discussion that there are various options available which need to be studied in detail in order to recommend the kind of intelligence unit that will maximize the efficient gathering and dissemination of intelligence while at the same time minimizing the legal problems posed by such a unit and the political concerns of those groups and individuals sensitive to the intelligence function in general.

6.4 Environment

It is our judgment that none of the recommended safeguards requirements at least at the conceptual level described, present a threat to the environment. However, it is recommended that NRC comply with the National Environment Policy Act (NEPA) in order to assure environmentalists and other concerned citizens that this is the case. Whenever a safeguards concept is developed to the point where it is ready to be adopted as a safeguards regulation, NRC should file an environmental impact statement.

6.5 Political and Legal Issues

There are a number of legal and political factors involved in the recommended safeguards requirements that should be stressed at this point. These factors influence the way in which the proposed concepts

should be refined and implemented and the various options available for doing so. It is not our intention to judge the legality or constitutionality of the recommendations. Such an effort is a major study in and of itself and can only be undertaken when the actual design is determined, as distinct from the design requirements. Rather, it is our intention to put forth some of the legal and political considerations that must be considered in evaluating the options available. Most of the controversial options are concerned with the kind of guard force that should be used.

6.5.1 Guard Force Options

These options may be detailed as follows:

- Should the guard force be private or federal?
- Should the guard force be nationally or locally organized?
- What kind of arms can guards carry and what is their authority to use deadly force?
- Should the guard force be dedicated or non-dedicated?
- What are the problems involved in agencies of government performing a protective reaction force function?

A recent report (Security Agency Study NUREG-0015) concluded that the creation of a Federal guard force for maintaining security in the nuclear industry would not result in a higher degree of guard force effectiveness that can be achieved by the use of private guards, properly qualified, trained, and certified. Moreover, creation of a guard force under NRC auspices would be more costly than an improved private guard system. A report by the Sandia Corporation also agrees with the conclusion of the National Security Agency study.

In addition, private guard forces, although operating under some disadvantages compared with federal officers, are not seriously compromised in their ability to perform as effectively.

Moreover, most of the legal problems involved in the use of guard force would apply equally to federal and private guards alike. There are no federal statutes as such governing the use of force and even federal officers have had their right to carry arms across state lines questioned by some state and local police. All guards are allowed to use "reasonably necessary force" to protect themselves or prevent

sabotage of the property they are protecting, but private guards are limited in the sense that they cannot easily effect arrest.

Moreover, the types of arms that may be carried are restricted by state and local law. NRC cannot, as a pure matter of regulation, require licensees to arm and instruct security forces whether private or federal in such a manner as to contravene state or local law. At present, guards cannot use greater firepower than that provided by handguns, shotguns, and semi-automatic carbines. It is strongly recommended that whatever the nature of the guard force used, special legislation is required to enable guards protecting nuclear shipments to carry weapons such as M-14 rifles or M-16 automatic rifles to match the potential firepower of adversaries.

It is appropriate at this juncture to discuss the issue of the use of deadly force. It is necessary that all guards of nuclear shipments, whether they are federal or private, should have the power to use deadly force in order to prevent the theft or sabotage of SSNM. It seems clear that they have this authority in the case of an actual attack. But the issues become less clear where "hot pursuit" to recover the material is concerned and particularly where crossing a governmental jurisdictional line is involved. There, the authority of private guard forces is much less clear cut. If the private guard force option is used, it is necessary to ensure that private guards have full legal authority to do everything necessary to protect shipments of SSNM.

Although private guard forces are not nationally organized or recruited at present, there is nothing to prevent the establishment of a body to do just that. A nationally organized guard force does not necessarily have to be a federal guard force. Many of the advantages that a federal guard force would have over locally organized and recruited guard forces apply equally to a privately operated, national guard force. The option of a privately operated, national guard force even has a few advantages not possessed by the option of a federal guard force.

An association could be created, which is responsible to the commercial nuclear industry and regulated by the NRC, that would be involved in the creation of a guard force, which would supply both escort and reaction forces. The association might also be involved in the collection and dissemination of intelligence. A precedent for such an organization exists in the fire investigation and automobile theft areas where such associations have been formed and provide support to insurance companies and others, in the investigation of arson or theft. Such a body would have a number of advantages. It would be national in scope and thus able to systematize procedures and standardize

requirements and share costs more easily than individual facilities operating independently. Since it would be essentially controlled by the commercial industry, it would not arouse the public hostility against "big brother" government that would probably develop if a federal agency adopted the task. As is detailed elsewhere in this report, a private guard force, organized nationally, would not necessarily be more constrained than a federal guard force if the necessary legal adjustments were made. There is, however, little enthusiasm for this type of arrangement in the commercial nuclear industry and as K. J. Toner and H. A. Feiveson point out in "Responsibility for Nuclear Security" traditionally, private industry has not been involved in law enforcement functions other than to protect against its own negligence or wrongdoing. Such a major expansion of the responsibility of private industry may in itself cause alarm among those who currently view the Federal government as the main culprit in the "big brother" syndrome.

Whatever the composition of the escort force and whatever degree of firepower they have available, if an extreme adversary action occurs, they may have to rely on a protective reaction force. The issue here is not so much whether such a protective reaction force be private or federal, national or local (since they would operate under a similar handicap) but whether or not it be "dedicated." The National Security Agency study concluded that it would be difficult to develop high-performance reaction forces that can be depended upon to arrive at a trouble spot within a few minutes of an alarm. Ground transportation is obviously subject to an adversary action anywhere along the route and to have forces ready for no other purpose than to respond to an attack on a nuclear shipment would be both expensive and wasteful. It would be expensive in that sophisticated transportation (possibly helicopters) would be needed to get to a trouble spot quickly. It would be wasteful in that these forces might (hopefully) never be needed and at most needed only rarely.

The Sandia Report agrees with the conclusion of the National Security Agency study. "The results of this analysis indicate that even when choosing assumptions partial to response forces, a transportation security system involving a dedicated response force appears unjustified economically for the foreseeable future" (Special Safeguards Study, Report to NRC, The Sandia Corporation, October 1975).

The alternative to a dedicated reaction force is to rely on in-place existing law enforcement agencies or military organizations. These options also are not fully acceptable for a number of reasons which are detailed below.

First, it is necessary to state that the composition and type of reaction force that is used will depend on the mode of transport. The use of a truck mode of transport will involve the necessity of a reaction force anywhere along the route if the escort force is unable to overcome an adversary action by itself. The units available will range from the LLEA, the State Police, the National Guard, and the U.S. Armed Forces.

The LLEA will be able to react in the shortest time because of its proximity, but many LLEA's do not have great strength available either in terms of manpower or firepower. The Delphi panel members were dubious of the value of relying on an LLEA even as an initial reaction force. Many LLEA's are ill-equipped and have resources which are stretched to the limit in dealing with everyday crime. Upgrading forces to a desired level would be difficult and pose severe practical problems. There is every likelihood that a LLEA reaction force would be inadequate (possibly more inadequate than the overpowered escort force) and ineffective. Local units of the State Police have similar drawbacks. The National Guard is probably of questionable value because of the time it would take to call up reservists -- perhaps 24 hours to gather together a force.

There are legal and practical problems involved in a reactive force assignment for the military. Konrad Keller (Reaction Force Against Nuclear Diversion or Sabotage: An Inventory of Considerations) argues the military should provide the reaction force, although not the escort force. But, military installations are widely scattered in a relatively small number of locations -- often far away from major population centers and freeways. There is some question as to their ability to act in a timely fashion. Moreover, it is quite possible that under current law, it would be illegal for the military to react on the basis of an assigned function. Under the terms of the Posse Comitatus Act (18 USC 1385), the military is prohibited from engaging in civilian police duties. The Security Agency study also reveals that the Department of Defense opposes the assignment of a nuclear reactive force mission on the grounds that it would defeat the Department's effectiveness in performing traditional military functions.

The U.S. Marshals Service is another option. In fact, the Marshals Service performed a study for NRC on alternative options for guard forces, the conclusion of which was that given sufficient funding, it could provide a reaction force capability. Unlike some other agencies of government, there appears to be no reluctance to accept the responsibility. There would be a number of advantages in using the U.S. Marshals Service. Police officers at the city, county, or state level have no official power to arrest offenders outside the jurisdictions which they serve. But this restriction does not apply to

U. S. Federal Marshals. Under the Federal Arrest Statute for U. S. Marshals (18 USC 3053):

> "United States Marshals and their deputies may carry firearms and may make arrests without warrant for any offense against the United States committed in their presence, or for any felony cognizable under the laws of the United States if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony."

The disadvantages of using the U.S. Marshals Service is that the assignment of this function would completely change the character of the agency from an arm of government essentially concerned with the courts and federal criminal law violations, to an operational department involved in a new area, with all kinds of possibilities of involvement with state and local law.

The above discussion is referenced to demonstrate the fact that no one guard force option has overwhelming superior value over any other. Choices are complicated by the fact that the world of commercial nuclear power is dynamic and the information on which decisions must be made is constantly changing. At a minimum the following factors should be considered when considering the options:

- The number of shipments and the existing industry framework.
- The state of law.
- The political climate.
- Responsibilities of federal agencies.
- The mix of transportation modes.

(As detailed elsewhere, an air transportation is recommended for the future. This will strongly influence the type of guard force that is selected.)

6.5.2 Publicity

The requirements for wide publicity to be given to stiff sentences for terrorist groups and for a hardline position against nuclear blackmail threats are not without problems. The suggestion that SSNM could be stolen, and moreover, the implicit suggestion that the lives of hostages would be sacrificed, if

necessary, in response to a blackmail threat is likely to exacerbate tension between pro and anti-nuclear power proponents. It is also possible that the publicity, inherent in the requirement, may backfire and give potential terrorist groups or individuals "ideas." There is considerable evidence that publicity, especially careless publicity, encourages certain individuals to attempt criminal acts they might otherwise not consider, but for the publicity. For example, after "Squeaky" Fromm's assassination attempt on President Ford, and the consequent publicity given to the attempt, there were a wave of assassination threats against the President and even another actual attempt within a few weeks. There is also considerable precedent for governments negotiating with terrorists which previously had stated they would never negotiate under blackmail. Democratic governments in particular would be under particular pressure to negotiate if enough human lives were at stake, whatever previous statements had been made about non-negotiation. It is possible that this requirement would have much more deterrence if it had the force of law, but it is very unlikely that such a law would be passed and even more unlikely that it would be obeyed if the situation at hand were extreme enough.

Thus, it is necessary to give care to the type of publicity that is encouraged on this issue.* It is also necessary to carefully consider the terms and conditions under which the government will and will not negotiate with terrorists.

6.6 Energy System and Effective Operation of the Transportation System

The effect of the design requirements on the energy system and fuel cycle configuration is largely a function of the cost of the requirements which is discussed in Section 6.8. No radical transformation of the energy transportation network is necessarily recommended at this time, although future considerations might lead to some significant changes. The dedicated shipment of SSNM by air (a recommended long-range option) would obviously impact the nuclear energy system somewhat, but the impact would be minimal compared to other major factors impacting that system such as the cost and supply of fossil fuels.

The essential energy network would remain very much the same under the implementation of the recommended design requirements. No major transformation, such as relocation of nuclear facilities,

*The wrong kind of publicity could help to enlarge the already exaggerated mystique surrounding nuclear materials and their use.

has been suggested as the total solution to the problem.

The existing interface between the commercial nuclear facilities and the transportation industry would be maintained with provision for gradual change in mode-use as the nuclear energy system evolves.

It should be noted, however, that the possibility of diluting plutonium discussed in Chapter 5 would be a direct intervention in the nuclear energy supply system which, if implemented, would involve the industry in further cost and technical effort.

6.7 Public Health and Safety

There are no immediately evident impacts in the area of public health and safety. However, provision for coding of SSNM, so that all but essential parties would be unaware of the contents of the shipment, has a number of trade-offs between public safety and effective safeguards. Currently, the Bill of Lading, has precise details of the nature of shipments. This requirement is to maximize the safety of any persons who come or may come in contact with the containers. Should there be an incident or accident, it is considered necessary that such persons know they are dealing with hazardous, radioactive material, that is extremely dangerous. It might be enough to warn them that the materials are hazardous, but such a limited warning might neither indicate the degree of caution necessary, nor deter law enforcement officials and others from performing emergency operations, in the event of an incident or accident, that might jeopardize safety.

From the point of view of safeguards, however, it is desirable to code the shipment so that potential adversaries would not be fully aware of which containers were filled with SSNM. It is possible that a viable trade-off could be made between these two conflicting considerations. There could be a partial coding and a partial warning. But the exact balance would need careful consideration based on the importance of this requirement as a safeguard and an evaluation of its impact on public safety.

6.8 The Issue of Cost

Cost is a difficult issue to discuss where safeguards are concerned because there are a number of complicated aspects to an assessment of what constitutes reasonable cost.

The first issue to resolve is: Who is to bear the burden of cost? Should it be the commercial nuclear industry itself? Should it be the federal government, and NRC in particular? Should it be the states

and local governments? Should it be a combination of part or all of the above? There is already considerable precedent for government incurring costs for protecting industry. Thus, for example, a bank which is robbed does not have to pay (other than through normal taxation) for the cost of any help provided by local law enforcement officers, either in thwarting a robbery or in apprehending the bank robbers. However, where the commercial nuclear industry is concerned, the burden on LLEA's or other possible reaction forces would be considerably greater, both for creating effective emergency response plans to deal with an adversary action, and in dealing with such an action if one were to occur. It is the scale of the law enforcement that causes concern and as shipments become more frequent, the size of the problem will grow. If reliance is placed on new forms of organization, such as a federal guard force, the cost will probably be greater and certainly more discernable than if reliance is placed on existing law enforcement organizations. If the latter option is used, the costs of planning could be mitigated by a federal subsidy and an outright federal payment could be made if a protective reaction is actually required. The cost of this option would be considerably less than the option of a dedicated reaction force.

These are questions which are not easily resolved, particularly as the cost of safeguards grows with the imposition of more standards and the provision for greater and more effective escort and reaction forces. Most likely, the cost of safeguards will continue to be borne by both the government and the industry with the precise burden a function of the political climate and the willingness and ability of the industry, itself, to increase its operating costs.

It is difficult to assess the cost of the safeguards requirements package that is advance here, if only because it has been developed essentially at the conceptual level and the actual cost has to be related to the way in which these concepts are refined and implemented. It seems unlikely, however, that the cost would be a significant proportion of the total cost of nuclear power. Willrich and Taylor (Nuclear Theft: Risks and Safeguards) estimate the cost of providing a dedicated security force to protect nuclear shipments at less than $10 million, even assuming 150 power plants. This figure is based on a projection of 150 nuclear shipments per year by 1980 and a 50-man transport task force assigned to each shipment. Willrich and Taylor project the total cost of generating nuclear electric power at approximately $8 billion by 1980. Even if the cost of safeguards were as high as $800 million per year, and this is unlikely, this would only represent ten percent of the total cost of generating nuclear electric power. Moreover, all the cost would not be borne by the commercial industry. Willrich and Taylor conclude, "Certainly, the costs of effective safeguards would not be so large as to make nuclear power economically uncompetitive in the future."

There is an important qualification to make to Willrich and Taylor's point of view, however. Their figures essentially depend on a ceiling on safeguards, however generous that ceiling may be. The point must be made that there is no realistic limit to the scale of a potential adversary action. A group of more than 100 heavily armed and trained adversaries not inconceivable though highly impronable. Certainly any group involving itself in the potentially dangerous area of nuclear theft is likely to be well-prepared and resourceful. Therefore, there is no assurance that any practical safeguards system can prevent an adversary attack from being initially successful. But an effective safeguards system can also deter, detect, and recover.

The economics of safeguards will ultimately be determined not only by the particular safeguard options that are selected, but also by the ability of the industry to keep the capital cost of nuclear power plants in check, by the cost competitive performance of other energy industries, and not least by international developments and the price and supply of fossil fuels.

The proposed system for optional flexibility so that it can be assessed not only against the perceived adversary action threat and the varying total of shipments needing protection, but also against the cost competitive position of the nuclear industry in the increasingly uncertain market of world energy supplies. Although, the demand and supply of energy is obviously going to depend on a large number of factors, the recommended safeguards requirements are not amongst them.

BIBLIOGRAPHY

BIBLIOGRAPHY

BOOKS, PAMPHLETS, AND BOOKLETS

AEC, Nuclear Power and the Environment, 1969.

Angelo, Jr., Joseph A., Stamps Tell the Story of Nuclear Energy, ERDA, 1975.

Asimov, Isaac, Worlds Within Worlds: The Story of Nuclear Energy, Vol. 3, ERDA, 1972.

Constanzi, F. A., et al., Diverter Preference and Vulnerability Index: New Measures for Safeguards in the Fuel Cycle, Kansas State University, Manhattan, Kansas, 1972.

Dukert, Joseph M., Atoms on the Move: Transporting Nuclear Material, ERDA, 1975.

Eaton, William W., Energy Storage, ERDA, 1975.

ERDA, A Bibliography of Basic Books on Atomic Energy, 1974.

ERDA, Nuclear Energy: Nuclear Power Plant Safety.

Fox, Charles H., Radioactive Wastes, AEC, 1969.

Good, I. J., The Estimation of Probabilities: An Essay on Modern Bayesian Methods, M.I.T. Press, Cambridge, Mass., 1965.

Graham, H. D., and T. R. Gurr, The History of Violence in America: Historical and Comparative Perspectives, revised edition, Bantam Book, New York City, 1970.

Gschneidner, Jr., Karl A., Rare Earths: The Fraternal Fifteen, AEC, July 1968.

Hiebert, Ray and Roselyn, Atomic Pioneers: Book 2, From the Mid-19th to the Early 20th Century, AEC, 1971.

Hogerton, John F., Atomic Power Safety, ERDA, 1964.

Hogerton, John F., Nuclear Reactors, ERDA, 1970.

Hyams, Edward, Terrorists and Terrorism, St. Martin's Press, New York, 1974.

International Atomic Energy Agency, The Physical Protection of Nuclear Material (INFCIRC/225), February 1976.

Keisch, Bernard, Lost Worlds: Nuclear Science and Archeology, ERDA, 1973.

Keisch, Bernard, The Mysterious Box: Nuclear Science and Art, ERDA, 1974.

Larus, J., Nuclear Weapons Safety and the Common Defense, Ohio State University Press, Columbus, Ohio. 1967.

Leachman, Robert B., and Phillip Althoff, Preventing Nuclear Theft: Guidelines for Industry and Government, Praeger Publishers, 1972.

Mallin, Jay, Terror and Urban Guerillas: A Study of Tactics and Documents, University of Miami Press, Coral Gables, Florida, 1971.

Mason, Willrich, International Safeguards and Nuclear Industry, John Hopkins University Press, 1973.

Morf, G., Terror in Quebec: Case Studies of the FLQ, Clarke, Irwin, and Co., Toronto, 1970.

Moss, Robert, The War for the Cities, Coward, McCarr, and Geoghager, New York, c. 1971.

Parker, Donn B., Threats to Computer Systems, March 1973.

Singleton, Jr., Arthur L., Sources of Nuclear Fuel, AEC, 1968.

Thom, Rene, Stabilite Structurelle et Morphogenese, Benjamin, 1972.

Union Carbide Corporation, The Petrified River: The Story of Uranium, 1967.

Willrich, Mason and Theodore Taylor, Nuclear Theft: Risks and Safeguards, Ballinger Publishing Company, Cambridge, Mass., c. 1974.

Woodburn, John H. and Frederick W. Lengemann, Whole Body Counters, AEC, February 1967.

NEWSPAPER, MAGAZINE, AND JOURNAL ARTICLES

Abrahamson, Dean E., "Energy Policy with Guns," Environment, October 1974.

Anatasia, George, "An A-plane Regenerates a Town," Philadelphia Inquirer, January 25, 197[illegible]

Anderson, Jack, "Bomb Detection," The Washington Post, September 9, 1973.

Anderson, Jack, and Les Whitter, "Terrorists Get Missiles," The Washington Post, May 14, 1976.

Anderson, Jack, "Urban Guerrilla Operations Feared," The Washington Post, April 23, 1974.

Anderson, Jack, "Will Nuclear Weapons Fall Into the Hands of Terrorists?," The Washington Post, September 29, 1974.

Avenhaus, R. and D. Gupta, "Effective Application of Safeguards, Manpower, and Other Techniques in Fuel Cycles," in IAEA, Vol. I, 1970.

Baldwin, D. A., "Thinking About Threats," Journal of Conflict Resolution, 15, 71, 1971.

Bupp, Jr., Irwin C. and Jean-Claude Derian, "Nuclear Reactor Safety: The Twilight of Probability," HBS Bulle[illegible], March/April 1976.

Burnham, David, "Nuclear Agency is Reported Ready to Oppose Special Force to Combat Terrorist Attacks at Facilities," New York Times, January 12, 1976.

Business Week, "New Alarms About Old Nuclear Wastes," February 2, 1976.

Camp, Patricia, "Atom Power Danger Cited," The Washington Post, November 17, 1975.

Cohen, Bernard, "Letter: 'Not So Malevolent,'" Bulletin of Atomic Scientists, February 1975.

Cole, Peter, "Battle Against Terror Turns International," The Washington Post, January 1, 1976.

Congressional Information Bureau, Inc., Atomic Energy Clearing House.

Congressional Record, "Activities and Accomplishments of the Joint Committee on Atomic Energy," Ninety-fourth Congress, Second Session, Vol. 122, No. 2, January 20, 1976, p. 5159.

Congressional Record, "The Safety and Security of Our Nuclear Exports," Ninety-fourth Congress, Second Session, Vol. 122, No. 21, February 18, 1976, p. 51800.

ERDA, Information from ERDA: Weekly Announcements, Washington, D. C.

Evans, Robert Dervel, "Brazil: The Road Back from Terrorism," Conflict Studies, No. 47, Institute for the Study of Conflicts, London.

Everts, Phillip P., "Developments and Trends in Peace and Conflict Research, 1965-1971: A Survey of Institutions," Journal of Conflict Resolution, Vol. XVI, No. 4, pp. 505-510.

Factory, "How Secure is Your Plant?," January, 1973.

Ferd, Bernard T., "Making the World Safe for Plutonium," Bulletin of the Atomic Scientists, May 1975.

Fialka, John, "Did Worker's Honor System Fail at Troubled Nuclear Plant?," The Washington Star, October 22, 1975.

Fialka, John, "Nuclear Waste Mounts and So Does the Peril," The Washington Star, February 29, 1976.

Frank, Forrest R., "An International Convention Against Nuclear Theft," Bulletin of the Atomic Scientists, December 1975.

Gapay, Les, "Fearsome Fuel: New Laws are Studied to Protect Shipments of Deadly Plutonium," The Wall Street Journal, October 23, 1975.

Gapay, Les, "Huge Power Stations for Solar Electricity are Decades in Future," Wall Street Journal, May 28, 1976.

Glenn, John, "Biting the Nuclear Bullet," The Washington Post, March 8, 1976.

Goin, Lauren J., "Terrorist Weapons of the Future," Public Safety Services, Inc., November 9, 1976.

Graham, N. F., "International Terrorism," Army Journal, No. 312, May 1975.

Halstead, Thomas A., "The Spread of Nuclear Weapons—Is the Dam About to Burst?," Bulletin of the Atomic Scientists, May 1975.

Hippel, Frank, "The Nuclear Debate," Bulletin of the Atomic Scientists, May 1975.

Hoffacker, Lewis, "The U. S. Government Response to Terrorism," Vital Speeches of the Day, February 15, 1975.

Horchem, Hans Josef, "West Germany's Red Army Anarchists," Conflict Studies, No. 46, Institute for the Study of Conflicts, London.

_____, "How Safe is Nuclear Power?," Newsweek, April 12, 1976, p. 70.

Howard, Bruce, "Living With Terrorism," The Washington Post, July 18, 1976.

Ingram, Timothy H., "Nuclear Hijacking: Now Within the Grasp of Any Bright Lunatic," Washington Monthly, January 1973, pp. 20-28.

Jenkins, Brian, "International Terrorism: A Balance Sheet," Survival, July, August 1975.

Johnson, Kenneth F., "Guatemala: From Terrorism to Terror," Conflict Studies, No. 23, Institute for the Study of Conflicts, London.

Jones, Robert A., "Danger of Nuclear Terrorism Likely to Increase," The Los Angeles Times, August 25, 1976.

Kahan, James and Amnon Rapoport, "Decisions of Timing in Conflict Situations of Unequal Power Between Opponents," Journal of Conflict Resolution.

Krieger, David, "Terrorists and Nuclear Technology," Bulletin of Atomic Scientists, June 1975.

Los Angeles Herald Examiner, "Nuclear Arms Fuel Missing," July 29, 1976.

Lyons, Richard, "House Bars Private Output of A-Fuel," The Washington Post, July 31, 1976.

McElhery, Victor, "Con Ed Defends Safety of Its Indian Point Nuclear Plant," The New York Times, February 19, 1976.

McPhee, John, "Profiles: The Curve of Binding Energy–Theodore B. Taylor, Parts I, II, and III," The New Yorker, December 3, 10, and 17, 1973.

Minogue, Joseph, "Costs of a Year of Terror," The Washington Post, October 12, 1976.

Mitchell, Henry, "A Tale of Terror, Peace and Our Times," The Washington Post, August 5, 1976.

The Montgomery Advertiser, "Ford Urged to Reject Uranium Proposal," November 9, 1975.

Moss, Robert, "Urban Guerrillas in Latin America," Conflict Studies, No. 8, Institute for the Study of Conflicts, London.

Moss, Robert, "Uruguay: Terrorism versus Democracy," Conflict Studies, No. 14, Institute for the Study of Conflicts, London.

The New York Times, "Agency is Reported Ready to Oppose Special Force to Combat Terrorist Attacks at Facilities," January 12, 1976.

The New York Times, "Special Forces to Combat Terrorist Attacks at Facilities," January 12, 1976.

The New York Times, "Vienna Panel Proposes Stricter Guarding of Nuclear Material," May 3, 1975.

Newsweek, "The Morality of Terrorism," February 25, 1974.

Nuclear News, "The Safeguards Issue," August 1974.

O'Toole, Thomas, "A-Bomb Proliferation Feared," The Washington Post, May 5, 1975.

O'Toole, Thomas, "G. E. Asks to Sell A-Plants to South Africa," The Washington Post.

O'Toole, Thomas, "U. S. Nuclear Stores in Europe Criticized," The Washington Post, May 1, 1975.

Peterson, John, "Scientists' Panel Sees More Terrorism Ahead," The National Observer, October 4, 1975.

_____, "The Plutonium Connection," TV Guide, March 8-14, 1975.

"Plutonium Recycle or Civil Liberties," Environmental Action, December 3, 1975.

Popov, Milorad, "The American Extreme Left: A Decade of Conflict," Conflict Studies, No. 29, Institute for the Study of Conflicts, London.

Quester, George H., "Can Proliferation Now Be Stopped?," Foreign Affairs, October 1974.

Reed, Thomas C., "Can We Reach Our Tricentennial?," Washington Report, August 1976.

Ross, Nancy L., "Detective Firm Says It Uses Right-Wing Group's Data," Washington Post, January 27, 1977.

Ruckle, William, et al., "Ambushing Random Walks 1: Finite Models," Operations Research, Vol. 24, No. 2, March-April 1976, pp. 314-323.

Sastre, C., "Summary of U. S. Qualitative Safeguards Technique," in IAEA, Vol. II, 1970.

Shapley, D., "Plutonium: Reactor Proliferation Threatens a Nuclear Black Market," Science, 172, 143, 1971.

Smith, Darryl B., and Ivan Waddoups, "Safeguarding Nuclear Materials and Plants," Power Engineering, November 1976, pp. 36-43.

Speth, Gus, Arthur Tamplin, and Thomas Cochran, "Plutonium Recycle or Civil Liberties? We Can't Have Both," Environmental Action, December 7, 1974.

Stenmeyer, W., "The Ideological Criminal," Congressional Record, S9185, June 16, 1971.

Stevenson III, Adlai E., "Nuclear Reactors: America Must Act," Foreign Affairs, October 1974.

Taylor, Theodore," Nuclear Terrorism: A Threat of the Future?," Science Digest, August 1974.

Time Magazine, "The City as Battlefield: A Global Concern," November 2, 1970.

Time Magazine, "The Great Nuclear Debate," December 8, 1975.

Time Magazine, "When Terrorists Become Respectable," November 25, 1974.

U. S. News and World Report, "Harnessing H-Bomb for Energy: 'Breakthrough in Five Years,'" February 17, 1975.

The Washington Post, "Australia Seeks 'Atom Guerrilla,'" April 23, 1974.

The Washington Post, "Congress Probes Resignations from G. E. A-Reactor Plant," February 4, 1976.

The Washington Post, "Terrorist Use of Atom Bomb Held Possible," April 7, 1974.

Washington Report, "If Terrorism Goes Nuclear . . .." May 1976.

The Washington Star, "No Danger Seen From A-Plant Leak," January 2, 1976.

The Washington Star, "Nuclear Plant Critics: Why They Quit G. E.," February 11, 1976.

Willrich, Mason, "Terrorists Keep Out!," Bulletin of the Atomic Scientists, May 1975.

Wilson, Richard, "Where Did We Put That Nuclear Reactor?," The New York Times, January 3, 1976.

REPORTS, DOCUMENTS, THESES, AND REGULATIONS

A.E.C., Directorate of Regulatory Standards, Analysis and Use of Process Data for the Protection of Special Nuclear Material, June 1974.

A.E.C., Directorate of Regulatory Standards, Environmental Survey of Transportation of Radioactive Materials To and From Nuclear Power Plants (WASH-1238), December 1972.

A.E.C., Everything You Always Wanted to Know about Shipping High-Level Nuclear Wastes (WASH-1264), August 1974.

A.E.C., Physical Protection of Classified Matter and Information: Security Handbook, January 21, 1970.

The Aerospace Corporation, The Escort Force for the Transport of Special Nuclear Materials (ATR-75(7251)-1), September 1975.

Anderson, Marion, Fallout on the Freeway: The Hazards of Transporting Radioactive Wastes in Michigan, Public Interest Research Group, Michigan, January 18, 1974.

Bain Jr., E. E. and Emanuel Gordon, Summary Report–Fuel Cycle Conference '76, Vol. 3, No. 3, June 1976.

Barlow, Richard, et al., Reliability and Fault Tree Analysis: Theoretical and Applied Aspects of System Reliability and Safety Assessment, 1975.

Bartkus, Robert and Gail Block, Conference on the Impact of Intensified Nuclear Safeguards on Civil Liberties, October 1975.

Barton, John H., Intensified Nuclear Safeguards and Civil Liberties, October 31, 1975.

Battelle, Final Report on the Development of a Statement of Objectives for the Safeguards Program, June 30, 1975.

The BDM Corporation, Draft Working Paper B–Summary of Findings, Analysis of the Terrorist Threat to the Commercial Nuclear Industry, September 12, 1975.

The BDM Corporation, Draft Working Paper C: Supporting Appendices–Analysis of the Terrorist Threat to the Commercial Nuclear Industry, September 30, 1975.

Bennett, Carl A., Validating Safeguards Information, Battelle, April 1972.

Bennett, Carl, William Murphey, and Theodore Sherr, Societal Risk Approach to Safeguards Design and Evaluation (ERDA-7), June 1975.

Berkowitz, B. J., et al., Superviolence: The Civil Threat of Mass Destruction Weapons, Adcom Corporation, September 29, 1972.

Billington, George R., Nuclear Terrorism.

Brown, William F., ed., A.M.R.'s Guide to Computer and Software Security, AMR International, Inc.

Central Electricity Generating Board, Basic Emergency Plan, Nuclear Health and Safety Department, January 1973.

Clark, R. G., A Methodology for Coping With Sabotage and Diversion at Commercial Nuclear Facilities, Battelle, July 1974.

Clune III, W. H., Standards and Decision Rules for Evaluating Trade-Offs Between Civil Liberties and Nuclear Materials Safeguards, October 31, 1975.

Cohen, Bernard L., The Hazards in Plutonium Dispersal, University of Pittsburgh, July 1975.

Collins, J. D., System Survivability Analysis, J. H. Wiggins Company.

Committee on Internal Security, House of Representatives, Terrorism: Part 4, Ninety-Third Congress, Second Session, July 30, August 1, 15, and 20, 1974.

Committee on Internal Security, United States House of Representatives, Terrorism: A Staff Study, Ninety-Third Congress, Second Session, August 1, 1974.

Connelly, Ralph William, Third Party Involvement in International Terrorist Extortion, Naval Postgraduate School, March 1976.

Cusack, J. H., et al., Draft Final Report on Confirming the NRC Safeguard Objective, Brookhaven National Laboratory, August 29, 1975.

Cusack, J. H., et al., Draft Final Report on Evaluation of the Impact of Safeguards Measures, Brookhaven National Laboratory, August 20, 1975.

Defense Documentation Center, Defense Documentation Center Referral Data Bank Directory (AD-A031 400), October 1976.

Deken, George T., Role of the Military in Combating Urban Terrorism in the United States.

deLeon, Peter, Scenario Designs: An Overview (R-1218-ARPA), The Rand Corporation, June 1973.

Delong, Thomas W., A Fault Tree Manual, Texas A and M University, December 1970.

DeNike, L. Douglas, Radioactive Malevolence, Science and Public Affairs, February 1974.

Department of Navy—Bureau of Aeronautics, Progress Report No. 7 (D.I.C.7269), August 1955.

DeWeerd, H. A., A Contextual Approach to Scenario Construction, The Rand Corporation, September 1973.

Dukert, Joseph M., High-level Radioactive Waste: Safe Storage and Ultimate Disposal, ERDA, 1975.

Edlow, S., Traffic Management in Nuclear Safeguards, and Discussion of Transportation Safeguards, in AEC, 1969a.

"Environmental Alert Group," Nuclear Terrorism, Public Interest Report (Environmental Index No. 75-03939).

E. R. Johnson Associates, Inc., An Upper Estimate of Safeguards for Handling Plutonium.

ERDA, Alternatives for Managing Wastes from Reactors and Post-Fission Operations in the LWR Fuel Cycle (ERDA-76-43), Volumes 1-5, May 1976.

ERDA, Societal Risk, Approach to Safeguards Design and Evaluation.

Ericson, C. A., System Safety Analytical Technology: Fault-Tree Analysis.

Executive Office of the President, Office of Civil and Defense Mobilization, Standards for Physical Security of Industrial and Governmental Facilities, October 1958.

FBI Uniform Crime Reports, United States Department of Justice, Bomb Summary: A Comprehensive Report of Incidents Involving Explosive and Incendiary Devices in the Nation, 1975.

Federal Register, Licensing of Production and Utilization Facilities, July 18, 1974.

Federal Register, Part II: Department of Transportation—Hazardous Materials Regulations, Vol. 41, No. 74, April 15, 1976.

Federal Register, Part II: Department of Transportation—Transportation or Storage of Military Explosives on Board Vessels, Vol. 41, No. 132, July 8, 1976.

Federal Register, Title 49, Transportation: Consolidation of Hazardous Material Regulations, Department of Transportation, June 24, 1976.

Frye, John C., Transportation of High-Level Nuclear Wastes (ERDA-8), February 12, 1975.

Fullwood, Ralph R., Review of Probabilistic LWR Safety Assessment.

Fussell, J. B., Synthetic Tree Model: A Formal Methodology for Fault Tree Construction, March 1973.

Goodman, Raymond, et al., Air Command and Staff College: A compendium of European Theater Terrorist Groups, Air University; May 1976.

Goodridge, W., A Review of Transport Accidents and Incidents Involving Radioactive Material—1948 to 1965 (AHSB (S) M 156), United Kingdom Atomic Energy Authority, 1966.

Gref, Lynn G. and Jack W. Rosengren, An Assessment of Evaluation Techniques for MOX Interim Safeguard Rules, R&D Associates, October 4, 1976.

Harden, Jon David, A Planning Model for Route Security, U. S. Naval Postgraduate School, December 1967.

Hartley, D. B., Terrorist Incident Reporting System (TIRS).

Hemphill, Jr., Charles F., and John M. Hemphill, Security Procedures for Computer Systems, Dow Jones-Irwin, Inc., 1973.

Hiltz, P. A., The Fundamentals of Fault-Tree Analysis, North American Aviation, Inc., March 1963.

Hodge, C. V., Fault Tree Approach to Transportation Safeguards, N.R.C., Division of Materials and Fuel Cycle Facility Licensing, August 1975.

Holmes & Narver, Inc., Hazards Evaluation of Nuclear Facility Related Transportation Accidents, (HN-8147.4), August 1973.

Horowitz, Irving L., Political Terrorism and Personal Deviance, Department of State, Office of Research and Analysis for Near East, Summary of Remarks at a Conference Sponsored by The Bureau of Intelligence and Research and the Planning and Coordination Staff, February 15, 1973.

International Bridge, Tunnel & Turnpike Association, Inc., Compendium of Regulations: Shipments of Radioactive Materials Over Toll Roads, Bridges, & Tunnels, February 1974.

Jacobson, Robert V., Computer Security Planning: An Annotated Bibliography, The Senator Security Group, Inc., 1974.

Jenkins, Brian Michael, High Technology Terrorism and Surrogate War: The Impact of New Technology on Low-Level Violence, The Rand Corporation, January 1975.

Jenkins, Brian, International Terrorism: A New Kind of Warfare, The Rand Corporation, June 1974.

Jenkins, Brian M., Terrorism and Kidnapping, The Rand Corporation, June 1974.

Jenkins, Brian M., Terrorism Works—Sometimes, The Rand Corporation, April 1974.

Jenkins, Brian, Will Terrorists Go Nuclear?, The Rand Corporation, November 1975.

Korcher, R. H., Safte-1, Version 4, Holmes & Narver, Inc., Los Angeles.

Kelley, Clarence M., Crime in the United States: 1975, FBI Uniform Crime Reports, August 25, 1976.

Kellen, Konrad, Reaction Forces Against Nuclear Diversion on Sabotage: An Inventory of Considerations, The Rand Corporation, October 1975.

Kingsley, S. G., Discussion of Transportation Safeguards, in AEC, 1969a.

Lambert, Howard E., Fault Trees for Decision Making in Systems Analysis, Lawrence Livermore Laboratory, October 9, 1975.

Larsen, Waldemar F., Fault Tree Analysis, Picatinny Arsenal, Dover, New Jersey, January 1974.

Lawrence Livermore Laboratory and Science Applications Incorporated, Executive Summary of the Special Safeguards Study on Material Control and Accounting Systems, September 15, 1976.

Lippian, Joseph M., The Transportation of Hazardous Material: Transport of Benzene by Tank Car, Army Materiel Command, May 1973.

Los Alamos Scientific Laboratory of the University of California, Preparation of Working Calibration and Test Materials: Plutonium Nitrate Solution (NUREG-0118), January 1977.

McGuire, Relationship Between Assignment of Responsibility and Assignment of Cost for Nuclear Security Forces.

Mabry, Jr., Robert Caldwell, Nuclear Theft: Real and Imagined Dangers, Naval Postgraduate School, March 1976.

The Mitre Corporation, The Threat to Licensed Nuclear Facilities, (MTR-7022), September 1975.

Monsanto Research Corporation, Mound Laboratory, Communication for Fixed Sites.

National Council on Radiation Protection and Measurements, Basic Radiation Protection Criteria, 1971.

Nehem, R. F., GERT: Graphical Evaluation and Review Technique: A Quantitative Hazard Analysis Tool (AD-771 106), USAMC Intern Training Center, May 1973.

Novotny, E. J., and A. G. Whitley, A Selected Bibliography on the Terrorist Threat to the Commercial Nuclear Industry, The BDM Corporation, September 30, 1975.

NRC, Final Generic Environmental Statement on the Use of Recycle Plutonium in Mixed Oxide Fuel in Light Water Cooled Reactors: Health, Safety, and Environment (NUREG-0002), Vol. 1-5, 1976.

NRC, Liquid Pathway Generic Study (NUREG-0140), September 1976.

NRC, Office of Nuclear Material Safety and Safeguards, Security Agency Study (NUREG-0015), August 1976.

NRC, Office of Special Studies, Special Safeguards Study: Scopes of Work (NUREG 75/06-), June 1975.

NRC, Office of Standards Development, Division of Engineering Standards, Transport of Radioactive Material in the U. S.: A Detailed Summary of "Survey of Radioactive Material Shipments in the United States" BNWL-1972 (NUREG-0073), May 1976.

N.R.C., Office of Standards Development, Draft Environmental Statement on the Transportation of Radioactive Material by Air and Other Modes (NUREG-0034), March 1976.

N.R.C., Office of Standards Development, Potential Releases of Cesium from Irradiated Fuel in a Transportation Accident: Supplement II to WASH-1238 (NUREG-0069), July 1976.

N.R.C., Reactor Safety Study: An Assessment of Accident Risks in U. S., Commercial Nuclear Power Plants, October 1975.

N.R.C., United States Nuclear Regulatory Commission: News Releases, NRC, Office of Public Affairs, Washington, D. C.

Nuclear Regulatory Commission Authorizing Legislation—Fiscal Year 1977, Hearings Before the Subcommittee on Legislation of the Joint Committee on Atomic Energy, Congress of the United States, Ninety-fourth Congress, January 29, February 17, and March 19, 1976.

Office of the Federal Register, Code of Federal Regulations: 10 Energy, January 1, 1976.

Office of the Federal Register, Code of Federal Regulations: 49 Transportation, Parts 100 to 199, October 1, 1975.

Patterson, D. E., The Accident Experience of the USAEC in the Shipment of Radioactive Material.

R&D Associates, Capabilities Statements for Assisting the NRC in Defining the Scope, Content, Structure, and Utilization of a Threat Assessment and Alert Dissemination Data Base.

R&D Associates, A Corporate Profile, October 1975.

R&D Associates, Support of the Decision Concerning the Wide-Scale Use of Mixed Oxide Fuel, Vol. 1, August 1976.

The Rand Corporation, Increasing Computer Security Via Entrapment Strategy (P-5084).

The Rand Corporation, Overview of Scenario Design (R-1218).

The Rand Corporation, Thoughts on Comparing Guard Force Concepts for the Protection of Nuclear Powerplants and Material, November 1975.

Reinking, A., et al., Public Health Risks of Thermal Power Plants: Appendix V—Transportation of Nuclear Fuel, School of Engineering and Applied Science, University of California, May 1972.

Roberts, Kenneth E., The Terror Trap, Strategic Studies Institute, U. S. Army War College, August 27, 1975.

Rosenbaum, David M., et al., Special Safeguards Study, April 1974.

Sandia Laboratories, Fixed-Site Physical Protection Systems.

Sandia Laboratories, Intrusion Alarm and Assessment Systems.

Sandia Laboratories, Limitations on Personnel Access to Material Access Areas and Vital Areas.

Sandia Laboratories, Role of Communications in Transportation Safeguards.

Schleter, John C., and William M. Murphey, Framework of the Safeguards Information System (NBS Document SIRM-59), Center for Radiation Research, National Bureau of Standards, May 21, 1975.

Simmons, J. L., M. O. Cloninger, and A. E. Medford, Survey of Radioactive Material Shipments in the United States (BNWL-1972), Battelle, April 1976.

Stewart, J. E., and Rainer Herter, Solid Radwaste Experience in Europe Using Asphalt (75-Pwr-21), The American Society of Mechanical Engineers, September 1975.

Subcommittee on Energy and the Environment of the Committee on Interior and Insular Affairs, Safeguards in the Domestic Nuclear Industry, Committee Print No. 17, August 1976.

Subcommittee to Investigate the Administration of the Internal Security Act and other Internal Security Laws of the Committee on the Judiciary, United States Senate, Terroristic Activity: Parts 1, 2, 3, and 4, Ninety-Third Congress, Second Session and Ninety-Fourth Congress, First Session.

Taylor, Theodore B., Response to Non-conventional Nuclear Threats.

Todd, J. L., and W. C. Nickell, Phyiscal Security System Effectiveness Evaluation: A Status Report (SAND 75-0391), Sandia Laboratories, July 1975.

Toner, Kevin J. and Harold A. Feiveson, Responsibility for Nuclear Security, September 1975.

U. S. Coast Guard, Annual Statistics of Casualties, January 1976.

United States Department of Justice, Federal Bureau of Investigation: Annual Report for Fiscal Year 1975.

United States Marshal Service, Security of Special Nuclear Material, October 1975.

Wasson, Muir M., Site and District Emergency Procedure, Bradwell Nuclear Power Station, Essex, England.

APPENDIX A
IDENTIFICATION OF FEASIBLE ADVERSARY ACTION CLASSES

Chapter 3, Adversary Action Sequences, dealt with the total number of possibly differing adversary action classes arising from variations in an adversary's resources and attributes (R&A's). They numbered in the millions. However, there are some practical considerations which limit the number of adversary action sequences which are feasible. For example, three unarmed people cannot mount a force type attack on an SSNM shipment. The scenario, although theoretically possible, is practically unrealistic. Thus, the number of different adversary action sequences can, for all practical purposes, be reduced considerably.

The objective in this Appendix is to identify the feasible or practical adversary action classes. First, it is necessary to have some idea of the defenses of a protective system. For purposes of illustration, a protective system around a truck means of transport is described. For another mode of transportation analogous protective mechanisms can be assumed.

Protective System

- Security clearance on all relevant personnel
- Armed escort for truck (semi-automatic weapons)
- Reinforces truck with immobilization facilities
- Frequent radio communications with LLEA's.

The R&A's Adversary Type, Objectives and Intended SSNM Use are now considered, and a description of the feasible adversary action classes arising from them is given. First, consider which Intended SSNM Uses may reasonably arise from the various objectives. Table A-1 describes the situation.

Table A-1. Feasible Adversary Action Classes Categorized by Objective and Intended SSNM Use

	INTENDED SSNM USE					
OBJECTIVES	Detonation of a Nuclear Device	Dispersion	Political Blackmail	Financial Blackmail	Sale to 3rd Party	Sabotage (On-Site Dispersion)
Revenge		X				X
Personal Gain				X	X	
Political/ Sociological	X	X	X			X

In theory, there are 7 x 3 = 21 combinations of adversary action classes representing differing values of the "objectives" and "intended SSNM use" parameters. However, from the table, one observes that only 8 of these combinations represent feasible adversary action descriptions.

We continue with a description of which combinations of "adversary type" and "objectives" are practical.

Table A-2. Feasible Adversary Action Categorized by Adversary Type and Objectives

ADVERSARY TYPE	OBJECTIVES		
	Revenge	Personal Gain	Political/ Sociological
Ad Hoc–Criminal		X	
Professional Criminal–Criminal		X	
Dissident Employee(s)–Dissident	X	X	
Sociopathic–Demented	X	X	
Separatists (Domestic)–Dissident			X
Revolutionaries (Domestic)–Dissident	X		X
Reactionary Extremists–Dissident			X
Issue Oriented (Violent)–Dissident			X
Separatists (Foreign)–Dissident			X
Revolutionaries (Foreign)–Dissident			X

Table A-2 shows that a significant reduction has been obtained. A further reduction in the number of feasible classes can be obtained by combining Tables A-1 and A-2, through the elimination of the "objective" parameter. Table A-3 describes the result.

Table A-3. Feasible Adversary Action Classes Categorized by Adversary Type and Intended SNM Use

ADVERSARY TYPE	INTENDED SNM USE: Detonation of a Nuclear Device	Dispersion	Political Blackmail	Financial Blackmail	Sale to 3rd Party	Sabotage (On-site Dispersion)
Ad Hoc–Criminal				X	X	
Professional Criminal–Criminal				X	X	
Dissident Employee(s)–Dissident		X		X	X	X
Sociopathic–Demented		X		X	X	X
Separatists (Domestic)–Dissident	X	X	X			X
Revolutionaries (Domestic)–Dissident	X	X	X			X
Reactionary Extremists–Dissident	X	X	X			X
Issue Oriented (Violent)–Dissident	X	X	X			X
Separatists (Foreign)–Dissident	X	X	X			X
Revolutionaries (Foreign)–Dissident	X	X	X			X

A similar analysis on the Number of Personnel, Arms, Intelligence Aid/Information and Mode of Attack categories may now be carried out. The idea is to give the modes of attack that are possible for a given level of personnel, arms, and intelligence aid/information. Table A-4 details only Arms and Intelligence Aid/Information.

(If a mode attack is given as mostly stealth or little deceit, etc., it is assumed that the rest of the attack is by force.)

Table A-4. Feasible Modes of Attack for a Given Arms/Intelligence Level

ARMS LEVEL	INTELLIGENCE AID/INFORMATION LEVEL		
	Low Threat Level	Medium Threat Level	High Threat Level
Low Threat Level	No Scenarios	Stealth Mostly Stealth	Stealth Deceit Mostly Stealth Mostly Deceit
Medium Threat Level	A Little Stealth	Stealth Mostly Stealth Little Stealth Little Deceit	Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit
High Threat Level	Force Little Stealth	Force Stealth Mostly Stealth Little Stealth Little Deceit	Force Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit

Next, the effect of the number of personnel on this situation is considered. Due to the number of concurrent tasks that need to be carried out in a Force attack, the meaning of this consideration is that a Force attack is only feasible when a small number of personnel are involved. The following possibilities then arise.

Table A-5. Feasible Modes of Attack for a Given Arms/Personnel/ Intelligence Level

PERSONNEL LOW THREAT LEVEL

ARMS LEVEL	INTELLIGENCE AID/INFORMATION LEVEL		
	Low Threat Level	Medium Threat Level	High Threat Level
Low Threat Level	No Scenarios	Stealth Mostly Stealth	Stealth Deceit Mostly Stealth Mostly Deceit
Medium Threat Level	No Scenarios	Stealth Mostly Stealth	Stealth Deceit Mostly Stealth Mostly Deceit
High Threat Level	Little Stealth	Stealth Mostly Stealth Little Stealth Little Deceit	Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit

PERSONNEL MEDIUM THREAT LEVEL

ARMS LEVEL	INTELLIGENCE AID/INFORMATION LEVEL		
	Low Threat Level	Medium Threat Level	High Threat Level
Low Threat Level	No Scenarios	Stealth Mostly Stealth	Stealth Deceit Mostly Stealth Mostly Deceit
Medium Threat Level	Little Stealth	Stealth Mostly Stealth Little Stealth Little Deceit	Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit
High Threat Level	Force Little Stealth	Force Stealth Mostly Stealth Little Stealth Little Deceit	Force Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit

PERSONNEL HIGH THREAT LEVEL

INTELLIGENCE AID/INFORMATION LEVEL

ARMS LEVEL	Low Threat Level	Medium Threat Level	High Threat Level
Low Threat Level	No Scenarios	Stealth Mostly Stealth	Stealth Deceit Mostly Stealth Mostly Deceit
Medium Threat Level	Little Stealth	Stealth Mostly Stealth Little Stealth Little Deceit	Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit
High Threat Level	Force Little Stealth	Force Stealth Mostly Stealth Little Stealth Little Deceit	Force Stealth Stealth Deceit Mostly Stealth Mostly Deceit Little Stealth Little Deceit

Feasible Modes of Attack for a Given Arms/Intelligence/Personnel Level

A further reduction on the number of scenario classes can be achieved by combining the following categories into two classifications:

Dedication
Training and Planning
Security Systems Knowledge and Combat-Type Experience

} Efficiency

Money
Transportation of Adversary Equipment

} Physical Resources (not including arms)

Each of these headings could be broken into 3 levels: Low, Medium and High Threat Levels.

Thus, a considerable reduction of the number of adversary action classes has been achieved. There are 36 adversary action classes for Adversary Type by Intended SNM Use, 85 feasible Modes of Attack for various Arms/Intelligence/Personnel Threat Levels, 3 Efficiency levels, and 3 levels of Physical Resources (not including Arms).

Altogether, there are 36 x 85 x 3 x 3 = 27540 possible adversary action classes.

Clearly, this is still too large a number. However, it is two orders of magnitude less than the original number of possibilities.

A further reduction on the number of adversary action classes can be achieved by combining more categories and by further detailed study of the divisions within the categories.

APPENDIX B
DEPENDENCE/INDEPENDENCE OF SAFEGUARD SYSTEM COMPONENTS

APPENDIX B
DEPENDENCE/INDEPENDENCE OF SAFEGUARD SYSTEM COMPONENTS

B.1 Observations

The vulnerability of protective mechanism PM_j to the kth class of advisary was defined to be $V(PM_j/S_k)$. Since the system consists of the set of PM_j, the total system vulnerability to the kth class of advisary is

$$V_k = \prod_{j=1}^{N} V(PM_j/S_k) \qquad \text{(B-1)}$$

Implicit in the above equation are the assumptions that (a) the PM_jLs are independent of one another, and (b) the system vulnerability is independent of the order in which the PM_j's are attacked.

It was evident during the early part of this study that errors in the vulnerability estimates will occur if the above assumptions are not addressed. It was felt, however, that for purposes of comparing and evaluating one system concept relative to another, the independence/dependence issue could be ignored in the first approximation. Furthermore, the Delphi panel would automatically consider these assumptions, and hence, temper their scores accordingly.

The matrix in Table 4-3 shows one such score sheet. Note the discrepancy between V_k as a result of the formula and as estimated by the panel. It is clear that the panel could not deal with numbers smaller than 10^{-3} ("one in a thousand"). Thus, although their computed system vulnerabilities are of order 10^{-6} (from the individual component vulnerabilities), their direct estimate of the total system vulnerability is of equal magnitude to the component vulnerability. When asked about this, the principal reason provided was that if an adversary was clever enough to successfully defeat one PM, he is most likely to also defeat another. Thus, if the system consists of two protective mechanisms, if the first one be defeated by one adversary class with a probability of 0.1, and the second one with a probability of 0.1, the mathematically calculated system vulnerability is 0.01, whereas the panel member will probably estimate the system vulnerability to be of order 0.1.

The above has far-ranging implications — and should be looked into — for example, in reactor safety calculations, system failure probabilities are after calculated to be of order 10^{-8} to 10^{-12} (from the subsystem failure probabilities), whereas, when equally knowledgeable people are asked to estimate the total system failure probability, a much larger answer is usually given.

B.2 Vulnerability Equations with Dependence

There are several ways of dealing with dependence and the order in which the PM's are attached. One such method is to formulate the equations directly:

Define the following:

A = attack occurs

$P(PM_j/A)$ = probability the protective mechanism PM_j will be successful in performing its function, given an attack A

$\overline{PM_j}$ = denotes protective mechanism PM_j has failed.

V_s = system vulnerability

Take a system consisting of two protective mechanisms, PM_1 and PM_2. If the two are independent, then:

$$V_s = [1-P(PM_1/A)]\ [1-P(PM_2/A)] \tag{B-2}$$

If they are not independent, and PM_1 is attacked first, then:

$$V_s = [1-P(PM_1/A)]\ [1-P(PM_2/\overline{PM_1}A)] \tag{B-3}$$

The above says that the system vulnerability is equal to the vulnerability of PM_1 given an attack, times the vulnerability of PM_2 given an attack and PM_1 has failed.

Similarly, if PM_2 is attacked first, then:

$$V_s = [1-P(PM_2/A)]\ [1-P(PM_1/PM_2A)] \tag{B-4}$$

A similar set of equations can be generated with three or more components. The same Delphi method can be used to estimate the component probabilities with one major difference: the sequence of the attack has to be considered.

APPENDIX C
VULNERABILITY INFORMATION FROM THE GENERIC VULNERABILITY ASSESSMENT

The Delphi panel assessed the vulnerabilities of three safeguards systems against three classifications of adversary actions. The systems, representative adversary actions and the panel's composite evaluations, are described below.

This evaluation was carried out by considering the protective mechanisms that comprise the safeguards systems. A further assessment was conducted by the panel when they assessed the vulnerability of the safeguards system as a whole. Their assessments are given at the end of this appendix.

SAFEGUARDS SYSTEMS

SAFEGUARDS SYSTEM A

This is a minimum safeguards system for a highway transport mode, based upon federal regulations (c.f. 10 CFR § 73.1). Daylight transit is required. This is not a protective mechanism in itself. It raises the efficiency of many of the following protective mechanisms which describe the system.

PM1—Vehicle Velocity

No intermediate stops are scheduled for the convoy. However, some unplanned stops can be made based on a need for fuel or vehicle maintenance and stops for the convenience of the truck crew.

PM2—Presence of the Crew in the Truck Cab

There are two crew members (unarmed). At least one is vigilant all the time and the other member of the crew may not be present in the cab during stops.

PM3—Presence of an Armed Escort

There is one escort car, which accompanies the SSNM truck. The escort car contains two armed guards. There is a continuous radio communication capability between the escort car and the SSNM truck.

PM4—Local Law Enforcement Agency (LLEA) Response Force

This protective mechanism addresses the ability of an LLEA response force to overcome the adversaries. There is not a special response force within the LLEA. Any response to an alarm call would be treated in a routine police fashion. The following factors must be considered:

- An alarm must be raised. This can happen in various ways:

  1. There is a radio-telephone connection between the truck cab and the convoy's headquarters. This is the means of calling for assistance, once an attack or suspicious activities are noted. The convoy's headquarters relays the message to an LLEA.

  2. The escort car has a radio telephone which duplicates the lines of communication in the SSNM truck.

3. The convoy calls headquarters every two hours, as a routine check. If this call is not received, an LLEA is informed and emergency procedures commence.

4. An alarm may be raised by a passer-by.

- An LLEA response force must arrive before the attack is completed. The time limit depends upon the nature of the attack taking place and the protective mechanisms which determine the length of time the adversary needs to complete his attack.

- The ability of the response force to overcome the assailants must be considered.

PM5—Specially Designed Truck

The truck walls are one inch thick and the doors have reinforced locks.

PM6—Container Weight, Lock and Temper Seal

The SSNM is locked and sealed in containers weighing not less than 500 lbs.

PM7—Minimal Transit Time

Routes are planned to minimize transit time, thus giving an adversary less opportunity to mount an attack.

If the transit time is less than one hour, then only the driver need be in the truck cab.

PM8—Convoy Camouflage

The truck is ordinary in appearance except that it is marked on the top, sides and rear with identifying letters or numbers. The markings on top allow the identification of the vehicle under daylight conditions from the air in clear weather at 1000 feet above ground level. The side and rear markings are of a similar nature. The escort car is commonplace in appearance and keeps a reasonable distance from the truck while not compromising its position as an escort.

PM9—Natural Wariness of Unusual Activities

This is a catch-all protective mechanism which is concerned with suspicious behavior by unauthorized persons that might be detected by legitimate employees in the nuclear power or transportation industries or law enforcement agencies. Such suspicious behavior may take the form of unauthorized persons working in the neighborhood of a nuclear power plant, unexpected road blocks, etc.

SAFEGUARDS SYSTEM B

This safeguards system for a highway transport mode is also based upon federal regulations. However, improvements have been made to the requirements of the safeguards described there, in order to more accurately reflect current practices. The first nine protective mechanisms have the same title and perform the same function as those described in System A, though in some cases they have increased capacity. This is an aid to a comparison between the two safeguards systems.

Daylight transit is required. This is not a protective mechanism in itself. It raises the efficiency of many of the following protective mechanisms which describe the system.

PM1–Vehicle Velocity

No intermediate stops are scheduled for the convoy. However, some unplanned stops can be made based on a need for fuel or vehicle maintenance and stops for the convenience of the truck crew.

PM2–Presence of the Crew in the Truck Cab

The truck crew of two are both armed with M16's. They have both been trained in the use of firearms and receive periodic recurrent training. At least one is vigilant all the time and the other member of the crew may not be present in the cab during stops.

PM3–Presence of an Armed Escort

There are two cars, each containing two armed guards which escort the truck. One car is positioned in front of the truck, the other one behind it. Both cars are in visual contact with the truck and there is a CB radio communication between all three vehicles. The armed guards, as is the case with the truck crew, have received initial and recurrent training.

PM4–Local Law Enforcement Agency (LLEA) Response Force

This protective mechanism addresses the ability of an LLEA response force to overcome the adversaries. There is not a special force within the LLEA. Any response to alarm call would be treated in a routine police fashion. The following factors must be considered:

- An alarm must be raised. This can happen in various ways:

  1. There is a radio-telephone connection between the truck cab and the convoy's headquarters. This is the means of calling for assistance, once an attack or suspicious activities are detected. The convoy's headquarters relay the message to an LLEA.

  2. The escort car has a radio telephone which duplicates the lines of communication in the SSNM truck.

  3. The convoy calls headquarters every two hours, as a routine check. If this call is not received, an LLEA is informed and emergency procedures commence.

  4. An alarm may be raised by a passer-by.

- An LLEA response force must arrive before the attack is completed. The time limit depends upon the actual attack taking place and the protective mechanisms in operation, which determine the length of time the adversary needs to complete his attack.

- One must consider the ability of the response force to overcome the assailants.

PM5—Specially Designed Truck

The truck has immobilization devices, operated from the cab, which blow out the tires and lock the brakes. The truck cab is "bullet proof," thus enabling the truck crew to operate these immobilization devices while they are under fire. The walls of the truck are one inch thick. The truck doors have alarms attached to them and have reinforced locks. If these alarms go off or if the truck crew raise an alarm, a foam is released inside the truck. This rapidly fills all the truck and sets into a hard, impermeable material, thus forming an extra barrier around the SSNM.

PM6—Container Weight, Lock and Temper Seal

The SSNM is locked and sealed in containers weighing not less than 500 lbs.

PM7—Minimal Transit Time

Routes are planned to minimize transit time, thus giving an adversary less opportunity to mount an attack.

PM8–Convoy Camouflage

The truck is ordinary in appearance and no special markings are visible. The escort cars are similarly commonplace in appearance and keep a reasonable distance from the truck while not compromising their position as an escort.

PM9–Natural Wariness of Unusual Activities

This is a catch-all protective mechanism which is concerned with suspicious behavior by unauthorized persons that might be detected by legitimate employees in the nuclear power or transportation industries or law enforcement agencies. Such suspicious behavior may take the form of unauthorized persons working in the neighborhood of a nuclear power plant, unexpected road blocks, etc.

PM10–Personnel Screening

All relevant personnel have undergone psychological tests and have had background checks carried out upon them. (Key figures at the various nuclear facilities have security clearance.)

PM11–Hardware Security

The truck and escort cars are kept at a secured facility, when they are not in use. They are regularly serviced and are guarded insofar as they are kept in a protected site.

PM12–Convoy Information Security

There are six options for schedule/routing. The decision on which one is to be used is made one week before the convoy takes place. A minimal number of people are informed and any written information is kept in a locked cabinet.

SAFEGUARDS SYSTEM C

This protective system is based upon a convoy operating under more stringent procedures that are described in the literature.

As before, daylight transit is required. This is not a protective mechanism in itself. It raises the efficiency of many of the following protective mechanisms which describe the system.

PM1—Vehicle Velocity

The convoy operates on a non-stop, no detour basis. Routes are surveyed shortly before the convoy passes through. Obstructions, etc., are noted and corrective action is taken.

PM2—Presence of the Crew in the Truck Cab

Two men are in the cab, both present and vigilant all the time. They are armed with handguns and automatic fire-arms, and have received special training.

PM3—Presence of an Armed Escort

There are five escort vehicles in this convoy. A pick-up truck with a crew of two to four men is immediately in front of the transporter and a five-ton truck with a crew of four follows immediately behind. All the crew are armed with handguns and automatic fire-arms and have received special training. They also carry out any maintenance of the convoy, as the need arises. There is an escort car immediately in front of these vehicles and another one immediately behind. They each contain two people who are armed with handguns. The convoy commander also sits in the lead car. He is armed with a handgun and an automatic weapon and has received special training. Finally, there is a third escort car, which contains two people who are armed with handguns. They patrol the area around the convoy looking for suspicious activities, etc.

PM4—Local Law Enforcement Agency Response Force

This protective mechanism addresses the ability of an LLEA response force, specially trained and on alert while the convoy is in progress, to overcome the adversaries. The following factors must be considered:

- An alarm must be raised. This can happen in various ways:

1. The convoy commander, sitting in the lead car, is in radio-telephone communication with the home base. This is a means of calling for assistance, once an attack or suspicious activities are detected. The home base relays the message to an LLEA.

2. The transporter, the pick-up truck and the five-ton truck each have radio-telephones which duplicate the lines of communication of the lead car.

3. Three escort cars have radio communications with the LLEA. This is another means of calling for assistance.

4. There is a helicopter which escorts the shipment. This helicopter is in almost continuous radio communication with the convoy commander to coordinate any detours, etc. Any unplanned changes in schedule result in the helicopter raising an alarm. The helicopter also surveys the area surrounding the convoy for suspicious activities. The helicopter has radio connections with the home base and the LLEA.

5. The convoy commander is in almost continuous communication with the home base. Consequently, any cessation in communications would be noted very quickly and would result in the home base making an alarm call to the LLEA.

6. An alarm can be raised by a passer-by.

- The response force must arrive before the attack is completed. The time limit depends upon the actual attack taking place and the other protective mechanisms which determine the length of time the adversary needs to complete his attack. Note that one function of the helicopter is to keep the SSNM shipment under surveillance until the response force arrives. This impacts the ability of the adversaries to make their get-away.

- One must consider the ability of the response force to overcome the assailants.

PM5--Specially Designed Truck

The truck is a 5-axle semi-trailer equipped with:

- inner armored container
- access denial system
- immobilization system
- deterrent control system.

PM6—Container Weight, Lock and Temper Seal

The SSNM is locked and sealed in containers weighing not less than 2000 pounds.

PM7—Minimal Transit Time

The distances that the convoy traverses vary from 50 to 150 miles.

PM8—Convoy Camouflage

None.

PM9—Natural Wariness of Unusual Activities

This is a catch-all protective mechanism which is concerned with suspicious behavior by unauthorized persons that might be detected by legitimate employees in the nuclear power or transportation industries or law enforcement agencies. Such suspicious behavior may take the form of unauthorized persons working in the neighborhood of a nuclear power plant, unexpected road blocks, etc.

PM10—Personnel Screening

All personnel concerned with the convoy have undergone screening and psychological testing.

PM11–Hardware Security

The transporter and escort vehicles are kept in a secure facility, when they are not in use. They are regularly serviced and are guarded insofar as they are kept in a protected site. (Note that the convoy personnel includes men who can carry out maintenance and repairs on vehicles.)

PM12–Convoy Information Security

There are six options for schedule/routing. The decision on which one is to be used is made one week before the convoy takes place. A minimal number of people are informed and any written information is kept in a locked cabinet.

REPRESENTATIVE ADVERSARY ACTIONS

NUMBER OF PERSONNEL
CLASSIFICATION

REPRESENTATIVE ADVERSARY ACTION – NO. 1 A

TRANSPORT MODE: Highway
ADVERSARY TYPE: Dissident

OBJECTIVE: Political/Sociological
INTENDED SSNM USE: Nuclear Explosion

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Low Threat Level

   1 dressed as policeman
   2 dressed in road repair crew garb
   1 dressed in work clothes suitable to the region
   4 TOTAL

2. Arms: Medium Threat Level

   Pistols
   High powered, night vision, sniper-scope equipped rifle
   Automatic weapons

3. Intelligence Information: Medium Threat Level

   Know that PuO_2 shipment will be made some time during the week from fuel reprocessing plant to plutonium storage site.
   Know that 3 routes are used.
   Know junction which determines commitment to a specific route.
   Know convoy communications frequency.

4. Experience & Knowledge: Medium Threat Level

The group has the full technical capabilities needed to fabricate a fissile explosive device. Two members of the group are combat infantry veterans.

5. Dedication: Medium Threat Level

Willing to accept sustained discomfort and injury.

6. Organization, Planning, Training, & Security: Medium Threat Level

Substantial

7. Money: Medium Threat Level

$100,000

8. Transportation: Medium Threat Level

1 Light van (CB radio & police band radio; EMR insulation & ECM; convoy communications frequency scanner).
1 "Police" car (CB radio and police band radio).
2 Pickup trucks (CB radio).

9. Equipment: Medium Threat Level

Power tools
Hand tools
Plastic explosives
"A" frame hoist

MODE OF ATTACK: Some deceit, mostly force

ATTACK FEATURES

1. Target SSNM:

   PuO_2

2. Attack Zone:

   Isolated area within 30 miles of urban region.
   Clear weather.
   At sunset.
   High tension electrical transmission lines parallel the road.

3. Preparation:

   The dissidents position personnel so as to observe activities around the fuel reprocessing plant. Over a period of time, several convoys are followed to their destination—the plutonium storage site. Ambush locations are selected at one place along each of the three routes. During the course of this activity, the convoy communications frequencies are monitored with a scanner and an attempt is made to ascertain the transmission routine.

   Within the limits of security, the dissidents train by executing a mock attack. The six potential attack locations, and the planned escape routes, are reconnoitered by all.

   When the target convoy departs, the observer alerts the adversaries' "base camp" by public telephone. The van is dispatched to the critical road junction and the convoy's communication frequency is monitored. When the convoy is committed to a specific route, the dissidents are notified by coded CB transmissions and deploy to their assigned areas.

4. Convoy Immobilization:

   The following actions are timed with respect to the convoy's position and coordinated among the dissidents by coded CB transmissions:

- Oncoming traffic is detoured by barricades placed miles up the road beyond the ambush site.
- Codirectional traffic is detoured miles down the road before the ambush site after the convoy has passed.
- A pickup truck is overturned across the road at the ambush site and its cargo spilled.
- A "police car," with siren screaming, passes the convoy and arrives at the scene of the "accident" minutes before the convoy does.

5. ECM:

The dissidents have the capability to jam the convoy's communications. This is accomplished just before the convoy sees the "accident." (If the ambush site coincides, fortuitously, with the location of the high tension lines, jamming probably won't be necessary.)

6. Access to SSNM Truck:

Convoy escort car approached by "police" car. Occupants used to approach SSNM truck and gain access to personnel in truck cab. All convoy personnel rendered unconscious. Entire operation covered by hidden sniper.

7. Access to SSNM Container:

Truck doors blown open with explosives. SSNM moved to light van by use of "A" frame hoist and manhandling.

8. Attack Duration:

15 minutes (through escape initiation).

9. Getaway (toward urban region):

Light van, station wagon.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. Ability of dissidents to observe movements around the fuel reprocessing plant and to follow the convoys without detection.

2. Ability to determine convoy's communication frequency, codes, routine, and procedures.

3. Ability to conduct training without exposing the plan.

4. Effectiveness of detour ruse.

5. Effectiveness of "accident" ruse and communications jamming.

6. Ability of "Police" car and its occupants to escape detection as a counterfeit and imposters, respectively.

7. Effectiveness of ploy used to approach SSNM truck and dislodge the drivers.

8. Ability to gain entrance to the SSNM truck with plastic explosives and to remove the PuO_2 containers.

9. Ability to perpetrate the attack—and escape—within 15 minutes.

10. Ability to reach the urban center with the SSNM and to disappear in the city with it.

REPRESENTATIVE ADVERSARY ACTION -- NO. 1 B

TRANSPORT MODE: Highway
ADVERSARY TYPE: Dissident

OBJECTIVE: Political/Sociological
INTENDED SSNM USE: Nuclear Explosion

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Medium Threat Level

   2 dressed as policemen
   5 dressed in road repair crew garb
   1 dressed in work clothes suitable to the region
   8 TOTAL

2. Arms: Medium Threat Level

   Pistols
   High powered, night vision, sniper-scope equipped rifle
   Automatic weapons

3. Intelligence Information: Medium Threat Level

   Know that PuO_2 shipment will be made some time during the week from fuel reprocessing plant to plutonium storage site.
   Know that 3 routes are used.
   Know junction which determines commitment to a specific route.
   Know convoy communications frequency.

4. Experience & Knowledge: Medium Threat Level

The group has the full technical capabilities needed to fabricate a fissile explosive device. Five members of the group are combat infantry veterans.

5. Dedication: Medium Threat Level

Willing to accept sustained discomfort and injury.

6. Organization, Planning, Training, & Security: Medium Threat Level

Substantial

7. Money: Medium Threat Level

$100,000

8. Transportation: Medium Threat Level

1 Station wagon (CB radio and convoy communications frequency scanner).
1 Light van (CB radio and police band radio; EMR insulation and ECM).
1 "Police" car (CB radio and police band radio).
2 Pick-up trucks (CB radio).

9. Equipment: Medium Threat Level

Power tools
Hand tools
Plastic explosives
"A" frame hoist

MODE OF ATTACK: Some deceit, mostly force

ATTACK FEATURES

1. Target SSNM:

PuO_2

2. Attack Zone:

Isolated area within 30 miles of urban region.
Clear weather.
At sunset.
High tension electrical transmission lines parallel the road.

3. Preparation:

The dissidents position personnel so as to observe activities around the fuel reprocessing plant. Over a period of time, several convoys are followed to their destination—the plutonium storage site. Ambush locations are selected at two places along each of the three routes. During the course of this activity, the convoy communications frequencies are monitored with a scanner.

Within the limits of security, the dissidents train by executing a mock attack. The six potential attack locations, and the planned escape routes, are reconnoitered by all.

When the target convoy departs, the observers alert the adversaries "base camp" by public telephone. A station wagon is dispatched to the critical road junction and the convoy's communication frequency is monitored. When the convoy is committed to a specific route, the dissidents are notified by coded CB transmissions and deploy to their assigned areas.

4. Convoy Immobilization:

The following actions are timed with respect to the convoy's position and coordinated among the dissidents by coded CB transmissions:

- Oncoming traffic is detoured by barricades placed miles up the road beyond the ambush site.
- Codirectional traffic is detoured miles down the road before the ambush site after the convoy has passed.
- A pickup truck is overturned across the road at the ambush site and its cargo spilled.
- A "police car," with siren screaming, passes the convoy and arrives at the scene of the "accident" minutes before the convoy does.

5. ECM:

The dissidents have the capability to jam the convoy's communications. This is accomplished just before the convoy sees the "accident." (If the ambush site coincides, fortuitously, with the location of the high tension lines, jamming probably won't be necessary.)

6. Access to SSNM Truck:

Convoy escort car approached by "police" car. Occupants used to approach SSNM truck and gain access to personnel in truck cab. All convoy personnel rendered unconscious. Entire operation covered by hidden sniper.

7. Access to SSNM Container:

Truck doors blown open with explosives. SSNM moved to light van by use of "A" frame hoist and manhandling.

8. Attack Duration:

15 minutes (through escape initiation).

9. Getaway (toward urban region):

Light van, station wagon.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. Ability of dissidents to observe movements around the fuel reprocessing plant and to follow the convoys without detection.

2. Ability to determine convoy's communication frequency, codes, routine, and procedures.

3. Ability to conduct training without exposing the plan.

4. Effectiveness of detour ruse.

5. Effectiveness of "accident" ruse and communications jamming.

6. Ability of "Police" car and its occupants to escape detection as a counterfeit and imposters, respectively.

7. Effectiveness of ploy used to approach SSNM truck and dismount the drivers.

8. Ability to gain entrance to the SSNM truck with plastic explosives and to remove the PuO_2 containers.

9. Ability to perpetrate the attack–and escape–within 15 minutes.

10. Ability to reach the urban center with the SSNM and to disappear in the city with it.

REPRESENTATIVE ADVERSARY ACTION – NO. 1 C

TRANSPORT MODE: Highway
ADVERSARY TYPE: Dissident

OBJECTIVE: Political/Sociological
INTENDED SSNM USE: Nuclear Explosion

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Medium Threat Level

   4 dressed as policemen
   4 dressed in road repair crew garb
   12 dressed in work clothes suitable to the region
   20 TOTAL

2. Arms: Medium Threat Level

   Pistols
   High powered, night vision, sniper-scope equipped rifle
   Automatic weapons

3. Intelligence Information: Medium Threat Level

   Know that PuO_2 shipment will be made some time during the week from fuel reprocessing plant to plutonium storage site.
   Know that 3 routes are used.
   Know junction which determines commitment to a specific route.
   Know convoy communications frequency.

CONTINUED

2 OF 3

4. Experience & Knowledge: Medium Threat Level

The group has the full technical capabilities needed to fabricate a fissile explosive device. Eleven members of the group are combat infantry veterans.

5. Dedication: Medium Threat Level

Willing to accept sustained discomfort and injury.

6. Organization, Planning, Training, & Security: Medium Threat Level

Substantial

7. Money: Medium Threat Level

$100,000

8. Transportation: Medium Threat Level

1 Station wagon (CB radio and convoy communications frequency scanner).
2 Light vans (CB radio and police band radio; EMR insulation and ECM).
2 "Police" cars (CB radio and police band radio).
4 Pick-up trucks (CB radio).

9. Equipment: Medium Threat Level

Power tools
Hand tools
Plastic explosives
"A" frame hoist

MODE OF ATTACK: Some deceit, mostly force

ATTACK FEATURES

1. Target SSNM:

   PuO_2

2. Attack Zone:

   Isolated area within 30 miles of urban region.
   Clear weather.
   At sunset.
   High tension electrical transmission lines parallel the road.

3. Preparation:

   The dissidents position personnel so as to observe activities around the fuel reprocessing plant. Over a period of time, several convoys are followed to their destination—the plutonium storage site. Ambush locations are selected at two places along each of the three routes. During the course of this activity, the convoy communications frequencies are monitored with a scanner and recorded. The tapes are analyzed. The transmission routine and techniques are determined. The responses of both the convoy and the base stations to transmission content is established, i.e., the "code" is essentially broken. The adversaries note that the convoy responds to law enforcement vehicles as any ordinary citizen would, i.e., on one occasion municipal police stop the convoy for speeding at the approaches to a town. The drivers of both the escort vehicle and the SSNM truck handed their licenses to the police and tickets were written.

   A mock convoy is used to add realism and the two ambush teams do not know in advance at which of the six sites the "attack" will be ordered. The actual stopping of a "convoy" and the planned subsequent actions are executed at a remote location so as to develop the necessary timing.

When the target convoy departs, the observers alert the adversaries "base camp" by public telephone and follow in one of the pickup trucks. A station wagon is dispatched to the critical road junction and the convoy's radio transmissions are monitored. Based either upon the radioed information or physical evidence of commitment to a specific route, the appropriate attack teams are notified by coded CB transmissions and deploys to the two pre-selected ambush sites along the convoy's chosen route: 2 snipers and a van (containing 1 person) at each site, plus a pickup truck (to be overturned) and two additional people at the primary ambush location; 2 pickup trucks (2 people each) at the point where detours will be set up. The rest of the dissidents, a reserve force, trail the convoy at a distance of several miles. In the final analysis, both the trailing dissidents and the team at the ambush site where the attack does not take place serve first as reserves and then in an escape-assurance capacity vis-a-vis the strike team.

4. Convoy Immobilization:

The following actions are timed with respect to the convoy's position and coordinated among the dissidents by coded CB transmissions:

- Oncoming traffic is detoured by barricades placed miles up the road beyond the ambush site.
- Codirectional traffic is detoured miles down the road before the ambush site after the convoy has passed.
- A pickup truck is overturned across the road at the ambush site and its cargo spilled.
- A "police car," with siren screaming, passes the convoy and arrives at the scene of the "accident" minutes before the convoy does.

5. ECM:

The dissidents have the capability to jam the convoy's communications. This is accomplished just before the convoy sees the "accident." (If the ambush site coincides, fortuitously, with the location of the high tension lines, jamming probably won't be necessary.)

6. Access to SSNM Truck:

Convoy escort car approached by "police" car. Occupants used to approach SSNM truck and gain access to personnel in truck cab. All convoy personnel rendered unconscious. Entire operation covered by hidden sniper.

7. Access to SSNM Container:

Truck doors blown open with explosives. SSNM moved to light van by use of "A" frame hoist and manhandling.

8. Attack Duration:

15 minutes (through escape initiation).

9. Getaway (toward urban region):

Light van, station wagon.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. Ability of dissidents to observe movements around the fuel reprocessing plant and to follow the convoys without detection.
2. Ability to determine convoy's communication frequency, codes, routine, and procedures.
3. Ability to conduct training without exposing the plan.
4. Effectiveness of detour ruse.
5. Effectiveness of "accident" ruse and communications jamming.
6. Ability of "Police" car and its occupants to escape detection as a counterfeit and imposters, respectively.
7. Effectiveness of ploy used to approach SSNM truck and dismount the drivers.
8. Ability to gain entrance to the SSNM truck with plastic explosives and to remove the PuO_2 containers.
9. Ability to perpetrate the attack—and escape—within 15 minutes.
10. Ability to reach the urban center with the SSNM and to disappear in the city with it.

INTELLIGENCE AID/INFORMATION
CLASSIFICATION

REPRESENTATIVE ADVERSARY ACTION – NO. 2 A

TRANSPORT MODE:	Highway
ADVERSARY TYPE:	Demented (Sociopathic) A "small autocratic group pledging allegiance to a hypnotic, father or god-like, charismatic leader . . . (who) is perceptive, imaginative, uninhibited, and (perhaps) unbalanced," i.e., in a paranoid state. (Berkowitz, et al., The Civil Threat of Mass Destruction Weapons; ADCON Report A72-034-10, 20 Sep 72, p. 3-3.)
OBJECTIVE:	Personal Gain
INTENDED SSNM USE:	Financial Blackmail The adversaries intend to extort a very large sum of money from the U. S. Government by threatening to detonate a fission device in a densely populated area of America.

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Low Threat Level

   1 group leader
   1 chemist
   1 metallurgist
   1 machinist
   2 chemical technicians
   6 TOTAL

   The scientists carry out the attack on the convoy as well as participating in the development and manufacture of the bomb.

2. Arms: Medium Threat Level

   Automatic Weapons, Pistols, Shotguns

3. Intelligence Aid/Information: Low Threat Level

   Casual observations are carried out to determine the route of a journey between a processing plant and a fuel-fabrication plant.

4. Experience & Knowledge: Medium Threat Level

   Capable of manufacturing a fission device but little combat-type experience, etc.

5. Dedication: High Threat Level

   Willing to accept loss of life.

6. Organization, Planning, Training & Security: Extensive

7. Money: Medium Threat Level

   $75,000

8. Transportation: Medium Threat Level

   1 "Police" Car
   1 Sand Truck

9. Equipment: Medium Threat Level

   2 CB Radios, Tarpaulin

MODE OF ATTACK: Mostly deceit, little force

ATTACK FEATURES

1. Target SSNM:

   $^{235}UO_2$ (90-95%)

2. Attack Zone:

   On an interstate highway near City A. (During daylight hours, and within a few miles of the adversaries' food processing plant.)

3. Preparation:

   The "mastermind" owns a small food processing and canning business which includes trucks, a warehouse, and a maintenance shop. It is located in an industrial part of City A where large trucks/vans and warehouses are commonplace. The chemical laboratory equipment necessary to reduce $^{235}UO_2$ to the metallic form is acquired and set up under cover of the existing product analysis laboratory. A member of the gang keeps a permanent watch on the processing plant to determine when the convoy leaves the plant. The rest of the gang are waiting at the warehouse with a sand truck and a "police" car.

4. Convoy Immobilization:

   When the convoy leaves the plant, the adversary, who is on surveillance, informs the rest of the gang via CB radio. The sand truck and "police" car leave the warehouse and are driven to a position along the route, not too far away. The sand truck is parked near an entrance to the interstate highway. The "police" car patrols the area and spots the convoy. The sand truck is notified via their CB radio communication. As the convoy passes the entrance under consideration, the sand truck is driven onto the highway. The sand truck overtakes the convoy and while doing so, apparently goes out of control and crashes into the escort car, immobilizing it. The SSNM truck stops. A couple of minutes later, the "police" car arrives. The "police" take control of the situation. They say that the SSNM truck is too dangerous to remain by the roadside. Consequently, they, the "police," will

escort the SSNM truck. The convoy personnel agree to this and the truck is driven off with the "police" car. (The convoy personnel will probably call their headquarters on the radio to get authorization for this procedure. If this happens, consent has to be given in order that the plot can proceed as planned.) Shortly thereafter, the "police" car stops the convoy and the adversaries approach the truck on some pretext, such as to warn of heavy traffic or a detour, etc.

5. Access to SSNM:

The truck crew are overcome by a surprise attack. A tarpaulin is thrown over the truck to camouflage it.

6. Attack Duration:

Less than fifteen minutes.

7. Getaway:

The "police" car is abandoned. The truck, indistinguishable from similar commercial traffic, is driven directly to the food processing plant and concealed there. The drivers of the sand truck leave the scene of the crash after exchanging particulars, etc.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. The ability to acquire and employ the necessary physical resources without detection (including cover at the food processing plant).

2. The ability to obtain convoy information, by surveillance.

3. The ability to coordinate and execute the removal of the escort car from the truck.

   - Ramming of escort car and arrival of "police" car.

   - Effectiveness of this ploy in immobilizing the escort car and not alarming the convoy personnel, so that the truck proceeds with the "police" car.

4. The ability to execute the overpowering of the truck crew.

   - Stopping the truck by the "police" car.
   - Approach of "police" to truck.
   - Overpowering of crew.
   - Sufficient time lag so that any eyewitness accounts of the assault are too late to enable an interception of the truck before it reaches the warehouse.

REPRESENTATIVE ADVERSARY ACTION – NO. 2 B

TRANSPORT MODE: Highway

ADVERSARY TYPE: Demented (Sociopathic)

A "small autocratic group pledging allegiance to a hypnotic, father or god-like, charismatic leader . . . (who) is perceptive, imaginative, uninhibited, and (perhaps) unbalanced," i.e., in a paranoid state. (Berkowitz, et al., The Civil Threat of Mass Destruction Weapons; ADCON Report A72-034-10, 20 Sep 72, p. 3-3.)

OBJECTIVE: Personal Gain

INTENDED SSNM USE: Financial Blackmail

The adversaries intend to extort a very large sum of money from the U. S. Government by threatening to detonate a fission device in a densely populated area of America.

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Low Threat Level

   1 group leader
   1 chemist
   1 metallurgist
   1 machinist
   2 chemical technicians
   6 TOTAL

   The scientists carry out the attack on the convoy as well as performing their technical roles in the manufacture of the bomb.

2. Arms: Medium Threat Level

   Automatic Weapons, Pistols, Shotguns

3. Intelligence Aid/Information: Medium Threat Level

Extensive surveillance of previous convoys is carried out, and convoy routing and scheduling is determined for the journey between a processing plant and a fabrication plant.

During these convoys, CB radio communications are monitored by use of a frequency scanner to determine which frequencies the convoy uses.

4. Experience & Knowledge: Medium Threat Level

Capable of manufacturing a fission device but little combat-type experience, etc.

5. Dedication: High Threat Level

Willing to accept loss of life.

6. Organization, Planning, Training & Security: Extensive

7. Money: Medium Threat Level

$75,000

8. Transportation: Medium Threat Level

1 "Police" Car
1 Sand Truck

9. Equipment: Medium Threat Level

Tarpaulin, CB Radio, Frequency Scanner

MODE OF ATTACK: Mostly deceit, little force

ATTACK FEATURES

1. Target SSNM:

$^{235}UO_2$ (90-95%)

2. Attack Zone:

On an interstate highway near City A. (During daylight hours, and within a few miles of the adversaries' food processing plant.)

3. Preparation:

The "mastermind" owns a small food processing and canning business which includes trucks, a warehouse, and a maintenance shop. It is located in an industrial part of City A where large trucks/vans and warehouses are commonplace. The chemical laboratory equipment necessary to reduce $^{235}UO_2$ to the metallic form is acquired and set up under cover of the existing product analysis laboratory. The adversaries' sand truck and "police" car are positioned near an entrance to the interstate highway along the convoy's route. The convoy's position is monitored by listening to the convoy communications on a CB radio.

4. Convoy Immobilization:

As the convoy passes the entrance under consideration, the sand truck is driven onto the highway. The sand truck overtakes the convoy and while doing so, apparently goes out of control and crashes into the escort car, immobilizing it. The SSNM truck stops. A couple of minutes later, the "police" car arrives. The "police" take control of the situation. They say that the SSNM truck is too dangerous to remain by the roadside. Consequently, they, the "police," will escort the SSNM truck. The convoy personnel agree to this and the truck is driven off with the "police" car. (The convoy personnel will probably call their headquarters on the radio to get authorization for this procedure. If this happens, consent has to be given in order that the plot can proceed as planned.) Shortly thereafter, the "police" car stops the convoy and the "police" approach the truck on some pretext, such as to warn of heavy traffic or a detour, etc.

5. Access to SSNM:

The truck crew are overcome by a surprise attack. A tarpaulin is thrown over the truck to camouflage it.

6. Attack Duration:

Less than fifteen minutes.

7. Getaway:

The "police" car is abandoned. The truck, indistinguishable from similar commercial traffic, is driven directly to the food processing plant and concealed there. The drivers of the sand truck leave the scene of the crash after exchanging particulars, etc.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. The ability to acquire and employ the necessary physical resources without detection (including cover at the food processing plant).

2. The ability to obtain convoy information, by surveillance.

3. The ability to coordinate and execute the removal of the escort car from the truck.

   - Ramming of escort car and arrival of "police" car.
   - Effectiveness of this ploy in immobilizing the escort car and not alarming the convoy personnel so that the truck proceeds with the "police" car.

4. The ability to execute the overpowering of the truck crew.

   - Stopping the truck by the "police" car.
   - Approach of "police" to truck.
   - Overpowering of crew.
   - Sufficient time lag so that any eyewitness accounts of the assault are too late to enable an interception of the truck before it reaches the warehouse.

REPRESENTATIVE ADVERSARY ACTION – NO. 2 C

TRANSPORT MODE: Highway

ADVERSARY TYPE: Demented (Sociopathic)

A "small autocratic group pledging allegiance to a hypnotic, father or god-like, charismatic leader . . . (who) is perceptive, imaginative, uninhibited, and (perhaps) unbalanced," i.e., in a paranoid state. (Berkowitz, et al., The Civil Threat of Mass Destruction Weapons; ADCON Report A72-034-10, 20 Sep 72, p. 3-3.)

OBJECTIVE: Personal Gain

INTENDED SSNM USE: Financial Blackmail

The adversaries intend to extort a very large sum of money from the U. S. Government by threatening to detonate a fission device in a densely populated area of America.

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Low Threat Level

   1 group leader
   1 chemist
   1 metallurgist
   1 machinist
   2 chemical technicians
   6 TOTAL

   The scientists carry out the attack on the convoy as well as performing their technical roles in the manufacture of the bomb.

2. Arms: Medium Threat Level

   Automatic Weapons, Pistols, Shotguns

3. Intelligence Aid/Information: Medium-High Threat Level

The metallurgist, a member of the gang who works at the fuel fabrication plant, obtains details relevant to the convoy schedule routing and communications frequencies for a journey from a processing plant to the fabrication plant. He also fixes a remote-controlled immobilization device to the escort car.

4. Experience & Knowledge: Medium Threat Level

Capable of manufacturing a fission device but little combat-type experience, etc.

5. Dedication: High Threat Level

Willing to accept loss of life.

6. Organization, Planning, Training & Security: Extensive

7. Money: Medium Threat Level

$75,000

8. Transportation: Low Threat Level

1 "police" car

9. Equipment: Medium Threat Level

CB radio, tarpaulin, remote-controlled car immobilization device and activator.

MODE OF ATTACK: Mostly deceit, little force

ATTACK FEATURES

1. Target SSNM:

$^{235}UO_2$ (90-95%)

2. Attack Zone:

On an interstate highway near City A. (During daylight hours, and within a few miles of the adversaries' food processing plant.)

3. Preparation:

The "mastermind" owns a small food processing and canning business which includes trucks, a warehouse, and a maintenance shop. It is located in an industrial part of City A where large trucks/vans and warehouses are commonplace. The chemical laboratory equipment necessary to reduce $^{235}UO_2$ to the metallic form is acquired and set up under cover of the existing product analysis laboratory. The adversaries "police" car is positioned on a side street near an entrance to the interstate highway, along the convoy's route. The convoy's position is monitored by listening to the convoy communications on a CB radio.

4. Convoy Immobilization:

As the convoy passes the entrance under consideration, the immobilization device is activated. The escort car breaks down but in a fashion that does not arouse the suspicion of the convoy personnel. The SSNM truck stops. The adversaries arrive in their "police" car and take control of the situation. They say that the SSNM truck is too dangerous to remain by the roadside. Consequently, they, the "police," will escort the SSNM truck. The convoy personnel agree to this and the truck is driven off with the "police" car. (The convoy personnel will probably call their headquarters on the radio to get authorization for this procedure. If this happens, consent has to be given, in order that the plot can proceed as planned.) Shortly thereafter, the "police" car stops the convoy and the adversaries approach the truck on some pretext, such as to warn of heavy traffic or a detour, etc.

5. Access to SSNM:

The truck crew are overcome by a surprise attack. A tarpaulin is thrown over the truck to camouflage it.

6. Attack Duration:

Less than fifteen minutes.

7. Getaway:

The "police" car is abandoned. The truck, indistinguishable from similar commercial traffic, is driven directly to the food processing plant and concealed there.

SPECIFIC ATTACK ELEMENTS INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. The ability to acquire and employ the necessary physical resources without detection (including cover at the food processing plant).

2. The ability of the "insider" to obtain convoy information.

3. The ability of the "insider" to sabotage the escort car.

4. The ability to coordinate and execute the removal of the escort car from the truck.

   - Breakdown of escort car and arrival of "police" car.
   - Effectiveness of this ploy in immobilizing the escort car and not alarming the convoy personnel so that the truck proceeds with the "police" car.

5. The ability to execute the overpowering of the truck crew.

   - Stopping the truck by the "police" car.
   - Approach of "police" to truck.
   - Overpowering of crew.
   - Sufficient time lag so that any eyewitness accounts of the assault are too late to enable an interception of the truck before it reaches the warehouse.

REPRESENTATIVE ADVERSARY ACTION – NO. 2 D

TRANSPORT MODE: Highway

ADVERSARY TYPE: Demented (Sociopathic)

A "small autocratic group pledging allegiance to a hypnotic, father or god-like, charismatic leader . . . (who) is perceptive, imaginative, uninhibited, and (perhaps) unbalanced," i.e., in a paranoid state. (Berkowitz, et al., The Civil Threat of Mass Destruction Weapons; ADCON Report A72-034-10, 20 Sep 72, p. 3-3.)

OBJECTIVE: Personal Gain

INTENDED SSNM USE: Financial Blackmail

The adversaries intend to extort a very large sum of money from the U. S. Government by threatening to detonate a fission device in a densely populated area of America.

ADVERSARY RESOURCES AND ATTRIBUTES

1. Number of Personnel: Medium Threat Level

1 group leader
1 chemist
1 metallurgist
1 machinist
2 chemical technicians
2 teamsters
8 TOTAL

The scientists aid the attack on the convoy as well as performing their technical roles in the manufacture of the bomb.

2. Arms: Medium Threat Level

   Automatic Weapons

3. Intelligence Aid/Information: High Threat Level

   The metallurgist, a member of the gang who works at the fuel fabrication plant, obtains details relevant to the convoy schedule and routing. (He also fixes a remote-controlled immobilization device to the escort car.) Two teamsters who are employed by the common carrier which hauls enriched uranium oxide from the processing to the fabrication plant have criminal connections. They are approached, cultivated, and bribed to aid in the hijacking.

4. Experience & Knowledge: Medium Threat Level

   Capable of manufacturing a fission device but little combat-type experience, etc.

5. Dedication: High Threat Level

   Willing to accept loss of life.

6. Organization, Planning, Training & Security: Extensive

7. Money: Medium Threat Level

   $75,000

8. Transportation: Low Threat Level

   1 Pickup Truck

9. Equipment: Medium Threat Level

   Radio Transmitter, Radio Receiver, Tarpaulin, Remote-controlled Car Immobilization Device and Activator.

MODE OF ATTACK: Deceit

ATTACK FEATURES

1. Target SSNM:

   $^{235}UO_2$ (90-95%)

2. Attack Zone:

   On an interstate highway near City A. (During daylight hours, and within a few miles of the adversaries' food processing plant.)

3. Preparation:

   The "mastermind" owns a small food processing and canning business which includes trucks, a warehouse, and a maintenance shop. It is located in an industrial part of City A where large trucks/vans and warehouses are commonplace. The chemical laboratory equipment necessary to reduce $^{235}UO_2$ to the metallic form is acquired and set up under cover of the existing product analysis laboratory.

   The adversaries' truck is positioned on a side street near an exit of the interstate highway, along the convoy's route. The teamsters carry a small transmitter that is operated periodically. The convoy's position is monitored thereby by the men in the truck.

4. Convoy Immobilization:

   As the convoy approaches the exit under consideration, the immobilization device is activated.

5. Access to SSNM Truck:

   The teamsters drive the SSNM truck off the highway and rendezvous with the waiting pickup. A tarpaulin is thrown over the SSNM truck to camouflage it.

6. Attack Duration:

   Less than five minutes.

7. Getaway:

Both trucks, indistinguishable from similar commercial traffic, are driven directly to the food processing plant and concealed there.

SPECIFIC ATTACK ELEMENTS (SAE) INTERFACING WITH SAFEGUARD PROTECTIVE MECHANISMS

1. The ability to acquire and employ the necessary physical resources without detection (including cover at the food processing plant).

2. The ability to enlist the criminal cohorts, and to maintain security.

3. The ability of the "insider" to obtain convoy information.

4. The ability to coordinate and execute the actual hijacking:

   - Breakdown of the escort car.
   - Effectiveness of this ploy in immobilizing the escort car and its occupants so that they either do not see the SSNM truck being camouflaged or are not even aware that a diversion is in progress.
   - Sufficient time lag so that any eyewitness accounts of the disappearing act are too late to enable an interception of the truck before it reaches the warehouse.

EFFICIENCY
CLASSIFICATION

REPRESENTATIVE ADVERSARY ACTION – NO. 3 A

TRANSPORT MODE: Highway

ADVERSARY TYPE: Demented

A Sociopathic Group. The Manson Family could typify this group. Knowledge of safeguards systems and combat experience is minimal. Dedication may be high and some members of the group may be willing to accept loss of life. However, their planning and training, etc., is at a minimal level.

OBJECTIVE: Political/Sociological

INTENDED SSNM USE: Sabotage

ADVERSARY RESOURCES AND ATTRIBUTES:

1. Number of Personnel: Medium Threat Level

   1 Group leader
   3 Women group members
   5 Physically capable intelligent, well educated young men
   9 TOTAL

2. Arms: Medium Threat Level

   Automatic Weapons, explosives

3. Intelligence Aid/Information: Medium Threat Level

   Female member of group working in local bar and restaurant near origin learns shipment schedule and destination. Observation team posted to determine exact moment of departure, convoy makeup and vehicle identification reports to remainder of group.

4. Experience & Knowledge: Low Threat Level

   Well educated intelligent politically active group. Little combat/security experience.

5. Dedication: Medium Threat Level

   Dedication high with some members of the group willing to accept loss of life.

6. Organization, Planning, Training & Security: Low Threat Level

   Minimal

7. Money: $25,000 - $50,000

8. Transportation:

   3 Automobiles
   1 Van

9. Equipment:

   CB Radios, Weapons, Explosives

MODE OF ATTACK: Deceit, Force Combination

ATTACK FEATURES

1. Target SSNM: PuO_2

2. Attack Zone:

   Remote section of highway

3. Preparation:

   The group identifies that the sabotage of a shipment of nuclear materials will generate mass fear and generate publicity and "respect" which they desire. A woman in the group obtains employment in a bar/restaurant frequented by personnel involved in the nuclear shipments. She eavesdrops on conversations and elicits valuable information including shipment date and convoy descriptions. The group acquires the necessary equipment and deploys it for the attack. A car with CB Radio observes the origin plant on shipment day and informs the remainder of the group of the convoy description and route.

4. Convoy Immobilization:

The group places one vehicle with apparent fire under hood in one lane and another vehicle apparently providing fire extinguisher to block the other lane. Female members of the group attempt to lure guards from convoy vehicles to assist injured person. Failing this the remainder of the group arrives in a van and attacks the guard force.

5. Access to SSNM:

While the guard force is engaged in the attack, two members of the group place an explosive on the SSNM vehicle and retire to detonate it.

6. Attack Duration:

Less than fifteen minutes.

7. Getaway:

The original decoy and observation vehicles are used for escape. The SSNM is not removed from the scene.

REPRESENTATIVE ADVERSARY ACTION – NO. 3 B

TRANSPORT MODE: Highway
ADVERSARY TYPE: Dissident
OBJECTIVE: Political/Sociological
INTENDED SSNM USE: Political Blackmail

ADVERSARY RESOURCES AND ATTRIBUTES

1. Personnel Characterization: Medium Threat Level

   1 Group leader
   9 Teamsters
   10 TOTAL

2. Arms: Medium Threat Level

   Automatic Weapons. plastic explosives

3. Intelligence Aid/Information: Medium-High Threat Level

   Have one member of the group working in the facility with access to shipping information: routes, convoy configuration, arms, escort strength, radio procedures.

4. Experience & Knowledge: Medium Threat Level

   Planning ability substantial, technical knowhow good, ability of manufacturing an effective home-made nuclear bomb uncertain.

5. Dedication: Medium Threat Level

   Reasonably high. unwillingness to sacrifice lives.

6. Organization, Planning, Training & Security: Medium Threat Level

   Minimum combat training (to use automatic weapons and plastic explosives).

7. Money: Medium Threat Level

   $50.000

8. Transportation: Medium Threat Level

   1 Truck
   2 Sedans
   1 Pickup Truck
   1 Terrain Car (4-wheel drive)

9. Equipment: Medium Threat Level

   Radio Transmitter and Receiver, Cable/Winer/A-Frame

MODE OF ATTACK: Force

ATTACK FEATURES

1. Target SSNM:

   PO_2

2. Attack Zone:

   Highway

3. Preparation:

   The attack site is chosen on a highway some 20 minutes from the nearest town. The following preparation has been made ahead of time: one adversary dressed as a construction flag man is ready at the nearest exit to divert the general traffic away as soon as the convoy passes by. The main body of the gang is connected with the "flag man" via two-way radio. When the convoy enters the critical section, and the general traffic is diverted, the adversaries position their truck across the highway lanes to create the impression of an accident and also to physically block the lanes.

4. Convoy Immobilization:

As the SSNM truck slows down, the adversaries open fire, kill the escort guards and one driver. The second driver is forced to leave the cab and is kept as a hostage, eventually to cooperate with the adversaries.

5. Access to SSNM Truck:

Expert cutting of locks, eventually using plastic explosives. SSNM is removed by cable/winer/A-frame and placed on the pickup truck and camouflaged.

6. Attack Duration:

10–15 Minutes

7. Getaway:

Fake-accident truck is abandoned. Group escapes in two sedans, in the pickup truck, and in the jeep.

REPRESENTATIVE ADVERSARY ACTION -- NO. 3 C

TRANSPORT MODE:	Highway
ADVERSARY TYPE:	Dissidents
ATTACK PURPOSE:	Diversion
OBJECTIVE:	Political/Sociological
INTENDED SSNM USE:	Detonation of a nuclear device

ADVERSARY RESOURCES AND ATTRIBUTES

1. Personnel Characterization: Medium Threat Level

   7 to 12 People

2. Arms: High Threat Level

   Pistols, Shotguns, 50-Caliber machine gun, AR-15's, bazooka, M-79 grenade launcher

3. Intelligence Information: High Threat Level

   Know convoy configuration, route, and destination, escort and crew strength, LLEA response capabilities, convoy radio frequencies schedules, and procedures; crew habits and operational patterns.

4. Experience & Knowledge: High Threat Level

   Adversaries have military combat and heavy equipment experience

5. Dedication: High Threat Level

   Willing to accept loss of life

6. Organization, Planning, Training & Security: High Threat Level

   Extensive

7. Money: Medium Threat Level

   $25,000 to $50,000

8. Transportation: High Threat Level

   1 Truck cab (Interchangeable with SSNM trucks)
   3/4 Ton Truck (with 50 caliber machine gun mounted on it)
   1 Van (containing men with M-79's)
   1 Camper (containing men with M-79's)
   1 Panel Truck (containing men with bazooka)

9. Equipment: High Threat Level

   Plastic explosives
   Heavy duty dollies and pneumatically operated jacks
   Variety of hand tools
   Scanners of convoy frequencies
   CB Radios

MODE OF ATTACK: Force

ATTACK FEATURES

1. Target SSNM:

   239 PuO_2

2. Attack Zone:

   On main highway artery in desolate area.

3. Preparation:

The activities around the shipping locations, enroute, and at the destination are continuously monitored so as to gain the overt information described under "Intelligence Information." A strategically placed "insider" supplies the dissidents with the balance of the information. Training is conducted in weapons use and coordinated attack timing is refined. Radio activated plastic explosives are attached to the base of the radio antenna at the LLEA site nearest to the attack zone. Two dissidents start out from the opposite direction with the truck cab. The rest of the vehicles pick up the convoy route at various points. The van and the 3/4-T truck stay in front of the convoy; the camper trails and keeps the convoy in sight. The panel truck with the bazooka is parked off the road at the ambush site. Coordination (timing) is maintained by coded CB transmissions.

4. Convoy Immobilization:

As the lead escort is sighted by the panel truck parked off the road, a radio signal is sent to the man near the LLEA antenna ordering him to demolish it; the van slows down and the camper speeds up: both open fire with the M-79's on the leading and trailing escorts, respectively. The SSNM truck is now in a position near the parked panel truck. The cab is destroyed with bazooka fire. Elapsed time: 30 seconds. The 3/4-T truck (with 50-caliber machine gun) is used to "take out" survivors and chance passers-by.

5. Access to SSNM Containers and Getaway

The dissidents' truck cab is hitched to the SSNM trailer and towed 30 miles to a wrecking yard owned by one of the attacking force. (Heavy duty dollies and pneumatic jacks are used, if required, to move the trailer; i.e., if immobilization devices were activated.) The SSNM is extracted from the truck within 24 hours and moved to a clandestine laboratory 200 miles away.

6. Attack Duration:

15 Minutes (through escape mitration).

VULNERABILITIES OF SAFEGUARD SYSTEMS
VIA ASSESSMENT OF PROTECTIVE MECHANISMS

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 1
NUMBER OF PERSONNEL CLASSIFICATION – PROTECTIVE SYSTEM A

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																	
No.	$P(S_k)$	Number of Personnel	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness								V_k	$P(S_k)V_k$
1A	.94	Low 1– 6	.85	.7	.6	.85	.85	.99	.8	.99	.7								1.4×10^{-1}	1.3×10^{-1}
1B	.04	Medium 7–12	.85	.7	.75	.85	.85	.99	.8	.99	.65								1.6×10^{-1}	6.6×10^{-3}
1C	.02	High 13+	.85	.8	.85	.85	.9	.99	.9	.99	.6								2.3×10^{-1}	4.7×10^{-3}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{3} P(S_k)V_k$$

$$= 1.3 \times 10^{-1} + 6.6 \times 10^{-3} + 47 \times 10^{-3}$$

$$= 1.4 \times 10^{-1}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 2
NUMBER OF PERSONNEL CLASSIFICATION – PROTECTIVE SYSTEM B

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																	
No.	$P(S_k)$	Number of Personnel	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
1A	.94	Low 1 – 6	.6	.3	.25	.65	.1	.99	.8	.9	.7	1.0	1.0	1.0					1.5×10^{-3}	1.4×10^{-3}
1B	.04	Medium 7 12	.6	.35	.4	.65	.1	.99	.8	.9	.55	1.0	1.0	1.0					2.1×10^{-3}	8.6×10^{-5}
1C	.02	High 13+	.7	.4	.65	.7	.1	.99	.8	.9	.5	1.0	1.0	1.0					4.5×10^{-3}	9.1×10^{-5}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{3} P(S_k)V_k$$

$$= 1.4 \times 10^{-3} + 8.6 \times 10^{-5} + 9.1 \times 10^{-5}$$

$$= 1.6 \times 10^{-3}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 3
NUMBER OF PERSONNEL CLASSIFICATION – PROTECTIVE SYSTEM C

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																	
No.	$P(S_k)$	Number of Personnel	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
1A	.94	Low 1 - 6	.1	.05	.02	.1	.1	.1	.6	.99	.5	1.0	1.0	1.0					3.0×10^{-8}	2.8×10^{-8}
1B	.04	Medium 7 - 12	.1	.05	.05	.1	.1	.1	.65	.99	.45	1.0	1.0	1.0					7.2×10^{-8}	2.9×10^{-9}
1C	.02	High 13+	.1	.05	.05	.1	.1	.3	.65	.99	.3	1.0	1.0	1.0					1.4×10^{-7}	2.9×10^{-9}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{3} P(S_k)V_k$$

$$= 2.8 \times 10^{-8} + 2.9 \times 10^{-9} + 2.9 \times 10^{-9}$$

$$= 3.4 \times 10^{-8}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 4
INTELLIGENCE AID/INFORMATION CLASSIFICATION – PROTECTIVE SYSTEM A

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																
No.	$P(S_k)$	Intelligence Aid/Information	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness							V_k	$P(S_k)V_k$
2A	.10	Low – Casual Observations	.6	.65	.55	.8	.9	.95	.7	.9	.7							6.5×10^{-2}	6.5×10^{-3}
2B	.20	Medium – Extensive Surveillance	.65	.65	.55	.8	.9	.95	.75	.9	.75							8.0×10^{-2}	1.6×10^{-2}
2C	.25	Medium High – Insider in Non-Sensitive Position	.75	.65	.65	.8	.9	.95	.75	.9	.75							1.1×10^{-1}	2.8×10^{-2}
2D	.45	High – Insider in Sensitive Position	.99	.99	.6	.8	.99	.95	.95	.99	.8							3.3×10^{-1}	1.5×10^{-1}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{4} P(S_k)V_k$$

$$= 6.5 \times 10^{-3} + 1.6 \times 10^{-2} + 1.5 \times 10^{-1}$$

$$= 2.0 \times 10^{-1}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 5
INTELLIGENCE AID/INFORMATION CLASSIFICATION – PROTECTIVE SYSTEM B

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																
No.	$P(S_k)$	Intelligence Aid/Information	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
2A	.40	Low–Casual Observations	.5	.4	.15	.7	.1	.95	.6	.8	.6	1.0	1.0	1.0					5.7×10^{-4}	2.3×10^{-4}
2B	.50	Medium - Extensive Surveillance	.5	.4	.15	.7	.1	.95	.65	.85	.45	1.0	1.0	1.0					5.0×10^{-4}	2.5×10^{-4}
2C	.08	Medium High–Insider in Non-Sensitive Position	.55	.4	.1	.7	.1	.95	.65	.85	.4	.3	.3	.4					1.2×10^{-6}	9.3×10^{-8}
2D	.02	High–Insider in Sensitive Position	.8	.9	.25	.75	.99	.95	.9	.9	.4	.2	.3	.4					9.9×10^{-4}	2.0×10^{-5}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{4} P(S_k)V_k$$

$$= 2.3 \times 10^{-4} + 2.5 \times 10^{-4} + 9.3 \times 10^{-8} + 2.0 \times 10^{-5}$$

$$= 5.0 \times 10^{-4}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 6
INTELLIGENCE AID/INFORMATION CLASSIFICATION – PROTECTIVE SYSTEM C

ADVERSARY ACTION CLASSES | PROTECTIVE MECHANISMS

No.	$P(S_k)$	Intelligence Aid/Information	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
2A	.40	Low–Casual Observations	.05	.05	.02	.05	.05	.9	.6	.99	.4	1.0	1.0	1.0					2.7×10^{-8}	1.1×10^{-8}
2B	.50	Medium–Extensive Surveillance	.05	.05	.02	.05	.05	.9	.6	.99	.4	1.0	1.0	1.0					2.7×10^{-8}	1.3×10^{-8}
2C	.08	Medium High–Insider in Non-Sensitive Position	.05	.05	.02	.05	.05	.9	.6	.99	.3	.3	.3	.4					7.0×10^{-10}	1.0×10^{-10}
2D	.02	High–Insider in Sensitive Position	.65	.4	.02	.05	.9	.9	.9	.99	.3	.2	.3	.4					1.4×10^{-6}	2.7×10^{-8}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{4} P(S_k)V_k$$

$$= 1.1 \times 10^{-8} + 1.3 \times 10^{-8} + 1.0 \times 10^{-10} + 2.7 \times 10^{-8}$$

$$= 5.1 \times 10^{-8}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 7
EFFICIENCY CLASSIFICATION – PROTECTIVE SYSTEM A

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																
No.	$P(S_k)$	Efficiency	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness							V_k	$P(S_k)V_k$
3A	.6	Low	.85	.9	.85	.85	.7	.9	.9	.95	.7							2.1×10^{-1}	1.3×10^{-1}
3B	.25	Medium	.9	.95	.9	.8	.9	.95	.95	.95	.85							4.1×10^{-1}	1.0×10^{-1}
3C	.15	High	.95	.95	.9	.9	.95	.99	.95	.95	.85							5.3×10^{-1}	7.9×10^{-2}

SAFEGUARDS SYSTEM VULNERABILITY $= \sum_{k=1}^{3} P(S_k)V_k$

$= 1.3 \times 10^{-1} + 1.0 \times 10^{-1} + 7.9 \times 10^{-2}$

$= 3.1 \times 10^{-1}$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 8
EFFICIENCY CLASSIFICATION – PROTECTIVE SYSTEM B

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																
No.	$P(S_k)$	Efficiency	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
3A	.53	Low	.7	.45	.55	.85	.3	.9	.9	.95	.7	1.0	1.0	1.0					2.4×10^{-2}	1.3×10^{-2}
3B	.32	Medium	.85	.8	.8	.75	.2	.95	.85	.95	.7	.4	1.0	.5					8.8×10^{-3}	2.8×10^{-3}
3C	.15	High	.95	.9	.9	.9	.5	.99	.95	.95	.7	.4	1.0	.5					4.3×10^{-2}	6.5×10^{-3}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{3} P(S_k)V_k$$

$$= 1.3 \times 10^{-2} + 2.8 \times 10^{-3} + 6.5 \times 10^{-3}$$

$$= 2.2 \times 10^{-2}$$

ADVERSARY ACTION – SAFEGUARDS SYSTEM INTERACTION MATRIX – NO. 9
EFFICIENCY CLASSIFICATION – PROTECTIVE SYSTEM C

ADVERSARY ACTION CLASSES			PROTECTIVE MECHANISMS																	
No.	$P(S_k)$	Efficiency	Vehicle Velocity	Truck Crew	Armed Escort	LLEA	Truck	Container	Transit Time	Camouflage	Natural Wariness	Personnel Screening	Hardware Security	Schedule Security					V_k	$P(S_k)V_k$
3A	.25	Low	.3	.05	.02	.6	.3	.5	.95	.99	.5	1.0	1.0	1.0					1.3×10^{-5}	3.2×10^{-6}
3B	.25	Medium	.4	.05	.02	.1	.2	.5	.85	.99	.4	.4	1.0	.5					2.7×10^{-7}	6.7×10^{-8}
3C	.5	High	.8	.8	.05	.1	.3	.6	.9	.99	.3	.4	1.0	.5					3.1×10^{-5}	1.5×10^{-5}

$$\text{SAFEGUARDS SYSTEM VULNERABILITY} = \sum_{k=1}^{3} P(S_k)V_k$$
$$= 3.2 \times 10^{-6} + 6.7 \times 10^{-8} + 1.5 \times 10^{-5}$$
$$= 1.8 \times 10^{-5}$$

OVERALL ASSESSMENT OF SAFEGUARDS SYSTEMS VULNERABILITIES

NUMBER OF PERSONNEL CLASSIFICATION – SAFEGUARDS SYSTEM A

No.	$P(S_k)$	Threat Level		Vulnerability
1A	.94	Low	1-6	.06
1B	.04	Medium	7-12	.08
1C	.02	High	13+	.12

Safeguards System Vulnerability = $.94 \times .06 + .04 \times .08 + .02 \times .12$

$= 6.2 \times 10^{-2}$

NUMBER OF PERSONNEL CLASSIFICATION – SAFEGUARDS SYSTEM B

No.	$P(S_k)$	Threat Level		Vulnerability
1A	.94	Low	1-6	.018
1B	.04	Medium	7-12	.024
1C	.02	High	13+	.04

Safeguards System Vulnerability = $.94 \times .018 + .04 \times .024 + .02 \times .04$

$= 2.6 \times 10^{-2}$

NUMBER OF PERSONNEL CLASSIFICATION – SAFEGUARDS SYSTEM C

No.	$P(S_k)$	Threat Level		Vulnerability
1A	.94	Low	1-6	.0003
1B	.04	Medium	7-12	.004
1C	.02	High	13+	.007

Safeguards System Vulnerability = $.94 \times .0003 + .04 \times .004 + .02 \times .007$

$= 5.8 \times 10^{-4}$

INTELLIGENCE AID/INFORMATION CLASSIFICATION–SAFEGUARDS SYSTEM A

No.	$P(S_k)$	Threat Level	Vulnerability
2A	.1	Low – Casual Observations	.022
2B	.2	Medium–Extensive Surveillance	.023
2C	.25	Medium High–Insider in Non-Sensitive Position	.04
2D	.45	High–Insider in Sensitive Position	.04

Safeguards System Vulnerability $= .1 \times .022 + .2 \times .023 + .25 \times .04 + .45 \times .04$

$= 3.5 \times 10^{-2}$

INTELLIGENCE AID/INFORMATION CLASSIFICATION – SAFEGUARDS SYSTEM B

No.	$P(S_k)$	Threat Level	Vulnerability
2A	.4	Low–Casual Observations	.005
2B	.5	Medium–Extensive Surveillance	.005
2C	.08	Medium High–Insider in Non-Sensitive Position	.005
2D	.02	High–Insider in Sensitive Position	.007

Safeguards System Vulnerability $= .4 \times .005 + .5 \times .005 + .08 \times .005 + .02 \times .007$

$= 5.0 \times 10^{-3}$

INTELLIGENCE AID/INFORMATION CLASSIFICATION – SAFEGUARDS SYSTEM C

No.	$P(S_k)$	Threat Level	Vulnerability
2A	.4	Low–Casual Observations	.0003
2B	.5	Medium–Extensive Surveillance	.0003
2C	.08	Medium High–Insider in Non-Sensitive Position	.0007
2D	.02	High–Insider in Sensitive Position	.0007

Safeguards System Vulnerability $= .4 \times .0003 + .5 \times .0003 + .08 \times .0007 + 02 \times .0007$

$= 3.4 \times 10^{-4}$

EFFICIENCY CLASSIFICATION – SAFEGUARDS SYSTEM A

No.	$P(S_k)$	Threat Level	Vulnerability
3A	.6	Low	.56
3B	.25	Medium	.75
3C	.15	High	.75

Safeguards System Vulnerability $= .6 \times .56 + .25 \times .75 + .15 \times .75$

$= 6.4 \times 10^{-1}$

EFFICIENCY CLASSIFICATION – SAFEGUARDS SYSTEM B

No.	$P(S_k)$	Threat Level	Vulnerability
3A	.53	Low	.34
3B	.32	Medium	.18
3C	.15	High	.42

Safeguards System Vulnerability $= .53 \times .34 + .32 \times .18 + .15 \times .42$

$= 3.0 \times 10^{-1}$

EFFICIENCY CLASSIFICATION – SAFEGUARDS SYSTEM C

No.	$P(S_k)$	Threat Level	Vulnerability
3A	.25	Low	.0001
3B	.25	Medium	.0001
3C	.5	High	.015

Safeguards System Vulnerability $= .25 \times .0001 + .25 \times .0001 + .5 \times .015$

$= 7.6 \times 10^{-3}$

APPENDIX D
DISCUSSION OF RECOMMENDED DESIGN REQUIREMENTS

SUBSYSTEM NO. 1 – DETERRENCE

Performance Parameters:

- An auditable program specifying strategies, media, timing and responsibilities.

Discussion:

Implementation would consist of a coordinated and credible mass media and industry wide program highlighting the capability of the safeguards system. It might include information on the generic safeguards measures though it would avoid providing any specific information which would assist an adversary. It might publicize issues such as the hard-line government position in negotiations with terrorists or criminals, the apprehension and incarceration of terrorists particularly those intercepted in activities relevant to the safeguards system, or new technology or advances in safeguards capability.

Also included would be the design of techniques which will present any obstacles created by safeguard measures which are visible to the public as insurmountable.

All other safeguards subsystems will contribute to the support of this subsystem. It is intended to convey to potential adversaries the information on each subsystem which will influence them.

The policy governing the deterrence campaign must be tempered with a concern for the impact on the general public. While an important by-product of the subsystem will be to generate an atmosphere of reliability and confidence for the general public it must not overwhelm the public with a concern that the safeguards system itself is a hazard to their safety or well being.

SUBSYSTEM NO. 2 – INTELLIGENCE MANAGEMENT

Performance Parameters:

- Establishment of an intelligence organization (federal government).
- Establishment of an intelligence interface responsibility (licensee).
- Procedures for data acquisition and analysis identifying sources (including informers and infiltrations), access, controls and threat assessment techniques.
- Procedures for communication of threat information to appropriate response elements.

Discussion:

The gathering and maintenance of intelligence related information is a very sensitive issue today. The subsystem must be implemented in full compliance with all statues, legal constraints and administrative regulations which govern such activities. Its operation must also be closely controlled within the policy guidelines of the administering agency. Use of the information, access to data, sources (use of informers, data acquired for other purposes, etc.) would require specific guidance and control.

The operation would be performed by a federal agency (possibly the FBI) with licensees required to furnish appropriate data. They would also be required to be alert to potential threats. The center should maintain an interface with all appropriate law enforcement agencies throughout the country.

In addition to immediate short-term threat assessment the center should conduct long-range assessments to assist in determining the level of guard capability which will be required in the future.

SUBSYSTEM NO. 3 – PERSONNEL MANAGEMENT

Performance Parameters:

- Procedures for personnel screening and periodic investigations, the level of detail to be related to the sensitivity of the position.
- Procedures for mandatory, periodic security education and training including content, responsibility, attendance, timing.
- Organizational and position descriptions.
- Necessary policies and procedures including pay, promotion, grievance.

Discussion:

It will be necessary to attract capable persons into the system and hold them through attractive salaries, benefit plans and working conditions. Because of some of the safety and safeguards requirements of the jobs, attractive employee packages are particularly important. It will also be necessary to carefully select and thoroughly screen those who will be assigned to sensitive positions in the transport system. Screening should include a comprehensive background investigation prior to sensitive assignment and periodic rechecks during assignment. The screening should focus on eliminating adversary infiltrators, assuring a staff which will not be susceptible to bribery, blackmail or influence, and will be of a high caliber to perform the required duties and maintain the necessary level of alertness.

In addition to careful selection and screening an effective program of employee training must be conducted. This training would include the normal job training plus training in safeguard system concepts and the operation of the safeguard measures for which the person will be responsible. Guard and response force personnel will require specialized training in the use of weapons and tactics to be employed in encountering adversary attacks. Field exercises should be included in this training. All employees should be sensitized to the special requirements of alertness required by the safeguards system.

A clear definition of the organizational relationships, lines of authority and responsibilities must be provided to all personnel. This is particularly critical in the operation of SSNM transport because of the threat of attempts by unauthorized persons to acquire access to SSNM, equipment or documentation and because of the potential for emergency operations in response to adversary action.

SUBSYSTEM NO. 4 – AUTHORIZATION PROCEDURES

Performance Parameters:

- Techniques and procedures for measuring SSNM quantity at exchange points.
- Auditable set of procedures controlling the authorization of SSNM shipment, verifying amounts, origin, destination and transporter.
- Central control facility capabilities for monitoring all SSNM shipments, verifying authorized transport and notifying appropriate response unit of any irregularity.
- Procedures, identification measures and documentation forms for controlling the exchange of SSNM among authorized parties.
- Requirements for paired or multiple authorizations at key operations throughout the transport sequence which ensure that no single person can authorize or redirect movement of SSNM.

Discussion:

The authorization procedures will control access to shipments of SSNM through the requirement for specification of shipment description (amount, origin, destination), the verification of authorization by specified persons, internal audit measures to ensure proper flow of information, intermediate verification of information and measurement of material quantities.

To improve the quality of these control procedures there should be a requirement that more than one person review, verify or authorize movement at key points throughout the sequence. This so called "buddy system" reduces the possibility that a single person can divert SSNM at any point.

There is also a requirement for procedures, credentials and devices (badges, etc.) to be used to verify the identity of persons and organizations during the shipment especially at points of exchange of custody.

A central facility, remote from individual shipments and operated by an organization which is not a party to shipments should be used to monitor shipment authorizations. This facility would be informed of all pertinent information related to a shipment and would verify authorization at each stage in the sequence.

The central control facility should be advised of shipment status through two channels: (1) security to security and (2) initiator to receiver. In some cases coded messages would be used to improve the integrity of the verification procedure.

Physical release of SSNM should require a two-part code—one controlled by each party (the one releasing and the one assuming responsibility).

Techniques and devices for measuring the quantity and quality of SSNM would be employed where appropriate in the sequence for verification. Between points where accurate measurement is possible tamper proof seals and periodic checks should be utilized for verification. Techniques for utilizing certain coded information for each shipment should be employed. These verification and authorization procedures should be employed throughout the transport sequence at a minimum each time a movement is initiated or needs, or a change in custody occurs.

Some techniques which might be employed include the following:

Transfer authenticating signatures should be verified with their source before the next authenticating signature is affixed. Additionally, and simultaneously, the information should be input to the central computer in code. Thus, even if a signature is forged (and that face successfully concealed during a telephonic attempt at verification by the next authorizing level), the computer would not accept this next authorizing level's signature code (since it would not have the prior-prerequisite-code) and an alarm would be sounded at the input source and at central security. Individual "central" computers at facilities and transfer points should be tied in (in real time) to a master NRC computer.

SUBSYSTEM NO. 5 -- INFORMATION CONTROL

Performance Parameters:

- Procedures, personnel training and physical devices which provide the capability to limit access to certain transport sequence information to those with a need to know.
- Procedures for scheduling SSNM shipment in a manner which will be difficult to anticipate by a potential adversary.
- Procedures for selecting routes for SSNM transport between origin and destination which will provide maximum safeguard.
- Procedures for selecting personnel for specific SSNM shipments in a manner in which it will be difficult for a potential adversary to anticipate.
- Procedures and devices to provide communication and exchange of information among the various elements of the transport sequence using techniques which make interception or deciphering by an adversary difficult.

Discussion:

To accomplish this safeguard it will be necessary to separate the overall information flow into segments and limit access to individual segments. Access to specific information on a shipment will be limited to those who have a valid need to know and they should gain access as late as possible. Procedures for marking and securing information must be utilized including locks for doors and vaults, or safes for storage.

As defined in other subsystems the personnel with access to restricted information should be carefully selected and trained, a system of credentials or badges should be utilized and physical facilities should be secured.

Scheduling of shipments should be as varied as possible within the constraints of efficient facility and equipment utilization. There should not be a pattern which will allow adversaries to know exactly when a shipment will be made.

The route should be selected specifically for each shipment. It should be based on minimizing the time/distance between points, the availability of response force capability, the presence of hazards and the hazard which the shipment might pose. Routes should also vary where possible to deny adversaries the advantage of advance planning of attack location. Access to route information should be restricted and released at the latest moment including possibly directing the convoy while in route. Alternate routes should be planned in case of an unforeseen problem.

The personnel to conduct a shipment should be selected by some technique which provides variation. Those involved should be informed at the latest moment. This is particularly applicable to the crew and guards which will accompany the shipment. This will minimize the potential matching of infiltrated personnel for a specific shipment.

Throughout the shipment techniques for coding critical information should be employed. The coding structures, access keys and procedures should be maintained in a secure facility with very limited access. During shipment some of the radio transmission should be coded with access limited.

SUBSYSTEM NO. 6 – PHYSICAL SECURITY OF TRANSPORT SYSTEM FACILITIES

Performance Parameters:

- Barriers, detection devices, personnel and procedures to provide security and limit access to areas where SSNM is being handled or stored, where transport equipment is serviced or stored including loading/unloading facilities, transfer points, intermediate stops, repair facilities, and equipment storage areas.
- Procedures and devices for regulating access to secured areas.
- SSNM containers which limit access to SSNM by size, locking devices, detection devices, and seals.
- Procedures, personnel, equipment and devices which are to be used to provide physical security to an area where an unscheduled stop is required (due to malfunction of equipment, road blockage or other unforeseen event).

Discussion:

While intermediate stops should be eliminated or minimized where they cannot be avoided the areas where they occur should be as secure as the origin and destination points. This may involve such tactics as bolstering the guard force to compensate for detection devices or other mechanisms available at a fixed site.

A shipment may also be vulnerable through the tampering or sabotage of the equipment being used to transport and safeguard the SSNM. For this reason security must also be provided at locations and facilities where the equipment is stored or serviced.

Access to all secured areas should be controlled and limited to those necessary to the performance of a function within the area. Identification and verification procedures credentials and devices should be utilized. The areas should be checked for unauthorized persons through constant surveillance or periodic checks.

All portals should have automatic closing devices. In addition to the normally planned stopping points, equipment malfunction or other problems may require an unscheduled, unplanned stop in transit. Contingency plans should be developed to quickly establish a security barrier in this case. Deployment of guard forces, and activation of special devices, establishment of special communication and other techniques may be employed.

The containers in which the SSNM is stored for shipment should limit access and inhibit unauthorized movement. The size and/or design should be such that special equipment is required for movement. Very secure locking devices requiring multiple keys should be used and the locks should include tamper proof seals. The containers should be integrally matched with the vehicle to limit unauthorized removal. The shielding of the container should withstand blast or projectiles which might be used to cause in situ dispersion of hazardous material.

SUBSYSTEM NO. 7 – CONTINUOUS MONITORING OF SSNM DURING TRANSIT

Performance Parameters:

- Equipment, devices, personnel and procedures which can maintain continuous visual, mechanical and/or electronic surveillance of SSNM at all stages in the transport sequence.
- Communications equipment and procedures which will provide reliable communication capability within the convoy and with a central control at all times during the transport of SSNM.

Discussion:

During the loading and unloading the secure areas in which this activity takes place will be monitored both within the immediate area and from a remote (control location).

During transit the SSNM should be monitored both from within the convoy and from the remote (central control) location. Within the convoy the surveillance should be maintained by visual observation from escort vehicles, intra-convoy communication, use of sensors and detection devices and periodic verification of status. A capability for rapid identification of suspicious vehicles or events would be required. When possible, airborne surveillance should also be maintained.

Remote surveillance should be maintained from a central control location through use of a fail-safe (multiple mode) continuous communications capability. This capability will provide real-time knowledge of the transporter's location and condition. This may be accomplished through a coded, digital, multi-frequency radio transmission backed up with periodic voice communications (radiotelephone) and/or independent observations en-route. Coded passive and active communications alarms should be transmitted periodically to the convoy operations monitoring center. Interruption in this communication will result in an automatic alert of response forces and verification of the problem with the convoy.

SUBSYSTEM NO. 8 -- DEFENSE TECHNIQUES

Performance Parameters:

- Program for organizing, preparing, positioning and alerting response force adequate to defeat a substantial adversary attack.
- Transport and escort vehicles equipped with armor and other physical protection for crews.
- Specific plans and tactics for response to each of the potential emergency situations including armed encounters with adversary forces which may be faced during the shipment.
- Specially designed and constructed vehicles and SSNM containers which deny adversary acquisition of SSNM.
- Control facility, staff, procedures and equipment for crisis management during an adversary attack or other emergency.
- Response forces trained, equipped and organized to respond in adequate numbers to defeat a maximum planned (15) adversary force.

Discussion:

A self-sufficient convoy has a number of advantages over a mixture of in-convoy guards and remote response forces. First, the time gap would be eliminated. If there should be an adversary attack, a well-equipped convoy would be able to react immediately, whereas if a small escort force were defeated it would take time for a response force to arrive. A self-sufficient convoy centralizes the security apparatus and the response capability. Second, the existence of a self-sufficient convoy could be easily discerned and would act as a greater deterrent. A low visibility or hidden security force would also probably generate less public confidence. Third, training could be more specialized and more easily accomplished with a self-sufficient convoy and necessary equipment more easily distributed.

The cost, however, of a self-sufficient convoy, although more readily apparent, would be considerably less than that of a relatively small escort force and reliance on trained and prepared response forces. A self-sufficient convoy would also call attention to a shipment.

On balance it seems that reliance on a strong convoy escort force is warranted under existing transportation conditions where the number of commercial shipments of SSNM is extremely small—about 20 a year. Under different conditions, however, in which the number of shipments is much greater, it might be preferable to adopt the small escort/reliance on response force option.

During transit the guards and accompanying escort forces should be deployed in a manner which will allow for surveillance of the SSNM and of the terrain ahead of the convoy at all times. Sufficient spacing will be necessary to minimize the simultaneous vulnerability of all elements and maximize the probability of transmitting a call for assistance will be necessary.

Armored and secure vehicles should be used to transport the SSNM. These should be specially designed with locking immobilization and security devices such as foaming. The containers for storage of SSNM during shipment should also be designed to withstand adversary attempts at removal both of the SSNM from the container and the container from the transport vehicle.

Obviously a container that could be made completely theft-proof in the sense that it couldn't be stolen from a truck or opened to obtain the SSNM would be the ultimate safeguards solution. Unfortunately, such a container does not exist at least as yet. Containers can be made, however, which are extremely heavy, difficult to move, and difficult to open (as are the containers which carry high-level waste).

The guards and response force must be trained in the use of weapons, combat tactics and the operation of safeguards measures. They must have weapons capable of defeating an enemy including automatic weapons and they must be authorized to use them in all jurisdictions through which the shipment passes. The guards must also be protected by armor and other protective devices within their vehicles.

To maintain control and direct activity in response to an adversary action, a central crisis management center should be established. The center should operate under procedures specifying the authorities and responsibilities of all parties. It should have sophisticated communication capability with the force at the scene and back-up resources to execute successful response to defeat an adversary action.

Proper tactics to be employed in dealing with emergency situations will be very important. The guard and escort forces must be able to recognize a hazard, evaluate it properly and take appropriate action. This may include recognizing an innocent situation and refraining from shooting at innocent persons. The tactics for dealing with a forceful adversary action will be based on a strategy of a strong self-sufficient convoy or one of dependence on a strong response force. If the former is employed, the

convoy force will attempt to defeat the adversary directly or remove the SSNM from the scene of the encounter. In the latter, the guard force will engage in a tactic of immediate signal for assistance and delay and harrassment of adversaries until response forces arrive.

If the response force strategy is utilized an adequate, trained and equipped force must be available within a reasonable distance of all points along the transport route. The force must be able to respond at the scene within 20 minutes of initiation of attack. This will require special arrangement and pre-planning to organize a sufficient force, and respond to the communication for assistance. It does not allow much time to verify calls and request assistance or to gather a dispersed team. At present LLEAs are depended upon to provide this capability. It appears, however, that additional preparation is required in most areas and that adequate forces do not exist.

SUBSYSTEM NO. 9 – RECOVERY CAPABILITY

Performance Parameters:

- Procedures specifying actions to be taken to recover SSNM in the event of an unauthorized acquisition.
- Detailed recovery action plans and tactics for each of the organizations involved.
- Identification of organizational responsibilities and resource assignments for SSNM recovery.
- Utilization of devices which will assist relocation efforts.
- Procedures and arrangements for notification of all agencies with responsibility to respond to an SSNM diversion, sabotage or in-situation dispersion.

Discussion:

One tactic for SSNM recovery is to seal off the area surrounding the attack immediately. By closing the area it may be possible to intercept adversaries with diverted SSNM before it can be removed to a safe haven. To accomplish this it will be necessary to develop the necessary contingency plans and tactics, to make arrangements with LLEAs or other response agencies, to carry out the tactics, and to develop communication procedures to notify the responding agencies. This may require special arrangements in remote areas where LLEA response capability is insufficient. In these areas techniques such as aerial surveillance may be required.

To assist in recovery operations, devices which indicate the location of the SSNM may be attached to or imbedded in the SSNM container. These devices such as multifrequency radio beacons, infrared-visible markings or command actuated transponders, will facilitate the tracking and location of diverted SSNM.

SUBSYSTEM NO. 11 – SAFEGUARDS SYSTEM VERIFICATION

Performance Parameters:

- Procedures and criteria for the evaluation of all aspects of safeguard system design implementation plans submitted by licensees.
- Procedures and criteria for the periodic test and evaluation of safeguards measures as implemented by licensees.
- Procedures, devices and criteria for testing and checking SSNM transport equipment for effective operation prior to each shipment.
- Procedures and criteria for the periodic testing of safeguards operating procedures and equipment by the licensee.

Discussion:

To achieve this it will be necessary for NRC to specify safeguards system design requirements in a manner which will facilitate implementation by the licensees and which may be measured and evaluated in return by NRC. NRC must develop procedures and measurement criteria for evaluating plans submitted by licensees for safeguards system implementation. NRC must also develop and conduct a program for the periodic audit, test and evaluation of safeguards measures as implemented by the licensees. This may include review and evaluation of procedures, testing of equipment and devices, observation of safeguards operations and in some cases "black hat" test operations. These evaluations should not only measure regulation compliance and the achievement of design requirements but also the actual effectiveness of safeguards measures.

In addition to NRC system evaluations, it will be necessary for the licensees and transport operators to develop and operate procedures for the periodic test and evaluation of their safeguards procedures and equipment to ensure that all components are in operating condition and will function effectively. Also, prior to each shipment, the vehicles and other equipment to be used in the shipment should be checked to ensure that they have not been sabotaged or tampered.

SAFEGUARDS SUBSYSTEM NO. 7 – (AIR) CONTINUOUS MONITORING OF SSNM DURING TRANSIT

Performance Parameters:

- Equipment, devices, personnel and procedures which can maintain continuous visual, mechanical and/or electronic surveillance of SSNM at all stages in the transport sequence.
- Communications equipment and procedures which will provide reliable communication capability with a central control at all times during the transport of SSNM.
- Communications equipment and procedures to confirm take-off and landing of aircraft with independent third party (airport control tower, possibly).
- Radar equipment and procedures to follow flight plan, which will indicate whether aircraft is following flight path.

Discussion:

Air travel can be split into two parts: one concerned with the time in the air, the other concerned with take-off and landing. (The parts of the transport sequence which involve loading and unloading or transfer points are covered in the discussion of these matters for road transport.)

While in the air, the status of the SSNM should be monitored both from within the aircraft and from remote (central control) location. The air crew should maintain surveillance against the unlikely event of an air attack. Sensor devices should be attached to the SSNM containers to detect tampering. Remote surveillance should be maintained from a central control location through use of a fail-safe (multiple mode) continuous communications capability. This capability will provide real-time knowledge of the aircraft's location and condition. This may be accomplished through a coded, digital, multifrequency radio transmission backed up with periodic voice communications. Coded passive and active communications alarms should be transmitted periodically to the aircraft operations monitoring center. Interruption in this communication will result in an automatic alert of response forces and verification of the problem with the aircraft. The aircraft should follow a strict flight pattern which would be monitored by radar from central control. Any divergence from the flight path will also result in an automatic alert of response forces and verification of the problem with the aircraft.

During take-off and landing, the plane is more vulnerable due to the inability to track it on radar. Consequently, immediate confirmation of take-off and landing should be given to a third party to maintain knowledge of the status of the SSNM. (This will presumably be with the airport control tower who would authorize take-off or landing anyway.) As before, any divergence from the pre-assigned routine would result in an immediate alarm being raised.

SAFEGUARDS SUBSYSTEM NO. 8 – (AIR) DEFENSE TECHNIQUES

Performance Parameters:

- Provision of trained armed guards to accompany SSNM shipments.
- Specific plans and tactics for response to each of the potential emergency situations which may be faced during shipment.
- Specially designed and constructed storage compartments and SSNM containers which deny adversary acquisition of SSNM.
- Control facility, staff, procedures and equipment for crisis management during an adversary attack or other emergency.
- Response force, trained, equipped and organized to respond to a malevolent act. Liaison with USAF to facilitate the response of aircraft.

Discussion:

To maintain control and direct activity in response to an adversary action, a central crisis management center should be established. The center should operate under procedures specifying the authorities and responsibilities of all parties. It should have sophisticated communication capability with the force at the scene and back-up resources to execute successful response to defeat adversary action. If the attack takes place during flight, this will necessitate liaison with the USAF. In the event of an attack on the ground at an airport, a response force must be ready to be called upon. This scenario is now similar to those discussed for road transport and similar comments apply.

The guards and response force must be trained in the use of weapons, combat tactics and the operation of safeguards measures. They must have weapons capable of defeating an enemy including automatic weapons and they must be authorized to use them.

Proper tactics to be employed in dealing with emergency situations will be very important. The guards and air crew must be able to recognize a hazard, evaluate it properly and take appropriate action. This

may include recognizing an innocent situation and refraining from shooting at innocent persons if an unusual situation occurs on the ground. The tactics for dealing with a forceful adversary action will be based on a strategy of a strong response force. The guard force will engage in a tactic of immediate signal for assistance and delay and harrassment of adversaries until response forces arrive. During flight the plane would take avoidance action. If an attack takes place on the ground and a response force is utilized, an adequately trained and equipped force must be available within a reasonable distance of the airport. The airport guards may provide at least a part of this response. If additional help is needed, this assistance must be able to respond within twenty minutes of initiation of attack. This will require special arrangement and preplanning to organize a sufficient force, and respond to the communication for assistance. It does not allow much time to verify calls and requirement for assistance or to gather a dispensed team. At present LLEA are depended upon to provide this capability. LLEA response capabilities to airports are probably higher than to other areas of a community; however, additional preparation may be necessary. To diminish the vulnerability of an aircraft to a malevolent act when it is outside of the secured area in the airport, but before it is airborne, the airport guard force should maintain visual surveillance of the plane until it is in the air. This will probably involve following the plane in a car.

SAFEGUARDS SUBSYSTEM NO. 9 – (AIR) RECOVERY CAPABILITY

Performance Parameters:

- Procedures specifying actions to be taken to recover SSNM in the event of an unauthorized acquisition.
- Detailed recovery action plans and tactics for each of the organizations involved.
- Identification of organizational responsibilities and resource assignments for SSNM recovery.
- Utilization of devices which will assist relocation efforts.
- Procedures and arrangements for notification of all agencies with responsibility to respond to an SSNM diversion, sabotage or in-situation dispersion.

Discussion:

In the event of an attack on the ground, tactics must be developed for immediate action to seal the area surrounding the attack. This action should be initiated at the first alert simultaneously with response force action. By closing the area, it may be possible to intercept adversaries with diverted SSNM before it can be removed to a safe haven. To accomplish this, it will be necessary to develop the necessary contingency plans and tactics, to make arrangements with LLEAs or other response agencies to carry out the tactics, and to develop communication procedures to notify the responding agencies.

In the event of diversion during flight, the capability to call upon an airborne response must be developed. This will presumably involve coordination with the USAF.

To assist in recovery operations, devices which indicate the location of the SSNM may be attached to or imbedded in the SSNM container. These devices, such as multifrequency radio beacons, infrared-visible markings or command actuated transponders, will facilitate the tracking and location of diverted SSNM. An aircraft in an adversary's control may endeavor to avoid radar tracking by flying at low altitudes. Devices of the sort just described could help to overcome this eventuality.

END