2
SAND79-1090
Unlimited Release

MASTER

Class Notes from the First International Training Course on the Physical Protection of Nuclear Facilities and Materials

Prepared by Sandia Laboratories, Albuquerque, New Mexico 87185
and Livermore, California 94550 for the United States Department
of Energy under Contract AT(29-1)-789

Sandia Laboratories

SF 2900 Q(7-73)

REPRODUCTION OF THIS DOCUMENT IS UNLIMITED

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE ON PHYSICAL PROTECTION OF NUCLEAR FACILITIES AND MATERIALS

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

PREFACE

The International Training Course on Physical Protection of Nuclear Facilities and Materials is being presented by Sandia Laboratories in Albuquerque, New Mexico, from 1 to 15 November 1978. It is offered under the direction of the Department of Energy (DOE), in consultation with the Nuclear Regulatory Commission (NRC), and under the general auspices of the International Atomic Energy Agency (IAEA). It is intended for representatives from the developing countries who are responsible for preparing regulations and designing and assessing physical protection systems.

The goals of the course are

1. To make the participants aware of the need for physical protection programs,
2. To familiarize the participants with the procedures and practices in the field of physical protection, and
3. To assist the participants in developing and implementing their state system with specific reference to organizational aspects, technical instrumentation, and methodology.

The first part of the course consists of lectures on the objectives, organizational characteristics, and licensing and regulations requirements of a state system of physical protection. Since the participants may have little experience in nuclear energy, background information is provided on the topics of nuclear materials, radiation hazards, reactor systems, and reactor operations. Transportation of nuclear materials is addressed and emphasis is placed on regulations.

Included in these discussions are presentations by guest speakers from countries outside the United States of America who present their countries' national approaches to physical protection and discuss, in panel, the international threat to nuclear facilities.

Effectiveness evaluation methodology is introduced to the participants by means of instructions which teach them how to use logic trees and the EASI (Estimate of Adversary Sequence Interruption) program. The following elements of a physical protection system are discussed: barriers, protective force, intrusion detection systems, communications, and entry-control systems.

Total systems concepts of physical protection system design are emphasized throughout the course. Costs, manpower/technology trade-offs, and other practical considerations are discussed.

PHYSICAL PROTECTION OF NUCLEAR FACILITIES AND MATERIALS

Approximately one-third of the course is devoted to practical exercises during which the attendees participate in problem solving. A hypothetical nuclear facility is introduced, and the attendees participate in the conceptual design of a physical protection system for the facility.

Development of this training course was a team effort and involved multiple reviews. The course has been supervised by the course director, Christopher E. Olson. Prestor B. Herrington functioned as the lead instructor and technical course developer. O. Gene Bates served as the instructional designer and course administrator. Course objectives and materials were reviewed by personnel at Sandia Laboratories as well as at the following agencies: The U.S. Department of Energy, Office of Safeguards and Security (DOE/OSS), the Nuclear Regulatory Commission (NRC), Washington, D.C., and the International Atomic Energy Agency (IAEA), Vienna, Austria.

A general overview of the course was provided by a Steering Committee consisting of Joe E. Stiegler, Sandia Laboratories; L. C. Brenner, DOE/OSS; Charles Hillman, NRC; Ken Cohen, NRC; and Frank Pagano, NRC. Jim Reilly, DOE/OSS, also provided very valuable support.

The instructional staff consisted of W. Morawiecki, IAEA; L. Brenner, DOE/OSS; J. R. Miller, NRC Office of Nuclear Reactor Regulation (NRR); G. W. McCorkle, NRC; B. Jenkins, Rand Corporation; and 17 Sandia staff members headed by Preston Herrington.

The written course materials are organized by modules and are contained in three volumes: Volume I General Information, Volume II Class Notes, and Volume III Hypothetical Facility.

The instructional staff would especially like to thank Perry Gore and his associates for their efforts in the editing, typing, and preparation of the visuals used in this course.

If more information is desired concerning this course, please contact C. E. Olson, Division of Safeguards Evaluation, Sandia Laboratories, Albuquerque, New Mexico, USA 87185.

INTERNATIONAL COURSE SCHEDULE

1980-1981 NOVEMBER 21 OCTOBER 1980 - REGISTRATION															
TIME	WEDNESDAY 1 NOVEMBER	THURSDAY 2 NOVEMBER	FRIDAY 3 NOVEMBER	SAT 4 NOV	SUN 5 NOV	MONDAY 6 NOVEMBER	TUESDAY 7 NOVEMBER	WEDNESDAY 8 NOVEMBER	THURSDAY 9 NOVEMBER	FRIDAY 10 NOVEMBER	SAT 11 NOV	SUN 12 NOV	MONDAY 13 NOVEMBER	TUESDAY 14 NOVEMBER	WEDNESDAY 15 NOVEMBER
0830	BREAKFAST	LICENSES & REGULATIONS MILLER, NRC	TRANS- PORTATION REGULATIONS MCCORMICK, NRC			APPROACH TO PHYSICAL PROTECTION IN IRAN	FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM	BARRIERS	INTRODUCTION TO EASI MODEL	INTRUSION DETECTION SYSTEMS II			COMMUNI- CATIONS	MANPOWER/ TECHNOLOGY CONSIDER- ATIONS	TOTAL SYSTEM DESIGN FOR A HYPOTHETICAL FACILITY (continued)
0900 0915	BYRE SPARKS														
0930	D. KERR, DOE	INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS				APPROACH TO PHYSICAL PROTECTION IN UNITED KINGDOM	BREAK	LOCKS	CALCULATOR OPERATION				TRANS- PORTATION TECHNOLOGY	BREAK	
1000			BREAK			BREAK	INTRO- DUCTION TO EVALUATION TECHNIQUES	INTRUSION DETECTION SYSTEMS I	BREAK	BREAK			BREAK	USE OF SYSTEM CONCEPTS IN PHYSICAL PROTECTION	
1030	BREAK	BREAK	REACTOR SYSTEMS			APPROACH TO PHYSICAL PROTECTION IN FRANCE			BREAK	ENTRY- CONTROL SYSTEMS			BREAK		
1100 1115 1130	INTRODUCTION TO TRAINING COURSE	NUCLEAR FUEL CYCLE				APPROACH TO PHYSICAL PROTECTION IN CANADA	INTRO- DUCTION TO LOGIC SYMBOLS		APPLICATION OF EASI				ROLE OF PROTECTIVE FORCE	INTRODUCTION TO TOTAL SYSTEM DESIGN	
1200	LUNCH					LUNCH	LUNCH	LUNCH					LUNCH	LUNCH	LUNCH
1230	IAEA ROLE MORAWIECKI, IAEA	LUNCH	LUNCH												
1300															
1330		NUCLEAR MATERIALS	REACTOR OPERATIONS			THREAT ANALYSIS JERKINS, RAND	VITAL AREA LOCATION	INTRO- DUCTION TO LOGIC TREES	LUNCH	FACILITY CHARACTER- IZATION			SYSTEM DESIGN APPROACH	TOTAL SYSTEM DESIGN FOR A HYPOTHETICAL FACILITY	HYPOTHETICAL FACILITY DESIGN CRITIQUE
1400	BREAK								PPS APPLICATION I	PPS APPLI- CATION II			SYSTEM DESIGN APPROACH APPLICATIONS		
1415	OBJECTIVES OF A STATE SYSTEM OF PHYSICAL PROTECTION MORAWIECKI, IAEA	BREAK	BREAK				INTRODUCTION TO HYPOTHETICAL FACILITY	APPLICATION OF LOGIC TREES							BREAK
1445															COURSE CRITIQUE
1500		RADIATION HAZARDS	REACTOR VULNERA- BILITIES				VITAL AREA LOCATION								COURSE SUMMATION FOWLER
1515						PANEL DISCUSSION ON INTERNATIONAL THREAT									
1530	ORGANI- ZATIONAL CHARACTER- ISTICS OF A STATE SYSTEM OF PHYSICAL PROTECTION BENNETT, DOE														
1600		REVIEW	REVIEW				REVIEW	REVIEW	REVIEW	REVIEW			REVIEW	REVIEW	
	SOCIAL HOUR 1700-1800					1800 - SOCIAL HOUR 1900 - DINNER								1800 - SOCIAL HOUR 1900 - DINNER	

1800-1900 TOUR NO. 1 - ALBUQUERQUE (continued)

1800-1900 TOUR NO. 2 - SANTA FE (continued)

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

SYLLABUS

Date: Tuesday, 31 October

TIME

1700 to 2100 Registration

Date: Wednesday, 1 November

Session Chairman: J. E. Stiegler, Manager, Facilities
Protection Dept. I, Sandia Labora-
tories

TIME

0800	Breakfast	
0900	Welcome	Morgan Sparks, President, Sandia Laboratories
0930	Keynote Address	D. M. Kerr, Deputy Assistant, Secretary for Defense Programs, U.S. Department of Energy
1030	Break	
1100	Introduction to the Training Course	C. E. Olson, Supervisor, Safe- guards Evaluation Division, Sandia Laboratories
1200	Lunch	
1300	1.0 The IAEA Role in Physical Protec- tion of Nuclear Facilities and Materials	W. Morawiecki, IAEA, Physical Protection Coordinator
1400	Break	

1430	2.1 Objectives of a State System of Physical Protection	W. Morawiecki, IAEA
1530	2.2 Organizational Characteristics of a State System of Physical Protection	L. M. Brenner, Deputy Director, Office of Safeguards and Security, U.S. Department of Energy
1700 to 1900	Social Hour	

Date: Thursday, 2 November

TIME

0830	2.3 Licenses and Regulations	J. R. Miller, Assistant Director of Reactor Safe- guards, U.S. Nuclear Regulatory Commission
0930	12.1 Introduction to Physical Protec- tion Systems	P. B. Herrington, Sandia
1030	Break	
1100	3.1 Fuel Cycle	R. Knief, Sandia
1200	Lunch	
1330	3.2 Nuclear Materials	R. Knief, Sandia
1430	Break	
1500	3.3 Radiation Hazards	R. Knief, Sandia
1600	Review	P. B. Herrington, Sandia

Date: Friday, 3 November

TIME

0830	10.1 Transporta- tion Regulations of the U.S. Nuclear Regulatory Commis- sion	G. W. McCorkle, Chief, Physical Security Licens- ing Branch, U.S. Nuclear Regulatory Commission
1000	Break	

1030	3.4 Reactor Systems	R. Knief, Sandia
1200	Lunch	
1330	3.5 Reactor Operation	R. Knief, Sandia
1430	Break	
1500	3.6 Reactor Vulnerabilities	G. B. Varnado, Supervisor, Nuclear Fuel Cycle Analysis Division, Sandia Laboratories
1600	Review	P. B. Herrington, Sandia

Date: Saturday, 4 November

TIME

0900 to 1800 Tour of Albuquerque Area
(optional)

Date: Monday, 6 November

TIME

0830	National Approaches to Physical Protection in Iran	M. Sarram, Atomic Energy Organization of Iran
0915	United Kingdom National Approach to Physical Protection	G. S. Constable, United Kingdom Atomic Energy Agency
1000	Break	
1030	Physical Protection of Nuclear Facilities and Materials in France	A. Haroyan, Ministry of the Interior, France
1115	The Approach to Physical Protection in Canada	D. B. Sinden, Chief, Security Section, Atomic Energy Control Board of Canada
1200	Lunch	
1330	4.0 Threat Analysis	B. M. Jenkins, Rand Corporation

1445	Break	
1515	Panel Discussion on International Threat	B. M. Jenkins, Chairman, M. Sarram, G. S. Constable, A. Haroyan, D. B. Sinden
1800	Social Hour	
1900	Dinner	

Date: Tuesday, 7 November

TIME

0830	12.2 Functions of a Physical Protection System	P. B. Herrington, Sandia
0930	Break	
1000	5.1 Introduction to Evaluation Techniques	C. E. Olson, Sandia
1130	5.2 Introduction to Logic Symbols	W. K. Paulus, Sandia
1200	Lunch	
1330	3.7 Vital Area Identification	G. B. Varnado, Sandia
1430	13.1 Introduction to the Hypothetical Facility	P. B. Herrington, Sandia
1500	3.8 Vital Area Identification (Subgroups Session)	Instructors*
1600	Review	P. B. Herrington, Sandia

*The instructors for the subgroups sessions are all Sandia Laboratories employees. Their names are listed below in alphabetical order.

Betty Biringer
Stephen Chester
Christopher Olson
William Paulus
Richard Smith
Preston Herrington, Alternate
Paul Robertson, Alternate
Leroy Stradford, Alternate

Date: Wednesday, 8 November

TIME

0830	6.1 Barrier Technology	M. R. Madsen, Supervisor, Barrier Technology Division, Sandia Laboratories
0930	6.2 Locks	M. R. Madsen
1000	Break	
1030	7.1 Sensors	J. D. Williams, Supervisor, Intrusion Detection and Assessment Technology Division, Sandia Laboratories
1200	Lunch	
1330	5.3 Introduction to Logic Trees	W. K. Paulus, Sandia
1430	5.4 Generic Logic Trees (Subgroups Session)	Instructors*
1600	Review	P. B. Herrington, Sandia

Date: Thursday, 9 November

TIME

0830	5.5 Introduction to the EASI Model	C. E. Olson, Sandia
0930	5.6 Hand-Held Calculator Operation	L. P. Robertson, Sandia
1030	Break	
1100	5.7 Application of EASI (Subgroups Session)	Instructors*
1230	Lunch	
1400	13.2 Physical Protection System Applications I (Subgroup Session)	Instructors*

*(See footnote on page 4.)

1600 Review P. B. Herrington, Sandia

Date: Friday, 10 November

TIME

0830	7.2 Alarm Assessment and Reporting Systems	J. D. Williams, Sandia
1000	Break	
1030	8.0 Entry-Control Systems	V. K. Smith, Supervisor, Entry-Control Systems Division, Sandia Laboratories
1200	Lunch	
1330	12.4 Facility Characterization	P. B. Herrington, Sandia
1400	13.3 Physical Protection System Applications II (Subgroups Session)	Instructors*
1600	Review	P. B. Herrington, Sandia

Date: Sunday, 12 November

TIME

0900 to 1900 Tour of Santa Fe, New Mexico Area (optional)

Date: Monday, 13 November

TIME

0830	9.0 Communications	W. D. Lyle, Sandia
0930	10.2 Transportation Technology	F. O. Luetters, Sandia
1030	Break	

*(See footnote on page 4.)

1100	11.0 The Role of the Protective Force	S. D. Chester, Sandia (Panel Discussion)
1200	Lunch	
1330	12.3 System Design Approach	W. K. Paulus, Sandia
1400	12.5 System Design Applications (Subgroups Session)	Instructors*
1600	Review	P. B. Herrington

Date: Tuesday, 14 November

TIME

0830	13.4 Manpower/Equip- ment Considerations (Subgroups Session)	Instructors*
0930	Break	
1000	The Use of System Concepts in Physical Protection	K. E. Wilson, Manager, Security Services Stone & Webster Engineering Corp. Boston, Massachusetts 02107
1130	13.5 Introduction to Hypothetical Facility PPS Design	P. B. Herrington, Sandia
1200	Lunch	
1330	13.6 Hypothetical Facility--Total PPS Design (Subgroups Session)	Instructors*
1600	Review	P. B. Herrington, Sandia
1800	Social Hour	
1900	Dinner	

*(See footnote on page 4.)

Date: Wednesday, 15 November

TIME

0830	13.6 Hypothetical Facility--Total PPS Design (Cont.) (Sub- groups Session)	Instructors*
1200	Lunch	
1330	Hypothetical Facility Design Critique	Panel Discussion (Instructors*)
1430	Break	
1500	Course Critique	O. G. Bates, Sandia
1530	Course Summation	G. A. Fowler, Vice- President, Sandia Labora- tories

*(See footnote on page 4.)

**INTERNATIONAL TRAINING COURSE ON THE PHYSICAL PROTECTION
OF NUCLEAR FACILITIES AND MATERIALS**

**COURSE MAP
1-15 NOVEMBER, 1978**

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

1.0 THE IAEA ROLE IN PHYSICAL PROTECTION OF NUCLEAR FACILITIES AND MATERIALS

Session Title: 1.0 The IAEA Role in Physical
Protection of Nuclear Facilities
and Materials

Date: Wednesday, 1 November

Presented By: W. Morawiecki, IAEA

Time: 1300 to 1400

Session Objectives:

After the session, the participants will be able to

1. State the two major roles of the IAEA, and
2. Identify which IAEA role concerns physical protection and which concerns IAEA safeguards.

Summary:

The IAEA has two major roles:

1. To assist Member States in developing peaceful uses for atomic energy, and
2. To ensure that such assistance is not used for military purposes.

Physical protection is a subset of the first role; IAEA safeguards are necessary to fulfill the second role.

The IAEA roles are presented, and the organization is described in the context of the objectives. A description of IAEA safeguards is presented. (This is the only time during the course that this subject is addressed.)

MODULE 1

THE IAEA ROLE IN PHYSICAL PROTECTION OF NUCLEAR FACILITIES AND MATERIALS

MAKING PEACEFUL USES OF NUCLEAR ENERGY SAFE

The International Atomic Energy Agency (IAEA) was set up when its Statute, approved on 23 October 1956 by a conference of States Members of the United Nations, came into force on 29 July 1957. The IAEA is an intergovernmental organization belonging to the United Nations family together with other specialized organizations such as the World Bank, the World Health Organization (WHO), and the Food and Agricultural Organization (FAO).

According to its Statute, the general objective of the IAEA is to "accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world. It shall ensure, so far as it is able, that assistance provided by it or at its request or under its supervision or control is not used in such a way as to further any military purpose" (Article II).

The Agency's role in this area has been based on the paramount assumption that the peaceful applications of nuclear energy may and should be clearly separated from its military uses. Consequently, the major function of the Agency has been defined by the Statute as follows: "To establish and administer safeguards designed to ensure that special fissionable and other materials, services, equipment, facilities, and information made available by the Agency or at its request or under its supervision or control are not used in such a way as to further any military purpose; and to apply safeguards, at the request of the parties, to any bilateral or multilateral arrangement, or at the request of a State, to any of that State's activities in the field of atomic energy" (Article III, A.5).

Based on these statutory provisions and on a number of international bilateral and multilateral treaties, including first of all the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT),* the Agency developed a comprehensive system of effective international safeguards. By 31 December 1977, the Agency safeguards had been applied to 559 nuclear facilities and during 1977, 706 inspections were carried

*By 31 December 1977, 99 States were parties to the Non-Proliferation Treaty. However, according to information available to the Agency, there were significant nuclear facilities in 13 non-nuclear-weapon States not party to the Non-Proliferation Treaty: Argentina, Brazil, Chile, Colombia, the Democratic People's Republic of Korea, Egypt, India, Indonesia, Israel, Pakistan, South Africa, Spain, and Turkey. The Agency was applying safeguards in 12 of these States, excluding Egypt, and in the case of 8 States, according to the information available to the Agency, all nuclear activities involving significant quantities of special fissionable material were covered by those safeguards. The five exceptions were Egypt, India, Israel, South Africa, and Spain. Egypt had signed but not yet ratified the Non-Proliferation Treaty.

out in 45 States. The Agency has a staff of 131 inspectors originating from 42 Member States. The Agency's safeguards operations did not detect any diversion of a significant quantity of nuclear material. The Agency has been able to confirm, taking into account all circumstances including qualitative observations, that in all States where safeguards agreements were in full implementation all safeguarded nuclear material remained in the declared peaceful nuclear activity or was otherwise adequately accounted for.

Another important function of the Agency dealing with a different aspect of safe uses of nuclear energy has been defined by the Statute as follows: "Establish or adopt . . . standards of safety for protection of health and minimization of danger to life and property (including such standards for labor conditions), and to provide for the application of these standards to its own operations as well as to the operations making use of materials, services, equipment, facilities, and information made available by the Agency or at its request or under its control or supervision; and to provide for the application of these standards, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of atomic energy" (Article III, A.6).

Within this function, the Agency developed a wide range of activities resulting in a number of regulations, recommendations, manuals, guidebooks, etc., regarding nuclear and radiological safety standards. Inspection and advisory safety missions are being sent to Member States and extensive technical assistance is rendered by the Agency in this area. By the end of 1977, the 206 commercial nuclear power stations in operation among the Agency's Member States had accumulated 1500 reactor-years of operating experience and no fatalities or serious injuries were reported which were directly attributable to the nuclear side of the industry--from mining and milling of uranium through the storage or disposal of radioactive wastes.

The international safeguards apply to measures for assurance that the Governments of States abide by their obligations under international treaties prohibiting diversion of nuclear materials and equipment from peaceful to military uses. The nuclear safety measures are destined to prevent unintended accidents due to the failure of materials or humans or to the forces of nature, e.g., hurricanes, earthquakes, which may cause material damage, health hazards, or loss of life to the personnel of nuclear installations and to the general public.

Physical protection consists of security measures designed to protect against willful hostile acts which take the form of theft or unauthorized removal of nuclear material or of sabotage of nuclear facilities committed on subnational (nongovernmental) levels by individuals or groups of individuals. Physical protection has been mentioned in the Statute in connection with the Agency's possible role as a supplier of nuclear material. The Agency was requested to "protect materials in its possession . . . against unauthorized removal or diversion, damage or destruction, including sabotage and forcible seizure" (Article IX, H and I).

The indicated distinctions between safeguards, safety, and physical protection reflect only some of the different aspects of the general problem of how to reduce, as much as possible, several serious risks connected with the peaceful uses of nuclear energy. However, there are also very close links between these aspects.

Physical protection can be considered as an important factor contributing to the effectiveness of safeguards against diversion of nuclear material for military purposes by assuring its containment within designated areas. This containment is accomplished through a system of barriers, detection instruments, surveillance, and other security measures. Conversely, the essential element of these safeguards, the material measurement and accounting system, is closely connected with physical protection, supplying information on the type, quantity, and location of nuclear material within the facility and detecting losses related to, *inter alia*, theft or unauthorized diversion. Similarly, the measures of nuclear safety which are aimed at the prevention of accidental damage to nuclear facilities and accompanying possible radiological hazards also serve the purposes of physical protection by helping to prevent the same kind of damage which might result from a willful hostile action in the form of sabotage. In other words, the systems of safeguards, safety, and physical protection are, to a great extent, mutually complementary and, therefore, the designing of each of these systems for a specific facility should also take into account the requirements of the other systems.

Concern about physical protection has acquired new dimensions in the 1970's. This was due first of all to the growth of terrorism in many parts of the world. The growth and spread of the nuclear power industry around the world has also increased the risks of hostile action due to the increasing number of nuclear facilities and to growing amounts of sensitive nuclear material being stored, used, and transported. These risks would increase considerably in possible future stages of development of the nuclear power industry involving operations such as separation of plutonium from spent fuel and transportation and recycling of plutonium since plutonium is the nuclear material most suitable for production of nuclear weapons.

To fulfill the preceding functions, the Agency acts through its main organs: the General Conference, the Board of Governors, and the Secretariat. The General Conference, composed of all Member States,* convenes once a year for a general debate on the Agency's policy and program, to consider the annual report, and to approve the budget, as well as to elect new members of the Board to replace those whose terms have expired.

The Board of Governors, composed of 34 Member States, meets about four times a year. Twelve of the Board members are designated by the Board itself, and 22 are elected by the General Conference. The designation criteria (level of advancement in nuclear technology and equitable geographic representation) ensure continuity of membership.

*In 1978, 110 States were members of the IAEA. Of the more important world States, only the People's Republic of China is not a member of the IAEA.

The Board is an important policymaking organ of the Agency. It considers all major questions, including applications for membership and the Agency's program of work. The annual budget and report require the approval of the Board as well as that of the General Conference. Under its own authority, the Board approves all safeguards agreements, important projects, and safety standards.

The Secretariat, consisting of about 1500 staff members recruited from more than 60 Member States, is headed by the Director General, who is responsible for the administration and implementation of the Agency's program. The Director General is appointed by the Board of Governors with the approval of the General Conference for a term of 4 years. The Director General functions under the authority of and is subject to control by the Board and is advised on scientific and technical matters by a Scientific Advisory Committee composed of, at present, 15 distinguished scientists whose appointments are for 3-year terms and who represent all fields of nuclear science.

OBJECTIVES OF A STATE PHYSICAL PROTECTION SYSTEM

Sovereign States are the basic units (actors) of the present international system. This means that it is for each of their governments to define its State's foreign and internal policies and, in particular, to make decisions--within the framework of the various constitutional regimes--on matters which are essentially within the State's domestic jurisdiction. According to this principle, the responsibility for physical protection of nuclear material and facilities remaining under a State's jurisdiction or control rests entirely with that State. As a matter of fact, the State government normally demonstrates a natural interest in fulfilling this responsibility as a part of the State's very fundamental function of maintenance of public order and security within its own territory.

In general, the objectives of a State's physical protection system are

1. To establish conditions which would minimize the possibilities for theft or unauthorized removal of nuclear material or for sabotage of nuclear facilities which could directly or indirectly endanger public health and security, and
2. To provide for rapid and comprehensive measures to locate and recover missing nuclear material.

In a more detailed manner, the objectives of a State's physical protection system may be identified as

1. To deter theft or unauthorized removal of nuclear materials and sabotage of nuclear facilities,
2. To detect any such attempts,
3. To protect nuclear materials and facilities against physical attack,
4. To deny or minimize the utility of nuclear material to an adversary or to minimize the effects of sabotage, and
5. To recover stolen or diverted nuclear material prior to any socially harmful use.

Sanctions, consisting of prosecution and punishment of criminals who perpetrate hostile acts against nuclear material or facilities, are not in themselves a part of a State's physical protection system. However, they obviously do support it and constitute indispensable elements of deterrence and repression on which the effectiveness of a State's physical protection system depends.

A State's physical protection system has to be designed taking into account the presence of nuclear material and facilities within the State's territory and the threat, as assessed, of hostile actions to which the nuclear material and facilities may be vulnerable. On this basis and balanced against implicit economic and social costs, the desirable level and specific measures of physical protection shall be determined.

As recommended by the IAEA document, The Physical Protection of Nuclear Material (INFCIRC/225), the State should promulgate and regularly review its comprehensive regulations for the physical protection of nuclear material and facilities whether in State or private possession. The legal character of such regulations may vary from State to State; for instance, they may be part of the national legislation or have the form of executive directives or instructions by competent State authorities.

At the facility level, the implementation of physical protection requirements, as laid down in a State's regulations, is normally the responsibility of its operator. The administration of physical protection measures should belong to a designated national authority. Such authority should be fully responsible for the licensing of nuclear activities only when they comply with the State's physical protection regulations and for the continuing confirmation of complete compliance with such regulations. In the case of international transfer of nuclear materials, the responsibility for physical protection should be the subject of agreement between the States concerned.

INTERNATIONAL CONCERNS

If it is true that the responsibility for physical protection of nuclear material and facilities remaining under a State's jurisdiction or control rests entirely with that State, it is also true that the governments may be legitimately interested in whether and to what extent such national responsibilities for nuclear material and facilities are being fulfilled by other States. Deficient physical protection in one State may create danger for other States since the theft of nuclear material or sabotage of nuclear facilities may have serious international implications. Therefore, it is a matter of common concern and interest among States that adequate physical protection be assured for nuclear material and facilities wherever they may be exposed to the threat of theft or sabotage. As a result, the recognition of a need for international cooperation for this particular purpose has been growing constantly, and the IAEA has been increasingly involved by its Member States in various forms of such cooperation. This has recently found particular expression in the resolutions adopted unanimously by the General Conference, the Agency's most representative policymaking body.

At its XIX session in September 1975, the General Conference encouraged the Agency's role in this area when, in a special resolution (GC, XIX/RES.328), it endorsed, inter alia, the Agency's intention to assist Member States in the development of their national systems for physical protection and called upon the Member States and the Director General to consider ways and means of achieving further cooperation in dealing with problems of physical protection.

An Advisory Group on physical protection, convened by the Director General in March 1977 and composed of governmental experts from various regions of the world,* formulated a set of more elaborate recommendations on what the contribution of the Agency in this field should be. The Agency's Secretariat was guided by those recommendations in its further activities. At its XXI session in September 1977, the General Conference issued a resolution (GC, XXI/RES.350) commending the Director General for what had been done so far and urged him to continue efforts, in consultation with Member States, to promote international cooperation in ensuring the adequate physical protection of nuclear facilities and materials and, in particular, to facilitate the development of an international convention as a legal instrument of such cooperation.

As developed by the Secretariat in consultation with Member States, the Agency's program to promote physical protection comprises, at present, the following projects:

1. Formulation of guidelines on adequate levels and measures of physical protection of nuclear material,
2. Assistance to Member States in the development of legal instruments for international cooperation, in particular in the negotiation of an international convention on physical protection of nuclear material,
3. Technical assistance on physical protection in the form of experts and fellowships supplied to Member States on their request,
4. Organization of training courses for physical protection personnel,
5. Publication of practical guidebooks on comprehensive physical protection systems for various types of nuclear facilities, and
6. Establishment of a bank of information on physical protection of nuclear material and facilities.

GUIDELINES FOR STATES' POLICIES

In general, the IAEA may play a role inherent in any international organization, i.e., to facilitate recognition, by its Member States, of existing and arising common problems and, consequently, to assist them in taking appropriate measures individually and collectively to satisfy their common interests. In particular, the main role of the IAEA may be to provide guidance for Member States and to assist them in their efforts to promote physical protection of nuclear material and facilities.

*Experts from the following 15 Member States participated: Austria, Australia, Canada, Egypt, France, the Federal Republic of Germany, the German Democratic Republic, India, Iran, Japan, Pakistan, Sweden, the Union of Soviet Socialist Republics, the United Kingdom, and the United States of America.

In 1971, consultants and experts were convened by the Director General and their work resulted in the publication, in June 1972, of Recommendations for Physical Protection of Nuclear Material (also called the "Grey Book"). Early in 1975, those recommendations were reviewed by a group of governmental experts and again published, this time as the Agency's document INFCIRC/225, under the title, The Physical Protection of Nuclear Material (also called the "Blue Book").

The recommendations contained in INFCIRC/225 were conceived as flexible guidelines subject to review and updating from time to time. The advisory group which met in March 1977 reviewed this document for the first time and introduced greater precision into its definition of three categories of nuclear material for which different levels and corresponding measures of physical protection were recommended.* No doubt further modifications of the text will be desirable in the future in order to take into account changes in the situation and progress in the state of the art of physical protection.

The recommendations of INFCIRC/225 were based on the current state of the art in physical protection and the existing experience of Member States advanced in nuclear energy programs. The levels of physical protection were set for different categories of nuclear material and some detailed security requirements were recommended for nuclear material in use, in storage, and in transit. The categorization was based on the potential hazard caused by the material, which itself depends on the type of material (i.e., plutonium, uranium, thorium), its isotopic composition (i.e., content of fissile isotopes), chemical form, radiation level, and quantity. The attention of the document was focused on physical protection against theft or unauthorized diversion of nuclear material. Sabotage against facilities was considered only if it could result in radioactive hazard.

The basic concepts of the recommendations are as follows:

1. The highest level of physical protection is required for category I material which comprises plutonium or U^{233} in quantities of 2 kg or more and U^{235} enriched to 20 percent or above in quantities of 5 kg or more. Nuclear material which falls into this category is to be used and stored within special inner areas encircled by the protected area, which is characterized by separate physical barriers, differentiated restrictions and controls on personnel access, monitoring and alarming systems, etc.
2. The medium level of physical protection is required for category II material. It comprises plutonium or U^{233} in quantities of less than 2 kg but more than 500 grams, U^{233} enriched to 20 percent or more in quantities less than 5 kg but more than 1 kg, and U^{235} enriched to 10 percent but less than 20 percent in quantities of 10 kg or more. Irradiated fuel in the form of depleted or natural uranium, thorium, or low-enriched fuel (less than 10 percent fissile content) is also included in this category. However, individual States would have the option, based upon evaluation of

*The modified version was published as an INFCIRC/225/Rev.1 in June 1977.

specific circumstances, to assign a different category to such irradiated fuel. Nuclear material in this category should be subject to a somewhat less rigid physical protection system which need only provide for protected area arrangements.

3. The lowest level of physical protection is required for category III material. It comprises plutonium or U^{233} in quantities of 500 grams or less, U^{235} enriched to 20 percent or above if less than 1 kg, U^{235} enriched to 10 percent but less than 20 percent if less than 10 kg,* and uranium enriched above the natural state but less than 10 percent if 10 kg or more. Nuclear materials in this category are to be kept in an area to which access should be controlled but no special protected area is necessary. Quantities not falling into category III as well as natural uranium should be protected in accordance with prudent management practice.

The recommendations formulated in INFCIRC/225 were favorably received and widely recognized by interested Member States as helpful in the design or improvement of their national systems of physical protection. Some States used the recommendations for guidance in the preparation of their national regulations on physical protection.

In the communications addressed to the Director General on 11 January 1978,** a group of 15 States agreed, inter alia, on certain criteria for adequate levels of physical protection as one of the conditions for exporting nuclear materials and equipment. In these communications, the definition of minimum levels of physical protection and, in particular, the categorization of nuclear material corresponded in terms with the recommendations contained in INFCIRC/225.

DEVELOPING INTERNATIONAL LEGAL NORMS

International legal norms emerge as a result of formal agreements on mutual relations between States or intergovernmental organizations. In the area of physical protection, such norms began to arise first as special clauses on physical protection. These clauses were incorporated into some new bilateral intergovernmental agreements on cooperation in the peaceful uses of nuclear energy and on

*At the second session of the Meeting of Governmental Representatives to Consider the Drafting of a Convention on the Physical Protection of Nuclear Material held in Vienna, 10 to 20 April 1978, an agreement was reached that for the purpose of the Convention less than 15 grams of plutonium or U^{233} or uranium enriched to 20 percent U^{235} or more and less than 1 kg of uranium enriched to 10 percent U^{235} but less than 20 percent should be considered as not significant from the physical protection point of view and hence be excluded from category III.

**The Member States who issued communications regarding guidelines for the export of nuclear material, equipment, and technology (INFCIRC/254) were Belgium, Canada, Czechoslovakia, France, the Federal Republic of Germany, the German Democratic Republic, Italy, Japan, the Netherlands, Poland, Switzerland, the Union of Soviet Socialist Republics, the United Kingdom, and the United States of America. A similar communication was received from Australia on 21 February 1978 (INFCIRC/254/Add.1).

provision of specified nuclear equipment and material. An example is the agreement between Brazil and the Federal Republic of Germany, signed on 27 June 1975. Article 5 of this agreement contained the following provisions:

1. Each Contracting Party shall take the measures required to ensure the physical protection of the nuclear materials, equipment and installations in its territory as well as during transportation between the territories of the Contracting Parties and to third countries.
2. These measures shall be designed to avoid, as far as practicable, hazards such as damage, accidents, theft, sabotage, hijacking, improper routing, interference or substitution.
3. The Contracting Parties shall for this purpose agree on suitable measures.

Consequently, special clauses regarding physical protection began to be incorporated into the bilateral and trilateral agreements concluded by the States, in particular those states already party to the previously mentioned agreements, with the IAEA in order to submit respective nuclear material and equipment to the Agency's safeguards system. The first in a series of such agreements was the Safeguards agreement of 26 February 1976* between the Agency, Brazil, and the Federal Republic of Germany which, in Part VI, "Physical Protection," contained the following wording from article 19: "Each contracting Government shall keep the Agency informed of the measures it will take to assure the physical protection of nuclear material, nuclear facilities and specified equipment".** In addition to similar provisions, some recent safeguards agreements made specific reference to the IAEA recommendations on physical protection. For instance, the Agreement of 2 March 1977 between the Agency and Pakistan for the application of safeguards in connection with the supply of uranium concentrate from Niger, section 16, read as follows: "Pakistan shall take all the measures necessary for physical protection of nuclear material, equipment and facilities subject to this Agreement and shall be guided by the recommendations of the Agency with regard to such measures" (INFCIRC/248, July 1977). Similar wording can be found in section 18 of the safeguards Agreement of 22 July 1977 between Argentina and the Agency in connection with a contract for cooperation between the Argentine Commission of Atomic Energy and a West German firm involved in the field of fuel element fabrication (INFCIRC/250, November 1977).

Some other safeguards agreements provided also for consultations with the Agency regarding physical protection. For instance, the Agreement of 22 July 1977 between Argentina and the IAEA for the application of safeguards in connection with a cooperation agreement between Argentina and Canada, section 24 states: "The Government of Argentine Republic shall take all the measures necessary for the physical protection of nuclear material, material, equipment and facilities required to

*Dates related to IAEA safeguards agreements are those of their entry into enforcement after approval by the Board of Governors and the Governments of the State parties.

**This safeguards agreement (INFCIRC/237, May 1976) was related to the agreement between Brazil and the Federal Republic of Germany cited in the footnote on p. 1-10.

be listed in the Inventory and shall be guided by the recommendations of the Agency with regard to such measures. The Government of the Argentine Republic and the Agency shall consult from time to time regarding physical protection. The Government of Canada shall be invited to participate in these consultations" (INFCIRC/251, November 1977).

The Agreement of 10 February 1977 between Canada, Spain, and the Agency on the application of safeguards distinguished itself by being more specific about the requirements of physical protection which were set forth in a special appendix and corresponded with the recommendations formulated in the Agency's document INFCIRC/225. Section 27 of this agreement contained the following provisions: "Each Government shall take all the measures necessary for the physical protection of nuclear material, material, equipment and facilities required to be listed in its Inventory, shall be guided by the recommendations of the Agency with regard to such measures and shall at a minimum meet the levels of physical protection which are set out in Appendix C to this Agreement. The Parties shall consult from time to time regarding physical protection." Appendix C contains the definitions of three categories of nuclear material and a characterization of minimum levels of physical protection to be applied to each of them (INFCIRC/247, May 1977).*

In the light of the preceding examples, there seemed to emerge, in the recent practice of the Agency, a trend toward inserting into its safeguards agreements special provisions on physical protection directly or indirectly related to the recommendations on this subject established under the Agency's auspices. This practice was, however, not completely uniform; some safeguards agreements concluded by the Agency with some States during the same period of time did not contain any provisions on physical protection. Being a part of international treaties, such provisions have the character of international legal norms, although some rights and obligations resulting from them, respectively, for the parties appear to be quite general, implying, for example, that, at present, the Agency has a right to receive some information on physical protection of nuclear material and equipment under the Agency's safeguards or to be consulted on the subject.

For some time, there has also been growing recognition of the need for an appropriate multilateral international convention on physical protection. This was indicated in a resolution adopted on 30 May 1975 by the Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons; it was also indicated in the IAEA publication, The Physical Protection of Nuclear Material (INFCIRC/225), in the resolution GC(XIX)/RES/328 of the General Conference in September 1975, and in the report of an Advisory Group on Physical Protection in March 1977.

*In the same way, physical protection issues were addressed in the Appendix of the draft of the Second Amendment to the Agreement for cooperation between the IAEA and the United States of America. The characterization of minimum levels of physical protection and the definition of three categories of nuclear material to which such different levels are to be applied corresponded with the provisions of INFCIRC/225/Rev.1 and of Annexes B of the communications from 15 States on their export policies. (See footnote, p. 1-10, regarding INFCIRC/254. For the text of the draft see IAEA document GOV/1879, 8 February 1978.

In June 1977, the Director General circulated to all Member States of the Agency the text of a "Draft Convention on Physical Protection of Nuclear Facilities, Material and Transports," which had been prepared by the United States. After a series of consultations with the representatives of Member States, the Director General invited all Member States to a meeting to consider the drafting of a convention on the physical protection of nuclear material and made the services of the Secretariat available for this meeting at the IAEA headquarters in Vienna.

In September 1977, the General Conference endorsed this initiative (Resolution GC, XXI/RES/350) and called upon all Member States to support the Director General's efforts to facilitate the development of a convention on the physical protection of nuclear material, facilities, and transports which would be suitable for adoption by as many States as possible.

The Meeting of Governmental Representatives to Consider Drafting of a Convention on the Physical Protection of Nuclear Material was held from 31 October to 10 November 1977. It was attended by 36 Member States from all parts of the world. Observers were sent by 10 more States and also by 3 international organizations: EURATOM, OECD/NEA, and OPANAL.

After general statements were made by most participants, two working groups were set up: one on legal issues and another on technical issues. The reports of the working groups, which were adopted by the Meeting, showed progress in the resolution of some of the substantive and drafting issues emerging from the original draft convention. The major issues, on which no agreement could be reached, concerned the scope of the convention: whether the convention should apply to the nuclear material in international transport only or also to material in storage and in national facilities and which categories of nuclear material the convention should cover.

The participants decided to continue the process of negotiating the convention at another session from 10 to 20 April 1978. It was attended by 40 Member States and several observers. At this second session, further progress was made within the working groups on technical and legal issues, as evidenced by the agreement reached on the draft texts of several articles and technical annexes. The number of reservations or alternatives to other draft articles was also reduced. However, again there was no agreement on the scope of the convention. At the present stage, further progress in negotiating the convention depends on the resolution of this issue and, for this purpose, the participants decided to hold a special meeting from 4 to 8 September 1978. The participants also decided to hold another session from 5 to 16 February 1979, at which they hope to agree on a widely acceptable text for the convention.

ASSISTANCE THROUGH EXPERTS AND FELLOWSHIPS

In a circular letter sent on 7 July 1977 to 24 Member States supposed to already possess some practical experience in dealing with physical protection matters, the Director General invited them to support the Agency's technical assistance program in this particular field in the following ways:

1. To make available experts on various aspects of physical protection who would be sent to assist Member States at their request in the elaboration or improvement of their national physical protection systems or in the solution of particular problems of physical protection,
2. To explore the possibility of offering fellowships for periods of 3 to 6 months for purposes of training personnel from Member States in specific physical protection topics, and
3. To consider receiving scientific visits of personnel from interested Member States for the purposes of familiarization with techniques, procedures, equipment, and performance of advanced physical protection systems.

A considerable number of governments, including, among others, those of France, the Federal Republic of Germany, the Union of Soviet Socialist Republics, and the United States of America, reacted positively to this enquiry, expressing their readiness to help satisfy the needs for all or some of the indicated forms of assistance in physical protection if specific requests were made through the customary channels and within the established framework of the Agency's Technical Assistance Programs. A number of requests were already filed with the Agency. The offers of assistance in physical protection already made and to be expected in the future make it possible for the Agency to respond to such requests in a satisfactory way.

TRAINING COURSES

A meeting of consultants was held at the IAEA headquarters from 17 to 21 October 1977 for the purpose of developing the concept of the first training course on physical protection for personnel from countries developing their nuclear power programs.

As a result, a report was produced in which the objectives of the training course were identified. It was recommended that the first course should be mainly orientated toward the staff members of the national authorities responsible for preparing regulations and designing and/or assessing physical protection systems. It was also recommended that the course should focus on physical protection of nuclear facilities and materials of the type currently used to satisfy the practical needs of developing countries, which means mainly nuclear power plants fueled with low-enriched or natural uranium. A detailed draft syllabus of the course was included into the report.

Early in 1978, the United States Department of Energy proposed to organize, in cooperation with the Agency, a training course corresponding to the preceding recommendations. The proposal was accepted by the Director General and the principles of cooperation have been defined in an arrangement between the United States of America and the IAEA covering organizational and financial issues.

Taking into account the experience gained through the first International Training Course on Physical Protection of Nuclear Facilities and Materials organized

at Sandia Laboratories in Albuquerque, New Mexico, it is expected that similar training courses can be organized in the future.

PUBLICATION OF PRACTICAL GUIDEBOOKS

A meeting of consultants was held at the IAEA headquarters in October 1977 to consider the preparation of an IAEA publication detailing and explaining comprehensive physical protection provisions for the nuclear power plants and in particular, taking into account the threat of all kinds of sabotage. The Adversary Group on Physical Protection indicated to the Agency that such a publication, which would complement the recommendations of INFCIRC/225 by focusing mainly on protection of the special nuclear materials against theft, could be of considerable use to many countries developing their basic nuclear programs by the construction of a nuclear power plant.

The consultants produced a report in which they recommended that a handbook be prepared and published within the IAEA Technical Reports Series under the title "Principles of Physical Protection of Nuclear Power Plants." Since this training course will be orientated toward the similar objective of assisting the countries developing nuclear energy programs to train their personnel in physical protection and since both projects should practically focus on nuclear power plants, the consultants advised that the texts of lectures and other materials of the course be developed into the proposed handbook and that persons responsible for the direction of the course assume the role of editors. The draft text of the handbook prepared in this way would then be reviewed by a technical committee of experts before its publication. It is expected that such a handbook can be published by the IAEA in 1979.

Publication of practical guidebooks dealing with other specific objects of physical protection, e.g., transport of nuclear materials, spent fuel storage, etc., may be envisaged by the Agency in the future.

THE IAEA AS A BANK OF INFORMATION

The Agency's Secretariat is establishing an information bank on physical protection of nuclear material and facilities. Its role will consist of collecting, processing, and making available to interested Member States unclassified information in the form of relevant books, articles, conference papers, and other publications, as well as national regulations on physical protection which the Member States are prepared to make available for this purpose. On the invitation of the Director General, several Member States offered their assistance in supplying relevant information.

It was decided that the Agency's library will be responsible for the functioning of such an information bank. The intent, at present, is to publish a physical protection bibliography bulletin which will include bibliographic data and abstracts of publications addressing problems of physical protection. The library cooperates

directly with respective national centers and also uses the resources and facilities of the Agency's International Nuclear Information System.

SUMMARY

The concern about physical protection of nuclear material and facilities has been growing in the 1970's due to the growth of terrorism in many parts of the world and to the expansion of the nuclear power industry resulting in an ever-increasing number of nuclear facilities and nuclear materials in use, storage, and transport.

On several occasions, the Member States of the IAEA have articulated their deep interest in assuring effective protection for nuclear materials and facilities and against theft, unauthorized removal, or sabotage. In particular they have stressed the need for international cooperation and the Agency's role in this area in the resolutions adopted by the IAEA General Conference in 1975 and 1977. Accordingly, the IAEA Secretariat in consultation with Member States developed a comprehensive program of Agency's activities in the field of physical protection which has actually been implemented.

First of all, the Agency is involved in formulating some guidelines for States' policies. The recommendations worked out by a group of experts were published in 1975 as an IAEA document, INF/CIRC/225, under the title, The Physical Protection of Nuclear Material. They are subject to review and updating from time to time. They were favorably received and used by interested States as guidance for designing their national physical protection systems. The definition of physical protection conditions for exporting nuclear material and equipment, as agreed upon in 1977 by a group of 15 States including main suppliers, was also based on these recommendations.

The Agency assists also the interested States in the development of international legal norms on physical protection. Special clauses on physical protection have, since 1976, been incorporated into a number of international agreements between States and the IAEA. An effort to draft a convention on physical protection has been undertaken and a series of governmental conferences on this subject were held at the IAEA headquarters in 1977 and 1978. It is hoped that an agreement on such a convention will be reached in the near future.

The Agency is in a position to render technical assistance to Member States on their request in the form of experts and fellowships in order to help in designing or improving national physical protection systems, in solving particular problems of physical protection, and in training specialized personnel. This last form of assistance is also rendered by organizing international training courses in physical protection.

The Agency intends to publish a series of practical guidebooks on physical protection. The first such publication is to be a handbook of physical protection principles for nuclear power plants. Similar publications regarding other types of nuclear facilities and transports are envisaged for a later date.

Finally, the IAEA library is prepared to supply interested Member States with bibliographical information on physical protection as well as to provide them with the copies of relevant publications on their request.

2.0 STATE SYSTEM OF PHYSICAL PROTECTION

Session Title: 2.1 The Objectives of a State
System of Physical Protection

Date: Wednesday, 1 November

Presented By: W. Morawiecki, IAEA

Time: 1430 to 1530

Session Objectives:

After the session, the participants will be able to

1. List two objectives of a State system of physical protection, and
2. List two objectives of the IAEA which are supported by physical protection.

Summary:

The State system of physical protection is introduced by a description, and what the IAEA physical protection objectives are and what the objectives of a State system of physical protection should be. The need for a State system is explained. The contents of the IAEA document, The Physical Protection of Nuclear Material, INFCIRC/225/Rev. 1, are summarized.

NOTE: The text of the material for this session is included in Module 1, "The IAEA Role in Physical Protection of Nuclear Facilities and Materials."

Additional Resource Materials:

INFCIRC/225/Rev. 1, The Physical Protection of Nuclear Material.

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

2.0 STATE SYSTEM OF PHYSICAL PROTECTION

Session Title: 2.2 Organizational Characteristics
of a State System of Physical
Protection

Date: Wednesday, 1 November

Presented By: L. Brenner, Department of Energy/
Office of Safeguards and Security

Time: 1530 to 1630

Session Objectives:

After the session, the participants will be able to

1. Describe the structure of a State system of physical protection, and
2. Describe the staffing considerations of the system.

Summary:

The structure of a State system is discussed with the aid of a basic organizational diagram, and an overview of the responsibilities of each organization is given. Each organization of the State system is discussed; emphasis is placed on staffing considerations and contingency planning.

ORGANIZATIONAL CHARACTERISTICS OF A STATE SYSTEM OF PHYSICAL PROTECTION

FUNDAMENTAL OBJECTIVE

The fundamental objective of a State system of physical protection is to physically protect all significant quantities of nuclear materials and nuclear facilities against acts of theft and sabotage.

The functions which must be performed by a physical protection system are

1. To detect and assess unauthorized acts of theft and sabotage,
2. To delay any attempts at theft or sabotage and to communicate their occurrence to the response forces, and
3. To respond to unauthorized acts in order to interrupt and neutralize them.

The integrated operation of detection, communication, delay, and response should be evaluated on a continuing basis in order to assure that the physical protection system provides effective protection over a wide range of credible threats.

RESPONSIBILITIES OF ORGANIZATIONS IN THE UNITED STATES

The responsibilities of the State system of physical protection are

1. To develop and enforce policies, standards, criteria, and procedures for the physical protection of nuclear materials and facilities in consultation with appropriate national nuclear organizations,
2. To assure the effectiveness of the State system requirements and its compatibility with that of the IAEA guidelines,
3. To provide guidance and technical assistance on the physical protection of nuclear materials and facilities to the national nuclear organizations and facility operators,
4. To immediately report any information related to actual or attempted theft of nuclear materials or sabotage of nuclear facilities or any other circumstances indicating a violation of State law concerning such material or facilities to the appropriate State law enforcement authorities,
5. To conduct evaluations of the adequacy of physical protection applicable to nuclear materials, facilities, and transport, to inform appropriate facility authorities of the results in a timely manner, and to take the action necessary to correct deficiencies,
6. To provide assistance for development of a physical protection plan for each new facility and for the upgrading of plans for each existing facility where assessments indicate deficiencies,
7. To interpret regulations,

8. To conduct all research and development as well as all test and evaluation necessary to meet the requirements for physical protection technology and to remain abreast of international technology and to transfer this technology to facilities, and
9. To provide liaison with other State systems where needed.

The physical protection responsibilities of the State nuclear organization are

1. To immediately report any information related to a possible or actual attempt at theft of nuclear materials or sabotage of nuclear facilities or any other circumstances indicating a violation of State law concerning such facilities or materials to the State system of physical protection and the contingency operations,
2. To direct the preparation of physical protection plans and procedures for facilities and activities for which they have responsibility, to refer such plans to the State system of physical protection for review and recommendations, and to assure that nuclear materials under their jurisdiction are protected,
3. To consult with the State system of physical protection on questions concerning physical protection requirements and other matters pertaining to the physical protection of nuclear materials and facilities,
4. To refer reports on noncompliance with requirements to the State system on physical protection,
5. To provide, in coordination with the State system on physical protection, appropriate guidance to responsible facility operators concerning the actions which need to be taken to implement physical protection systems and procedures, and
6. To perform reviews of activities involving nuclear materials and facilities under their jurisdiction whenever necessary to assure compliance.

The physical protection responsibilities of the nuclear facilities are

1. To assure that nuclear materials and facilities are afforded physical protection in accordance with the State system of physical protection regulations,
2. To submit written requests for any interpretations of the requirements to the State system of physical protection,
3. To request the State system of physical protection to review protective equipment, monitors, and other equipment planned for installation where test results and environmental and application considerations are not given in previously published guidelines,
4. To immediately report any information related to an actual theft of nuclear materials or sabotage of nuclear facilities or any other circumstances indicating a violation of State law concerning such materials to the appropriate authorities,
5. To report to the State system of physical protection changes in operations or arrangements which would affect the physical protection being provided,

6. To submit security plans for a new facility to the State system of protection, and
7. To establish and document a formal understanding of the support expected from local law enforcement agencies.

BACKGROUND

Physical protection standards are recommended by the IAEA in the INFCIRC/225 documents, The Physical Protection of Nuclear Materials, for three categories of nuclear materials. These categories are listed in Table 2-I.

TABLE 2-I
Categorization of Nuclear Material^a

Material	Form	I	Category II	III
Plutonium ^{a,f}	Unirradiated ^b	2 kg or more	Less than 2 kg but more than 500 grams	500 grams or less ^c
Uranium-235 ^d	Unirradiated ^b			
	• uranium enriched to 20 percent U ²³⁵ or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less ^c
	• uranium enriched to 10 percent U ²³⁵ but less than 20 percent	-	10 kg or more	Less than 10 kg ^c
	• uranium enriched above natural, but less than 10 percent U ²³⁵	-	-	10 kg or more
Uranium-233	Unirradiated ^b	2 kg or more	Less than 2 kg but more than 500 grams	500 grams or less ^c

^aAll plutonium except that with isotopic concentration exceeding 80 percent in Pu²³⁸.

^bMaterial not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 100 rads/h at 1 metre unshielded.

^cLess than a radiologically significant quantity should be exempted.

^dNatural uranium, depleted uranium, and thorium and quantities of uranium enriched to less than 10 percent not falling in category III should be protected in accordance with prudent management practices.

^eIrradiated fuel should be protected as category I, II, or III nuclear materials depending on the category of the fresh fuel. However, fuel, which by virtue of its original fissile material content is included as category I or II before irradiation, should only be reduced one category level, while the radiation level from the fuel exceeds 100 rads/h at 1 metre unshielded.

^fThe State's competent authority should determine if there is a credible threat to disperse plutonium malevolently. The State should then apply physical protection requirements for category I, II, or III of nuclear materials as it deems appropriate and without regard to the plutonium quantity specified under each category herein, to the plutonium isotopes in those quantities and forms determined by the State to fall within the scope of the credible dispersal threat.

These standards, when integrated with State materials control and accountability standards, provide the basis for an in-depth protection system for the deterrence and prevention of theft and sabotage of nuclear materials and facilities by either a violent outside terrorist group, an insider, or a combination of both.

ORGANIZATIONAL CHARACTERISTICS

The State system of physical protection can consist of the following five groups: (1) policy and regulation, (2) liaison, (3) technology, (4) inspectorate and rule enforcement, and (5) contingency. Figure 2-1 is a block diagram which shows the mechanism of interaction involved in the implementation of a State system of physical protection.

Figure 2-1. Interaction Mechanism for a State System of Physical Protection

The policy and regulation group sets standards or rules for the different facilities based on the level of threat concerns, international standards, State laws, facility characteristics, and technological developments.

Feedback is received from facility evaluations and, through the liaison section, from appropriate nuclear organizations and national police.

These regulations are then implemented by the facility through the use of a technology/protective force physical protection system. The technology group keeps abreast of international physical protection technology. It may operate a research and development program to fulfill facility needs as well as test and evaluate equipment and systems for performance capabilities. The group also provides recommendations to facilities or regulation-forming groups.

The inspectorate group reviews the physical protection of a facility with respect to the established regulations and enforces the rules which have not been met. This evaluation provides feedback for both the technology and policy groups.

The contingency operations group responds to any attempted acts of theft of nuclear materials or sabotage of nuclear facilities in order to interrupt and neutralize these attempts. This group provides for a response system for each facility as well as a centralized operation center which functions in conjunction with State authorities.

MANPOWER REQUIREMENTS

Manpower for inspection is dependent upon the number and complexity of the specific facility. In general, a facility should be inspected twice per year and inspectors should spend one-third of their time at sites and two-thirds of their time at the State office.

Policy and regulations depend upon the complexity and variety of the facilities involved. Manpower is needed to keep abreast of threat concerns, facility types, international standards, and contingency capabilities and also to maintain a practical understanding of facility operations.

In the technology group, manpower is needed to keep abreast of international developments in order to provide any needed research and development, test and evaluation, and system studies. Depending on its orientation and emphasis, this section may have a separate office from the State system of physical protection center and manpower requirements will vary. Initially, a small group will be required to accomplish technology transfer to facilities.

CONCLUSION

An effective State system for physical protection includes groups which can fulfill the roles of policy, regulation-forming, technology transfer, inspection and enforcement liaison, and contingency. These groups will vary in size depending on the complexity and number of facilities which need to be protected. The size of the groups is also dependent on the emphasis placed on technology and response capabilities. The total State system will need to be reevaluated for its overall effectiveness through feedback from facilities and international standards.

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

2.0 STATE SYSTEM OF PHYSICAL PROTECTION

Session Title: 2.3 Licenses and Regulations

Date: Thursday, 2 November

Presented By: F. Pagano, U.S. Nuclear
Regulatory Commission*

Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. Identify the major regulatory activities of the State system,
2. Describe licensing and inspection procedures, and
3. Discuss the need for a State system of physical protection (SSOPP).

Summary:

The development of regulations and guidelines will be discussed. A USA view of licensing and inspection procedures will be given.

*The text for this session was prepared from notes provided by the presenter.

LICENSES AND REGULATIONS

SAFEGUARDS RESPONSIBILITIES

The U.S. Nuclear Regulatory Commission has the responsibility for regulating the physical protection of commercial nuclear facilities within the United States of America. This responsibility is limited to commercial nuclear facilities; the protection of nuclear power plants operated under the authority of the U.S. Department of Defense and the U.S. Department of Energy is not the responsibility of the Nuclear Regulatory Commission.

Information Circular/225 (INFCIRC/225), The Physical Protection of Nuclear Materials, which is published by the International Atomic Energy Agency, recommends measures for the physical protection of nuclear materials in use, in transit, and in storage. The domestic regulatory policy concerning the physical protection of nuclear facilities within the United States exceeds the requirements of INFCIRC/225.

Safeguards responsibilities within the Nuclear Regulatory Commission are divided between two major offices: the Office of Nuclear Materials Safety and Safeguards and the Office of Nuclear Reactor Regulation. The prime responsibilities of each of these offices are summarized in Table 2-II.

TABLE 2-II
Nuclear Regulatory Commission
Safeguards Responsibilities

<u>Facility</u>	<u>Concern</u>	<u>Prime Responsibility</u>
Reactors (power and nonpower)	Sabotage Theft*	Office of Reactor Regulation
Fuel-cycle facilities	Theft Sabotage	Office of Nuclear Materials Safety and Safeguards
Transportation	Theft Sabotage	Office of Nuclear Materials Safety and Safeguards

*For breeder reactors, mixed-oxide fuels, and some nonpower reactors.

The Office of Nuclear Materials Safety and Safeguards is responsible for the safeguarding of fuel-cycle facilities and the transportation of nuclear material. The Office of Nuclear Reactor Regulation is responsible for the licensing of facilities and for regulations associated with the construction and operation of all nuclear reactors. This responsibility includes both safety and safeguards for

(1) commercial nuclear power reactors, (2) nonpower (research) reactors, and (3) demonstration nuclear reactors. As of July 1978, there were 213 reactors operational or under construction within the United States; the status of these reactors is shown in Table 2-III. The location of all the commercial nuclear power plants in the United States is shown in Figure 2-2. The regional offices for the Nuclear Regulatory Commission are also shown in this figure.

TABLE 2-III
Status of Nuclear Power Plants--31 July 1978

Number of Units	Status	Rated Capacity (MWe)
70	Licensed to operate*	51,000
88	Construction permit granted** 32 Under operating license review 56 Operating license not yet applied for	95,000
39	Under construction permit review 6 Site work authorized, safety review in process** 33 Other units under CP review	44,000
9	Ordered	11,000
7	Publicly announced	8,000
213	Total	209,000

*To date, there have been 402 reactor-years of operation. Not included are two operable U.S. Department of Energy-owned reactors with a combined capacity of 940 MWe.

**Total of units authorized construction (construction permit granted plus site work authorized): 94 units, 102,000 MWe.

In addition to commercial nuclear power plants, the Office of Nuclear Reactor Regulation is also responsible for safeguarding nonpower reactors. Currently, there are 37 low-power research and training reactors, 32 medium-power research reactors, and 3 high-power research and test reactors licensed to operate.

GENERIC SAFEGUARDS CONCERNS

The Nuclear Regulatory Commission's generic safeguards concerns are twofold: (1) the sabotage of nuclear facilities which could lead to the dispersal of radioactive materials and (2) the theft of special nuclear materials which could be used to fabricate nuclear weapons. The greatest safeguards concern for power reactors is the sabotage of reactor systems or components which could endanger the public health and safety through the release of radioactive substances into the atmosphere. The theft of new fuel elements from advanced reactor designs, e.g., high-temperature gas-cooled reactors and mixed-oxide fueled reactors, is also a principal concern but of lesser magnitude than sabotage. In the case of nonpower reactors, the principal concern is the theft of special nuclear materials; for breeder reactors, the concern is for both sabotage and theft.

Figure 2-2. Commercial Nuclear Power Reactors in the United States and Nuclear Regulatory Commission Regional Offices

The sabotage scenarios that must be protected against in the commercial nuclear power plant are acts which lead to reactor core meltdown, e.g., massive loss-of-coolant accidents and the subsequent loss of core cooling capability. Also, protection must be provided against acts of sabotage directed at spent-fuel storage facilities. In this case, explosives could be used to disperse stored fuel or to rupture the spent fuel pool with the subsequent loss of cooling to the fuel. Another concern is the rupture of radwaste storage tanks which may also contain large amounts of radioactive materials.

The current Nuclear Regulatory Commission approach to safeguarding nuclear reactors from sabotage is to emphasize physical protection. The Nuclear Regulatory Commission has issued a regulation, Title 10, Code of Federal Regulations, Part 73 (10CFR73.55), which requires the use of physical protection systems. All utilities that have been issued a license to operate a nuclear reactor must have a security plan which describes the methods and procedures to be employed to meet these requirements. Also, reliance is placed on the inherent protection afforded by the safety design of the nuclear reactor which requires defense in depth with multiple barriers to contain fission products and system design based on redundant and separate components as well as massive structures designed to withstand a severe natural catastrophe. Specific procedures are also required for the establishment of contingency plans and an incident response plan.

In order to prevent the theft of special nuclear materials, the licensee must adhere to a set of physical protection requirements for those cases where the licensee has greater than the formula quantities of special nuclear materials on

hand. In order to comply with these requirements, the licensee must submit a security plan for Nuclear Regulatory Commission review and approval. When a licensee has less than formula quantities of special nuclear materials on hand there are no specific physical protection requirements. Fuel in the reactor core and spent fuel of a specific radiation level are also exempt from these physical protection requirements.

REGULATORY GUIDES

The Nuclear Regulatory Commission issues regulatory guides which describe those methods that are acceptable to the Commission for implementing specific parts of the regulations. Note that these regulatory guides are not substitutes for regulations and compliance is not mandatory. The current regulatory guides that are concerned with reactor safeguards are itemized in Table 2-IV.

TABLE 2-IV
Regulatory Guides

<u>Regulatory Guide</u>	<u>Title</u>
1.17	Protection of Nuclear Power Plants Against Industrial Sabotage
5.7	Control of Personnel Access to Protected Areas, Vital Areas, and Material Access Areas
5.12	General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials
5.20	Training, Equipping, and Qualifying of Guards and Watchmen
5.43	Plant Security Force Duties
5.44	Perimeter Intrusion Alarm Systems
5.54	Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants

ELEMENTS OF REACTOR SAFEGUARDS

The Nuclear Regulatory Commission has three major regulation areas for reactor safeguards: (1) physical security, (2) guard training, and (3) contingency planning. Physical security regulations will be discussed in detail in this session; guard training and contingency planning will be discussed briefly. Regulatory requirements for physical security are outlined in 10CFR73.55. Guard training requirements are outlined in Appendix B to 10CFR73; contingency planning is contained in Appendix C to 10CFR73.

The regulations for physical protection of nuclear power plants use the concept of a general performance requirement plus the delineation of specific system requirements. The general performance requirement allows the safeguards system to be measured against a specific threat but allows the nuclear power plant operator flexibility in the design of the safeguards system. The delineation of specific system requirements provides specific guidance as to what is required, as a minimum, to meet the general performance requirement. The regulation has two significant areas: the general performance requirements contained in paragraph (A)

and specific requirements contained in paragraphs (B) through (H). To meet the general performance requirements, the physical protection system and the security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements of the regulation. However, the Commission may authorize measures for protection against sabotage other than those required by the specific requirements if the alternate system provides protection equivalent to the specific requirements and is capable of meeting the general performance requirements.

The general performance requirement is worded as follows:

The licensee shall establish and maintain an on-site physical protection system and security organization which will provide protection with high assurance against successful industrial sabotage by both of the following: (1) a determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance, and equipment: (a) well-trained (including military training and skills) and dedicated individuals, (b) inside assistance which may include a knowledgeable individual who attempts to participate in both a passive role, e.g., provide information, and an active role, e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack, (c) suitable weapons, up to and including handheld automatic weapons, equipped with silencers and having effective long-range accuracy, (d) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or otherwise destroying reactor integrity, and (2) an internal threat of an insider, including an employee (in any position).

The specific system requirements as set forth in paragraphs (B) through (H) are divided into the following categories:

1. Physical security organization,
2. Physical barriers,
3. Detection aids,
4. Access requirements,
5. Communications requirements,
6. Testing and maintenance,
7. Response requirements, and
8. Records.

The design of the reactor systems and specific security procedures are also major elements of a reactor safeguards program, but these requirements are not covered in 10CFR73.55.

Security Plan

Regulation 10CFR73.55 requires that the licensee provide the Nuclear Regulatory Commission with a security plan that describes the physical protection methods to be used for a facility. The security plan concept allows the licensee flexibility in meeting regulatory requirements. Basically, for a reactor, the licensee's plan must define vital areas and show how protection requirements will be met. Details of the protection program are not made public.

Physical Security Organizations

The licensee must maintain a security organization which includes armed guards to protect the facility against industrial sabotage. The security organization must provide protection 24 hours each day. At least one full-time member (supervisor) of the security organization who has the authority to direct the protective force shall be on-site at all times. Generally, the security organization will consist of 5 to 10 on-duty armed guards. The licensee must employ properly trained and qualified security personnel who have an understanding of the licensee's security procedures and have the ability to execute all duties required by the procedures. The protective force must be trained, requalified annually, and meet training requirements published by the Nuclear Regulatory Commission. The plan must have written procedures that detail how the plan is to be implemented.

Physical Barriers

The licensee must protect the vital equipment of the nuclear power plant. Vital equipment is defined as any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

Vital equipment must be located in a vital area which is constructed of stone, brick, cinder block, concrete, steel or comparable materials (the openings of which are secured by grates, doors, or covers of construction and fastening material of sufficient strength so that the integrity of the wall is not lessened by any opening), or an 8-foot wall of similar construction, not part of a building, provided with a barbed topping.

The vital area must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers. The protected area barrier is normally a fence constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire or similar material on brackets angled outward between 30 degrees and 45 degrees from the vertical, with an overall height of not less than 8 feet, including the barbed topping. More than one vital area may be located within a single protected area.

The physical barrier at the perimeter of the protected area must be separated from the vital area barrier. The protected area perimeter must have an isolation zone on each side of the barrier to permit observation of any activity. The normal isolation zone extends 20 feet on each side of the fence. The isolation zones and all exterior areas within the protected area must be illuminated to at least 0.2 footcandle measured horizontally at ground level.

The licensee must provide a system for the detection of penetration or attempted penetration of the protected area. The licensee normally utilizes an electronic intrusion detection system, e.g., microwave or infrared, for this purpose.

The licensee must periodically patrol all exterior areas within the protected area to detect unauthorized persons, vehicles, and materials. In addition, the reactor control room must be bullet resistant.

Access Control

The licensee must control all points of personnel and vehicle access into a protected area. Identification and search of all individuals must be made and authorization must be checked at these points. The search for firearms, explosives, and incendiary devices must be conducted either by a physical search or by use of equipment capable of detecting these contraband items. The individual responsible for controlling admission to the protected area must be isolated within a bullet-resisting structure. In addition to personnel searches, all hand-carried packages must be searched for any items which could be used for industrial sabotage.

All packages and material for delivery into the protected area must be checked for proper identification and authorization and searched prior to entering into the protected area, except those Commission-approved delivery and inspection activities specifically designed by the licensee to be carried out within vital or protected area for reasons of safety, security, or operational necessity.

All vehicles, except under emergency conditions, must be searched prior to entry into the protected area. Vehicle areas to be searched include the cab, engine compartment, undercarriage, and cargo area. All vehicles, except designated licensee vehicles, requiring entry into the protected area must be escorted by a guard while within the protected area and, to the extent practicable, must be off-loaded in the protected area at a specific designated materials receiving area that is not adjacent to a vital area. Designated licensee vehicles shall be limited to use for on-site plant functions and shall remain in the protected area except for operational, maintenance, repair security, and emergency purposes. The licensee must exercise positive control over all designated vehicles to assure that they are used only by authorized persons and for authorized purposes.

A numbered picture badge identification system must be used for all individuals who are authorized access to protected areas without escort. An individual not employed by the licensee but who requires frequent and extended access to protected and vital areas may be authorized access to such areas without escort provided that the individual receives a picture badge upon entrance into the protected area which must be returned upon exit.

Individuals not authorized to enter protected areas without escort must be escorted by a watchman or other individual designated by the licensee while in a protected area and must be badged to indicate that an escort is required. In addition, each such individual must register his name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited.

The licensee must positively control all points of personnel and vehicle access into vital areas. Access to vital areas must be limited to individuals who are authorized access to vital equipment and who require such access to perform their duties. Authorization for such individuals must be provided by the issuance of specially coded numbered badges indicating the vital areas to which access is authorized. Access to vital areas for the purpose of general familiarization and other non-work-related activities must not be authorized except for good cause shown to the licensee. Unoccupied vital areas must be locked and protected by an active intrusion alarm system.

Access to the reactor containment must be through doors or hatches which must be alarmed and have locks of substantial construction to offer penetration resistance and impede both surreptitious and forced entry. Any time frequent access is permitted to containment such as during refueling or major maintenance, positive access control to assure that only authorized personnel and materials are for major maintenance, positive access control to assure that only authorized personnel and materials are permitted into the containment must be exercised by the licensee through the use of a guard or watchman.

All keys, locks, combinations, and related equipment used to control access to protected and vital areas must be controlled to reduce the probability of compromise. Whenever there is evidence that any key, lock, combination, or related equipment may have been compromised, it must be changed. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access must be changed.

Personnel Screening

Personnel screening is not specifically required by the regulations but, in general, all persons working at a nuclear power plant are subject to a company-sponsored investigation as well as a psychological screening conducted by doctors or licensed psychologists. In addition, there is a program of continued observations of their behavior.

Detection Aid Requirements

Intrusion detection systems are required for the protected area barrier, all vital area doors, and all emergency exits from the protected area and vital areas. All alarms must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station, not necessarily on-site, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm. The on-site central alarm station must be considered a vital area and its walls, doors, ceiling, floor, and any windows in the walls and in the doors must be bullet-resisting. The on-site central alarm station must be located within a building so that the interior of the central alarm station is not visible from the perimeter of the protected area. These stations must not contain any operational activities that would interfere with the execution of the alarm response function. All alarms must also annunciate in a secondary alarm station similar to the central alarm station.

In addition, all alarm devices, including transmission lines to annunciators, must be tamper-indicating and self-checking. The annunciation of an alarm at the alarm stations must indicate the type of alarm and location.

Communications Requirements

Each guard, watchman, or armed response individual on duty must be capable of maintaining continuous communication with an individual in each continuously manned alarm station. The alarm stations must have conventional telephone service for communication with the law enforcement authorities.

In addition to conventional telephone service, radio or microwave transmitted two-way voice communication, either directly or through an intermediary, must be established between local law enforcement authorities and the facility and shall terminate in each alarm station. Nonportable communications equipment controlled by the licensee and required by the regulations must remain operable through the use of independent power sources in the event of the loss of normal power.

Testing and Maintenance

The licensee must test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment as follows:

1. All alarms, communication equipment, physical barriers, and other security-related devices or equipment must be maintained in operable condition. The licensee must develop and employ compensatory measures including equipment, additional security personnel, and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operations of the security-related equipment or structures.
2. Each intrusion alarm must be tested for performance at the beginning and end of any period that it is used for security. If the period of continuous use is longer than 7 days, the intrusion alarm must also be tested at least once every 7 days.
3. Communications equipment required for on-site communications must be tested for performance not less frequently than once at the beginning of each security personnel work shift. Communications equipment required for off-site communications must be tested for performance not less than once a day.

For any system that does not operate properly, the licensee must position guards or use other methods to maintain security.

Response Requirements

The licensee must execute, when appropriate, a safeguards contingency plan for dealing with threats, thefts and industrial sabotage. Safeguards contingency plans must be in accordance with published criteria. The licensee must establish and document liaison with local law enforcement authorities.

Nominally, the total number of guards and armed, trained personnel immediately available at the facility to fulfill these response requirements must total 10 unless specifically changed on a case-by-case basis by the Nuclear Regulatory Commission; however, this number may not be reduced to less than 5 guards.

Upon detection of abnormal activity by persons or vehicles within an isolation zone, a protected area, or a vital area or upon evidence of intrusion into a protected area or a vital area, the facility security organization must

1. Determine whether or not a threat exists,
2. Assess the extent of the threat, if any,
3. Inform local law enforcement agencies of the threat and request assistance, if necessary,
4. Require guards or other armed response personnel to interpose themselves between vital areas and any adversary attempting entry for purposes of industrial sabotage, and
5. Instruct guards or other armed response personnel to prevent or delay an act of industrial sabotage by applying a sufficient degree of force to counter that degree of force directed at them, including the use of deadly force when there is a reasonable belief it is necessary in self-defense or in the defense of others.

To facilitate initial response to the detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area must be provided, preferably by means of closed-circuit television or by other suitable means which limit the exposure of responding personnel to possible attack.

GUARD TRAINING REQUIREMENTS

The second major requirement of reactor safeguards regulation is guard training. In this area, performance-oriented requirements for guards are specified which require that the licensee determine what training is required to implement both the physical protection and the contingency plan. The regulation also requires the establishment of standards of performance for all critical security-related tasks and that the licensee require demonstrated acceptable performance of skills before assignment of a guard to a job.

CONTINGENCY PLANS

The third requirement of reactor safeguards regulation is contingency planning which requires licensees to develop plans to deal with all types of contingencies or incidents that could occur at a facility, e.g., fire, civil disorder, guard strike, attack by an adversary, etc. Regulatory Guide 5.54, Standard Format and Content of Safeguards gives the licensee specific guidance for meeting these rules. Regulatory Guide 5.54 also includes a representative safeguards contingency plan for a nuclear power plant.

SESSION 2.3

VISUALS

NOTES

**UNITED STATES
NUCLEAR REGULATORY
COMMISSION**

REACTOR SAFEGUARDS

**SAFEGUARDS FOR
NUCLEAR POWER PLANTS**

**NUCLEAR REGULATORY COMMISSION
SAFEGUARDS RESPONSIBILITIES**

<u>FACILITY</u>	<u>CONCERN</u>	<u>PRIME RESPONSIBILITY</u>
REACTORS (POWER & NON-POWER)	SABOTAGE THEFT*	NUCLEAR REACTOR REGULATION
FUEL CYCLE FACILITIES	THEFT SABOTAGE	NUCLEAR MATERIALS SAFETY AND SAFEGUARDS
TRANSPORTATION	THEFT SABOTAGE	NUCLEAR MATERIALS SAFETY AND SAFEGUARDS

*FOR BREEDER REACTORS, MIXED OXIDE FUELS, AND SOME NON-POWER REACTORS

OFFICE OF NUCLEAR REACTOR REGULATION

THE OFFICE OF NUCLEAR REACTOR REGULATION HAS RESPONSIBILITY FOR THE PRINCIPAL LICENSING AND REGULATION ASSOCIATED WITH THE CONSTRUCTION AND OPERATION OF NUCLEAR REACTORS INCLUDING REVIEW OF THE SAFETY AND SAFEGUARDS OF ALL SUCH FACILITIES.

- COMMERCIAL NUCLEAR POWER REACTORS
- NON-POWER (RESEARCH) REACTORS
- DEMONSTRATION NUCLEAR REACTORS

STATUS OF NUCLEAR POWER PLANTS — JULY 31, 1978

Number Of Units	Rated Capacity (MW _e)
*70 LICENSED TO OPERATE	51,000
**88 CONSTRUCTION PERMIT GRANTED	95,600
22 Under Operating License Review	2,000
66 Operating License Rule Yet Applied For	93,600
26 UNDER CONSTRUCTION PERMIT REVIEW	44,000
** 9 Site Work Authorized, Safety Review In Progress	7,000
23 Other Units Under CP Review	37,000
8 ORDERED	11,000
7 PUBLICLY ANNOUNCED	8,000
215 TOTAL	209,600

*12 units have been less than 400 reactor years of operation. Not included are two operating DPC-qualified reactors with a combined capacity of 200 MW_e.

** Total of units authorized construction (Construction Permit Granted plus Site Work Authorized): 94 units, 193,600 MW_e.

VISUALS

NOTES

- 37 LOW POWER RESEARCH AND TRAINING REACTORS (≤ 100 KW)
- 32 MEDIUM POWER RESEARCH REACTORS (> 100 KW AND ≤ 5000 KW)
- 3 HIGH POWER RESEARCH AND TEST REACTORS (> 5000 KW)

GENERIC SAFEGUARDS CONCERNS

- SABOTAGE OF NUCLEAR FACILITIES LEADING TO DISPERSAL OF RADIOACTIVE MATERIALS
- THEFT OF SPECIAL NUCLEAR MATERIAL LEADING TO FABRICATION OF NUCLEAR WEAPONS

VISUALS

NOTES

REACTOR SAFEGUARDS CONCERNS

- POWER REACTORS
 - SABOTAGE OF REACTOR SYSTEMS OR COMPONENTS WHICH COULD ENDANGER THE PUBLIC HEALTH AND SAFETY
 - THEFT OF NEW FUEL ELEMENTS (ADVANCED REACTOR DESIGNS - HIGH TEMPERATURE GAS COOLED REACTORS MIXED OXIDE FUELS)
- NON-POWER REACTORS
 - THEFT OF SPECIAL NUCLEAR MATERIAL (NEW, IN CORE, AND SPENT FUEL ELEMENTS)
- DEMONSTRATION REACTORS (BREEDER REACTOR)
 - SABOTAGE
 - THEFT OF SPECIAL NUCLEAR MATERIAL (NEW FUEL ELEMENTS)

SABOTAGE SCENARIOS

- ACTS LEADING TO REACTOR CORE MELTDOWN
 - MASSIVE LOSS-OF-COOLANT ACCIDENT
 - LOSS OF CORE COOLING CAPABILITY
- ACTS DIRECTED AT SPENT FUEL STORAGE
 - MASSIVE EXPLOSIVE ATTACK - DISPERSAL OF FUEL
 - RUPTURE OF SPENT FUEL POOL - LOSS OF COOLING
- RUPTURE OF RADWASTE STORAGE TANKS

CURRENT REACTOR SAFEGUARDS APPROACH SABOTAGE

- PHYSICAL PROTECTION
 - 10 CFR 73.55
MUST HAVE SECURITY PLAN
SPECIFIC REQUIREMENTS
- INHERENT PROTECTION -- SAFETY DESIGN BASIS
 - DEFENSE IN DEPTH -- MULTIPLE BARRIERS TO THE RELEASE OF FISSION PRODUCTS
 - SYSTEM DESIGN BASED ON REDUNDANT AND SEPARATE COMPONENTS
 - MASSIVE STRUCTURES DESIGNED TO WITHSTAND SEVERE NATURAL PHENOMENA
- PROCEDURES
 - CONTINGENCY PLANNING
 - INCIDENT RESPONSE

VISUALS

NOTES

CURRENT REACTOR SAFEGUARDS APPROACH THEFT OF SNM

- GREATER THAN FORMULA QUANTITIES OF SPECIAL NUCLEAR MATERIAL
 - APPLY SPECIFIC REQUIREMENTS OF 10 CFR 73.50 AND 10 CFR 73.40 AS APPLICABLE
 - FUEL IN CORE EXEMPT
 - SPENT FUEL OF HIGH DOSE RATE EXEMPT
- LESS THAN FORMULA QUANTITIES
 - NO SPECIFIC REQUIREMENTS
 - CASE BY CASE REVIEW — SUBMITTAL OF SECURITY PLAN PER 10 CFR 73.40
- PROCEDURES
 - CONTINGENCY PLANNING
 - INCIDENT RESPONSE

REGULATORY GUIDES

- 1.17 PROTECTION OF NUCLEAR POWER PLANTS AGAINST INDUSTRIAL SABOTAGE
- 5.7 CONTROL OF PERSONNEL ACCESS TO PROTECTED AREAS, VITAL AREAS, AND MATERIAL ACCESS AREAS
- 5.12 GENERAL USE OF LOCKS IN THE PROTECTION AND CONTROL OF FACILITIES AND SPECIAL NUCLEAR MATERIALS
- 5.20 TRAINING, EQUIPPING, AND QUALIFYING OF GUARDS AND WATCHMEN
- 5.43 PLANT SECURITY FORCE DUTIES
- 5.44 PERIMETER INTRUSION ALARM SYSTEMS
- 5.54 STANDARD FORMAT AND CONTENT OF SAFEGUARDS CONTINGENCY PLANS FOR NUCLEAR POWER PLANTS

REGULATORY REQUIREMENTS

- 10 CFR 73.55 — PHYSICAL SECURITY
- APPENDIX B TO 10 CFR 73 — GUARD TRAINING
- APPENDIX C TO 10 CFR 73 — CONTINGENCY PLANNING

VISUALS

NOTES

10 CFR 73.55

"REQUIREMENTS FOR PHYSICAL PROTECTION
OF LICENSED ACTIVITIES IN NUCLEAR POWER
REACTORS AGAINST INDUSTRIAL SABOTAGE"

- CONCEPT OF PERFORMANCE REQUIREMENT
- PERFORMANCE OF SAFEGUARDS SYSTEM MEASURED AGAINST DESIGN BASIS THREAT
- LICENSEE HAS FLEXIBILITY IN DESIGN OF SYSTEM
- CONSISTENT WITH COMMISSION'S OBJECTIVE OF PERFORMANCE ORIENTED RULES
- DELINEATION OF SPECIFIC SYSTEM REQUIREMENTS
- SIMILAR TO REQUIREMENTS IN PREVIOUS RULES
- PROVIDES SPECIFIC GUIDANCE AS TO WHAT IS REQUIRED, AS A MINIMUM, TO MEET THE PERFORMANCE OBJECTIVE OF THE RULE

PERFORMANCE OBJECTIVE

- DETERMINED VIOLENT ASSAULT — SEVERAL PERSONS
 - WELL TRAINED
 - INSIDE ASSISTANCE
 - HAND HELD AUTOMATIC WEAPONS
 - INCAPACITATING AGENTS
 - EXPLOSIVES
- AN INSIDER IN ANY POSITION

ELEMENTS OF REACTOR SAFEGUARDS

- PHYSICAL SECURITY
 - PHYSICAL SECURITY ORGANIZATION
 - PHYSICAL BARRIERS
 - DETECTION AIDS
 - ACCESS REQUIREMENTS
 - COMMUNICATION REQUIREMENTS
 - TESTING AND MAINTENANCE
 - RESPONSE REQUIREMENT
- DESIGN
 - REDUNDANCY
 - HARDENING
 - BARRIERS
 - SEPARATION
- PROCEDURES
 - CONTINGENCY PLANNING
 - INCIDENT RESPONSE

VISUALS

NOTES

THE SECURITY PLAN

- PLAN CONCEPT ALLOWS LICENSEE FLEXIBILITY IN MEETING REQUIREMENTS
- PLAN MUST
 - DEFINE VITAL AREAS
 - SHOW HOW PROTECTION REQUIREMENTS WILL BE MET
- DETAILS OF PROTECTION PROGRAM NOT MADE PUBLIC

PHYSICAL SECURITY ORGANIZATION

- ORGANIZATION OF ONSITE GUARDS AND WATCHMEN 24 HOURS EVERY DAY
- RESPONSIBILITIES OF THE PROTECTION FORCE
 - IMPLEMENT PLAN
 - RESPOND TO ALARMS
 - RESPOND TO INTRUSION
- SIZE OF FORCE
- TRAINING OF FORCE
- PLAN IMPLEMENTED BY WRITTEN PROCEDURES

PHYSICAL BARRIERS

- VITAL EQUIPMENT PROTECTED BY TWO BARRIERS
- ILLUMINATED AND MONITORED ISOLATION ZONE AROUND OUTERMOST BARRIER
- ILLUMINATED PROTECTED AREA

VISUALS

NOTES

ACCESS CONTROLS

- ACCESS TO PROTECTED AREA CONTROLLED
- PICTURE BADGE IDENTIFICATION
- VISITORS REGISTERED AND ESCORTED
- PERSONNEL, PACKAGES, AND VEHICLES ENTERING PROTECTED AREA SEARCHED
- ADMITTANCE TO VITAL AREAS CONTROLLED AND LIMITED
- KEYS, LOCKS AND COMBINATIONS CONTROLLED

PERSONNEL SCREENING

- BACKGROUND INVESTIGATION
- PSYCHOLOGICAL SCREENING
- CONTINUED OBSERVATION

DETECTION AID REQUIREMENTS

- INTRUSION DETECTION SYSTEMS REQUIRED FOR
 - PROTECTED AREA BARRIER
 - VITAL AREAS
 - EMERGENCY EXITS
- ALARMS ANNUNCIATE IN CENTRAL ALARM STATION WHICH IS
 - CONTINUOUSLY MANNED
 - BULLET-RESISTING
 - VITAL AREA
- ALARMS ALSO ANNUNCIATE IN SECONDARY ALARM STATION
- INTRUSION DETECTION SYSTEMS MUST MEET DETAILED PERFORMANCE REQUIREMENTS

VISUALS

NOTES

COMMUNICATION REQUIREMENTS

- EACH GUARD MUST CARRY RADIO
- CENTRAL ALARM STATION MUST HAVE RADIO AND TELEPHONE COMMUNICATION WITH LOCAL LAW ENFORCEMENT AGENCY
- SECONDARY ALARM STATION MUST HAVE RADIO AND TELEPHONE COMMUNICATION WITH LOCAL LAW ENFORCEMENT AGENCY
- RADIO MUST HAVE EMERGENCY POWER SOURCE

TESTING AND MAINTENANCE

- ALARMS, COMMUNICATIONS, AND OTHER SECURITY RELATED EQUIPMENT SHALL BE TESTED
- SECURITY SYSTEMS SHALL REMAIN OPERABLE
- COMPENSATORY MEASURES

RESPONSE REQUIREMENTS

- LIAISON WITH LOCAL LAW ENFORCEMENT AGENCY
- PLANNED REINFORCEMENTS
- ONSITE GUARDS MUST
 - RESPOND TO ALARMS
 - ASSESS THREAT
 - TAKE ACTION TO NEUTRALIZE THREAT
- CLOSED CIRCUIT TELEVISION FOR ASSESSMENT

VISUALS

NOTES

GUARD TRAINING PERFORMANCE ORIENTED REQUIREMENTS

- DETERMINE WHAT IS REQUIRED TO IMPLEMENT 73.56 AND CONTINGENCY PLANNING RULE
- SET STANDARDS OF PERFORMANCE FOR TASKS
- REQUIRE PERFORMANCE OF OBJECTIVES BEFORE ASSIGNMENT TO JOB

REACTOR SAFEGUARDS CONTINGENCY PLANNING

- CONTINGENCY PLANNING RULE
 - REQUIRES LICENSEES TO DEVELOP CONTINGENCY PLANS
 - CONTINGENCY PLANS DUE MARCH 1979
- REGULATORY GUIDE 5.54 STANDARD FORMAT AND CONTENT OF SAFEGUARDS
 - GENERIC PLANNING BASE
 - LICENSEE PLANNING BASE
 - RESPONSIBILITY MATRIX
 - REPRESENTATIVE SAFEGUARDS CONTINGENCY PLAN FOR A NUCLEAR POWER PLANT

3.0 REACTORS

Session Title: 3.1 Fuel Cycle

Date: Thursday, 2 November

Presented By: R. Knief, University of New Mexico
and Sandia Laboratories
Consultant

Time: 1100 to 1200

Session Objectives:

After the session, the participants will be able to

1. Identify the steps in the light water reactor fuel cycle,
2. Describe the basic difference between light water reactor, heavy water reactor, and graphite reactor fuel cycles, and
3. Identify the fuel cycle facilities which are most likely to require physical protection.

Summary:

The basic features of the nuclear fuel cycles now in use or expected to be in use in the near future are considered. Emphasis is placed on identification of the facilities which would be the most likely targets of diversion, theft, or sabotage attempts.

MODULE 3

REACTORS

FUEL CYCLE

The production of energy from most fuel materials is a relatively straightforward process which consists of the following general steps:

1. Exploration,
2. Mining or drilling,
3. Processing,
4. Use, and
5. Waste disposal.

A means of transporting the fuel between the various steps in the process is also required.

NUCLEAR FUEL CYCLE

The use of nuclear fuels for energy production is complicated by a number of factors:

1. The very low abundance of the sole naturally occurring fissile nuclide, U^{235} , in elemental uranium,
2. The presence of very small to very large amounts of radioactivity,
3. The potential for production of fissile nuclides U^{233} and Pu^{239} from irradiation of Th^{232} and U^{238} , respectively, and
4. The potential use of all fissile materials for the production of weapons.

Each of these problems is discussed in this module.

Figure 3-1 shows the basic features of the uranium fuel cycle for the light water reactor, a system which is used extensively around the world. The solid arrows represent the cycle as it is presently employed in the United States and elsewhere. The dashed arrows show a closed fuel cycle which is already employed in some parts of the world. The closed cycle may be used more extensively in the future.

The major component operations of the closed fuel cycle include

1. Exploration and mining,
2. Milling or refining,
3. Processing or conversion,
4. Enrichment,
5. Fuel fabrication,
6. Reactor use,
7. Interim spent fuel storage,

Figure 3-1. Uranium Fuel Cycle for a Light Water Reactor

8. Spent fuel reprocessing,
9. Uranium and/or plutonium recycling, and
10. Waste disposal (high-level wastes from spent fuel as well as wastes from the other component operations).

Also included in the fuel cycle are transportation of fuel from one operation to another and physical protection of material, where appropriate.

The steps preceding reactor use are often referred to as the front end of the fuel cycle, while those that follow are designated as the back end of the fuel cycle.

Exploration and Mining

The process of exploring for uranium ore typically consists of the following sequence of steps:

1. Geological evaluation,
2. Chemical and radiological testing, and
3. Site evaluation by means of drilling.

At present, major uranium resources have been found in southern Africa, Australia, Canada, the United States, and the Union of Soviet Socialist Republics.

Uranium may be mined by open-pit (strip mining) or underground operations, depending upon the nature of the deposit. A few deposits have been found which have assays of as high as 10 percent uranium metal content. However, most deposits have assays on the order of a few tenths of 1 percent uranium.

Milling

Separation of uranium metal from ore is accomplished during the milling process by a series of primarily chemical operations. Major steps commonly include

1. Crushing and grinding of ore,
2. Leaching to place the metal ions into solution,
3. Separation of solids from the leach,
4. Ion exchange or solvent extraction to remove uranium from other metals, and
5. Production of "yellow cake" (U_3O_8).

Conversion and Enrichment

Natural uranium is composed of two isotopes: fissile U^{235} (0.711 percent) and nonfissile U^{238} (99.3 percent). Since the design of light water reactors requires uranium with a higher U^{235} content, it is necessary to separate the two uranium isotopes. These isotopes cannot be separated by chemical methods. In general, physical processes are used to perform this isotopic separation. The first step in the conversion process involves the production of high-purity uranium hexafluoride (UF_6) from yellow cake. At a temperature of about 100° C, uranium hexafluoride becomes a gas. In this state, the fractional content of U^{235} can be enhanced through an enrichment process utilizing gaseous diffusion or gas centrifuge techniques.

A schematic of a cylindrical gaseous diffusion enrichment stage is shown in Figure 3-2. When the uranium hexafluoride gas in this system is forced against a porous barrier, the lighter component formed from the U^{235} molecules passes through the barrier more readily than do the heavier molecules formed from U^{238} . Since the kinetic theory of gases indicates that all molecules will have equal average kinetic energy, the lighter U^{235} molecules will exhibit the greater velocity and have a larger barrier penetration probability.

By cascading individual stages, as shown in Figure 3-3, the overall process of isotope separation can be greatly enhanced. The resulting product is uranium

Figure 3-2. Gaseous Diffusion Stage

enriched to about 2 to 4 percent U^{235} , which can be used as fuel in light water reactors. The residual or depleted stream typically contains 0.3 to 0.35 percent U^{235} .

The gas centrifuge process is based on the same physical principle used for the gaseous diffusion technique. The advanced technology represented by the gas centrifuge process has been developed to provide the increased capacity needed for present and near-future enrichment requirements. The use of the gas centrifuge process will also reduce energy requirements for the enrichment step of the fuel cycle.

Figure 3-3. Gaseous Diffusion Process

Fabrication

Fabrication, the next step in the fuel cycle, converts low-enriched uranium into a form which is suitable for reactor use. Typical steps in the fabrication process include

1. Conversion of low-enriched UF_6 to uranium dioxide (UO_2),
2. Formation of the UO_2 into fuel pellets,
3. Placement of the pellets into zirconium-clad tubes in order to form fuel pins, and
4. Assembly of the fuel pins into fuel bundles (or fuel assemblies).

Once the enriched uranium has been assembled into fuel bundles, it is ready for use in the reactor.

Reactor Use

After the enriched uranium fuel bundles are loaded into the reactor, the fission process is initiated and the production of thermal energy begins. As fission progresses, the system loses its ability to sustain the fission rate due to depletion of fissile U^{235} and the build-up of fission products which act as "poisons." Although the depletion effect is partially offset by production ("breeding") of fissile plutonium from U^{238} , the reactor eventually loses its ability to sustain the fission chain reaction.

At present, standard procedure at a light water reactor is to replace one-fourth to one-third of the fuel assemblies on an approximately annual basis. Careful fuel management can maximize energy extraction from each fuel batch during the 3 to 4 years it remains in the reactor core.

Interim Spent Fuel Storage

Spent fuel assemblies are very highly radioactive when discharged from the reactor. Interim storage in an on-site water basin allows both the radiation and heat production levels to decrease through the natural radioactive decay process. After a reasonable amount of storage time has been expended, the spent fuel assemblies may be transported to a reprocessing facility. If the spent fuel is not to undergo reprocessing, it can be stored indefinitely at the on-site facility or at a designated off-site facility.

Reprocessing

It is possible to reprocess spent fuel in order to extract residual uranium and the bred plutonium for further use in the fuel cycle. The fission-product and actinide wastes produced are handled in the waste disposal step. The basic steps in the reprocessing operation include

1. Temporary storage,
2. Mechanical disassembly of fuel assemblies,
3. Dissolution,
4. Separation of uranium and plutonium from wastes, and
5. Separation of uranium from plutonium.

Because of the large amounts of radioactive material present during reprocessing, as well as during waste disposal, very stringent environmental controls are required.

Recycling

The residual uranium and the plutonium extracted from the spent fuel by the reprocessing operation may be reintroduced into the fuel cycle. Use of these recycled materials can reduce uranium resource requirements by up to 25 percent. The residual uranium is returned to the fuel cycle for reenrichment. The plutonium is returned to the fabrication operation where it is mixed with depleted uranium to produce a mixed oxide with a fissile content roughly comparable to that of low-enriched uranium.

Waste Disposal

All steps in the fuel cycle (including the waste disposal step itself) produce radioactive waste. Prior to reactor use, the wastes are "low-level." Reactor use and reprocessing produce "high-level" wastes.

Disposal of wastes from reprocessed fuel, in general, consists of the following steps:

1. Storage of waste as a liquid for approximately 5 years,
2. Solidification and storage of waste on-site for an additional period of 5 years, and
3. Transference to a repository for final disposal.

Final disposal is likely to occur in a stable geologic formation, a seabed, or an extraterrestrial destination.

Transportation

The fundamental principles for transportation of nuclear materials are concerned with prevention of the following hazards:

1. Release of dangerous chemical or radioactive materials into the environment,
2. Accidental nuclear chain reaction (criticality) outside the reactor environment,
3. Damage to components (economic- and safety-related), and
4. Theft of valuable and potentially dangerous materials.

Based on the nature of these risks, specially designed containers are used at each step of the fuel cycle. Examples of these containers include

1. "Chemical" containers for the preenrichment steps where no criticality problems exist,
2. "Chemical"/"criticality" containers for enriched, unirradiated materials, and
3. Large, shielded shipping casks for irradiated fuels and high-level wastes.

PHYSICAL PROTECTION OF MATERIAL

Materials in the nuclear fuel cycle may require protection due to the radiation hazard they pose and/or their potential for use in nuclear explosives. These concerns and their application to reactors are considered elsewhere in this workshop.

The requirements for physical protection of the fuel cycle depend largely on the characteristics of the group perceived to be the antagonist. The aims of a subnational, or terrorist, group which would be of major concern are

1. Sabotage and dispersal of radioactive materials, and
2. Theft of highly-enriched uranium (greater than 20 percent U^{235}) or separated plutonium for use in weapons.

OTHER FUEL CYCLES

Reactor design concepts other than that of the light water reactor require fuel cycles which have many similarities to the uranium fuel cycle. The greatest differences occur when thorium is introduced as the source for production of fissile U^{233} , as shown in Figure 3-4.

Figure 3-4. General Fuel Cycle

Figure 3-4 shows a composite fuel cycle which can be applied to nearly any reactor concept. For example, when applied to the pressurized heavy-water reactor, the fuel cycle is characterized by the following elements:

1. Natural uranium fuel,
2. No UF_6 processing or enrichment,
3. Long-term interim storage of spent fuel assemblies, and
4. Future options for recycling plutonium only.

When applied to the high-temperature, gas-cooled reactor, the fuel cycle is characterized by

1. 93 percent enriched uranium fuel,
2. Thorium mining, milling, and fabrication, and
3. U^{235} and U^{233} recycling.

A fuel cycle for advanced concepts applicable to the light water reactor or the systems just described may employ various combinations of uranium and thorium fuels in a single reactor or in interaction among different reactor types. The latter are known as "symbiotic" or "crossed-progeny" fuel cycles.

MODULE 3

VISUALS

SESSION 3.1

NOTES

GENERAL FUEL UTILIZATION

- EXPLORATION
- MINING/DRILLING
- PROCESSING
- USE
- WASTE DISPOSAL

NUCLEAR FUEL COMPLICATIONS

- U^{235}
 - ONLY NATURALLY-OCCURRING FISSILE NUCLIDE
 - LOW ABUNDANCE
- RADIOACTIVITY
- CONVERSION
 - $U^{238} \rightarrow Pu^{239}$
 - $Th^{232} \rightarrow U^{233}$
- WEAPON POTENTIAL

VISUALS

NOTES

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

3.0 REACTORS

Session Title: 3.2 Nuclear Materials

Date: Thursday, 2 November

Presented By: R. Knief, Univ. of New Mexico and
Sandia Laboratories
Consultant

Time: 1330 to 1430

Session Objectives:

After the session, the participants will be able to

1. Describe the radioactive decay processes and the nuclear reactions which are important to reactor operation,
2. Explain the difference between fissile, fissionable, and fertile materials,
3. Explain the concepts of neutron multiplication, criticality, and reactivity, and
4. Describe the power behavior of a reactor which is associated with reactivity changes.

Summary:

The basic nature of the reactor fuel materials in their relationship to other materials in a chain-reacting system is considered. Emphasis is placed on providing an understanding of reactor behavior under normal operating conditions and accident or sabotage conditions.

NUCLEAR MATERIALS

STRUCTURE OF MATTER REVIEW

The basic building block of all matter is the atom, which consists of a massive nucleus surrounded by orbiting electrons. The nucleus is made up of protons and neutrons. Table 3-I shows the relationship between the atom and its component parts in terms of arbitrary mass, m , and electron charge, q .

TABLE 3-I
The Atom and Its Component Parts

	<u>Mass</u>	<u>Charge</u>
Electron	0.00055 m	$-q$
Proton	m	$+q$
Neutron	m	0
Nucleus	$\sim Am$	$+Zq$
Atom	$\sim Am$	0

The atomic number, Z , is the number of charges of each type in a neutral atom, i.e., the number of electrons or the number of protons. The atomic mass number, A , is the total number of particles in the nucleus.

Each identifiable nuclear species, or nuclide, can be characterized in terms of its atomic number and its atomic mass number. Since the atomic number is the same as the number of orbital electrons, it uniquely identifies the chemical species, or element. The shorthand notations which follow have each been used for nuclide identification:

where X is the chemical element symbol and Z and A have the values defined earlier. Atoms of a single element which differ from each other only by the number of nuclear particles are called isotopes of that element.

Although the mass of an atom is approximately the mass of the particles from which it is formed, there is a small difference which is extremely important. The atom is actually slightly less massive than the sum of its constituents. The difference in mass is equivalent to the amount of energy needed to bind the parts of the atom together. This "binding" energy is calculated according to the well-known formula

$$E = mc^2$$

where E = energy, m = mass, and c = the speed of light. The difference in mass caused by the binding energy of the atom forms the basis for radioactive decay and nuclear reactions.

RADIOACTIVE DECAY

When, for any reason, a nucleus has excess energy, it may undergo a spontaneous disintegration process known as radioactive decay. Naturally occurring nuclides decay according to one of the following three processes:

1. Alpha-particle emission (${}_2^4\alpha = {}_2^4\text{He}$ = helium nucleus),
2. Beta-particle emission (${}_{-1}^0\beta = {}_{-1}^0\text{e}$ = electron), or
3. Gamma-radiation emission (${}_0^0\gamma$ = high-energy, electromagnetic radiation).

All radioactive decay conforms to the laws of conservation of total energy (the sum of kinetic energy and rest mass energy), charge, atomic mass number, and linear and angular momentum.

It is not possible to determine when a specific nuclide will experience radioactive decay. However, for a statistically large sample, the probability that decay of the nuclides will occur can be assigned a value. The half-life of a given nuclide is defined as the average time required for one-half of a large radioactive sample to experience radioactive decay. Half-life and activity (the number of decays per unit time) are useful concepts in describing the behavior of a particular nuclide population. Activity is often measured in curies (Ci), where

$$1 \text{ curie} = 3.7 \times 10^{10} \frac{\text{decays}}{\text{second}}$$

or in the more recently established unit, the becquerel (Bq), where

$$1 \text{ becquerel} = 1 \frac{\text{decay}}{\text{second}}$$

NUCLEAR REACTIONS

Many of the radionuclides, or radioactive nuclides, which are important in reactor systems are produced when nuclear particles and nuclei interact with each other. Such reactions obey the same conservation laws stated for radioactive decay. A common shorthand notation for such reactions is

$$X(x,y)Y$$

for target X , projectile x , product nucleus Y , and product particle(s) y . In many cases, the assignment of symbols is somewhat arbitrary.

When the target and projectile come together, they are thought to form a compound nucleus which only exists for a very short time before splitting into a product nucleus and product particle(s). In nuclear reactor systems, one dominant

reaction takes the form of a neutron projectile interacting with a U^{235} target to produce one of the following outcomes:

1. A charged particle,
2. Gamma rays,
3. A neutron (generally not the initial neutron),
4. Multiple neutrons, or
5. Fission.

This reaction and the five outcomes possible are represented by the diagram in Figure 3-5. The gamma rays and neutrons may constitute a radiation hazard. The fission process is the basic method of energy production in nuclear reactors. The charged particle and gamma reactions are also of importance in that they lead to the loss of neutrons which might otherwise have produced fission.

Figure 3-5. U^{235} /Neutron Reaction Outcomes

Other reactions of interest are those which produce neutrons. Two specific examples of such reactions are

1. Beryllium-alpha particle reactions

(In this reaction, the α -particle is usually produced by radioactive decay of a heavy radionuclide.)

2. Photodisintegration of U^{236}

NUCLEAR FISSION

Almost any nuclide is fissionable if a projectile with sufficient energy is provided. However, nuclides of heavy ($Z \geq 90$) elements undergo neutron fission most readily and provide optimum net energy production. These nuclides may be placed into one of three categories:

1. Fissile--Fission is produced by the mere presence of an extra neutron. (Included in this category are U^{233} , U^{235} , Pu^{239} , and Pu^{241} ; of these only U^{235} occurs in nature.)
2. Fissionable--Fission is produced by neutrons. (This category includes fissile nuclides plus those nuclides that fission only when bombarded by neutrons of high energy; the latter category includes Th^{232} , U^{238} , and Pu^{240} .)
3. Fertile--Fissile materials are produced from the nuclides following neutron irradiation. (This category includes all of the nuclides categorized above as fissionable only if bombarded with high-energy neutrons.)

The fertile nuclides convert, or breed, new fissile material. For example, U^{238} may capture a neutron and ultimately produce Pu^{239} . This process is illustrated in Figure 3-6. Conceptually, U^{233} is produced from Th^{232} in a similar manner. Conversion of Pu^{240} is based on a simple neutron capture which produces fissile Pu^{241} .

Figure 3-6. U^{238} to Pu^{239} Chain

The most important results of the fission process, shown in Figure 3-7, are the production of

1. Heat energy,
2. Neutrons and gamma radiation, and
3. Fission fragment nuclides.

Each of these results has an important impact on the design and operation of nuclear reactor systems.

Each fission produces an energy of about 200 MeV. (This energy production is nearly eight orders of magnitude greater than the 2 to 3 eV produced in a standard chemical combustion reaction.) The very large energy production per unit mass allows nuclear fission systems to be extremely compact.

Figure 3-7. Uranium Fission and Beta Decay Chains

Neutron production is the basis for achieving a self-sustaining chain reaction which can produce energy at the uniform rate required for the generation of electricity. Proper balancing of net neutron production facilitates startup, at-power, and shutdown operations.

Gamma radiation produced at the time of fission is a potentially serious hazard. However, this hazard is eliminated as soon as the system is shut down.

The presence of fission-fragment nuclides is another major drawback to the nuclear fission process. The fragments undergo beta decay in chains of up to six nuclides, as shown in Figure 3-7. Thus, they constitute long-term sources of both radiation and heat. The radiation levels require remote handling for all operations in the back end of the fuel cycle. If cooling is not provided, the decay heat source may be sufficient to cause melting of irradiated fuel.

The neutron population produced by fission leads to other effects which are not specifically attributable to the fission process. Neutron capture in nonfuel materials may produce immediate gamma radiation as well as radioactive products. Nonfission capture in fuel materials leads to the formation of transuranic* nuclides, many of which are alpha-active with long half-lives. These latter products are a major constituent of high-level, fuel cycle waste.

*Atomic number greater than uranium.

FISSION CHAIN REACTION

The fission process is initiated by a neutron and terminates by producing neutrons. In a reactor,* the general aspects of the neutron population will be described by a neutron balance equation as follows:

$$\left\{ \begin{array}{l} \text{rate of increase} \\ \text{in the number} \\ \text{of neutrons} \end{array} \right\} = \left\{ \begin{array}{l} \text{rate of} \\ \text{production} \\ \text{of neutrons} \end{array} \right\} - \left\{ \begin{array}{l} \text{rate of} \\ \text{absorption} \\ \text{of neutrons} \end{array} \right\} - \left\{ \begin{array}{l} \text{rate of} \\ \text{leakage} \\ \text{of neutrons} \end{array} \right\}$$
$$\{ \text{accumulation} \} = \{ \text{production} \} - \{ \text{absorption} \} - \{ \text{leakage} \}$$

This equation implies only that neutrons are conserved, i.e., neither created nor destroyed.

A convenient parameter which can be used to describe the balance in a system is the multiplication factor, k , which is defined as

$$k = \frac{\text{production}}{\text{absorption} + \text{leakage}}$$

When k is unity, production and losses are exactly balanced to produce a critical system, i.e., one which remains at a steady neutron level. The three states of criticality can be represented by

- $k > 1$ supercritical (exponentially increasing neutron level)
- $k = 1$ critical
- $k < 1$ subcritical (exponentially decreasing neutron level or shutdown)

Another measure of criticality is reactivity ρ , which is defined by

$$\rho = \frac{k - 1}{k}$$

Since $k = 1$ represents the condition of a critical reactor, reactivity is a measure of "excess multiplication." In terms of ρ , the three states of criticality are given by

- $\rho > 0$ supercritical
- $\rho = 0$ critical
- $\rho < 0$ subcritical

REACTOR CONTROL

Prompt neutrons emitted at the time of fission exist in a reactor system for a period of from 10^{-7} to 10^{-4} second (depending on design specifics) before they cause another fission or are lost. If this sort of time scale were dominant in fission reactions, external control of a supercritical system would be impossible.

Not all neutrons, however, appear at the time of fission. A small fraction of the total neutron population is produced when certain fission fragments undergo

*The term reactor is used here to signify any collection of materials in which fission can occur.

initial beta decay. These neutrons appear in the system on the same time scale as the decay processes (which have half-lives in the 0.1- to 55-second range) rather than at the time of fission.

As long as the reactivity changes which occur during reactor operation are small in comparison to the delayed neutron fraction (about 0.65 percent for U^{235} , 0.21 percent for Pu^{239}), the time scale for system changes can be kept relatively long. Such a system may be readily controlled by human operators and various electromechanical systems.

If reactivity is large enough for the system to be categorized as prompt critical, i.e., having a large enough multiplication that just the prompt neutrons are sufficient for criticality, the characteristic time scale becomes very short, as noted previously. Operation in this time regime would lead to very rapid power escalation, which could, in turn, produce core disruption and perhaps even meltdown.

A major goal of reactor system design and operation is to preclude the occurrence of an inadvertent meltdown, which would release substantial quantities of radioactive material into the environment. The goal of physical protection is aimed at assuring that a meltdown is not initiated by a malicious act.

STRUCTURE OF MATTER

● ATOM

NUCLEUS

PROTONS

NEUTRONS

● ELECTRONS

	<u>MASS</u>	<u>CHARGE</u>
ELECTRON	0.00055 m	-q
PROTON	m	+q
NEUTRON	~m	0
NUCLEUS	~Am	+Zq
ATOM	~Am	0

$Z \Rightarrow$ ATOMIC NUMBER = $\#p = \#e$

$A \Rightarrow$ ATOMIC MASS NUMBER = $\#p + \#n$

NUCLIDES

● NUCLEAR SPECIES

$Z \rightarrow$ CHEMICAL ELEMENT

$A \rightarrow$ NUCLEAR IDENTIFICATION

● SHORTHAND NOTATION

$$\begin{array}{c} A \\ \text{OR} \\ {}_Z^AX \end{array} \left\{ \begin{array}{l} X - \text{CHEMICAL ELEMENT} \\ Z - \text{ATOMIC NUMBER} \\ A - \text{ATOMIC MASS NUMBER} \end{array} \right.$$

● ISOTOPES

GIVEN X AND Z, DIFFERENT A

● URANIUM ISOTOPES

● HYDROGEN ISOTOPES

NUCLEAR MASSES

- MASS (ATOM) < MASS (Σ CONSTITUENTS)

- BINDING ENERGY

$$\bullet E = mc^2 \quad \left\{ \begin{array}{l} E \Rightarrow \text{ENERGY} \\ m \Rightarrow \text{MASS} \\ c \Rightarrow \text{SPEED OF LIGHT} \end{array} \right.$$

- [RADIOACTIVE DECAY
NUCLEAR REACTIONS]

RADIOACTIVE DECAY

- EXCESS ENERGY

- NATURAL PROCESSES

- CONSERVATION LAWS

- CHARGE

- ATOMIC MASS NUMBER

- LINEAR/ANGULAR MOMENTUM

- TOTAL ENERGY (KINETIC ENERGY + MASS)

VISUALS

NOTES

"LARGE" SAMPLE

- PROBABILITY
- HALF-LIFE → TIME FOR ONE-HALF OF SAMPLE TO DECAY
- ACTIVITY → DECAYS PER UNIT TIME
 - 1 CURIE (Ci) = $3.7 \times 10^{10} \frac{\text{DECAY}}{\text{SEC}}$
 - 1 BECQUEREL (Bq) = $1 \frac{\text{DECAY}}{\text{SEC}}$

NUCLEAR REACTIONS

- COMPOUND NUCLEUS

NEUTRON REACTIONS

RADIATION
FISSION
NEUTRON LOSS

OTHER REACTIONS

● NEUTRON PRODUCTION

NUCLEAR FISSION

● FISSION → FISSION BY PRESENCE OF NEUTRON

● FISSIONABLE → FISSION BY FISSION NEUTRON

+

FISSION BY HIGH ENERGY NEUTRONS

● FERTILE → FISSION PRODUCED AFTER NEUTRON IRRADIATION

● CONVERSION BREEDING

VISUALS

NOTES

FISSION RESULTS

- HEAT ENERGY

200 MeV (2-3 eV FOR COMBUSTION!)

- NEUTRONS/GAMMAS

SHIELDING REQUIRED

CHAIN REACTION

- FISSION FRAGMENTS

LONG-TERM RADIATION/HEAT

OTHER EFFECTS

- NEUTRON CAPTURE

GAMMA RADIATION (n, γ)

RADIOACTIVE PRODUCTS

- NONFISSION CAPTURE IN FUEL

TRANSURANICS ($Z > 92$)

WASTE CONSTITUENTS

VISUALS

NOTES

FISSION CHAIN REACTION

● NEUTRON BALANCE

$$\left[\begin{array}{c} \text{RATE OF} \\ \text{INCREASE} \end{array} \right] = \left[\begin{array}{c} \text{RATE OF} \\ \text{PRODUCTION} \end{array} \right] - \left[\begin{array}{c} \text{RATE OF} \\ \text{ABSORPTION} \end{array} \right] - \left[\begin{array}{c} \text{RATE OF} \\ \text{LEAKAGE} \end{array} \right]$$
$$[\text{ACCUMULATION}] = [\text{PRODUCTION}] - [\text{ABSORPTION}] - [\text{LEAKAGE}]$$

MULTIPLICATION FACTOR

$$k = \frac{\text{PRODUCTION}}{\text{ABSORPTION} + \text{LEAKAGE}}$$

CRITICALITY

$$k > 1 \quad \text{SUPERCRITICAL}$$

$$k = 1 \quad \text{CRITICAL}$$

$$k < 1 \quad \text{SUBCRITICAL}$$

REACTIVITY

$$\rho = \frac{k - 1}{k}$$

"EXCESS MULTIPLICATION"

$$\rho > 0 \quad \text{SUPERCRITICAL}$$

$$\rho = 0 \quad \text{CRITICAL}$$

$$\rho < 0 \quad \text{SUBCRITICAL}$$

REACTOR CONTROL

- PROMPT NEUTRONS
 - $10^{-7} - 10^{-4}$ SECOND CONTROL
- DELAYED NEUTRONS
 - SMALL FRACTION AFTER ONE BETA DECAY
HALF-LIVES 0.1-55 SECONDS
- SMALL REACTIVITY CHANGES
 - COMPARED TO DELAYED NEUTRON FRACTION
 - U²³⁵ 0.65%
 - Pu²³⁹ 0.21%
 - " LONG " TIME SCALE
- LARGE REACTIVITY CHANGES
 - PROMPT CRITICAL
 - SHORT TIME SCALE
 - ↓
 - POWER ESCALATION
 - ↓
 - MELTDOWN
- { DESIGN GOAL } → { PRECLUDE
MELTDOWN }
- { PHYSICAL
PROTECTION
GOAL } → { PRECLUDE
MELTDOWN BY
MALICIOUS ACT }

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

3.0 REACTORS

Session Title: 3.3 Radiation Hazards

Date: Thursday, 2 November

Presented By: R. Knief, Univ. of New Mexico and
Sandia Laboratories
Consultant

Time: 1500 to 1600

Session Objectives:

After the session, the participants will be able to

1. Distinguish among alpha, beta, and gamma radiations in terms of their identities and relative ranges,
2. Identify the levels of various radiations which would be expected to be lethal, and
3. Describe the bases for requiring shielded and glovebox operations.

Summary:

The basic nature of nuclear radiation and radioactivity is considered in the context of the design and operation of nuclear fuel cycle systems.

RADIATION HAZARDS

The radiation produced by atomic and nuclear phenomena is potentially harmful to humans. Radiation hazards, however, are not significantly different from those associated with chemical, physical, or biological agents.

Public attitude toward radiation hazards has been influenced by the following considerations:

1. The discovery of radioactivity is relatively recent dating back to only about 1900,
2. The detonation of two nuclear weapons in Japan in 1945 provided the world with a dramatic and terrifying introduction to nuclear energy and radiation effects, and
3. Nuclear radiation is not directly detectable by the human senses except at levels well above lethality.

Thus, radiation is viewed by the uninformed as a new, deadly, and silent hazard. In reality, the effects of radiation on the environment are understood substantially better than are the effects produced by other methods of energy production which may have more severe consequences.

RADIATION

Radiation from the fission process presents potential hazards in the form of

1. Prompt-neutron and gamma radiation emitted at the time of fission,
2. Activation-gamma radiation emitted as a result of (n, γ)-reactions, and
3. Delayed alpha, beta, and gamma radiation, with half-lives from fractions of a second to millions of years, emitted by fission fragments and by activation and transmutation products.

These potential sources of health hazards merit serious consideration from the standpoint of the safety of both operating personnel and the general public.

All radiation is energetic and has the potential to cause damage to biological tissue or to other materials. Since nuclear radiation is especially energetic, its effects may be quite harmful. Prompt neutrons carry 3 to 4 percent of the energy released in fission. Prompt-gamma radiation from the fission process and activation-gamma radiation account for another 12 percent of the energy associated with fission. The presence of these radiation sources requires that the reactor core be well-shielded from personnel and sensitive equipment.

Up to about 7 percent of equilibrium reactor power is due to delayed radiation. After shutdown, the radiation activity decreases roughly as the 1/5th power of time, e.g., 1 percent of reactor power 1 day after shutdown, 0.1 percent 2 months

later. Long-lived radiation activity may require remote operation and/or virtually constant shielding for reactor, spent-fuel, reprocessing, and waste-management facilities.

Charged Particle Interactions

Alpha particles (He^{++}), beta particles (e^-), and fission-fragment ions experience electrostatic (Coulomb) interaction between their charges and the atomic electrons in the material medium of travel. Because the Coulomb forces extend for large distances, each particle will interact with a very large number of atoms. A combination of ionization and electron-state excitation results in an energy loss of about 35 eV per collision.

For a given energy and material medium, a charged particle can be described by the following two characteristics:

1. Range--The average distance of travel with a fairly well-defined "minimum-to-maximum spread" of possible values, and
2. Linear energy transfer (LET) function--The energy disposition per unit path length, $\frac{dE}{dX}$.

Range and linear energy transfer functions are essentially inverse concepts, each of which makes a separate contribution to radiation-damage magnitude.

Electromagnetic Radiation Interactions

X-ray and gamma-ray photons interact with matter in one of three ways:

1. Photoelectric effect--Photon energy is completely converted to the kinetic energy of an orbital electron,
2. Compton scattering--A portion of the photon energy is transferred to the kinetic energy of an orbital electron as a result of a scattering interaction; the scattered photon has a correspondingly lower energy, and
3. Pair production--Photon energy is converted into the mass and kinetic energy of an electron-positron pair (in the electric field of a nucleus); the positron (a positively charged electron) will later be annihilated with another electron, giving off two 0.511-MeV photons.

Individual photons do not have a specified range or linear energy transfer function because interaction occurs on a "one-shot" basis when a photon chances to "hit," i.e., approach very closely to, an electron. Instead, the range and linear energy transfer function must be quantified in terms of a model based on interaction probabilities for a statistically large sample.

As a "rule of thumb," alpha, beta, and gamma radiation which have comparable energy levels may be considered to have the relative range and linear energy transfer function values given in Table 3-II.

TABLE 3-II

Radiation Range and Linear Energy
Transfer Function Values

<u>Radiation</u>	<u>Relative Range</u>	<u>Relative Linear Energy Transfer</u>
Alpha	1	10,000
Beta	100	100
Gamma	10,000	1

Neutron Interactions

Neutrons interact with materials through absorption and scattering reactions. The absorption process is followed by emission of a charged particle or photon and often by delayed radiation. In the scattering reaction, a neutron transfers some of its energy to a nucleus; the latter then interacts in the system as a charged particle. As is the case for electromagnetic radiation, neutron interactions occur on a "one shot" basis. Thus, neutrons do not have a well-defined range and linear energy transfer function.

RADIATION DOSE

A useful unit for measuring radiation effects is radiation absorbed dose (rad), defined by

$$1 \text{ rad} = \frac{100 \text{ ergs}}{1 \text{ g of material}}$$

It is applicable to any radiation and any material but is used mostly in reference to biological systems.

The effect of radiation on a system will depend on the absorbed dose and on the linear energy transfer function of the radiation. For biological systems, it is convenient to define a relative biological effectiveness (RBE) for the various types of radiation as

$$\text{RBE} = \frac{\text{dose of 250 keV X-rays producing a given effect}}{\text{dose of reference radiation for the same effect}}$$

Relative biological effectiveness depends on the effect studied, the dose, the dose rate, the physiological condition of the subject, and other factors.

The upper limit of relative biological effectiveness for a specific type of radiation is called the quality factor (QF). Factors for the radiation sources of greatest interest are shown in Table 3-III.

TABLE 3-III
Radiation Quality Factors

<u>Radiation</u>	<u>Quality Factor</u>
X-ray, γ-ray	1
Beta	1 to 1.7
Neutrons (thermal)	3
Neutrons (fast)	10
Alpha, proton	10
Fission fragments	20

The most useful unit of radiation dose is the rem (Roentgen equivalent man) which is defined by

$$\text{Dose (rem)} = \text{QF} \times \text{Dose (rad)}$$

By using this unit, the potential effects (since the quality factor is an upper limit) of all types of radiation can be considered from a common reference. Doses given in rem are additive, independent of the specific radiation types involved.

A radiation dose accumulated over a very short period of time is designated as acute, while a dose accumulated over an extended period is designated as chronic. For a given total dose, an acute dose is considered the more harmful of the two because natural repair mechanisms in the human body can operate during the acquisition of a chronic dose.

Human Response to Radiation Dose

Very large acute doses of radiation have readily identifiable effects on the human body. Although individual differences occur, these effects can be grouped according to general trends, as shown in Table 3-IV. It should be noted that even doses of 1000 rem or more cannot be detected by the human senses until the medical effects appear.

Lethal dose estimates for a given radiation are often expressed in the short-hand form, LD 50/30, which means "Lethal Dose for 50 percent of the population within 30 days." A whole body dose of about 500 rem is considered to be LD 50/30 for a human population.

The delayed effects of large acute doses and of comparable chronic doses include

1. Leukemia and cancers,
2. Cataracts,
3. Genetic damage,
4. Blood disorders, and
5. Shortened lifespan.

TABLE 3-IV
Effects of Acute Whole-Body Radiation Doses

Acute Dose (rem)	Probable Clinical Effect
0-75	No effects are apparent. Chromosome aberrations and temporary depression in white blood cell levels have been found in some individuals.
75-200	Vomiting occurs in 5 to 50 percent of the exposed individuals within a few hours, accompanied by fatigue, loss of appetite, and moderate blood changes. Recovery occurs within a few weeks for most symptoms.
200-600	For doses of 300 rem or more, all exposed individuals will exhibit vomiting within 2 hours or less. Severe blood changes, accompanied by hemorrhaging and an increased susceptibility to infection, particularly at higher doses, occur. Loss of hair occurs after 2 weeks for doses over 300 rem. Recovery occurs within 1 month to 1 year for most individuals exposed to a rem dose having a value at the lower end of the range; only 20 percent survive a dose value at the upper end of the range.
600-1000	Vomiting occurs within 1 hour, accompanied by severe blood changes, hemorrhaging, infection, and loss of hair. From 80 to 100 percent of the exposed individuals will succumb within 2 months; those who survive will be convalescent over a long period of time.

Although considerable controversy exists over the magnitude of delayed effects, especially for low-dose-rate chronic exposure, the effects of radiation are substantially better known than comparable environmental hazards of other origin.

Radiation Dose Standards

Ideal standards, or limits, for radiation exposure are those which assure that the health of operations personnel and the public will be protected, while allowing for reasonable efficiency in operations involving radioactive materials. To determine appropriate standards, two types of exposure must be considered: (1) external radiation, and (2) internal radiation. The practical basis for setting standards considers natural background radiation levels and experimental data on dose-effect relationships.

Natural background radiation varies throughout the world but, in general, its major constituents are

1. Cosmic radiation--40 to 130 mrem/year,
2. Terrestrial radiation (U, Th, K^{40})--30 to 115 mrem/year (as high as 800 mrem/year in India's thorium fields), and
3. Internal radiation (Rn^{220} , Rn^{222} , K^{40})--15 mrem/year.

The average range of natural background radiation is 100 to 250 mrem/year with an average of about 130 mrem/year.

Experimental dose-effect data on human subjects have been limited mainly to post-exposure studies of groups of individuals who have received very large acute or chronic radiation exposure caused by nuclear devices, accidents, or other inadvertent means. Detailed, controlled experiments have been performed only with animal populations; however, these have provided valuable information.

In the case of occupational exposure where dose monitoring is required, specific standards are set for individuals on the basis of age, exposure history, type of radiation and energy absorbed, and organ or tissue exposed. Standards for the general public must encompass all possibilities and are, therefore, set at a low level. Current regulations call for exposures to be "as low as practicable" or "as low as reasonably achievable" with the standards serving as upper bounds.

Exposure standards on external radiation prepared by the National Council on Radiation Protection are provided in Table 3-V.

TABLE 3-V
Dose-Limiting Recommendations Proposed by the
National Council on Radiation Protection*

Type of Exposure	Dose
Combined Whole-Body Occupational Exposure	
Prospective annual limit	5 rem in any 1 year
Retrospective annual limit	10 to 15 rem in any 1 year
Long-term accumulation to age N years	(N-18) x 5 rem
Skin	15 rem in any 1 year
Hands	75 rem in any 1 year (25 per quarter year)
Forearms	30 rem in any 1 year (10 per quarter year)
Other organs, tissues, and organ systems	15 rem in any 1 year (5 per quarter year)
Fertile women (with respect to fetus)	0.5 rem in gestation period
Dose limits for the public or occasionally exposed individuals	0.5 rem in any 1 year
Population Dose Limits	
Genetic	0.17 rem average per year
Somatic	0.17 rem average per year
Emergency Dose Limits--Life-Saving	
Individual (older than 45 years if possible)	100 rem
Hands and forearms	200 rem, additional (300 rem, total)
Emergency Dose Limits--Less Urgent	
Individual	25 rem
Hands and forearms	100 rem, total

*Adopted from National Council on Radiation Protection and Measurements (1971).

Dose Reduction

Since radiation levels from nuclear power facilities could exceed the exposure standards by a substantial amount, it is very important to implement dose reduction procedures. The three basic principles for reducing accumulated radiation dose are

1. To restrict the time of proximity,
2. To increase the distance from the source, and
3. To use shielding material to attenuate the radiation.

Time restriction is valid only in situations where distance and shielding cannot be used and where the necessary task can be performed within the set short-term exposure period. In high-radiation environments, workers may accumulate maximum weekly or quarterly doses very quickly, i.e., be "burned-out," and then must be excluded from further exposure for a specified period of time.

The decrease of dose rate with distance can be most readily illustrated by reference to a point radiation source. Since the photons or particles from the source S_0 "spread out" to progressively larger $4\pi r^2$ spherical areas, the flux becomes

$$\psi(r) = \frac{S_0}{4\pi r^2}$$

or a familiar "one-over-r-squared" attenuation. The use of this geometrical attenuation is of value mainly in situations where radiation levels are reasonably low and where substantial amounts of unused space are available.

For the very high radiation levels associated with an operating power reactor, shielding becomes the only viable option. Charged particles have definite, relatively short ranges and are easily shielded. Shielding of photons and neutrons, however, presents a very complex problem.

Composite Reactor Shields

To equip a reactor with shields that are effective against both gamma and neutron radiation requires considerable design analysis since all primary and secondary radiation must be considered. Figure 3-8 shows the processes and types of radiation that are involved in such a design.

An example of a composite reactor shield is shown in Figure 3-9. The design includes

1. A steel "thermal shield" (to remove heat energy from the neutrons and gammas) surrounded by adjacent cooling water,
2. Steel and lead for gamma attenuation,
3. Water to thermalize fast neutrons so that they can be absorbed by the water, steel, or lead, and a
4. Slab arrangement to handle secondary radiation.

Figure 3-8. Radiation from a Nuclear Reactor*

Another common shield material is concrete. Because of its relatively low cost, massive amounts can be used to attenuate gamma radiation. At the same time, its low density works well to slow down neutrons. In addition, many concrete constituents function as good radiation absorbers.

Internal Dose Reduction

Radiation exposure due to sources internal to the human body may be reduced only if the material can be extracted by some means. Since this may be a difficult process, great care is taken to limit the amounts of radionuclides which are available for intake into the body.

Guidelines for limiting internal dose are in the form of maximum permissible concentrations in air and water for the various radionuclides. In practice, maximum permissible concentrations are calculated based on an evaluation of intake patterns and nuclide behavior in the human body. The maximum permissible concentration levels should correspond to those levels of radiation for which no known medical effects are expected.

*Based on figures in Reference 1.

Figure 3-9. Gamma-Ray-Dose and Neutron-Flux Distributions in a Composite Shield for a 70-MW Reactor*

For operations involving toxic materials, i.e., those having a very low maximum permissible concentration level, very strict environmental controls are necessary. Air filtration and glovebox operations are characteristic methods used for handling such materials. All fuel cycle operations involving plutonium, except handling of sealed fuel pins or samples, are conducted under tight environmental controls.

*Based on figures in Reference 1

RADIATION

- POTENTIALLY HARMFUL
- CHEMICAL/ PHYSICAL/ BIOLOGICAL HAZARD
- ATTITUDES
 - RECENT DISCOVERY
 - WEAPON DETONATION
 - NOT DETECTABLE BY SENSES
{	NEW, DEADLY,	}	↔	{	UNDERSTANDING OF	}
{	SILENT	}		{	ENVIRONMENTAL	}
{	HAZARD	}		{	EFFECTS	}

RADIATION HAZARDS

- PROMPT FISSION RADIATIONS (n and γ)
- ACTIVATION-GAMMAS
- DELAYED ALPHA, BETA, AND GAMMA
- HEALTH CONCERN
 - OPERATING PERSONNEL
 - GENERAL PUBLIC

VISUALS

NOTES

GENERAL RADIATION

- **ENERGETIC**
- **DAMAGE**
 - BIOLOGICAL TISSUE
 - MATERIALS

NUCLEAR RADIATION

- **HIGH ENERGY**
- **DAMAGE**

FISSION ENERGY

- **NEUTRONS** 3-4%
- **PROMPT/DELAYED GAMMAS** }
- **ACTIVATION GAMMAS** } 12%
- **SHIELDING**
 - PERSONNEL
 - EQUIPMENT

DELAYED RADIATION

- **7% OF EQUILIBRIUM POWER DECREASES AS $(\text{TIME})^{-1/5}$**
 - 1 DAY 1%
 - 2 MONTHS 0.1%
- **EFFECT ON OPERATIONS**
 - REMOTE HANDLING } LONG-TERM
 - SHIELDING }

CHARGED PARTICLE INTERACTIONS

● ALPHA/BETA/FISSION FRAGMENTS

CHARGED PARTICLES

COULOMB INTERACTIONS

CHARACTERISTICS

RANGE

LINEAR ENERGY TRANSFER (LET)

$$\text{LET} = \frac{dE}{dx}$$

● DAMAGE

RANGE AND LET**ELECTROMAGNETIC INTERACTIONS**

● PHOTOELECTRIC EFFECT

PHOTON CONVERTED TO ELECTRON ENERGY

● COMPTON EFFECT

PORTION OF PHOTON ENERGY TRANSFERRED TO ELECTRON

● PAIR PRODUCTION

PHOTON ENERGY CONVERTED TO MASS AND KINETIC ENERGY
OF ELECTRON-POSITRON PAIR

ANNIHILATION

E/M CHARACTERISTICS

"ONE-SHOT" INTERACTION STATISTICAL RANGE/LET

RADIATION COMPARISON

<u>RADIATION</u>	<u>RELATIVE RANGE</u>	<u>RELATIVE LET</u>
ALPHA	1	10,000
BETA	100	100
GAMMA	10,000	1

NEUTRON INTERACTIONS

- ABSORPTION

- CHARGED PARTICLE
 - GAMMA PHOTON
 - DELAYED RADIATION

- SCATTERING

- ENERGY TRANSFER TO NUCLEUS

- RANGE/LET NOT WELL DEFINED

RADIATION DOSE

RADIATION ABSORBED DOSE

$$1 \text{ rad} = \frac{100 \text{ ERGS}}{1 \text{ g OF MATERIAL}}$$

ANY MATERIAL
MOSTLY FOR BIOLOGICAL SYSTEMS

RADIATION EFFECTS

{ ABSORBED DOSE
{ LET

RELATIVE BIOLOGICAL EFFECTIVENESS

$$\text{RBE} = \frac{\text{DOSE OF 250 keV X-RAY}}{\text{DOSE OF REFERENCE RADIATION}}$$

VISUALS

NOTES

RBE DEPENDENCE

EFFECT

DOSE

PHYSIOLOGICAL CONDITION

OTHER FACTORS

QUALITY FACTOR

UPPER LIMIT ON RBE FOR GIVEN RADIATION

<u>RADIATION</u>	<u>QF</u>
X-RAY, γ -RAY	1
BETA	1-1.7
NEUTRON (THERMAL)	3
NEUTRON (FAST)	10
ALPHA, PROTON	10
FISSION FRAG.	20

ROENTGEN EQUIVALENT MAN

$\text{DOSE (rem)} = \text{QF} \times \text{DOSE (rad)}$

COMMON REFERENCE ADDITIVE

TYPES OF DOSE

ACUTE

CHRONIC

VISUALS

NOTES

HUMAN RESPONSE

LARGE ACUTE DOSES

GENERAL TRENDS

DOSE	EFFECT
0-75 rem	NO APPARENT EFFECTS
75-200 rem	ILLNESS WITH RECOVERY
200-600 rem	ILLNESS WITH LONG-TERM RECOVERY; SOME FATALITY
600-1000 rem	SEVERE ILLNESS; HIGH FATALITY

LETHALITY

LD50/30 ~ 500 rem FOR HUMANS

DELAYED EFFECTS

LEUKEMIA/CANCERS

CATARACTS

GENETIC DAMAGE

BLOOD DISORDERS

SHORTENED LIFESPAN

CONTROVERSY/ KNOWLEDGE

RADIATION DOSE STANDARDS

- IDEAL STANDARDS

{ ASSURANCE } ↔ { EFFICIENCY
{ OF HEALTH } { OF OPERATIONS }

- EXPOSURES

EXTERNAL
INTERNAL

- BASES

NATURAL BACKGROUND
EXPERIMENTAL DATA

NATURAL BACKGROUND

COSMIC	40-130 $\frac{\text{mrem}}{\text{yr}}$
TERRESTRIAL	30-115 $\frac{\text{mrem}}{\text{yr}}$
INTERNAL	25 $\frac{\text{mrem}}{\text{yr}}$
<hr/>	
AVERAGE RANGE	100-250 $\frac{\text{mrem}}{\text{yr}}$
AVERAGE	~130 $\frac{\text{mrem}}{\text{yr}}$

EXPERIMENTAL DATA

- POST-EXPOSURE STUDIES

- LABORATORY EXPERIMENTS

ANIMAL POPULATIONS ONLY
VALUABLE INFORMATION

OCCUPATIONAL EXPOSURE

- DOSE MONITORING

- STANDARDS

AGE
EXPOSURE HISTORY
RADIATION TYPE/ENERGY
ORGAN/TISSUE EXPOSED

VISUALS

NOTES

NATIONAL COUNCIL ON RADIATION PROTECTION RECOMMENDATIONS

[TABLE]

- OCCUPATIONAL

WHOLE BODY ANNUAL	5 REM
LONG-TERM ACCUMULATION	(N-18) x 5 REM

- GENERAL POPULATION

ANNUAL MAXIMUM	170 mREM
AS LOW AS REASONABLY ACHIEVABLE (ALARA)	

DOSE REDUCTION

- DOSE REDUCTION

{ RADIATION LEVELS FROM NUCLEAR POWER }	>> STANDARDS
---	--------------

- REDUCTION PRINCIPLES

TIME
DISTANCE
SHIELDING

VISUALS

NOTES

TIME

OPERATING LIMITATIONS
"BURN-OUT"

DISTANCE

POINT SOURCE

$$\phi(r) = \frac{S_0}{4\pi r^2}$$

LOW LEVELS
UNUSED SPACE

SHIELDING

ONLY VIABLE OPTION
CHARGED PARTICLES
PHOTONS AND NEUTRONS

COMPOSITE REACTOR SHIELDS

● RADIATIONS

PRIMARY
SECONDARY

● SHIELD DESIGNS

THERMAL SHIELD
GAMMA ATTENUATION
NEUTRON THERMALIZATION
SECONDARY RADIATIONS
COMPOSITE SHIELD
CONCRETE

VISUALS

NOTES

INTERNAL DOSE REDUCTION

EXTRACTION GENERALLY NOT FEASIBLE

LIMIT INTAKE

{ MAXIMUM PERMISSIBLE } ←→ MPC
CONCENTRATIONS }

BASIS

INTAKE PATTERNS
NUCLIDE BEHAVIOR
KNOWN MEDICAL THRESHOLD

TOXIC MATERIALS ←→ LOW MPC

CONTROLS

FILTRATION
GLOVEBOXES

PLUTONIUM

3.0 REACTORS

Session Title: 3.4 Reactor Systems

Date: Friday, 3 November

Presented By: R. Knief, Univ. of New Mexico and
Sandia Laboratories
Consultant

Time: 1030 to 1200

Session Objectives:

After the session, the participants will be able to

1. Explain the multiple barrier concept for nuclear reactor design,
2. Sketch the basic steam cycles and identify the working fluids for the following reactors: the boiling water reactor, the pressurized water reactor, the pressurized heavy-water reactor, and the high-temperature, gas-cooled reactor, and
3. Identify the major difference between power reactors and research reactors.

Summary:

The basic features of the present and near-future generations of nuclear power reactors are examined.

Additional Resource Materials:

Literature provided by various reactor vendors.

REACTOR SYSTEMS

Nuclear reactor designs may be classified according to one or more of the following:

1. Steam cycle,
2. Coolant,
3. Moderator (material used in some designs to reduce neutron energy and enhance reaction rates), and
4. Neutron energy.

These four design features are considered in more detail for the following types of nuclear facilities, which have been extensively implemented on a world-wide basis:

1. The boiling water reactor,
2. The pressurized water reactor,
3. The pressurized heavy-water reactor, and
4. The high-temperature, gas-cooled reactor.

STEAM CYCLES

The direct-cycle boiling water reactor boils water directly in the core fuel region in order to produce steam as illustrated in Figure 3-10.

Figure 3-10. Direct-Cycle Boiling Water Reactor

Three reactors, the pressurized water reactor, the pressurized heavy-water reactor, and the high-temperature, gas-cooled reactor, use an indirect, two-loop cycle. Core fuel heat is transferred first to a pressurized, primary fluid and then to a steam-water loop via a heat exchanger, called a steam generator. As their names imply, the pressurized water and pressurized heavy-water reactors use regular water and heavy water, respectively, as primary fluids. The high-temperature, gas-cooled reactor uses helium as its primary fluid. Figure 3-11 illustrates the general configuration of the two-loop reactor cycle.

Figure 3-11. Two-Loop Indirect Reactor Cycle

The boiling water reactor and the pressurized water reactor are both classified as light water reactors, based on their use of regular water as coolant. The high-temperature, gas-cooled reactor is representative of a broad range of gas-cooled reactors which use carbon dioxide or helium as the coolant.

RESEARCH REACTORS

A very wide range of nuclear reactors have been and are being built to perform fundamental research and development activities related to commercial nuclear power. Many research reactors have certain similarities to one or more of the power reactor types in terms of fuel, coolant, and/or moderator.

Research reactors operate at a low power level accompanied by low coolant pressure. Many designs employ a reactor vessel where a water coolant/moderator is maintained in an open pool at atmospheric pressure.

NUCLEAR REACTOR SYSTEMS

Since the fission process creates radioactive fission products, reactor systems must be designed to minimize the risk of release of these products to the environment. Consequently, basic reactor design philosophy must make provision for

1. Inherently safe systems capable of withstanding major, unanticipated mishaps and preventing the occurrence of hazards to public health or safety.
2. Multiple barriers which shield against the escape of radioactivity to the environment, including
 - a. The fuel pellet,
 - b. Cladding,
 - c. The reactor vessel, and
 - d. The containment structure.
3. Redundant safety devices and systems which protect against human error, equipment failure, severe accidents, and natural disasters, e.g., earthquakes, tornados, hurricanes, etc.

More specific design features, based on representative data, for the reactors under consideration are provided in Tables 3-VI through 3-IX and Figures 3-12 through 3-29.

TABLE 3-VI
Design Specifications for the
Boiling Water Reactor^{a,b}

Steam Cycle	<ul style="list-style-type: none"> • direct, single-loop water system operating at approximately 6.9 MPa and 290° C • jet pumps control flow and reactivity • steam and water are separated at the top of the reactor vessel • efficiency approximately 32 percent
Initial Fuel	<ul style="list-style-type: none"> • 2 to 4 percent enriched U²³⁵ in sintered UO₂ pellets, approximately 10 mm in diameter by 13 mm long
Fuel Produced	<ul style="list-style-type: none"> • Pu²³⁹ from U²³⁸ in the fuel pellets
Cladding Material	<ul style="list-style-type: none"> • Zircaloy-4 tubes, approximately 3.6 metres long
Coolant/Moderator	<ul style="list-style-type: none"> • water/water
Fuel Assemblies	<ul style="list-style-type: none"> • 7 by 7 or 8 by 8 array of fuel pins surrounded by a Zircaloy-4 fuel channel
Reactor Core	<ul style="list-style-type: none"> • approximately 780 fuel assemblies surrounded by a water reflector
Reactor Vessel	<ul style="list-style-type: none"> • steel, 21.6 metres high, 6.3 metres in diameter, and 150 to 180 mm thick
Containment	<ul style="list-style-type: none"> • primary containment consists of a dry well and pressure suppression chamber • secondary containment consists of the reactor building with leak-tight steel liner

^aRepresentative data.

^bFigures 3-12 through 3-16 illustrate various component parts of a boiling water reactor.

Figure 3-12. Boiling Water Reactor Steam Cycle Schematic (Reference 5)

Figure 3-13. Boiling Water Reactor Fuel Assembly (Reference 5)

Figure 3-14. Reactor Vessel for a Boiling Water Reactor (Reference 4)

Figure 3-15. Mark III Reactor Building (Containment and Shield Building) for a Boiling Water Reactor (Reference 5)

Figure 3-16. Mark III Reactor Building, Fuel Building, and Auxiliary Building for a Boiling Water Reactor (Reference 5)

TABLE 3-VII

Design Specifications for a
Pressurized Water Reactor^{a,b}

Steam Cycle	<ul style="list-style-type: none"> • primary water loop operating at approximately 15.5 MPa and 340° C • secondary water loop operating at approximately 6.9 MPa and 290° C • pressurizer maintains primary system pressure • two to four steam generators • efficiency approximately 32 percent
Initial Fuel	<ul style="list-style-type: none"> • 2 to 4 percent enriched U²³⁵ in sintered UO₂ pellets, approximately 10 mm in diameter by 13 mm long
Fuel Produced	<ul style="list-style-type: none"> • Pu²³⁹ from U²³⁸ in the fuel pellets
Cladding Material	<ul style="list-style-type: none"> • Zircaloy-4 tubes, approximately 3.8 metres long
Coolant/Moderator	<ul style="list-style-type: none"> • water/water
Fuel Assemblies	<ul style="list-style-type: none"> • 14 by 14 to 17 by 17 array of fuel pins in an open fuel lattice, 16 to 36 fuel locations replaced by nonfuel compositions
Reactor Core	<ul style="list-style-type: none"> • approximately 240 fuel assemblies surrounded by a water reflector
Reactor Vessel	<ul style="list-style-type: none"> • steel, 12 metres high by 4.2 metres in diameter by 200 mm thick
Containment	<ul style="list-style-type: none"> • reinforced concrete building with leak-tight steel liner

^aRepresentative data.^bFigures 3-17 through 3-21 illustrate various component parts of a pressurized water reactor.

Figure 3-17. Pressurized Water Reactor Steam Cycle Schematic

Figure 3-18. Pressurized Water Reactor Fuel Assembly (Combustion Engineering)

Figure 3-19. Reactor Vessel for a Pressurized Water Reactor (Reference 4)

Figure 3-20. Typical Primary Coolant System and Containment for a Large Pressurized Water Reactor System (Reference 7)

Figure 3-21. Schematic Arrangement of Pressurized Water Reactor NSSS (Reference 7)

TABLE 3-VIII
Pressurized Heavy-Water Reactor^{a,b}

Steam Cycle	<ul style="list-style-type: none"> • primary heavy-water loop operating at approximately 10 MPa and 310° C • secondary water loop operating at approximately 4.7 MPa and 260° C • pressurizer to maintain primary system pressure • four steam generators • efficiency approximately 29 percent
Initial Fuel	<ul style="list-style-type: none"> • natural uranium in sintered UO₂ pellets, approximately 12.5 mm in diameter
Fuel Produced	<ul style="list-style-type: none"> • Pu²³⁹ from U²³⁸ in fuel pellets
Cladding Material	<ul style="list-style-type: none"> • Zircaloy-4 tubes, approximately 500 mm long
Coolant/Moderator	<ul style="list-style-type: none"> • heavy water/heavy water
Fuel Assemblies	<ul style="list-style-type: none"> • 37 fuel pins per bundle, approximately 102 mm in diameter • 12 bundles per fuel channel
Reactor Core	<ul style="list-style-type: none"> • 4560 bundles in a calandria tank filled with heavy water
Reactor Vessel	<ul style="list-style-type: none"> • 380 zirconium-2.5 percent niobium pressure tubes, with an inside diameter of approximately 103 mm and 4.34 mm thick • calandria tank, with a 3.14-metre radius and 5.94 metres long; the tank contains 0.260 Mg of D₂O at approximately 93° C • pressure tubes in two separate systems; reverse flow in alternate tubes
Containment	<ul style="list-style-type: none"> • reinforced concrete building with steel liner • vacuum building

^aRepresentative data for CANDU concept.

^bFigures 3-22 through 3-25 illustrate various component parts of a pressurized heavy-water reactor.

Figure 3-22. CANDU Reactor Simplified Flow Diagram (Reference 2)

Figure 3-23. 37-Element Fuel Bundle (Reference 2)

Figure 3-24. CANDU Nuclear Reactor (Reference 4)

Figure 3-25. Reactor Building Cutaway (Reference 4)

TABLE 3-IX
High-Temperature, Gas-Cooled Reactor^{a,b,c}

Steam Cycle	<ul style="list-style-type: none"> • primary helium loop with reheat cycle operating at approximately 4.5 MPa and 725° C • secondary water loop operating at approximately 17.2 MPa and 515° C • helium circulators • primary and auxiliary heat exchangers • efficiency approximately 40 percent
Initial Fuel	<ul style="list-style-type: none"> • 93 percent enriched U²³⁵ in UC₂ TRISO microspheres, approximately 200 μm in diameter
Fuel Produced	<ul style="list-style-type: none"> • U²³³ from Th²³² in BISO microspheres
Cladding Material	<ul style="list-style-type: none"> • graphite and silicon carbide coatings on microspheres
Coolant/Moderator	<ul style="list-style-type: none"> • helium/graphite
Fuel Assemblies	<ul style="list-style-type: none"> • fuel particles in pitch rods stacked into 360-mm, hexagonal graphite blocks, 790 mm high
Reactor Core	<ul style="list-style-type: none"> • approximately 4000 fuel assemblies surrounded by graphite moderator
Reactor Vessel	<ul style="list-style-type: none"> • 27-metre-high prestressed concrete reactor vessel 30 metres in diameter, containing steam generators
Containment	<ul style="list-style-type: none"> • reactor building

^aRepresentative data.

^bThe particles are designed so that the U²³⁵ and the U²³³ may be separated by physical means during reprocessing.

^cFigures 3-26 through 3-29 illustrate the various component parts of the high-temperature, gas-cooled reactor.

Figure 3-26. Schematic of a High-Temperature, Gas-Cooled Reactor Flow Diagram

Figure 3-27. BISO (fertile) and TRISO (fissile) Microsphere Fuel Particles for a High-Temperature, Gas-Cooled Reactor

Figure 3-28. High-Temperature, Gas-Cooled Reactor Fuel Assembly (General Atomic)

Figure 3-29. Reactor Vessel for a High-Temperature, Gas-Cooled Reactor (Reference 3)

REACTOR DESIGN CLASSIFICATION

STEAM CYCLE

COOLANT

MODERATOR

NEUTRON ENERGY

NUCLEAR REACTORS

BOILING WATER REACTORS (BWR)

PRESSURIZED WATER REACTORS (PWR)

PRESSURIZED HEAVY-WATER REACTORS (PHWR)

HIGH-TEMPERATURE GAS-COOLED REACTORS (HTGR)

RESEARCH REACTORS

STEAM CYCLES

DIRECT CYCLE

BOILING WATER REACTOR (BWR)

TWO-LOOP CYCLE

STEAM GENERATOR

PRESSURIZED WATER REACTOR (PWR)

PRESSURIZED HEAVY-WATER REACTOR (PHWR)

HIGH-TEMPERATURE GAS-COOLED REACTOR (HTGR)

RESEARCH REACTORS

SIMILARITIES

LOW POWER

LOW PRESSURE

OPEN

VISUALS

NOTES

RADWASTE SYSTEMS

WASTE-HANDLING PROCEDURES

DILUTION AND DISPERSION

DELAY AND DECAY

CONCENTRATION AND CONTAINMENT

REACTORS

DELAY IN STORAGE TANKS

GASES/LIQUIDS

SOLID WASTES

CONTENT

VISUALS

NOTES

LIGHT WATER REACTORS (LWR)

BWR

PWR

GAS-COOLED REACTORS

HTGR

HELIUM/CARBON DIOXIDE

VISUALS

NOTES

REACTOR SYSTEMS

MINIMIZE RISK

DESIGN PHILOSOPHY

INHERENT SAFETY

MULTIPLE BARRIERS

FUEL PELLENT

CLADDING

REACTOR VESSEL

CONTAINMENT STRUCTURE

REDUNDANT SAFETY DEVICES AND STRUCTURES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

3.0 REACTORS

Session Title: 3.5 Reactor Operation

Date: Friday, 3 November

Presented By: R. Knief, University of New Mexico
and Sandia Laboratories
Consultant

Time: 1330 to 1430

Session Objectives:

After the session, the participants will be able to

1. Describe the basic meltdown accident for a reactor and identify differences for the following reactor systems: light water, heavy water, and gas-cooled,
2. Discuss the susceptibility of reactors to sabotage during refueling or spent fuel storage, and
3. Identify the three methods for handling radioactive wastes and discuss their relationship to physical security.

Summary:

The basic features of routine and accident-initiated reactor operations are considered. The causes of and procedures for mitigation of serious accidents are discussed in relationship to the potential for sabotage.

Additional Resource Materials:

Literature provided by various reactor vendors.

REACTOR OPERATION

As noted previously, an important goal in the design and operation of reactor systems is to minimize the potential hazard of release of radioactive materials. The multiple barrier design concept provides substantial protection against radioactive release from the fuel core. Equipment design and operational procedures must work together to minimize risks associated with radioactive materials external to the core.

The major sources of radioactivity which must be protected in order to prevent accidental and/or malicious dispersal of radioactive materials are

1. The fission product content of the operating reactor core,
2. The fission product content of spent fuel during refueling or on-site storage, and
3. The radionuclides contained in various waste handling (radwaste) systems associated with the reactor.

Since the fuel core of a power reactor is, in general, inaccessible during normal operation, it is unlikely that anything but a very severe accident would result in substantial release of radioactivity. On the other hand, during core refueling the irradiated fuel becomes relatively available at a time when its activity is still very high. After the spent fuel has been placed in a storage pool and as time elapses, the fuel becomes less and less radioactive. The radionuclide inventory of a waste handling system at any given time is a strong function of the recent operational mode of the reactor system.

REACTOR CORE

During normal operation, only a very small fraction of the fission product inventory leaves the fuel pellet and penetrates the cladding to enter the coolant. These radionuclides may, in general, be controlled through cleanup systems external to the primary coolant system. Essentially, only a meltdown of all or part of a reactor core could cause extensive release of fission products. However, since the design requirements of the reactor system minimize the accidental occurrence of such an event, only very severe and very unlikely circumstances may be expected to produce a meltdown.

MELTDOWN SCENARIOS

A reactor core will melt only if the reactor heat production rate exceeds the maximum heat removal rate for the coolant. In such a circumstance, the overall energy available for the accident will depend on several sources:

1. Stored energy (sensible and latent heat) in the fuel, cladding, structure, and coolant,

2. Nuclear transient energy accompanying possible reactivity insertions,
3. Decay heat from the irradiated fuel, and
4. Chemical reaction energy from exothermal interactions among system constituents.

A typical, postulated meltdown sequence for a light water reactor would include

1. Loss of primary coolant through a large, double-ended guillotine break in a major pipe,
2. Neutronic shutdown with loss of the moderator (neutron multiplication in low-enriched fuel depends on the presence of a material to slow down neutrons),
3. Decay heat from the fission products provides a heat source sufficient to melt the fuel and/or to produce an exothermal reaction between the zirconium cladding and steam,
4. Meltdown propagates until an entire molten core falls to the bottom of the reactor vessel,
5. Potential vapor explosion, i.e., very violent chemical reaction, if the core contacts water in the bottom of the vessel,
6. Molten fuel penetrates the reactor vessel and falls to the containment floor,
7. Interaction of molten fuel and concrete leads to the evolution of hydrogen and carbon dioxide, and
8. Fission products are released to the outside environment following failure of the containment due to overpressure (preceded by steam explosion, hydrogen combustion, or concrete interaction) or containment meltdown ("China syndrome").

If the highly improbable initiating event were to occur, redundant safety systems would be expected to mitigate the consequences of such an accident before a substantial amount of fuel meltdown could occur.

Hypothetical meltdown scenarios for other reactor systems would basically be similar to that postulated for a light water reactor except for the differences described below.

For the pressurized heavy-water reactor (CANDU), the meltdown sequence differs in that

1. Major pipe rupture would expel coolant from only one-half of the channels, and
2. The loss of coolant would not imply loss of the moderator; therefore, rapid shutdown would not occur. In fact, under some circumstances, the system could be supercritical.

For the high-temperature, gas-cooled reactor, the meltdown sequence is different because

1. Rapid coolant loss is not credible since the entire primary system is

contained in the prestressed concrete reactor vessel; the basic accident becomes, instead, a loss of forced cooling,

2. The loss of helium coolant has little, if any, effect on the state of criticality since the graphite moderator is unaffected, and
3. The high graphite heat capacity results in a very slow escalation of temperatures.

For research reactors, meltdown is, in general, an unlikely occurrence because of the low power level and the correspondingly low fission-product radioactivity and decay-heat source. On the other hand, the fuel may be relatively more accessible to theft. Open-pool designs provide access to the core fuel which is somewhat similar to that for spent power reactor fuel in storage.

ENGINEERED SAFETY SYSTEMS

Each major reactor system includes a multiplicity of features which are designed to mitigate the consequences of accident-caused radiation release sequences which potentially can lead to core meltdown. Figure 3-30 depicts the basic intent

Figure 3-30. Engineered Safety Features of a Light Water Reactor

of the engineered safety features for a light water reactor. The five major constituents are

1. Reactor trip (RT), or "scram," to provide shutdown of the nuclear chain reaction,
2. Emergency core cooling (ECC) to limit fuel melting,
3. Postaccident heat removal (PAHR) to prevent containment overpressurization and to assure the continuing effectiveness of emergency core cooling,
4. Postaccident radioactivity removal (PARR) to reduce the radionuclide inventory available for release, and
5. Containment integrity (CI) to limit radioactivity release.

Note that the features listed are not all independent of each other, e.g., a containment spray system may be used for removal of both heat and radioactivity.

Every reactor system has automatic shutdown systems which act after receipt of any of the large number of signals. The initial trip function for a light water reactor is accomplished by insertion of poison control rods. If the rods fail, secondary shutdown is assured through the boric acid content of the emergency core cooling water supplies. The pressurized heavy-water reactor and the high-temperature, gas-cooled reactor systems each have two independent mechanisms for immediate shutdown. Each of the three described water reactors has multiple emergency core cooling systems which can operate at various times during an accident. Typically, these emergency systems include injection systems which operate through coolant lines or spray systems within the reactor vessel. The high-temperature, gas-cooled reactor does not have comparable emergency cooling systems.

Postaccident heat removal systems in the high-temperature, gas-cooled reactor consist of auxiliary pumps and heat exchangers designed to restore at least partial coolant flow after an accident. In the water reactors, the function is accomplished through containment sprays for pressure reduction and through pump and heat-exchanger sets which remove heat from the circulating emergency coolants.

Postaccident radioactivity removal in each of the reactor designs is provided by various filtration systems. In the water reactors, additives in the containment sprays provide for additional removal of some of the more chemically reactive radionuclides.

Containment integrity is based on a leak-tight design which is capable of countering all anticipated accident conditions. Concentric shells with controlled release from inner to outer regions provide the basis for recently developed, highly promising designs. Provision for automatic isolation of all containment penetrations is another important aspect in the preservation of overall reactor integrity against fission product release.

Since many of the engineered safety systems depend upon the availability of electric power, multiple sources (both on-site and off-site) are provided. The reliability and security of such power supplies must be assured if core meltdown is to be prevented after adverse initiating sequences.

SPENT FUEL OPERATIONS

Spent fuel assemblies from power reactors usually contain less radioactivity than the active fuel assemblies located in an operating core. However, the heat loads they produce are high enough years after removal to cause fuel melting if adequate cooling is not available. Spent fuel may also pose greater risks in terms of accidents or sabotage because of its higher accessibility.

In all major power systems except the CANDU pressurized heavy-water reactor, the head of the reactor vessel is removed for refueling (and defueling) operations. Assemblies are removed remotely and transferred for storage through tubes in the containment vessel into water basins located in a separate building.

The CANDU system uses on-line refueling. Fuel bundles are inserted or removed from pressure tubes by specially designed fueling machines. The steps involved in the transfer of the bundles from the machines to their final storage locations are depicted in Figure 3-31. In this case, storage is again located outside of the containment building.

Figure 3-31. Fuel Handling Sequence (Reference 2)

An additional factor which must be taken into consideration is the location of the spent fuel storage site with respect to ground level. Elevated facilities may be more subject to inadvertent water removal than those located below grade and hence may be potentially more hazardous.

RADWASTE SYSTEMS

Radioactivity is present in and around reactor systems in a variety of forms and concentrations. Three basic procedures for dealing with such waste problems are

1. Dilution and dispersion--Radioactive wastes are reduced to concentrations below maximum permissible concentration levels and then released into the air or water,
2. Delay and decay--Wastes are stored until such time as decay reduces the radioactivity to within maximum permissible concentration limits, and
3. Concentration and containment--The volume of radioactive wastes is reduced and immobilized.

In reactor environments, few radionuclides are released without some amount of delay. Thus, most systems make use of storage tanks which contain relatively large quantities of radioactive materials. The noble gases which escape from fuel assemblies are subject to containment prior to release. Liquid wastes from water reactors are also detained in delay tanks. Filters, ion-exchange resins, and other devices for removal of radioactive materials constitute solid wastes which must also be contained.

The amount of radioactivity within the various radwaste systems at any given time is likely to be small compared to that contained in the reactor or in the spent fuel. However, these systems may be more susceptible to accident or sabotage and, thus, may represent significant risk.

DESIGN AND OPERATION

MINIMIZE RADIOACTIVITY HAZARD

MULTIPLE BARRIERS —————→ CORE

EQUIPMENT DESIGN		—————→	EX-CORE
OPERATIONAL PROCEDURES			

SOURCES OF RADIOACTIVITY

REACTOR CORE

SPENT FUEL OPERATIONS

WASTE HANDLING (RADWASTE) SYSTEMS

REACTOR CORE

INACCESSIBLE

SEVERE ACCIDENT

SPENT FUEL

REFUELING/STORAGE

TIME-DEPENDENT SOURCE

RADWASTE SYSTEM

OPERATIONAL MODE OF REACTOR

VISUALS

NOTES

REACTOR CORE

NORMAL OPERATION

SMALL RADIOACTIVITY RELEASE

CLEANUP SYSTEMS

LARGE RELEASES

MELTDOWN

DESIGN REQUIREMENTS

SEVERE/UNLIKELY CIRCUMSTANCES

MELTDOWN SCENARIOS

$$\left\{ \begin{array}{c} \text{REACTOR} \\ \text{HEAT} \\ \text{PRODUCTION} \end{array} \right\} > \left\{ \begin{array}{c} \text{MAXIMUM} \\ \text{HEAT} \\ \text{REMOVAL} \end{array} \right\}$$

ENERGY SOURCES

STORED ENERGY

NUCLEAR TRANSIENT ENERGY

DECAY HEAT

CHEMICAL REACTION ENERGY

VISUALS

NOTES

MELTDOWN SEQUENCE FOR LWR

LOSS OF COOLANT

NEUTRONIC SHUTDOWN

DECAY HEAT

MELT FUEL

ZR-STEAM REACTIONS

MELTDOWN PROPAGATION

POTENTIAL VAPOR EXPLOSION

VESSEL PENETRATION

CONCRETE INTERACTION

FISSION PRODUCT RELEASE

CONTAINMENT OVERPRESSURE

CONTAINMENT MELTHROUGH

SAFETY SYSTEMS

REDUNDANT

MINIMIZE MELTING

CANDU PHWR

LOSS OF ONLY ONE-HALF OF COOLANT

NO NEUTRONIC SHUTDOWN

HTGR

RAPID COOLANT LOSS NOT CREDIBLE

LITTLE EFFECT ON CRITICALITY

SLOW TEMPERATURE RISE

RESEARCH REACTORS

LOW POWER LEVEL

ACCESSIBILITY

ENGINEERED SAFETY SYSTEMS

MULTIPLE FEATURES

CONSEQUENCE MITIGATION

BASIC CONSTITUENTS

TRIP OR "SCRAM"

EMERGENCY CORE COOLING

POSTACCIDENT HEAT REMOVAL

POSTACCIDENT RADIOACTIVITY REMOVAL

CONTAINMENT INTEGRITY

VISUALS

NOTES

REACTOR TRIP

POISON CONTROL RODS

BORIC ACID (LWR)

INDEPENDENT SHUTDOWN SYSTEMS

EMERGENCY CORE COOLING

LWR ONLY

INJECTION/SPRAY

POST ACCIDENT HEAT REMOVAL

AUXILIARY PUMPS/HEAT EXCHANGERS

CONTAINMENT SPRAYS (LWR)

POST ACCIDENT RADIOACTIVITY REMOVAL

FILTRATION

SPRAY ADDITIVES (LWR)

CONTAINMENT INTEGRITY

LEAK-TIGHT DESIGN

CONCENTRIC SHELLS

AUTOMATIC ISOLATION

ELECTRIC POWER

SAFETY SYSTEMS

RELIABILITY/SECURITY

SPENT FUEL OPERATIONS

SPENT FUEL ASSEMBLIES

HEAT LOAD

ACCESSIBILITY

REFUELING

MOST REACTORS → HEAD REMOVAL

CANDU PHWR → ON-LINE FUELING

LOCATION/ELEVATION

3.0 REACTORS

Session Title: 3.6 Reactor Vulnerabilities

Date: Friday, 3 November

Presented By: B. Varnado, Sandia Laboratories

Time: 1500 to 1600

Session Objectives:

After the session, the participants will be able to

1. Identify the sources of radioactive material in nuclear power reactors,
2. Define the major safeguards concerns for light water reactors and high-temperature, gas-cooled reactors, and
3. List the fundamental failure mechanisms which could be induced by sabotage to cause release of radioactive material from each type of reactor.

Summary:

Nuclear power reactors contain radioactive material in several systems: the reactor core, the spent fuel pool, and the radioactive waste system. The material in these systems could potentially be a target for sabotage or theft attempts. The safeguards concerns vary for different types of power reactors depending upon the quantity, physical form, chemical composition, radiation level, and toxicity of the material contained in these systems. The attractiveness and accessibility of the radioactive material in several types of power reactors are discussed.

In order for sabotage to cause release of amounts of radioactive material hazardous to the public, a number of safety systems must be disabled. The fundamental failure mechanisms which could lead to release and the minimum system functions which must be protected to prevent release are discussed.

Additional Resource Materials:

SAND75-0504, Safety and Security of Nuclear Power Reactors to Acts of Sabotage

SAND76-0428, Safeguards System Effectiveness Modeling

SAND77-0116C, Protection of Nuclear Power Plants Against Sabotage

SAND77-0644, Reactor Safeguards System Assessment and Design

WASH 1400

REACTOR VULNERABILITIES

Radioactive material is contained in several different parts of a nuclear power reactor: the core of the reactor, the spent fuel storage pool, and the radioactive waste system. At certain times, nuclear material will also be present in the new fuel storage area and in spent fuel shipping casks. Although acts of sabotage or theft could be directed against any of these sources of radioactive material, their attractiveness as targets depends upon the adversary's purpose, technical ability, and resources as well as the accessibility, physical form, chemical composition, amount, radiation level, and toxicity of the material contained in each source. A discussion of the factors which affect the attractiveness and the vulnerability of these possible targets with respect to several types of power reactors follows.

The hazards to the public posed by radioactive material can take two forms: (1) the blast effects of a nuclear explosion and (2) the internal or external radiation damage resulting from dispersal of radioactive material or from criticality incidents. The fuels used in power reactors do not contain sufficient concentrations of fissile atoms to produce a nuclear explosion. Therefore, it is not possible to rearrange the fuel in any manner which will cause a nuclear explosion in the reactor, nor is it possible to use the fuel material directly in a nuclear explosive device. An adversary would have to steal and then process the material in order to obtain a concentration of fissile atoms sufficient to use in a nuclear device; only if this were done would the threat of a nuclear explosion become a possibility. The degree of difficulty involved in processing reactor fuel material for use in a nuclear explosive device varies according to the type of reactor from which the fuel is obtained.

Dispersal of radioactive material could be accomplished either by theft of radioactive material from a reactor facility and release of the material at some other location or by sabotage of the facility in such a way that the material is released directly. Direct explosive dispersal of radioactive material from the reactor facility is not really practical because of the massive containment structures surrounding the material. Extremely large explosive charges would be necessary to breach the containment and disperse the material off-site. It is possible, however, to use the energy which is stored in the fuel in the form of radioactive decay heat as the driving force for dispersal of radioactive material from the facility. Therefore, through acts of theft or sabotage, dispersal can pose a threat to the public safety.

Criticality incidents could be initiated with some of the nuclear materials at reactor facilities; however, the radiation damage would be confined to a limited region near the source. Because of the structure of reactor facilities and the size of facility sites, criticality incidents induced at a facility would have

little or no direct consequences for the general public. However, the theft of fuel followed by initiation of a criticality incident in a highly populated area could produce a significant public hazard.

The hazards of radioactive material and the related safeguards concerns for power reactors are summarized in Table 3-X. The following discussion deals with the safeguards concerns related to each of two major types of power reactors: (1) light water reactors and (2) high-temperature, gas-cooled reactors.

TABLE 3-X
Hazards of Radioactive Materials and Related Safeguards
Concerns for Power Reactors

<u>Hazard</u>	<u>Mechanism</u>	<u>Potential Reactor Safeguards Concern</u>
Blast effects	Nuclear explosion	Theft
Radiation damage	Dispersal	Sabotage or Theft
	Criticality incident	Theft

LIGHT WATER REACTORS

There are two types of light water reactors: pressurized water reactors and boiling water reactors. Both types use water as the coolant and moderator. Light water reactors use low-enrichment (2 to 4 percent fissile content) fuel composed of uranium oxide or mixed uranium-plutonium oxides. During reactor operation, some of the nonfissile uranium atoms in the fuel capture neutrons and are converted to plutonium atoms. After the fuel is removed from the reactor, it can be reprocessed to recover the plutonium, which can then be used in mixed-oxide fuel assemblies.

The uranium oxide or mixed-oxide fuel is formed into compacted, sintered pellets approximately 12.5 mm in diameter and 20 mm in length. The pellets are inserted into a metal tube which is welded shut at both ends to form a fuel rod. The rods are bundled together into fuel assemblies. A pressurized water reactor fuel assembly consists of approximately 200 fuel rods and weighs approximately 500 kg. A boiling water reactor assembly typically contains about 50 fuel rods and weighs about 200 kg. The fuel assembly is the unit handled at the reactor facility; fuel rods are not separated from the assemblies. A boiling water reactor fuel assembly is shown in Figure 3-32.

Fresh Fuel

Fresh reactor fuel is shipped to the reactor site 3 or 4 weeks prior to refueling. The reactors are refueled roughly once a year. While awaiting the refueling operation, the fuel assemblies are stored in dry vaults in the fuel handling area of the reactor facility or in the spent fuel pool. At this stage, before the fuel is brought into a critical configuration in the reactor core, it is not highly radioactive and does not require heavy shielding.

Figure 3-32. Boiling Water Reactor Fuel Assembly

Low-enriched uranium fresh fuel would not be a likely target for theft since its low toxicity makes it unsuitable for dispersal and its low fissile isotope content makes it unsuitable for use in a nuclear explosive device. Isotopic separation and enrichment facilities, which are necessary to convert the fresh fuel into material useful in a nuclear explosive device, are probably beyond the resources of any but highly industrialized nations. In the case of mixed-oxide fuel, the fresh fuel contains plutonium which can be chemically separated from uranium for use in both dispersal of radioactive material and in nuclear explosive devices. Of course, the toxic properties of plutonium necessitate special handling procedures.

For sabotage of the fresh fuel in the storage area to be accomplished, the fuel would have to be rearranged into a critical configuration and a moderator would have to be added. Such a procedure could produce a criticality incident with minor on-site consequences.

Reactor Core

The largest inventory of radioactive material in a facility is found in the core of the reactor. Most of this material is contained in the sealed, metal fuel rods in the form of fission products trapped in pellets or in the spaces at the tops of the rods. The core is located within a thick, steel reactor pressure vessel which is surrounded by a massive steel and concrete containment structure. This multiple containment system, intended primarily as a safety measure, also provides protection against malevolent acts, such as penetration from the exterior, which could lead to release of radioactive material. A cross-sectional view of a pressurized water reactor containment structure is shown in Figure 3-33.

Figure 3-33. Cross Section of a Pressurized Water Reactor Containment Structure

Theft of material from the core is practically impossible. During reactor operation, the material is inaccessible. During refueling, the reactor pressure vessel is open, but the fuel is highly radioactive and produces large quantities of decay heat.

Sabotage leading to dispersal of radioactive material from the core is a possibility at a light water reactor. The greatest hazard to public safety is posed by the consequences of sabotage leading to core meltdown. Neither direct explosive dispersal nor induced criticality presents a realistic public hazard.

Core meltdown can occur even after the reactor has been shut down if continuous cooling is not available to remove fission product decay heat. If the core melts, it is likely that the containment will be breached by one of several possible mechanisms (containment meltthrough, steam explosions, or overpressurization). Fuel melting would, in general, be more hazardous than would direct explosive dispersal of radioactive fuel because the thermal energy of the meltdown processes would release more of the semivolatile fission products in the fuel pellets and would distribute the radioactive material over a large area.

Reactor coolant can be lost from the reactor vessel in two ways:

1. Immediate loss of coolant occurs if the reactor coolant system boundary is breached; the coolant is lost through the break.
2. Delayed loss of coolant occurs if all significant heat sinks and coolant sources are removed from the reactor coolant system; the coolant inventory eventually boils off through the overpressure relief valves.

In general, sabotage which could lead to core meltdown requires that the loss of coolant be accompanied by disablement of one or more systems of the engineered safety features. Sabotage of these vital systems may involve (1) direct action, such as cutting of pipes and destruction of pumps, or (2) indirect action, such as manipulation of motor-operated valves from remote locations (motor control centers or the control room) and elimination of power sources. Many of these acts require the use of explosives or other contraband. Most of them necessitate access to the site and to one or more of the facility buildings.

Spent Fuel

Spent fuel removed from the core is placed in the spent fuel storage pool to allow radioactive fission products to decay sufficiently for off-site transport. The level of radioactivity of the fuel necessitates remote handling and the use of special shipping casks for transport. For some time after the fuel is removed from the core, the heat produced by the radioactive decay process is sufficient to cause fuel melting if the fuel is not cooled. The pool, which has walls of reinforced concrete 1 to 2 metres thick and is lined with stainless steel, contains roughly 1350 m³ of circulating water to dissipate the decay heat and to provide shielding. The fuel assemblies, located about 7 metres below the surface of the water, must be removed by an overhead crane. Figure 3-34 shows a typical spent fuel pool.

Because of the size and weight of the fuel assemblies, the high level of radioactivity, and the need for cooling, theft of spent fuel would be very difficult. If stolen, the spent fuel conceivably could be used directly in crude dispersal schemes. Plutonium, which could be separated from the fuel only if the adversary had the technology and the facilities for handling the toxic materials, could be used in sophisticated dispersal devices or in nuclear explosive devices.

Figure 3-34. Light Water Reactor Spent Fuel Storage Pool

Sabotage of the spent fuel pool might be accomplished in several ways. A fuel assembly could be removed from the pool; this would result in overheating and cladding failure, which, in turn, would result in the release of volatile fission products. The off-site consequences of such an act would be minor. Another possible method of sabotage would be explosive ejection of the fuel from the pool; this would release the gaseous fission products from the fuel rods and disperse the fuel fragments. Consequences would be limited primarily to on-site contamination. A third option would be an explosive attack that either purposely or by chance forced the fuel into a critical configuration; however, such an incident is not likely to occur because of the neutron poisons in the pool. As indicated earlier, the direct consequences of criticality incidents are limited to areas near the source, i.e., on-site.

The final sabotage option of interest for the spent fuel pool is interruption of the cooling process. This would allow the fuel to heat to the melting point with a resultant release of volatile and semi-volatile fission products from the fuel. The cooling process could be interrupted by isolation of the pool from its normal water source or by drainage of the pool. In the former case, it would take several days for the water to boil off to the point where the fuel assemblies would be exposed. It is not feasible to drain the pool by cutting outlet or inlet

pipng because all piping penetrates the pool high enough to prevent serious loss of water due to external rupture. Even if the water could be drained through the piping, the water loss would be gradual and there would be time for corrective action. Explosive breaching of the pool wall is the only means of rapid pool drainage, and this would require a large amount of explosives.

After a period of cooling and decay, the spent fuel assemblies are loaded into special shipping casks for shipment. The shipping casks are heavily shielded and provide cooling for the fuel. A truck cask weighs about 23,000 kilograms and will carry up to 7 fuel assemblies; a rail cask can weigh as much as 100,000 kilograms and carry 18 assemblies. Theft of a shipping cask would be somewhat less difficult to accomplish than theft of spent fuel from the pool, particularly if the cask were already loaded on a transport vehicle. However, successful escape would be a major problem because the adversary would have to transport the large, bulky package in a slow-moving vehicle (tractor-trailer rig). Theft of a rail car seems an even more remote possibility. Sabotage by explosive attack on a shipping cask awaiting shipment could cause limited dispersal of some of its radioactive contents, but dispersal would be primarily on-site.

Radioactive Waste System

The radioactive waste system contains only a small amount of radioactive material in comparison to the other potential sources in the facility. Liquid and gaseous wastes are stored in large tanks for a decay period prior to release into the environment. Solid wastes, such as spent resins, are mixed with sand and cement and then cast into steel drums. None of these waste materials are suitable for use in nuclear explosive devices but they could be used for dispersal. Theft of liquid or gaseous wastes requires transfer of the material from a tank to a container in which it can be transported from the site. Drummed solid waste is easy to handle if transportation off the site can be arranged. Rupture of the liquid or gaseous waste storage tanks could cause minor off-site release.

Summary

The primary mechanisms for release of radioactive materials from each of the sources at a light water reactor are summarized in Table J-XI. The events which

TABLE J-XI

Primary Safeguards Concerns for Light Water Reactors

Source	Primary Adversary Mechanism
Reactor core	Sabotage leading to core meltdown
Spent fuel storage pool	Sabotage leading to fuel melting or ejection from the pool
Fresh fuel (mixed-oxide)	Theft and ultimate use for radioactive dispersal or in a nuclear explosive device
Spent fuel shipping cask	Theft and ultimate use for dispersal
Radioactive waste system (liquid and gaseous)	Sabotage leading to rupture of holding tanks
Radioactive waste system (solid)	Theft and ultimate use in dispersal
Fresh fuel (uranium)	No likely threat

have the greatest public consequences are melting of fuel in the core or in the spent fuel pool. Theft is not considered as a serious problem at a light water reactor; sabotage is the major safeguards concern. The material most likely to be of interest to a thief is fresh mixed-oxide fuel; the material that would probably be easiest to steal is solid waste. Diversion of small amounts of material over a period of time is not a likely option because fresh fuel is the only material that could be safely handled. To gain access to this fuel, a thief would have to remove the fuel bundle from the storage vault, disassemble the fuel bundle, and open the fuel rod. It is unlikely that repeated occurrence of such a sequence of acts would go unnoticed.

HIGH-TEMPERATURE, GAS-COOLED REACTORS

The high-temperature, gas-cooled reactor uses graphite as the moderator and helium as coolant. The fuel used in this reactor consists of highly enriched uranium (93.5 percent fissile content*) mixed with thorium. During reactor operation, some of the thorium atoms capture neutrons and are converted to the fissile uranium isotope U^{233} . The fuel can be reprocessed to recover this U^{233} for recycling into new fuel assemblies.

The fuel for high-temperature, gas-cooled reactors consists of a mixture of fissile (uranium-bearing) and fertile (thorium-bearing) particles in pitch fuel rods. The fuel particles are microspheres coated with graphite and silicon carbide. The fissile and fertile particles are differentiated by size so that they can be mechanically separated for reprocessing. The fuel rods are loaded into machined graphite blocks, each of which contains about 200 fuel rods. Figure 3-35 shows a fuel assembly for a high-temperature, gas-cooled reactor.

Fresh Fuel

High-temperature, gas-cooled reactors are refueled once a year. As is the case for light water reactors, the fresh fuel for high-temperature, gas-cooled reactors is on-site only a short time before being placed into the core. The highly enriched, fresh uranium fuel could be an attractive target for theft since it could eventually be used in a nuclear explosive device. However, a considerable amount of processing would be required to recover the highly enriched material from the fertile particles. Several layers of ceramic coating would have to be removed from the small fissile particles to gain access to the uranium. In some high-temperature, gas-cooled reactor fuel schemes, the uranium is mixed with thorium in the fissile particles. If this is the case, additional chemical processing may be necessary to recover the fissile material.

The complicated fuel handling system at a high-temperature, gas-cooled reactor makes access to the fresh fuel for sabotage purposes practically impossible. The fuel is stored in dry vaults and must be placed in a heavy fuel-transfer cask to be moved. Arrangement of the fuel in a critical configuration outside the core does not appear to be possible. Recycled fuel for the high-temperature, gas-cooled

*Research is currently underway on high-temperature, gas-cooled reactor fuels which could use uranium enriched to less than 20 percent in the fissile isotope.

Figure 3-35. High-Temperature, Gas-Cooled Reactor Fuel Assembly

reactor has only small amounts of radioactive material. It is possible that some of this material could be released if a fresh fuel container were dropped during fuel-handling operations. However, this event would pose, at most, only a minor public hazard.

Reactor Core

The core of a high-temperature, gas-cooled reactor is contained in a large prestressed concrete reactor vessel which is poured into place at the facility site. The primary coolant piping and steam generators are imbedded into the prestressed concrete reactor vessel. Figure 3-36 presents a cross section of a high-temperature, gas-cooled reactor core and prestressed concrete reactor vessel. After the fuel has been loaded into the core, it is inaccessible and is therefore no longer a practical theft target.

The primary coolant and the fuel particles contain radioactive material which could be released by sabotage. The entire primary coolant system is contained within the prestressed concrete reactor vessel and is not accessible to direct attack. Because of the massive structure of the reactor vessel, it is unlikely that a

Figure 3-36. High-Temperature, Gas-Cooled Reactor Core and Prestressed Concrete Reactor Vessel

saboteur could cause radioactive release by damaging it. However, the primary coolant could be released through any of several pipes which connect to the primary coolant barrier and pass through the reactor vessel and, in some cases, through the containment.

Most of the radioactive material in the core is contained in the fuel particles; a smaller amount is contained in the graphite structure. Release of radioactive material from fuel or from structural materials would be accomplished in the same way. The only way to release significant quantities of radioactive material from the fuel particles is to heat them to a very high temperature. The only way to cause massive overheating of the core is to eliminate cooling for extended periods of time. Forced circulation of the coolant in the primary system is necessary to maintain cooling; therefore, either the main coolant loops or the core auxiliary cooling system must function. Sabotage events which could cause failure of these systems are the most likely to lead to core meltdown.

The graphite moderator in a high-temperature, gas-cooled reactor core can absorb a significant amount of heat following loss of cooling capability. As a result, the time interval between the loss of cooling and the start of core meltdown

may be several hours. In order to cause core meltdown, a saboteur must disable the redundant systems which are designed to prevent release and ensure that cooling cannot be restored for a period of time following the sabotage acts.

Spent Fuel

Following refueling, spent fuel elements are stored in fuel storage wells in the reactor service building adjacent to primary containment. The storage wells are circular holes in a thick concrete structure. Helium coolant is circulated around the fuel assemblies in the well by natural convection. The walls of the well contain cooling tubes through which water is circulated. Heat is transferred from the fuel to the helium to the cooling water. Figure 3-37 shows a fuel storage well for a high-temperature, gas-cooled reactor.

Figure 3-37. High-Temperature, Gas-Cooled Reactor Fuel Storage Well

Theft of spent fuel from a high-temperature, gas-cooled reactor would be very difficult for the same reasons cited for a light water reactor. In addition, the fuel handling system of a high-temperature, gas-cooled reactor is more complicated than that of a light water reactor and thus provides further limitations on the accessibility of the spent fuel. Presumably, the object of theft would be recovery

of the fissile U^{233} produced in the fertile particles by neutron capture in thorium. This material could be used in a nuclear explosive device. The toxicity of the U^{233} and the presence of U^{232} (a strong gamma emitter) would make remote handling of the U^{233} necessary during and after recovery of the U^{233} from the spent fuel. The spent fuel could be used directly in dispersal devices.

The possibilities for sabotage leading to release of radioactive material from the spent fuel are limited. Loss of cooling to the fuel storage wells would eventually cause melting of the fuel; however, the high heat capacity of the graphite would delay melting for some time. Also, only a few fuel assemblies are placed in each well; therefore, a massive pool of molten fuel cannot be created. Direct dispersal of fuel from the storage wells is not a practical alternative. However, if one or more of the wells could be opened, creating an outlet into the reactor service building atmosphere, some of the radioactive gases could be released. The addition of water to the wells could lead to hydrolysis of failed fuel particles and increase the magnitude of release.

Spent fuel loaded in a shipping container or cask would be somewhat easier to steal than the fuel stored in a storage well; however, the problem of moving the heavy cask off-site would still have to be dealt with. The fuel assemblies are placed in shipping containers, sealed, and then transferred down a 20-metre vertical chute to the railcar shipping cask. One sabotage option would be to drop a container down the chute onto the concrete floor below. This would probably violate the container integrity. The addition of water to the breached container would cause hydrolysis and the release of semi-volatile fission products in particles with failed coatings. It is unlikely that radioactive release from the spent fuel shipping cask produced by an explosive attack would cause significant public hazard.

Radioactive Waste System

Gaseous waste is produced in the helium purification system in the top of the prestressed concrete reactor vessel. The entire system is within containment. When filters in the helium purification system are regenerated, the gaseous waste is circulated outside of containment to a gaseous waste surge tank. Rupture of this surge tank could cause limited release into the atmosphere.

There is very little liquid waste at a high-temperature, gas-cooled reactor. Rupture of the liquid waste tank would present a negligible public hazard. There is a small amount of solid waste. Minor off-site release of radioactive material could result if the waste container used to store the solid waste were dropped during handling. Since solid waste could be utilized in a crude dispersal device, it is a potential theft target.

Summary

The primary safeguards concerns for each of the major sources of radioactive material at a high-temperature, gas-cooled reactor are listed in Table 3-XII. Theft of fresh fuel is a viable concern for high-temperature, gas-cooled reactors because of the use of highly-enriched uranium in the fissile particles. Sabotage

of a high-temperature, gas-cooled reactor which results in core meltdown could have significant off-site consequences. In comparison, other sources rank relatively low in terms of potential public hazard.

TABLE 3-XII
Primary Safeguards Concerns for a High-Temperature,
Gas-Cooled Reactor

<u>Source</u>	<u>Primary Adversary Mechanism</u>
Fresh fuel	Theft and ultimate use in a nuclear explosive device
Reactor core	Sabotage leading to core meltdown
Spent fuel storage wells	Sabotage leading to hydrolysis of fuel or fuel melting
Gaseous waste	Sabotage leading to rupture of surge tank
Spent fuel shipping container	Sabotage leading to rupture of container
Spent fuel shipping cask	Theft and ultimate use for dispersal
Solid waste	Theft and ultimate use for dispersal
Liquid waste	Sabotage leading to rupture of holding tank

SESSION 3.6

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

OPOR NUCLEAR STEAM SYSTEM

VISUALS

NOTES

STUDY CONCLUSIONS - SUSCEPTIBILITY

1. DESIGN FEATURES OF NUCLEAR PLANTS PROVIDE INHERENT RESISTANCE TO SABOTAGE.
2. ORDINARY ACTS OF WILLFUL DESTRUCTION PRESENT NEGLIGIBLE RADIOLOGICAL RISK TO PUBLIC HEALTH AND SAFETY.
3. SABOTAGE WHICH COULD ENDANGER THE PUBLIC WOULD REQUIRE A HIGH DEGREE OF TECHNICAL COMPETENCE, CAPABLE PERSONNEL, AND THOROUGH PLANNING.

STUDY CONCLUSIONS - CONSEQUENCES

1. ALL IDENTIFIED SABOTAGE OPTIONS LEAD TO PLANT FAILURE SEQUENCES IDENTICAL TO THOSE CONSIDERED BY THE REACTOR SAFETY STUDY.
2. SABOTAGE CANNOT CREATE MORE SEVERE CONSEQUENCES THAN THE MAXIMUM CONSEQUENCES PREDICTED BY THE REACTOR SAFETY STUDY.
3. THE EXPECTED CONSEQUENCES OF SUCCESSFUL SABOTAGE WOULD BE A SMALL FRACTION OF THESE MAXIMUM CONSEQUENCES.

CONSEQUENCES OF REACTOR ACCIDENTS

(REACTOR SAFETY STUDY: WASH - 1400)

CHANCE PER REACTOR-YEAR	EARLY FATALITIES	LATENT CAN- FATALITIES (PER YEAR)	PROPERTY DAMAGE \$10 ⁹
ONE IN 20,000	< 1.0	< 1.0	< 0.1
ONE IN 1,000,000	< 1.0	170	0.9
ONE IN 10,000,000	110	460	3
ONE IN 100,000,000	900	860	8
ONE IN 1,000,000,000	3,300	1,500	14

FACTORS AFFECTING CONSEQUENCES

- SITE ATTACKED
- SABOTAGE OPTION
- OPERATING STATUS OF ENGINEERED SAFETY FEATURES
- CONTAINMENT FAILURE MODE
- METEOROLOGICAL CONDITIONS
- WIND
- EXTENT OF EMERGENCY RESPONSE

LIGHT WATER REACTORS**CORE SABOTAGE** **REACTOR SABOTAGE**INCIDENTENGINEERED SAFETY FEATURES

BREACH PRIMARY COOLANT BOUNDARY
(LOCA)

EMERGENCY CORE COOLING SYSTEM

INDUCE CORE HEAT IMBALANCE
(TRANSIENT)

REACTOR TRIP SYSTEM
DECAY HEAT REMOVAL SYSTEM

VISUALS

NOTES

SIMPLIFIED PWR SYSTEM

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

3.0 REACTORS

Session Title: 3.7 Vital Area Identification

Date: Tuesday, 7 November

Presented By: G. B. Varnado, Sandia Laboratories

Time: 1330 to 1430

Session Objectives:

After the session, the participants will be able to

1. State the basic steps in the identification of vital component locations in power reactor facilities, and
2. Explain the use of fault trees in the identification of vital component locations.

Summary:

The first step in the design or evaluation of safeguards systems for a power reactor is the identification of the areas of the facility for which protection is required. This session discusses the use of fault tree analysis to identify the areas of a nuclear reactor facility that must be protected in order to prevent acts of sabotage that could lead to significant release of radioactive material.

VITAL AREA IDENTIFICATION

One of the first steps in the design of a physical protection system for a nuclear facility is to identify the equipment and areas of the facility which must be protected. To develop a physical protection system for power reactors, it is necessary to determine the equipment that a saboteur must damage in order to initiate radioactive release and the location of that equipment within the facility. Because both the function and structure of a power reactor are very complex, the choice of which components and facility areas to classify as vital to the prevention of radioactive release caused by sabotage is usually not obvious. To identify the vital areas of a facility in a comprehensive and consistent way, a structured analytical approach is required. This section of the discussion on reactors presents techniques which are useful to the performance of the required analysis.

GENERAL PROCEDURE

The basic steps used in the process of identifying vital areas in nuclear reactor facilities are summarized in Figure 3-38. First, the analyst must define the level of radioactive release that is of concern. This, in turn, determines the release threshold that must be considered and helps to establish the required scope of the analysis. A standard commonly used for this purpose is the maximum release allowed from a facility under accident conditions, as specified by applicable regulations.

The second step is to identify the sources of radioactive material in the facility from which a release in excess of the defined limit could occur. Sources which do not contain enough radioactive material to exceed the limit, even if completely released, do not have to be considered further.

In the third step, the release mechanisms by which the material could be transported off-site are identified. Three types of release mechanisms are considered: direct dispersal, induced criticality, and radioactive decay heating. The analyst must determine whether any of these release mechanisms can cause an off-site release of radioactive material from any of the sources identified.

Fourth, the facility operational states which need to be considered in the analysis must be identified. For power reactors, the operating states include power operation, refueling outage, and shutdown. Some of the equipment necessary to prevent release of radioactive material during one operational state may not be required during another; thus, it may be appropriate to define different sets of vital areas for the different modes of operation at a facility.

The system failures which could lead to radioactive release must be determined next. Because of the diverse, as well as redundant, safety-based design of nuclear power reactors, this is the most complicated and time-consuming step in the process.

Figure 3-38. Steps in Vital Area Identification

A systematic analytic technique is required in order to ensure that the many possible failure mechanisms are comprehensively reviewed. Fault tree analysis procedures have been found useful for this purpose.

FAULT TREE ANALYSIS

Fault tree analysis procedures are used to identify the sabotage events which, in proper combinations, can lead to release of radioactive material from a reactor facility. In order to identify vital areas, it is also necessary to determine all the locations in the facility at which each event can be accomplished. After the detailed information on system failures and component locations is collected, the fault trees are analyzed by means of a computer code for Boolean algebra manipulation. Analysis of the fault trees with this code yields the vital areas for the facility being analyzed. Procedures for developing and analyzing the fault trees are discussed in more detail in the following paragraphs.

A fault tree is a logic diagram which graphically represents the combinations of component and subsystem events that can result in a specified undesirable system state. The undesired state (or event) for the purposes of this discussion is considered to be the release of significant amounts of radioactive material from a reactor facility as a result of sabotage. In the fault tree analysis, this undesired event is developed into logical combinations of contributing events, each of which is further developed, in turn, until primary events terminate each branch of the tree. Primary events are individual sabotage acts such as the disabling of a pump or the severing of a pipe. As an example, Figure 3-39 describes the top portion of the sabotage fault tree for a pressurized water reactor. In this figure,

Figure 3-39. Top Portion of a Sabotage Fault Tree for a Pressurized Water Reactor

the undesired event is developed into intermediate events which represent release from each of the primary sources of radioactive material. Fault tree symbols are identified in Table 3-XIII. Each gate in the tree represents the logical operation

TABLE 3-XIII
Symbols Used in the Graphical Representation of a Fault Tree

(OR or AND) by which the inputs combine to produce an output. Each branch of the tree is developed by identification of the immediate, necessary, and sufficient conditions leading to each event. An example showing how one branch of the tree is developed is contained in Figure 3-40.

Figure 3-40. Continued Development of One Branch of the Sabotage Fault Tree

From a fault tree, an equivalent Boolean logic equation can be developed. Each event in the tree is given a label, as indicated in Figure 3-44. In the Boolean equation for the fault tree, these labels are referred to as literals. The literals are joined together by the logical operators $\vee$ (OR) and $\wedge$ (AND), as indicated by the fault tree gates. The Boolean equation for the top event of the tree shown in Figure 3-40 is

$$\text{RMR-PWR} = \text{RRCC} \vee \text{RSNFC} \vee \text{RFRADWSC} \quad (3-1)$$

Replacing the event RRCC with its logical equivalent gives

$$\text{RMR-PWR} = \text{RDRS} \vee \text{RDRR} \vee \text{RDRO} \vee \text{RSNFC} \vee \text{RFRADWSC} \quad (3-2)$$

In the Boolean equations, the $\wedge$ (AND) operation is performed before the $\vee$ (OR) operation, just as multiplication precedes addition in ordinary algebra. Equation 3-2 contains five terms separated by OR operators. The occurrence of any term in such an equation produces the output event found on the left-hand side of the equation. A logic equation, equivalent to the fault tree, is obtained by successive substitution of events lower in the tree for events higher in the tree until the undesired event is expressed solely in terms of primary events. Each combination of primary events sufficient to cause release appears as a term in the logic equation that represents the tree; thus, each term represents a "scenario" which must be prevented. Boolean algebraic manipulation of the equation provides a powerful analytic tool for determination of protection requirements.

Vital Location Analysis

The primary events in the fault trees are sabotage actions which, in proper combinations (as specified by the logic of the tree), can lead to release of radioactive material from the reactor facility. It is also important to know the specific locations in the facility to which an adversary must gain access in order to accomplish these acts. This knowledge can be used to ensure that the physical protection system design includes protective mechanisms for the buildings, rooms, and compartments within which the sabotage actions can be accomplished. In vital location analysis, each primary event in the system fault tree is replaced by the location or logical combination of locations at which the sabotage action can be accomplished. This amounts to a transformation of variables in the event equation. This transformation produces a location equation which represents the combinations of locations to which the adversary must gain access in order to cause the undesired event. Each combination of locations (each term in the location equation) may represent a single combination or thousands of combinations of primary events, depending upon how many events can be accomplished at each location and how the events combine to produce release. Because there are usually fewer locations than primary events, the location equation is typically much simpler than the event equation.

Figure 3-41 uses a simple example to illustrate the mapping from the event space to the location space. The 10 initiating events (E1 through E10) combine in 6 ways to produce the undesired event, SAB; that is, there are six terms in the event equation (Equation 3-3); each term is enclosed in parentheses.

$$SAB = (E3) \vee (E4) \vee (E5) \vee (E1 \wedge E2) \vee (E6 \wedge E7) \vee (E8 \wedge E9 \wedge E10) \quad (3-3)$$

Figure 3-41. Example Fault Tree Events and Locations

The dashed lines in Figure 3-41 indicate the locations (L1 through L5) at which the events can be accomplished. For example, primary events E1, E2, E3, E4, and E5 can all be accomplished at facility location L1. If the events in Equation 3-3 are replaced with locations and the appropriate Boolean identities* are applied, three combinations of locations at which the undesired event can be initiated are produced. This procedure is illustrated in the following equation.

$$SAB = (L1) \vee (L2 \wedge L3) \vee (L3 \wedge L4 \wedge L5) \quad (3-4)$$

Figure 3-42 illustrates a location tree for the example. The six terms in the event equation are translated into three terms in the location equation, as follows:

$$\begin{aligned} SAB &= (E3) \vee (E4) \vee (E5) \vee (E1 \wedge E2) \vee (E6 \wedge E7) \vee (E8 \wedge E9 \wedge E10) \\ &= \underbrace{(L1)} \vee \underbrace{(L2 \wedge L3)} \vee \underbrace{(L3 \wedge L4 \wedge L5)} \quad (3-5) \end{aligned}$$

*In Boolean algebra, the following identities hold: $A \vee A = A$; $A \wedge A = A$; $A \vee (A \wedge B) = A$.

Figure 3-42. Example Location Tree

As in the case of this simple example, the transformation from sabotage acts to locations generally reduces both the number of literals and the number of terms in the equation. This reduction is essential if some of the subsequent analyses are to be performed.

Because there are too many event combinations in the reactor fault tree to list them all, it is impossible (and unnecessary) to list all of the event combinations in each location set, as was done in the example. Rather, the location equation is processed further to identify a minimum set of locations (minimum critical location set) the protection of which will interrupt all possible sequences leading to release. This is done by taking the Boolean complement (logical NOT) of the location equation.

A Boolean equation for an event represents the ways in which the event can occur in terms of the occurrence of the literals in the equation; conversely, the complement of the equation represents the ways the event can be precluded in terms of nonoccurrence of the literals. The complement of SAB is

$$\overline{\text{SAB}} = (\overline{\text{L1}} \wedge \overline{\text{L3}}) \vee (\overline{\text{L1}} \wedge \overline{\text{L2}} \wedge \overline{\text{L4}}) \vee (\overline{\text{L1}} \wedge \overline{\text{L2}} \wedge \overline{\text{L5}}) \quad (3-6)$$

The overline indicates the complement (nonoccurrence) of the event. For the locations identified in Equation 3-6, the complement implies that access has been denied. The equation shows that SAB will not occur if access is denied to both L1 and L3, to L1 and L2 and L4, or to L1 and L2 and L5. If access is denied to all the locations in one term of the complement equation, then none of the event combinations leading to release can be accomplished. The terms in the complement equation

can be ordered according to the number of locations in each term or according to any quantitative values, such as cost of protection or impact on operability, which can be associated with each location.

Generic Sabotage Fault Trees

All nuclear power reactors have a number of features in common. All have the same basic sources of radioactive material (core, fuel storage, and radioactive waste) and the same general functions necessary for prevention of radioactive release (reactor shutdown, decay heat removal, etc.). Because of these common characteristics, portions of the fault trees for different power reactors will have very similar structures. Generic sabotage fault trees which can be applied to a broad spectrum of reactor types have been developed based on these common features.

The details of facility design and layout are usually not common to different facilities. The systems used to provide the functions necessary to prevent radioactive release, the subsystems and components comprising these systems, and particularly the locations of components can vary significantly from facility to facility. Because of these site-specific differences, the details of the sabotage fault trees and, consequently, the number and locations of vital areas will be different for different facilities, even if the facilities are of the same type and vintage. General procedures have been developed to aid the analyst in gathering appropriate site-specific information and incorporating that information into generic fault trees to produce detailed sabotage fault trees for specific facilities. The advantages to using generic sabotage fault tree procedures are that they (1) make it unlikely that a sabotage event will be overlooked in the development of sabotage fault trees for specific facilities, (2) reduce the time required to develop the specific trees, and (3) make it possible for someone with only minimal knowledge of fault tree analysis to develop the detailed trees efficiently.

The top of the generic sabotage fault tree is shown in Figure 3-39. The branch of the tree dealing with release of radioactive materials from the core during normal operation is developed further in Figure 3-40. As indicated by the AND gate labeled RODCM, three barriers must be breached if release is to occur. A conservative assumption often used in analysis of the trees is that core meltdown will breach all three barriers. Core meltdown can be caused in any one of three ways, as shown by the OR gate labeled CBBFM: (1) if a loss of coolant accident is initiated which exceeds the makeup capacity of the mitigating systems, (2) if a loss of coolant accident is initiated and the mitigating systems designed to respond to the accident are disabled, or (3) if a transient is created and the appropriate transient mitigating systems are disabled. The development of these events is dependent on the functional design and capacity of the systems used to mitigate loss of coolant and transient incidents. It is at this point that site-specific differences begin to appear in the trees.

At many places in the further development of the tree, events occur which involve insufficient heat transfer in a heat removal loop. The types of loops encountered in reactor systems have been classified according to common characteristics,

and fault trees have been developed for each type. An example of one such generic loop tree is shown in Figure 3-43. Within each class, the loop trees are made very general so that they can cover possible variations in system design. The analyst must determine the type of loop to be analyzed and the appropriate labels for component identification. Any events that do not apply to the particular loop under study must also be indicated.

Figure 3-43. Generic Sabotage Fault Tree for an Open Loop Without Pumping Power

Eventually, the analysis reaches the level of individual component failures. Components such as valves and pumps, which are commonly found in all facilities, have been classified according to type, and subtrees have been developed for each. A typical valve subtree is shown in Figure 3-44. In the case of valves, the analyst

Figure 3-44. Simplified Sabotage Fault Tree for Motor-Operated Valve

must determine the type of valve used, its normal state (open or closed), and its disabled state. Knowledge of what constitutes the disabled state of a valve is important since different sabotage actions could depend upon the application of the valve. For example, the disabled state for an isolation valve would be open, while the disabled state for a similar valve used in an injection system would be closed. The tree shown in Figure 3-44 describes the ways in which a saboteur could disable a motor-operated valve which is normally closed and for which the disabled state is closed, i.e., it must open in response to some abnormal system condition. As is the case for the loops, the analyst must add the appropriate labels for each component.

To complete the vital area analysis, the analyst must add the location information for each primary event in the tree. Every location at which each event can be accomplished must be identified. For a detailed fault tree, it is usually a straightforward matter for someone familiar with the layout and operation of the facility to make the required location assignments.

The generic sabotage fault trees provide a means of quickly developing a detailed logic model of a complicated reactor facility. Thus far, these logic models have been used primarily to study sabotage vulnerability. There are other possible applications of these generic modeling approaches in the study of reactor safety problems as well. It is anticipated that the basic techniques used for vital area analysis will play an expanding role in the study of related reactor safety issues and the extension of the generic fault tree analysis procedures to other types of facilities.

CONCLUSIONS

The vital area analysis procedures described in this section provide a disciplined, logical, repeatable method for determining vital areas in nuclear facilities. The fault trees clearly document the assumptions made in the analysis and allow the analyst to examine the effect of different sets of assumptions on the number and location of vital areas. The results are consistent in form and level of detail for every facility analyzed so that uniform criteria can be applied. The analysis identifies the minimum set of areas which must be considered as vital and, therefore, will help reduce the costs of physical security. The use of generic sabotage fault trees makes it possible for an analyst knowledgeable in fault tree analysis techniques to develop detailed fault trees for specific nuclear power reactor facilities.

VISUALS

NOTES

VISUALS

NOTES

ONE GATE

THE EXISTENCE OF ALL INPUT EVENTS IS REQUIRED FOR THE OUTPUT TO OCCUR

OR GATE

THE OUTPUT EVENT WILL OCCUR IF ONE OR MORE OF THE INPUT EVENTS OCCUR

TRANSFER-ON

THE EVENT LOGIC FLIPS FROM THE TRANSFER-OUT LOGIC TO THE TRANSFER-ON LOGIC IN A MANNER WHICH RESULTS IT BEING AS IF THE EVENT OR GATES WERE CONNECTED DIRECTLY TO THE SINGLE LINE

TRANSFER-OFF

THE EVENT LOGIC FLIPS FROM THE TRANSFER-ON LOGIC TO THE TRANSFER-OFF LOGIC IN A MANNER WHICH RESULTS IT BEING AS IF THE EVENT OR GATES WERE CONNECTED DIRECTLY TO THE SINGLE LINE

INTERMEDIATE EVENT

A RECTANGLE ABOVE A GATE REPRESENTS THE GATE'S STATE PROVIDED BY THE GATE'S LOGIC

SMALL EVENT

THE RECTANGLE ABOVE A GATE IDENTIFIES A SMALL EVENT A SMALL EVENT IS ONE WHICH CANNOT BE IDENTIFIED

INTERMEDIATE EVENT

THE RECTANGLE ABOVE A DIAMOND IDENTIFIES AN INTERMEDIATE EVENT WHICH CANNOT BE IDENTIFIED OR IDENTIFIED BY THE GATE'S LOGIC

VISUALS

NOTES

NOTE: INT. - INTERMEDIATE

VISUALS

NOTES

SIMPLIFIED SADDOTIME FAULT TREE FOR MOTOR-OPERATED VALVE

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

4.0 THREAT ANALYSIS

Session Title: 4.0 Threat Analysis

Date: Monday, 6 November

Presented By: B. M. Jenkins, Rand Corporation

Time: 1330 to 1430

Session Objectives:

After the session, the participants will be able to describe adversary attributes, tactics, and motivation in order to address threats to nuclear facilities and materials.

Summary:

A methodology which can be used to assess threats against nuclear facilities or special nuclear materials is presented; emphasis is placed on methods which can be used to determine adversary characteristics and actions.

MODULE 4

THREAT ANALYSIS

In 1975, The Rand Corporation was contracted by Sandia Laboratories in Albuquerque, New Mexico, to undertake a study of the potential malevolent threat to United States nuclear activities. This continuing study focuses on the attributes of potential criminal adversaries, including possible motivations, physical resources, knowledge, planning skills, technical expertise, dedication, armament, and methods of operation. The results of this study have contributed to the formation, design, and operation of security systems and measures to protect nuclear materials from theft and diversion and to prevent the sabotage of nuclear facilities. This study may also prove useful for overall emergency contingency planning, assessing the credibility of nuclear threat messages, or possible negotiations with adversaries who might hold nuclear materials or facilities.

The principal methodological problem encountered in conducting this threat analysis is that there have not been serious actions directed against United States nuclear facilities that can be examined. No nuclear installations in the United States have been attacked, seized, or sabotaged in a manner that caused public risk by the release of radioactive materials. No nuclear weapons have been stolen or illegally detonated. No nuclear materials have been diverted or taken by force from installations or while in transit and used for blackmail or made into bombs. No radioactive matter has been maliciously released, endangering public safety.

Bomb threats have been telephoned to nuclear facilities; in fact, this is now not an uncommon occurrence in both government and industry. A number of threats to use nuclear materials have occurred, but all proved, on investigation, to be hoaxes. Minor sabotage has been carried out in a handful of cases. In one incident, a miniscule quantity of special nuclear materials was removed from a fuel fabrication facility. Political extremists attempted to sabotage nuclear reactors on two occasions in France and twice in Spain, and urban guerrillas temporarily seized control of a nuclear facility under construction in Argentina. These incidents are discussed later.

USE OF ANALOGS

In the absence of past major actions directed against nuclear programs, several categories of conventional crimes and political violence have been selected that come closest, in their aims and methods of operation, to possible but as yet uncommitted crimes against nuclear facilities or involving nuclear materials. The explicit assumption is that a study of these analogs can provide knowledge and

insights into the capabilities and the modus operandi of various types of potential adversaries of nuclear programs. However, there is one extremely important reservation on the use of analogs to extrapolate the possible actions of adversaries of nuclear programs and that is that the analogous actions selected do not involve nuclear targets.

The adversary motivations, attributes, and actions characteristic of terrorist activity or crimes committed for gain may differ significantly from those related to possible attacks on nuclear installations or the theft of special nuclear materials or nuclear weapons. Still, adversaries who aim at nuclear malevolence of any kind--be it theft, sabotage, malicious release, or destruction--must engage in actions and use methods also found in regular criminal acts: They must obtain extensive prior knowledge of objectives, installations, and routines; they must accomplish unauthorized entry by stealth, force, or deceit; they must successfully cope with alarm systems and armed guards; they may have to assemble teams; and they may have to recruit outside help. For these reasons, it appears that sufficient similarities exist between the two types of action to allow certain inferences to be made regarding the attributes of possible nuclear adversaries. For example, while no known attempt has been made in the United States to steal significant quantities of plutonium or any other types of special nuclear materials, there is a richly documented history of well-planned burglaries and armed robberies of other valuable and protected commodities, e.g., cash, jewels, and art objects. In many such cases, thieves were able to penetrate multiple and elaborate security systems to gain access to and remove the materials. Similarly, an attack on a nuclear installation or the theft of nuclear materials would have to be conducted either by stealth or deceit (as in a burglary or an embezzlement) or by force (as in a robbery). In material terms, the attack would require the adversaries to possess such resources as tools, weapons, transportation, and possibly alarm suppressants; in nonmaterial terms, it would require these same adversaries to demonstrate such characteristics and attributes as daring, dedication, leadership, knowledge, and experience. The analogs offer examples of the methods or assets that could be employed in such actions.

The following analog is also applicable. Although there have been no publicized seizures or attempts to seize nuclear facilities (except for the single incident in Argentina involving a reactor still under construction), numerous forcible building takeovers and hostage seizures by terrorists have occurred. While political extremists in the United States have thus far not waged any campaigns of violence against nuclear facilities, they have claimed credit for the bombings of government buildings, corporate offices, and public utilities. An examination of all of these actions offers possible insights into the style, dedication, and capabilities of groups that may, at some future date, select a nuclear target.

THE DATA BASE

Data have been assembled on several hundred incidents of different categories of analogs applicable in some specified ways to potential actions against nuclear

facilities. The primary criterion for the selection of analog categories, or incidents within the categories, is that their attributes be closely similar to and, in some instances, identical to what might reasonably be expected from a possible action against a nuclear facility. For this reason, common street crimes and simple robberies were excluded from the data base. Even though such criminal actions might have some features in common with an attack on a nuclear installation or repository, the differences are too great to provide useful insights. A system that could defeat the more serious criminal actions used as analogs would frustrate the lesser criminal actions as well. This data base also helps to link motives or objectives with probable modes of action and with the attributes of the most likely adversaries in each case.

Analog Categories

For this study, the following analog categories have been selected for examination: (1) task force crimes, i.e., major armed robberies and burglaries, (2) terrorist assaults, (3) military commando raids, (4) industrial sabotage, and (5) symbolic bombings. In addition, a limited number of domestic and foreign nuclear incidents which posed a potential threat to public safety are described and examined.

Task force crimes were examined because they represent criminal assaults on well-protected targets or facilities (such as bank vaults, arsenals, and museums), and often require remarkable planning, technical skills, and execution. In the 45 cases reviewed, criminals were able to assemble teams of as many as 20 people and yet remain undiscovered, to breach thick walls and vaults and neutralize modern alarm systems, and to devote up to 2 years of planning to the accomplishment of a single "caper." Task force members often displayed considerable technical competence, e.g., in overcoming electronic alarm systems, but had little inclination to accept a high risk of capture or death.

Terrorist assaults were examined because, in general, they involve individuals who are highly dedicated and willing to accept great personal risks. In the 34 cases reviewed, the terrorists, unlike the professional criminals, were quick to brandish weapons and explosives. Nevertheless, they rarely assaulted facilities if the probability was very great that they might be defeated before they gained their objectives. The terrorists almost always had highly political objectives as a primary purpose for their actions. For this reason, they usually chose to attack very conspicuous targets that would be certain to bring them publicity.

Commando raids were studied since these cases provided the only incidents in which well-armed, specially trained, and dedicated personnel attacked well-defended targets, usually with the explicit intent of destroying them. Seventy-five small-scale military and paramilitary commando raids were reviewed. These raids are particularly relevant because they highlight the importance of accurate intelligence and the element of surprise. These two attributes are central to an

understanding of the extraordinarily high success rate (close to 80 percent) of the commando raids. This success rate is particularly remarkable in that the attacks were launched against defended targets.

Industrial sabotage against private industry, transportation facilities, and public utilities is an obvious analog. Examination showed that the saboteur's objective was the destruction or disruption of facilities or equipment on a significant scale. Industrial sabotage is especially relevant to possible nuclear sabotage because saboteurs typically have privileged information about or access to the target. A survey of 40 incidents revealed that the saboteurs had a wide range of motivations (including the grievances of a disgruntled employee and a rejected suitor) and usually chose unprotected targets. In general, saboteurs were strongly adverse to taking risks and did not deliberately endanger the lives of the general public. The disproportionately high effectiveness of the saboteurs (in terms of accomplishing their objectives), was achieved by a limited number of people with minimal means (in one case, literally one person with a few bolts) and at low personal risk. This was largely due to an accurate knowledge of the facility's operations and vulnerabilities on the part of the saboteur, as well as access to restricted areas.

Symbolic bombings are included in the data base because nuclear facilities are viewed by some as symbols of unwarranted and dangerous technology and might, therefore, be subject to such bombings. Over 100 cases of symbolic bombings form part of the analog data base. A symbolic bombing is defined as a deliberate act of violence calculated to express a grievance or to make a political statement; the damage to, or destruction of, the target may be secondary or even irrelevant to the adversary's aims. A survey of symbolic bombings showed that bombs were usually placed on unprotected targets. The bombers did not display a great deal of technical expertise or dedication; indeed, the bombers were almost cavalier in their approach to their activities.

Finally, a number of nuclear-related threats and incidents were examined, even though they are not, of course, analogs. Between 1969 and 1975, there were 288 known recorded threats against, or incidents at, nuclear facilities in the United States. Two hundred and forty of these were conventional bomb threats, almost all of which were hoaxes. There were 9 actual bombings, 22 cases of arson or suspected arson, and a variety of miscellaneous actions, e.g., felling a meteorological tower. A serious fire was set at the Indian Point nuclear power reactor. One widely publicized case in which nuclear materials were removed from the controlled area occurred at a fuel fabrication facility in Oklahoma; only minuscule amounts of nuclear materials were involved. Thus, even though the overall number of nuclear-related threats and incidents within the United States has been quite high, no nuclear threat to public safety has been realized.

Internationally, however, a larger number of serious nuclear-related incidents have occurred. Perhaps more importantly, the frequency and potential danger of these incidents have been increasing. For example, in France between 1975 and 1976, eight major explosions occurred at French nuclear facilities (such as reactors,

processing facilities, and uranium mines). In England, 20 unenriched uranium fuel elements were stolen from the Bradwell nuclear power station in 1966; the elements were recovered when the culprits tried to sell them. In March 1973, a leftist urban guerrilla group temporarily occupied an atomic power facility under construction at Atucha, Argentina; the reactor had not yet been installed.

An examination of the analogs described provides insights into the capabilities that could be mobilized by an adversary in an action against nuclear facilities. However, such an examination cannot provide assessments of the probabilities of occurrence of any action against nuclear programs, such as sabotage, theft of nuclear materials, symbolic bombings, or terrorist seizures.

It should not be inferred from the emphasis placed on a data base of analog events that it is possible to use rigorous quantitative methodology to predict or describe nuclear threats. The data base is not large enough to allow accurate statistical profiles. The sample is neither complete nor randomly chosen. The scope of the research project limited the coverage of analogous events. In many of the incidents examined, complete information was not available. Furthermore, a full accounting was not given of the cases that were deterred, let alone those that failed. No attempt was made to assign numerical probabilities or confidence intervals in the same way that other studies have estimated values on the occurrence of various types of accidents involving nuclear facilities. However, the events chosen are considered to be representative of their categories and provide an adequate basis for eventually offering judgments on the "comparative likelihood," as opposed to probability of occurrence, of certain kinds of action.

LIMITATIONS TO THE METHODOLOGY

There are limitations to the analog methodology. The data base is composed of incidents, which, for the most part, do not involve nuclear targets. Nuclear targets might attract qualitatively and quantitatively different adversaries. Professional criminals and less dedicated terrorists might be dissuaded from mounting an operation against nuclear targets because nuclear commodities--unlike precious jewels and other normally stolen goods--have no ready street market or because they expect that nuclear facilities and material are likely to be better guarded. On the more pessimistic side, nuclear targets could attract adversaries with entirely different motivations and goals, e.g., the disruption or suspension of nuclear programs themselves. Potential adversaries might include those supported by large well-financed political organizations with more resources than are likely to be possessed by a small band of professional criminals or political extremists. The anticipated gains from the successful theft of nuclear materials might be considered great enough to warrant an effort hitherto unseen in the annals of conventional crime. In addition, the motivations of nuclear adversaries could induce them to assume greater risks than the analog adversaries examined in this study were willing to assume. Still, if the proper care is taken, adversary capabilities and methods of attack can be extrapolated from the analogs on the basis of the similarities previously noted.

MOTIVATIONS OF POTENTIAL ADVERSARIES

This methodology made possible the production of a formal report entitled Attributes of Potential Criminal Adversaries to U.S. Nuclear Programs (Santa Monica: The Rand Corporation, February 1978) and pointed out the need for a companion report on the possible motivations and objectives of these adversaries.

The possible motivations and intentions of potential criminal adversaries of nuclear programs pose a more difficult subject for research than an analysis of the resources, capabilities, and methods of operation of these adversaries. At least, the latter can be extrapolated from a data base of analogous events in which the data are fairly straightforward. An examination of the former, however, requires dealing with a less well-understood area of human behavior. There are a few signposts. The available literature on human motivations is, for the most part, highly theoretical and is concerned only with the individual's behavior rather than group behavior. It cannot readily be translated to the specific problem of nuclear security posed by adversary groups. Much basic research remains to be done. What the motivational analogs might be is not entirely clear and, therefore, researchers are truly faced with a piece of terra incognita, i.e., unknown territory. Consequently, the conclusions offered will necessarily be more speculative. It appears that several concurrent lines of inquiry will have to be pursued.

Existing Work on Motivation

There is fairly extensive literature, much of it highly theoretical, on the general subject of motivation. How much of this literature would be applicable in an examination of the motives of possible nuclear adversaries is not clear. In any event, explorations of the subconscious should be avoided; therefore, this study remains fairly close to the surface. For the time being at least, it will suffice to describe manifest motives and intentions, although some limited attempts to analyze the mind-set of terrorists or the decisionmaking of terrorist groups will be made.

An extensive body of literature also exists on that specific behavior, designated as criminal, which is more applicable to this examination of motivation and intentions. The research is specifically concerned with focusing on the criminal personality or criminal mind as it relates to the commission of certain categories of crime, especially crimes that in some way are analogous to possible actions against nuclear programs or facilities, e.g., theft or sabotage. Some of the more recent research conducted, in particular the work of Yochelson and Samenow on how criminals implement their ideas, would seem to offer a rich source of relevant insights.¹

Regrettably, no similar body of knowledge regarding the motivations of those political fanatics designated as terrorists yet exists. The motivational aspects of terrorism have hardly been explored. Some information is available concerning what might be called the mechanics of terrorism; the organization, financing, weaponry, and tactics have been studied (although much more could be done). A great deal of what might be called "order of battle" information about terrorist

groups exists. In some cases, a sizable portion of their membership has been identified; the names of the members are known. Articles and, in some cases, books have been written about a few of the more notable leaders of terrorist groups. A few terrorists have written about their own experiences. Some terrorists have even been interviewed by journalists.

It has been possible to construct a kind of census data profile of the "typical terrorist" on the basis of apprehended or identified members of terrorist groups. Dr. Charles Russell of the United States Air Force Office of Special Investigations has done much of the pioneer work in this area.² The typical terrorist is a male (although there are some notable female terrorists), in his early twenties, single, from a middle- or upper-class family, with some university training (although the terrorist may be a university dropout), who often joins or is recruited into the group while at a university. The common psychological profile, if it exists, is far more speculative.

There are a number of current theories to explain terrorist (and similar kinds of criminal) behavior. These theories include physiological explanations (inner ear disorders, blood chemistry, dietary deficiencies, heredity), and psychological explanations (psychoses, pathologies, paranoia, anonymity, deprivation, latent homosexuality, fear of assaults on masculinity, suicidal tendencies, the normal mental problems associated with adolescence or perhaps prolonged adolescence, an abnormal fascination with firearms and explosives, a desire for intimacy with national figures, and permissive upbringing). In general, terrorists appear to share certain personality characteristics: They can be described as risk takers, absolutists, or "true believers" and can be characterized as rigid, action prone, or guilt-ridden. A preliminary exploration of the terrorist's mental attitude and notions of social time, social space, and social action have been explored. "Environmental" and social explanations have been offered, such as student revolt, unemployment, lack of alternatives, a permissive society, inefficient police, repression, discrimination, major social change, and a lack of ways to absorb inherent violent tendencies. Terrorism has also been explained in terms of group-induced behavior: the need to maintain status as a member and violent, often bloody, initiation rites. Until more basic research is done, however, these theories will remain unproven.

Why terrorists decide to do what they do (after they have become terrorists) is another area of uncertainty. Why a terrorist group may decide to perform an assassination instead of a kidnapping, how they select their target, and whether and when they will escalate their violence are not known.

However, terrorist behavior does seem to follow certain patterns of action. Each terrorist group has its own repertoire, its own style of operations, and its own modus operandi. The Irish Republican Army does not engage in hijacking or kidnapping. The Red Brigade kidnaps and shoots industrialists and journalists in the legs. West German terrorists seem to be thorough planners. The New World

Liberation Front, a tiny organization in California, bombs on behalf of local political issues, while the Weather Underground, another United States group, carries out actions which focus on national and international issues.

The particular operational pattern of a terrorist group appears to be determined by several factors. Clearly, the composition of the group--whether the members are university dropouts or ex-soldiers--has something to do with it. Many of the Tupamaros (terrorists in Uruguay) came from the school of architecture in the University of Montevideo, a fact reflected in their elaborately constructed underground hideouts. The Popular Front for the Liberation of Palestine-General Command (PFLP-GC) favors elaborately fused bombs and other advanced gadgetry, reflecting the skills of its leader, a former Syrian army engineer. The resources of the group also dictate its style of operations. Bombings are easier to carry out than assassinations. Assassinations are easier to perform than kidnappings.

The size of a group also may determine the nature of its activities. It is not simply that a larger group is likely to possess greater resources. The actions of a smaller group may be determined more by the personality or idiosyncrasies of a single leader. A smaller group might contemplate actions a larger group would not and vice versa. A larger group may feel more vulnerable to infiltration or reprisal, which may constrain its activities.

Cultural factors may determine a group's actions. Ideology may dictate its victims and targets. The idiosyncrasies of a key personality may be a factor in what a group does. Its circumstances may also play a part. Research showed that with regard to the seizure of hostages (a popular terrorist tactic), groups operating on their home territory and supported by an underground apparatus generally favored conventional kidnappings, while groups operating abroad, or at home but not supported by a well-organized underground, favored the seizure of buildings, making the occupants as well as themselves hostage in what police have come to call barricade and hostage situations.

Finally, some universal rules can be postulated. Thus far, no terrorist group has entered the domain of murder on a grand scale. The reason for this is uncertain. It does not appear to be solely a matter of technical constraints. Terrorists seem to operate well below their technological capabilities. They have already demonstrated their capacity to use conventional explosives and could, without resorting to exotic chemical, biological, or nuclear weapons, kill greater numbers of people, but they have not.

In spite of all the research that has been done on terrorism, there is no substantial data on what arguments are made inside a terrorist group for or against a certain action, what factors terrorists may consider more important than others, or even how systematic terrorist decision making works.

MOTIVATIONS OF POTENTIAL NUCLEAR TERRORISTS

Although the amount of attention given to the possibilities of nuclear terrorism has grown rapidly in the last 10 years, comparatively little attention has been devoted to the question of motivation. Most authors posit the standard criminal and political motives of profit and power. A few go further. Martha Hutchinson in a 1976 review of the literature on the possibilities of nuclear terrorism examines the possible motivations of potential nuclear terrorists.³ The Jenkins monograph, Will Terrorists Go Nuclear?, speculates on the range of motivations of various criminal and politically motivated adversaries and suggests that the utility of nuclear devices to terrorists, at least as a means of mass murder, is not so readily apparent upon close examination. Although terrorists may seek to exploit the fear inherent in the word "nuclear" itself, the actual use of nuclear weapons to kill or harm hundreds or thousands of people might split the ranks of the terrorist organization, alienate the terrorists' perceived constituents, cause widespread public revulsion, and provoke severe repression.⁴ Roberta Wohlstetter in "Terror on a Grand Scale" states that there has been very little analysis of the possible motives of nuclear terrorists. The article points out that historically few terrorists have used chemical or biological weapons, which suggests some sort of self-imposed constraints.⁵

There thus emerges a certain amount of debate between those who see terrorists as likely to engage in nuclear terrorism and those who see the existence of counter-arguments and self-imposed constraints which may not prevent but would seem to limit serious nuclear terrorism. A similar debate is taking place regarding the likelihood that organized crime, which has the resources and capabilities necessary to engage in nuclear theft, blackmarketing in nuclear material, and potentially nuclear blackmail, might engage in such activities. Some see organized crime as a basically conservative service industry which probably will not risk the huge and continuing profits from gambling, prostitution, and narcotics by engaging in nuclear actions of any sort, while others view the greed of organized crime as virtually unlimited. With regard to nuclear theft by professional criminals outside of the so-called "mob," the lack of a readily accessible market for nuclear material is seen as a deterrent. If such thefts were to take place, they would more likely be commissioned crimes with buyers arranged in advance or else be carried out with the intention of ransoming the stolen material back to the original owner, as occurs in many art thefts.

METHODOLOGY

Common criminals and political fanatics comprise only part of the spectrum of potential adversaries. Disgruntled employees, psychotics, opponents of nuclear programs, and even foreign agents must be included. The question of what methodology will enable the possible motivations of these adversaries to be explored cannot be answered simply. There is no single approach that seems to work best. Therefore, several lines of inquiry must be followed concurrently. This report reflects the insights gained and conclusions reached in four lines of inquiry: (1) the structural approach, (2) the psychological approach, (3) the motivational analog approach, and (4) motivations observed in past nuclear incidents.

The Structural Approach

In the first line of inquiry, which can be called the purely structural approach, certain categories of perpetrators, motivations, intentions, and actions are postulated and then the most likely combinations are identified. For example, a disgruntled employee (whose motivation is labeled "personal") might want to cause an employer some economic damage. The employee could accomplish this by temporarily disabling a facility, disrupting its operation, or damaging its equipment. This objective could be achieved by a wide variety of specific actions, including vandalism, sabotage, and hoax bomb threats against the facility. However, such actions would have little appeal for a group with economic motives since such a group would be more likely to resort to theft of material or various extortion schemes involving threats to personnel or facilities.

The structural approach is context free. The nature of the threat does not vary according to changes in the political or social environment, nor does it attempt to deeply penetrate the mind of the perpetrator. There is an element of tautology in this approach. For example, thieves steal, and terrorists seek to cause alarm. Nonetheless, it is useful in the identification of likely combinations of perpetrators and actions, and, ultimately, to predict capabilities and targets.

The Psychological Approach

The psychological approach comprises an attempt to penetrate and understand the mind-set of the potential adversary more deeply than is done in the structural approach, although it does not involve an exploration of the subconscious. Rather, it is possible that examination of the communiques and manifestos of terrorist groups, the biographies and autobiographies of terrorists, and the various theories of terrorist behavior may provide some insights that are relevant to an investigation of the possible motivations and intention of terrorist groups in the nuclear domain. Similarly, existing literature on the criminal mind and criminal behavior offers possible insights into this category of potential adversary.

Research has shown that terrorist groups who have more millennial aims, as opposed to those which focus on immediate political issues, may be less constrained in their actions and hence more willing to cause or risk mass casualties. This hypothesis appears to be borne out in at least two groups. The goals of the Japanese Red Army are indeed vague, while its members have demonstrated a willingness to kill and to die that exceeds that of other terrorist groups. In May 1972, members of the Japanese Red Army carried out the Lod Airport massacre in which 25 persons were killed and 76 others were wounded; also in 1972, because of internal disputes, the Red Army tortured and murdered 14 of its own members. In contrast, the New World Liberation Front, a small terrorist group active in northern California, has concentrated on local issues, e.g., utility rates, low income housing, jail conditions. This group is extremely sensitive to its own public image and is extremely careful that its bombs do not cause casualties.

The Motivational Analog Approach

The analog methodology, as it relates to the resources, capabilities, and methods of operation of potential criminal adversaries, has already been discussed. The same approach can be used to examine the motivations of possible adversaries. Motivations and intentions have been discussed in some of the analogs already examined. Sophisticated burglaries and robberies are analogous to possible thefts of nuclear material not solely because, in both cases, the thieves must penetrate elaborate security measures to remove precious commodities, but also because the motivations (economic) and the intentions (to steal something of value) are the same.

Potential actions directed against nuclear programs may also have some purely motivational analogs. Nuclear programs, because they are like other large industries, because they involve a valuable commodity, because they produce pollutants, and because they sometimes experience labor strikes, are targets for the same reasons that other such industries are targets. Nuclear programs also have attributes which may attract special categories of adversaries. Nuclear programs often include large, high technology facilities associated with the production of weapons. They are vital to national security and are symbolic of national government. To many, these programs symbolize aggression, war, and death. Hiroshima and Nagasaki conceivably could provide motives for vengeance by future generations.

Nuclear materials are dangerous as well as intrinsically valuable. To many, the word "nuclear" is inherently sinister and frightening. The detonation of even a crude nuclear explosive device could conceivably cause hundreds or even thousands of casualties and extensive destruction of property. The sabotage of a reactor or the dispersal of radioactive materials are often publicly perceived as having similar consequences, even though these events might present little or no risk to the public. Nuclear programs also have certain, almost mystical qualities associated with them which are similar to those perceived in the sun, great explosions, and fire. Consequently, an examination of the motivations of saboteurs, eco-guerrillas, bombers, arsonists, and mass murderers should offer some insights here as well.

Crimes are not ordinarily categorized by motivation and, of the perpetrators mentioned above, apparently only the arsonist's motivation has been the subject of psychological investigation. This discussion has touched upon the motivations of saboteurs and symbolic bombers postulated in a previous work on the attributes of potential criminal adversaries. At present, the motivation of arsonists is being examined and, to the degree the information is available, the category of "mad bombers" may be included in the study. Incidents in which the intent of the perpetrator (or the result of the action) was the killing of large numbers of people are also a topic of study.

A preliminary investigation of mass murder shows that such incidents occur only infrequently outside of war. The investigation also revealed that the original determination of how many people had to be killed during a single incident for that incident to be classified as a mass murder had to be revised downward several times in order to produce a sufficient number of cases for examination as an analog. A

single incident in which more than twenty persons are intentionally killed or intended to be killed constitutes, according to the revised definition, an incident of "mass murder." This, in itself, indicates the degree of rarity of such instances. Personal and often irrational motives appear in many of the incidents. Another observation is that thus far terrorist groups show little inclination toward mass murder. Most terrorist incidents involve either one or only a few casualties. In the few incidents that involve more deaths, there appears to be a threshold of around 100. Neither fact can be entirely explained by technical constraints.

Motivations Observed in Past Nuclear Incidents

Although few serious criminal actions involving nuclear facilities or material have occurred, there have been, as mentioned previously, a large number of incidents of vandalism, minor sabotage, theft, and symbolic acts of violence at nuclear facilities. Threats to bomb nuclear facilities or to use nuclear devices also have been made. These incidents display a broad range of conceivable motivations: economic, political, antinuclear, environmental, psychotic, etc. The occurrence of these incidents frees any analysis from relying entirely on postulated motives or motivational analogs. The fourth line of inquiry, then, is the examination of all such nuclear incidents for motivation and comparison of the results with the conclusions reached by means of other lines of inquiry.

THE NEXT STAGE

Completion of the work on motivations will allow what has already been learned about the possible motivations and intentions of potential adversaries to be combined with what has been learned about these adversaries' resources, capabilities, and methods of operation. Undoubtedly, these findings will show that adversaries with certain motivations are more likely to possess certain capabilities and to operate in certain ways. Assembling those likely combinations of motivations, objectives, resources, capabilities, and methods of operation will provide a more complete portrait of the potential adversary. The final task will be to match these adversaries to their most likely nuclear targets or actions.

REFERENCES

1. Samuel Yochelson and Stanton E. Samenow, The Criminal Personality, A Profile for Change, Vol. I., Jason Aronson, New York, 1976.
2. Charles A. Russell and Captain Bowman H. Miller, "Profile of a Terrorist," in Military Review, 57, No. 8 (August 1977), pp. 21-34.
3. Martha Crenshaw Hutchinson, "Terrorism and the Diffusion of Nuclear Power," paper presented at the International Studies Association annual convention in Toronto, Canada, February 1976.
4. Brian Michael Jenkins, Will Terrorists Go Nuclear?, California Seminar on Foreign Policy and Arms Control, January 1976.
5. Roberta Wohlstetter, "Terror on a Grand Scale," Survival, 28, No. 3 (May-June 1976), pp. 98-104.

5.0 EVALUATION TECHNIQUES

Session Title: 5.1 Introduction to Evaluation Techniques

Date: Tuesday, 7 November

Presented By: C. E. Olson, Sandia Laboratories

Time: 1000 to 1130

Session Objectives:

After the session the participants will be able to

1. Distinguish between path evaluation and scenario evaluation,
2. List one advantage and two disadvantages of path-level models, and
3. List one advantage and two disadvantages of scenario-level models.

Summary:

This session will introduce the two types of evaluation techniques to be used. It will describe appropriate uses for each type of technique. The concept of system performance deriving from component performance will be introduced.

MODULE 5

EVALUATION TECHNIQUES

INTRODUCTION TO EVALUATION TECHNIQUES

PERSPECTIVE

Whether based on a feature criteria approach or a performance criteria approach, both the design process and the system assessment process are dependent on sound techniques to evaluate the performance of the physical protection system. System performance evaluation in this context refers to estimates of the capacity of the physical protection system to respond to a range of adversary actions in a manner which prevents theft of special nuclear materials or sabotage resulting in a radioactive release endangering the public.

A physical protection system design process based on a specification of required features cannot be expected to lead to a high performance system unless those features, taken together, are sufficient to assure adequate levels of protection. In this case, the agency responsible for specifying the required features might apply evaluation techniques to estimate the minimum performance levels achieved by systems which comply with the requirements. A physical protection system design process based on performance criteria will necessarily incorporate evaluation techniques in order to assure that the performance requirements are met.

The assessment or certification of a finished physical protection system design will also normally require the application of evaluation techniques. Even an existing physical protection system at an operational facility cannot be fully tested as a system. The nature of the protected nuclear facilities and materials prevents tests involving simulated adversary teams which penetrate barriers or steal special nuclear materials and protective forces which carry out the response neutralization functions. Since direct systems tests are ruled out, physical protection system evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates by application of system models.

Figure 5-1 depicts the relationship of the model to the physical protection system and its role in performance evaluation. In general, a model of a system is a representation of the structure of the system in mathematical or physical terms. The model can be subjected to mathematical manipulation or experimentation to give insight into the behavior or performance of the real-world system so represented. For example, the motion of a missile traveling through the atmosphere might be modeled either by a set of equations or by a wind tunnel experiment; in each case, the model represents the interaction of the missile and the air. In the case of models of a complex physical protection system, physical experiments of total system performance are not feasible. Thus, the evaluation techniques described

in this section rely on mathematical representations of the interactions between the physical protection system and adversaries who attempt to steal special nuclear materials or commit an act of sabotage.

Figure 5-1. Relationship of the Model to the Physical Protection System

The first steps in evaluating physical protection system performance are to identify what is to be protected and to specify what results will be judged to constitute successful protection. The session on Vital Location Analysis (3.7) presents a methodology for determining operational components of a reactor which might be protected in order to prevent sabotage. This methodology can also determine, at the operational component level, the specific adversary acts of sabotage which must be protected against in order to prevent the potential release of radioactive materials.

The vital location and vital component analyses characterize the protection to be afforded by the physical protection system. The next step in the evaluation process is to characterize the threat. Component performance may depend on the skills and resources that an adversary can bring to bear on the component. The step of threat characterization should include the level of physical capability and skill of adversaries against which the physical protection system must perform. It is convenient to organize this part of threat characterization in terms of physical attributes and human attributes. Physical attributes include number of adversaries, armament, tools, vehicle (type and number), and communications. Human attributes might include technical skill, military training, knowledge of the facility (operational and physical protection system), willingness to risk death or capture, group organization, etc.

An additional factor in threat characterization is adversary intent. Intent by itself is usually too general to be of use as a basis for evaluation methodology. Figure 5-2 illustrates a structure for decomposing intent into four levels or ways

of organizing the relationship between adversary intent and specific adversary actions. The top level is intent or what initial objective the adversary wishes to accomplish. The figure uses theft of special nuclear materials and sabotage as examples of adversary intent. These two examples are meant to be illustrative and not necessarily comprehensive. Yet, even though other examples of adversary intent might be cited, the number of different intents that can be ascribed to an adversary acting against a nuclear facility is small. The second level is labeled strategy or overall method of accomplishing intent. For any particular adversary intent, there will be, in general, a number of strategies from which an adversary might choose. For example, if the intent of sabotage is considered, an adversary might choose from strategies of stand-off attack, collusion with an insider, penetration to a vital area using a fake credential, or frontal assault. By no means does this list contain every strategy that could conceivably be available to an adversary attempting sabotage. Although the number of intents is few, the number of adversary strategies may be considerable.

Figure 5-2. Hierarchic Threat Structure

The third level of this hierarchic threat structure will contain many more entries. For each strategy, there will generally be a large number of scenarios on which an adversary might base his plans. An adversary scenario is a collection of adversary actions which, if accomplished, will result in the adversary achieving his objective. Evidently, the distinction between a strategy and a scenario can be imprecise at times. The exact difference is not important except in that a scenario can be described in sufficient detail so that the successive actions can be related

to physical protection system measures which may affect the ease with which an adversary can perform them.

The path level of the hierarchic threat structure represents the actual physical paths that an adversary might follow in attempting to penetrate a facility. Each scenario might be reflected in a large number of possible distinct paths. Although the intent level contains only a few entries, decomposition to the path level generally leads to literally millions of paths. It is at the path level that the direct interaction takes place between the adversary and the physical protection system.

EVALUATION MODELS

It is feasible to model physical protection system performance at either the path level or the scenario level. Path level models have the advantage of providing a direct relationship between component performance parameters and system performance parameters for a particular path. The principal disadvantages are (1) the enormous number of paths that would have to be examined to ensure that no potential vulnerability was overlooked, and (2) the difficulty in validating the manner in which the performance of various components and subsystems are modeled. Table 5-1 summarizes the evaluation tasks to which path-level models can be applied most advantageously.

TABLE 5-1

Summary of Evaluation Tasks Appropriate for Path Level Models

System Assessment Tasks:

- Demonstrate vulnerability along a particular path
- Analyze performance against critical adversary paths
- Evaluate system against preselected adversary paths

Design Tasks:

- Sensitivity analysis for component performance characteristics
- Sensitivity analysis for component placement

The concept of a critical path is important for path models. A critical path is an adversary path for which path models predict lower physical protection performance than for any other path of a given set. In general, it is not feasible to identify a critical path from among all paths. However, if attention is limited to paths representing a limited set of scenarios, e.g., forcible entry, it is often possible to identify a path which is critical with respect to a particular system performance parameter. Identifying critical paths can, at this time, only be accomplished with complex graph-theoretic techniques and only for relatively simple, easily calculated system performance parameters.

No matter how complex the path model, the basis of the model usually lies in a comparison between (1) the time required for an adversary to carry out his plan and (2) the time required for the protective force to respond and to interrupt the progress of the adversary. Adversary task time or delay which occurs before detection is not accounted for in this comparison since response by the protective force begins only with the first detection event.

Figure 5-3 illustrates this comparison. The baseline event sequence represents successive delays or the times required for the adversary to traverse the segments of his path and to perform tasks required along the way. The adversary path in this example ends at time t_c , at which point the adversary would complete his plan (at least those portions which the physical protection system is designed to prevent). The inverted triangle at time t_o signifies the time of a reliable detection. The time interval between t_o and t_c , shown by the dashed line, represents the time during which the protective force must respond and interrupt the adversary to prevent success of the adversary's plan.

Figure 5-3. Time Comparisons

The usefulness of path models based on this time comparison in conducting sensitivity analysis is also illustrated in Figure 5-3. The effect of decreasing the time necessary for response and interruption can be determined with reference to the baseline event sequence. If response time can be reduced to less than the interval from t_o to t_c , then the physical protection system can, in principle, cope with the adversary path under study. This conclusion depends, of course, on the proper

function of the detection, communication, delay, and response elements, as well as on the ability of the protective force to neutralize the adversary once an interruption has been achieved. The second time axis in Figure 5-3, labeled "Event Sequence with Earlier Detection," illustrates the effect of modifying the physical protection to achieve an earlier detection. In this case, more time is made available for response. The third axis in the figure, labeled "Event Sequence with Additional Delay After Detection," shows another modification which allows for a longer response time. This case illustrates the effect of physical protection measures which impose additional delay on the adversary beyond the point in his path where detection occurs.

The time lines depicted in Figure 5-3 are a simplification of the way in which more sophisticated path models represent component and system performance. Figure 5-4 provides a summary account of the key features of path-level models which have been used extensively for physical protection system evaluation.

Model Name	Model Type	Primary System Performance Parameter	System Functions Modeled				
			Detection	Delay	Communication	Response	Neutralization
EASI ¹ (Estimate of Adversary Sequence Interruption)	Analytical	Probability of Interruption	X	X	X	X	
FESEM ² (Forcible Entry Safeguards Effectiveness Model)	Simulation	Probability of System Win	X	X	X	X	X
ISEM ³ (Insider Safeguards Effectiveness Model)	Simulation	Probability of System Win	X	X	X	X	X

Figure 5-4. Path-Level Model Summary

Scenario- or strategy-level models have the advantage of dealing with a level of the threat structure which contains far fewer entities than the path level. For this reason, it is possible to achieve a fuller comprehensiveness in evaluations of performance against all available adversary attacks. This advantage is enhanced by the fact that most adversary scenarios appear to be constructed from a large but limited set of generic adversary actions and decisions. Disadvantages of scenario-level models include (1) difficulty in incorporating time factors directly into the model and (2) a need for additional selected path-level model application for sensitivity analysis. Table 5-II summarizes the evaluation tasks that scenario- or strategy-level models are especially suited for.

TABLE 5-II
Summary of Evaluation Tasks
Appropriate for Scenario-Level Models

System Assessment Tasks:

- Verify existence of positive measures to accomplish required physical protection functions
- Select critical paths

Design Tasks:

- Formulate system concept
- Identify role and performance requirements for components

The fault tree concept has been productively applied to the development of scenario-level models. Fault tree analysis (or, more generally, logic tree analysis) consists, briefly, of decomposing an undesired event into its antecedent or component events. Fault trees were originally developed for application to reliability and safety analyses. Their application to physical protection provides a formalism for many intuitive ideas and principles. Because many physical protection fault trees contain a large number of events and their logical relationships, this formalism also provides the analyst with powerful tools for manipulating and resolving complex interactions among events.

Fault tree representations admit both qualitative and quantitative analysis techniques. To date, both types of analyses have been applied to physical protection fault trees. Major examples of the application of qualitative techniques are presented in later sections. Quantitative techniques include the Adversary Sequence Diagram model,⁴ a model of potential vulnerability to collusion by insiders,⁵ and a soon-to-be-published users manual for the fault tree analyst on SETS.⁶

EVALUATION TECHNIQUES

Practical evaluations of physical protection systems usually involve the application of several models in stages. As a general rule, evaluation begins at the scenario or strategy level and proceeds with the analysis of selected adversary paths. Figure 5-5 presents a map of how this progression fits into the process of physical protection system concept formulation. This pattern will be followed in the subgroup working sessions of the training course.

This pattern can also be adapted to facility inspection and vulnerability assessment. In this case, the final step in the diagram (concept formulation) would be replaced by a step comparing estimated system performance to standards or criteria set in an earlier phase of the evaluation process.

Whether the aim of the evaluation process is concept formulation or assessment, the starting points are threat analysis and facility characterization. The purpose of threat analysis is to identify the range and combination of threat

Figure 5-5. Progressive Steps in the Process of Physical Protection System Concept Formulation

attributes, motivation, and modus operandi against which physical protection system performance is to be evaluated. Facility characterization includes both the identification of adversary target areas (vital areas, material access areas, etc.) and the characterization of distinct facility operational states. Performance criteria may be stated in terms of threat analysis and facility characterization.

This first application of evaluation tools in Figure 5-5 (logic tree analysis) is qualitative and is performed at the scenario or strategy level. In concept formulation, this step has, as its output, the rough outline or functional outline of the physical protection system concept. In facility assessment, the output of this stage will be a first-order estimate of potential system vulnerabilities.

The second step in applying evaluation tools in Figure 5-5 (path analysis) consists of the quantitative analysis of system performance against selected adversary paths. At this step, the concept formulation process progresses by sensitivity analyses of generic component features and configurations. The facility assessment process is refined at this step, and potential vulnerabilities identified in the preceding step are either verified or refuted.

REFERENCES

1. EASI Program Improvements for HP-67 and TI-59 Calculators, SAND78-0506, Sandia Laboratories, Albuquerque, New Mexico, July 1978.
2. Users Guide for Evaluating Alternative Fixed-Site Physical Protection Systems Using "FESEM", SAND77-1367, Sandia Laboratories, Albuquerque, New Mexico, November 1977.
3. Insider Safeguards Effectiveness Model (ISEM) Users Guide, SAND77-0043, Sandia Laboratories, Albuquerque, New Mexico, November 1977.
4. A Systematic Approach to the Conceptual Design of Physical Protection Systems for Nuclear Facilities, HCP/DO77-01, DOE/OSS, Washington, DC, May 1978.
5. A Method for Determining the Susceptibility of a Facility to Sensor System Nullification by Insiders, SAND77-1916C, Sandia Laboratories, Albuquerque, New Mexico, February 1978.
6. A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, Sandia Laboratories, Albuquerque, New Mexico, November 1978.

MODULE 5

SESSION 5.1

VISUALS

NOTES

ADVERSARY'S
INTENT

STRATEGY

SCENARIO

PATH

VISUALS

NOTES

Summary of Evaluation Tasks Appropriate for Path Level Models

System Assessment Tasks:

- Demonstrate vulnerability along a particular path
- Analyze performance against critical adversary paths
- Evaluate system against preselected adversary paths

Design Tasks:

- Sensitivity analysis for component performance characteristics
- Sensitivity analysis for component placement

Model Name	Event Type	Primary System Performance Parameter	Series Function Model				
			Detection	Alarm	Communication	Response	Interception
Fig. 1 (Sensitivity of Primary Performance Parameter)	Detection	Probability of Interception	1	1	1	1	1
Fig. 2 (Sensitivity of Primary Performance Parameter)	Alarm	Probability of Alarm	1	1	1	1	1
Fig. 3 (Sensitivity of Primary Performance Parameter)	Communication	Probability of Communication	1	1	1	1	1
Fig. 4 (Sensitivity of Primary Performance Parameter)	Response	Probability of Response	1	1	1	1	1
Fig. 5 (Sensitivity of Primary Performance Parameter)	Interception	Probability of Interception	1	1	1	1	1

VISUALS

NOTES

Summary of Evaluation Tasks Appropriate for Scenario-Level Models

System Assessment Tasks:

- Verify existence of positive measures to accomplish required physical protection functions
- Select critical paths

Design Tasks:

- Formulate system concept
- Identify role and performance requirements for components

5.0 EVALUATION TECHNIQUES

Session Title: 5.2 Introduction to Logic Symbols Date: Tuesday, 7 November

Presented By: W. Paulus, Sandia Laboratories Time: 1030 to 1130

Session Objectives:

After the session, the participants will be able to

1. Identify the symbols used in logic trees,
2. Explain the function of an AND gate and an OR gate,
3. Identify the three kinds of basic events,
4. Identify an end event, and
5. Explain the transfer operation.

Summary:

Symbols which are used in logic trees are defined. The function of the AND gate, OR gate, and transfer operation are explained. The three primary events and the end event are defined.

INTRODUCTION TO LOGIC SYMBOLS

The logic tree is an important tool used to evaluate the effectiveness of physical protection of nuclear facilities and materials. The purpose of the logic tree is to describe all of the ways that an adversary can achieve his objective by defeating elements of a physical protection system. Each act against a physical protection system that an adversary must perform to achieve his objective is called an event. In a logic tree, these events, which are represented by special symbols, are logically connected. In order to use logic trees, it is necessary to understand the individual parts of the tree and the symbols used in the composition of the trees. Figure 5-6 illustrates the symbols that are used for logic trees.

Figure 5-6. Sample Logic Tree Which Shows Various Symbols Used

Each event has a written description which is contained in a rectangular symbol in the logic tree diagram. The description of the topmost event in Figure 5-6 is "Defeat Perimeter Boundary Undetected." A smaller rectangle, which is placed immediately under the description, is used to provide the event name. For example, S is the name of the topmost event shown in Figure 5-6. Event names are usually brief and are formed from combinations of letters and numbers. Event names are used in the computer processing of logic trees.

The symbol which appears below the event name is used to designate either how that event is logically related to other events or how well the causes of the event are known. Two kinds of logic gates, the AND gate and the OR gate, are used in the logic trees. Gates must have at least two inputs and may or may not have an output. Inputs enter the bottom of the gate, while outputs exit the top of the description rectangle above the gate. If the gate for a particular event has no output, it is called an end event. The objective of the adversary is always the end event of a logic tree. The logic trees which are described in this module each have only one end event, the topmost event of the tree. In Figure 5-6, S is the end event. The shape of the AND gate is a round arch with a flat bottom (see Figure 5-7). For an adversary to accomplish the event described above the AND gate, the adversary must accomplish all of the events which provide an input into the AND gate. If the physical protection system can prevent any one of the input events, the adversary is prevented from accomplishing the event described above the AND gate. For example, suppose event 1 is defined by an AND gate whose inputs are events 2, 3, and 4. Event 1 will occur if and only if event 2 and event 3 and event 4 all occur. Figure 5-7 summarizes the properties of the AND gate.

For the logic tree shown in Figure 5-6, event S will occur only if event S1 (Avoid Personnel Undetected), event S2 (Penetrate Boundary Undetected), and event S4 (Avoid or Confront Patrol Guards Undetected) all occur. The adversary can penetrate a boundary without being detected only by accomplishing all three of the tasks associated with events S1, S2, and S4; i.e., (1) by avoiding accidental detection by personnel, (2) by physically surmounting the boundary undetected by elements of the physical protection system which are designed to detect an intrusion, and (3) by avoiding detection by patrol guards.

Adversary must accomplish all events input to the gate
Preventing any one input event defeats the adversary.

Event 1 occurs if event 2 and event 3 and event 4 occur.

Figure 5-7. Example of an AND Gate

The shape of the OR gate is a pointed arch with a curved bottom (see Figure 5-8). For an adversary to accomplish the event described above the OR gate, the adversary need only accomplish any one (or more) of the events which provide input into the OR gate. The physical protection system must prevent all of the input events in order to prevent the adversary from accomplishing the event described above the OR gate. For example, suppose event 1 is defined by an OR gate whose inputs are events 2, 3, and 4. Event 1 occurs if any one of events 2, 3, or 4 occurs. Figure 5-8 summarizes the properties of the OR gate. For the logic tree shown in Figure 5-6, event S2 (Penetrate Boundary Undetected) will occur if either event S3 (Defeat Boundary Barriers Undetected) or event S5 (Defeat Boundary Emergency Exits Undetected) occurs. Thus, the adversary can penetrate a boundary without being detected in either of two ways: (1) by undetected passage through an emergency exit or (2) by undetected penetration of the barriers which comprise the boundary.

Adversary has alternative ways to achieve success.

All events input to the gate must be prevented.

Event 1 occurs or event 2 or event 3 or event 4 occur.

Figure 5-8. Example of an OR Gate

An event which is defined by a logic gate must have two or more inputs. A gate with only one input is prohibited. Events which do not have an input are called primary events; they represent the causes of the end event. A logic tree is a logical combination of primary events. Three types of primary events are distinguished by the symbol which appears immediately below the name of the primary event: the basic event, the undeveloped event, and the developed event.

The basic event is symbolized by a circle. A basic event can be understood and evaluated qualitatively or quantitatively, depending on the purpose of the analysis, without breaking the event into causes or cases. In Figure 5-6, event S1 (Avoid Personnel Undetected) is the only basic event. It is reasonable to call S1 a basic event because an analyst would only be asked to evaluate one possibility:

Can an adversary avoid facility personnel without being detected? Event S1 can be contrasted with event S4, which is not a basic event. For event S4, the analyst is asked to evaluate whether the adversary can avoid or confront patrol guards without being detected. It is also reasonable to call S1 a basic event because it is judged that except for an accident it would be easy for an adversary to accomplish S1. There is no significant benefit to be derived from including in the logic tree those events that describe the various unlikely circumstances by which an adversary could avoid detection by nonsecurity personnel.

The undeveloped event is symbolized by a diamond. An undeveloped event is an event whose causes are insufficiently understood to be included in the logic tree. It is not possible to say whether an undeveloped event could be adequately treated as a basic event. The conclusions drawn from the analysis of a tree which contains an undeveloped event are tentative and subject to revision if the effects of the undeveloped event are included in the analysis. In Figure 5-6, event S5 (Defeat Boundary Emergency Exits Undetected) is the only undeveloped event. This event is considered an undeveloped event since all of the various kinds of emergency exits have not been studied. Also, there is no information by which the logic tree could show how all of the types of emergency exits could be defeated without the adversary's being detected.

The developed event is symbolized by two concentric diamonds. A developed event is an event whose causes have been shown in another logic tree.* The developed event is used as a convenience. For example, a full logic tree for physical protection studies might be quite large in size and contain a considerable number of events. However, in order to become familiar with the type of information contained in the tree, it is sufficient to examine only the uppermost parts of the tree. In this case, many events could be deleted from the tree and numerous logic gates would be replaced by undeveloped events. The resultant tree would be similar to the tree shown in Figure 5-6 and could be printed on a small piece of paper.

The transfer operation is represented by an upright triangle. Since many logic trees expand greatly from left to right across a page during development of the tree, it might be necessary to disconnect the development of an event and place it at a more convenient position on the page. To relate the event and its development, since they are not connected by a line, the transfer symbol is used. An example of the transfer symbol is shown in Figure 5-9. The tree shown on the left is equivalent to the tree shown on the right; however, the lefthand tree contains no transfer symbol. In the righthand tree, the development of event 8 is transferred so that it is centered directly below event 2. Note that event 8 is shown twice in this tree: once in the tree whose development is truncated by the transfer and once at the top of the subtree that develops event 8. In general, an event may occur at several places in a logic tree, and the common development of that event

*In the other logic tree, the event would be generated by a logic gate, so it would have inputs. It would not be a developed primary event.

may be transferred. The development will appear only once on the page. The number 2 which appears below the transfer symbol and to the left of event 8 is the name of the event for which event 8 is an input. In general, there will be a list of every event to which the transferred event is an input.

Figure 5-9 Example of Transfer Symbols

Adversary must accomplish all events input to the gate
Preventing any one input event defeats the adversary.

Event 1 occurs if event 2 and event 3 and event 4 occur.

VISUALS

NOTES

Adversary has alternative ways to achieve success.

All events input to the gate must be prevented.

Event 1 occurs or event 2 or event 3 or event 4 occur.

Transfer Symbols show connections that are not drawn directly among events of the Logic Tree.

5.0 EVALUATION TECHNIQUES

Session Title: 5.3 Introduction to
Logic Trees

Date: Wednesday, 8 November

Presented By: W. K. Paulus, Sandia
Laboratories

Time: 1330 to 1430

Session Objectives:

After the session, the participants will be able to

1. Discuss why logic trees are used,
2. Discuss an efficient analysis technique,
3. List three questions regarding a potential adversary which must be answered,
4. List the 13 types of generic logic trees,
5. Select a logic tree to analyze a zone, and
6. Read a logic tree.

Summary:

The following topics as they relate to logic trees are discussed:

1. Why qualitative evaluation of logic trees is used,
2. Definitions of terminology,
3. The design/analysis cycle,
4. Analysis techniques,
5. Information required about the adversary and the site,
6. The zone,
7. Functions of a physical protection system,
8. Types of logic trees,
9. Selection of logic trees,
10. Reading a logic tree,
11. Fitting a generic logic tree to a particular facility, and
12. Evaluation of a physical protection system.

INTRODUCTION TO LOGIC TREES

Logic trees may be used by managers, designers, and analysts to plan and evaluate the physical protection of nuclear facilities and materials. A qualitative estimate of the effectiveness of a physical protection system and a list of physical protection weaknesses can be obtained through the use of logic trees. Qualitative analysis answers the question, "How effective is the physical protection system?" with either of two responses: "The system is not effective," or "The system is likely to be effective." This information can be used to establish the need for redesign and, together with cost data, to accept or reject system designs.

The topics included in this introduction to logic trees are

1. Why qualitative evaluation of logic trees is used,
2. Definitions of terminology,
3. The design/analysis-cycle,
4. Analysis techniques,
5. Information required about the adversary and the site,
6. The zone,
7. Functions of a physical protection system,
8. Types of logic trees,
9. Selection of logic trees to analyze a zone,
10. Reading logic trees,
11. Fitting a generic logic tree to a particular facility, and
12. Evaluation of a physical protection system.

The method of constructing logic trees is not explained. The necessary logic trees are supplied with this text or as an appendix.

The technique of qualitative analysis using logic trees is illustrated by the example of a nuclear power generating station which requires protection against sabotage of its vital components by outsiders. The technique and the logic trees that are provided have been applied to other parts of the fuel cycle and to attacks which have theft of nuclear materials as their objective.

Two important preparatory steps for qualitative analysis using logic trees have been discussed in previous modules. First, targets for sabotage have been identified by vital area location analysis. Second, a spectrum of threats has been discussed against which the power station may require protection. This information will be used as it is needed.

WHY QUALITATIVE EVALUATION OF LOGIC TREES IS USED

Several techniques for analyzing physical protection systems have been developed, but qualitative evaluation using logic trees is especially suitable as an introductory technique. The effectiveness of the total physical protection

system is analyzed. The technique is general, not specialized. Any sort of interaction between adversary and physical protection system can be analyzed by qualitative techniques, though with less detail than is provided by quantitative techniques. Some other techniques have relatively limited applications, being most useful in the study of particular tactics or objectives of attack.

Qualitative evaluation can be performed quickly through the use of logic trees. During this training course, 6 hours have been scheduled for the evaluation of a total system design for a simplified hypothetical facility. Although evaluation of a real facility would take a greater amount of time, all the steps of analysis can be experienced through this example analysis of the hypothetical facility. Because there is not enough time during this course to collect background information, this information will be provided. Session 5.2 on logic tree symbols and this session on logic trees contain all the specialized material needed for this qualitative analytic technique.

Qualitative analysis of logic trees is accomplished entirely by the activity of the analyst. He is required to think about the interactions between the physical protection system and the adversary. He must be more than a mere collector of the data that is input to a computer. In addition, it is not necessary to spend time to learn the capabilities and limitations of computerized models so that simulation results can be correctly understood. Finally, if the analyst finds that he wishes to use another technique to obtain quantitative results or to study a special situation in greater depth, logic trees can be used in preliminary screening to select attack scenarios for quantitative analysis.

DEFINITIONS OF TERMINOLOGY

There are several words that are frequently used in the discussion of logic trees and their applications. These words, listed alphabetically, and their definitions follow:

- Adversary--An adversary is an individual or group of individuals who attempts theft of special nuclear materials or radiological sabotage.
- Communication--Communication is the function of transmitting or interchanging information, in particular, the signals or messages used to summon security personnel who are intended to neutralize the adversary.
- Deceit--Deceit is the tactic by which an adversary misleads elements of the physical protection system into perceiving improper conditions, such as a faked badge or hidden explosives, as proper conditions.
- Delay--Delay is the function of impeding an adversary's progress.
- Detection--Detection is the function of determining that an unauthorized action is occurring or has occurred. Detection includes sensing of the unauthorized action, communication of an alarm to a control center, and assessment of the alarm.
- Elements--A physical protection system is a composite entity, and elements are its distinct parts. Physical protection elements have the same name as the physical protection functions which they implement. (See Table 5-VI for the list of functions and examples of the elements which implement them.)

TABLE 5-VI

Physical Protection System Elements and Functions

Function	Example Elements
Detection	
a. Sensor	Fence disturbance sensor Identity check Metal detector Microwave
b. Assessment (real time)	Guard patrol Television
c. Alarm/display	Television Warning lights/sounds
d. Track	Guard in a tower Radar
Delay	Television Barrier Distance of travel
Communication	Radio Telephone
Response	Guards Police

- Force--Force is the tactic by which an adversary commits overt aggressive actions in order to overcome elements of the physical protection system; the adversary expects to be detected and is prepared to defend against the response.
- Functions--The functions of a physical protection system comprise the group of related actions which together make up the performance of the physical protection system; the functions are detection, delay, communication, and response. (See Table 5-VI.)
- Insider--An insider is a person authorized to enter a protected area or a vital area; insiders include employees, contractors, service personnel, and visitors.
- Outsider--An outsider is a person who is not authorized to enter a protected area or a vital area.
- Positive Features--Positive features are physical protection elements that have predictable levels of performance. The performance of an element which has positive features will not deteriorate abruptly or unpredictably should the severity of the attack be increased by a small amount. There are four methods of implementing or recognizing positive features in a facility design.
 1. Implement a function with at least two elements so that loss of one element will not cause complete loss of the function,
 2. Select an element to block as many kinds of attack as possible,
 3. Use elements which have complementary strengths together. (For example, a microwave intrusion sensor and a seismic intrusion sensor have complementary strengths. The microwave device can sense an intrusion made using a bridge or ramp to isolate the intruder

from the seismic sensor. The seismic device can sense an adversary who is crawling on the ground to avoid the microwave beam which is aimed high to avoid false alarms.)

4. Simple redundancy can be used for reliability. (The use of two seismic intrusion sensors is an example of simple redundancy.)

 - Response--Response is the function of reacting, especially by security personnel, to the detection of an unauthorized act to prevent the adversary success.
 - Stealth--Stealth is the tactic by which an adversary seeks to avoid or inactivate elements of the physical protection system; the adversary attempts to prevent detection.
 - Tactics--Tactics are the methods used by the adversary to achieve his objectives. (See also Deceit, Force, and Stealth.)

DESIGN/ANALYSIS CYCLE

Analysis of the effectiveness of the physical protection of nuclear facilities and materials is part of the cycle of design and analysis shown in Figure 5-10.

Figure 5-10. Design Analysis Cycle

The cycle begins with the initial design of a physical protection system. Then the qualitative effectiveness of the physical protection system is analyzed against a range of threats. The result of the analysis answers the question, "Is the physical protection system adequate or inadequate?" If the physical protection system is found to be adequate, the design/analysis cycle ends. If the system is found to be inadequate, it must be redesigned. Weak points identified by the analysis are the parts of the design which must be improved. The design/analysis cycle is closed by analysis of the redesigned system. The cycle is repeated until an adequately effective design is achieved. The credibility of the improvements to the design of the physical protection system is enhanced by the fact that their impact on total system performance has been analyzed.

ANALYSIS TECHNIQUE

The analysis technique has four major parts. Instructions on how to perform the four parts of physical protection analysis follow.

First, define the general problem. This requires collection of information about the spectrum of potential adversaries and about the site. Based on the design of the physical protection system, identify the zones of the site where the system and the adversaries may interact. Then, select the logic trees needed to trace the interactions between system and adversary.

Second, select a specific problem for analysis. This requires that one adversary be selected from the spectrum of potential adversaries. Next, choose the zone and logic trees most appropriate to the selected adversary's attack. It is not easy to design a physical protection system that is both practical and effective against a well-trained, well-equipped threat consisting of several individuals. A suggested practice is to begin the analysis with an adversary rated near the weak end of the threat spectrum. This type of analysis has relatively few complications and can be done quickly. If the initial design for this analysis fails, relatively little effort has been used to establish that there is a need for improvement. Analysis of a redesigned system can reasonably begin with the least severe threat that caused failure of the previous design. If the system passes the test of a weak threat, the second analysis can use a threat from the strong end of the spectrum. If the design also passes this test, little effort has been used to test the entire threat spectrum. If the design fails the test of a strong threat, try a threat from the middle of the spectrum. A search strategy such as this can avoid a lengthy series of analyses where severity of threat is increased or decreased steadily by small amounts to cover the full spectrum.

Third, perform the qualitative analysis using logic trees. There are three questions to ask in conjunction with the use of logic trees:

1. Does the physical protection system include all of the necessary functions? If not, name the missing functions.
2. Do the functions operate against all attacks that the design threat can mount? If not, identify which functions have weaknesses and the attacks for which they are subject to failure.

3. Do the physical protection elements have positive features? If not, list the deficiencies. If better positive features are known, list them.

Fourth, select another specific problem for analysis. This requires selection of another tactic for the same adversary, or the selection of another adversary. Then return to the third part of the analysis.

The analysis is complete when the design of the physical protection system is shown to be adequate after having been tested against the most severe attack which can be mounted by the spectrum of potential adversaries. The evaluation must be repeated for each operational state of the facility. If the design fails the test, the analyst has the option of improving the design by addressing only those weak points which were involved in the failure identified or else continuing the analysis to find other possible weak points that were not tested by the case that first exposed a potential system failure. The latter procedure should make the redesign more efficient.

INFORMATION REQUIRED ABOUT THE ADVERSARY AND THE SITE

Information must be collected to answer three questions about the adversary:

1. What class of adversary must be addressed?
2. What are the adversary's capabilities?
3. What are the variables of the adversary's plan of attack?

Adversaries can be put into one of three classes: (1) outsiders, (2) insiders, and (3) outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be analyzed. In this text, the examples involve the outsider adversary.

Important capabilities of the adversary include such items as his knowledge of the physical protection system, level of motivation, skills that would be useful in the attack, speed with which the actions that make up the attack are carried out, and ability to carry tools and weapons. Since it is not generally possible to test and evaluate the capabilities of a known adversary, the analyst must make assumptions about the adversary. These assumptions can be based on published information about human performance and tested vulnerability of physical protection elements.

Knowledge of the physical protection system can be gained in many ways. Fences, lights, some sensors and assessment devices, guard posts, and patrol schedules are among the objects that can be directly observed from outside a protected site. Visitors may be able to observe some indoor system elements such as door switches, space alarms, and perhaps a security control center. Insiders would be able to gather extensive information over an extended period of time. They may obtain system plans; they may be part of the system. Obtaining extensive knowledge of the physical protection system through the collusion of insiders is a major benefit to outsiders. Even without deliberate, conscious collusion, the outsider may gain extra information from conversation with insiders. And information may be available in public documents. Finally, an adversary can benefit from

general knowledge of commercial security practices and hardware. The analyst should be cautious in assuming that any aspect of the physical protection system would not be known to an adversary.

The level of the adversary's motivation seems likely to be high. An attack on a nuclear facility is an unconventional act clearly associated with great hazards. It seems plausible that an unusually strong motivation would be required to initiate the attack. To the extent that deterrence to initiating an attack is high, it will also be difficult to discourage the adversary from continuing the attack once begun.

The skills useful in the attack can be determined from the analyst's knowledge of the properties of the protection elements. Lacking identifiable individual adversaries, it is impractical to catalog their skills. Judgements about the likely size of an attack force may be made by the analyst from a list of special skills that are not likely to be possessed by a single individual.

The speed with which any step in an attack is carried out will vary. For example, where several tests of the same activity have been performed, such as climbing over a particular type of fence, the results give a minimum time, a maximum time, and an average time. When these data are available, the analyst needs a rationale for the selection of a particular time within the range. In an adversary group not rated for top performance and essentially untrained, speed would vary from one individual to another and from one task to another. The simplest assumption would assign average speed for all tasks. If the group of adversaries is assumed to consist of individuals selected for high potential performance and if they are well-trained, the analyst may assign maximum speed for all tasks.

The capacity to carry tools and weapons can be set at a nominal level. For example, the analyst may assume that an adversary could carry an 18-kg (40-pound) load in a hiker's backpack. For a particular attack, the analyst can keep track of the necessary tools and weapons. As the accumulated weight or volume exceeds 18 kg (40 pounds) and hence is no longer portable, the carrying capacity of additional adversaries or vehicles is required.

Variables of the adversary's plan of attack include such items as the environment and weather chosen for the attack, the mode and speed of travel, the number of adversaries, the operational state of the facility, the path taken to reach the target(s), the time of day, the tools carried, and the weapons carried.

Mode of travel may be by foot, boat, ground vehicle, or aircraft. Speed of travel may be significant after detection of the attack when a response force is moving as quickly as possible to intercept the attackers.

Number of adversaries is a variable that could allow for a diversionary attack or specialized tasks such as explosive demolition, disablement of electronic

equipment, a driver, a battle specialist, etc. A small number of attackers may be preferable where stealth or deceit are the principal tactics used and avoidance of detection is important.

Operational states of the facility include the normal work shifts, the number of operational employees and guards working each shift, and the locations in a facility where these individuals are situated. Emergency states such as a fire, a radiation leak, or other abnormal conditions may be used to advantage by the adversary and, in fact, the adversary may even cause a fire alarm or a radiation alarm.

Several paths to the targets of the attack may exist. The adversary would choose the path which he perceives as being the most advantageous to him. Time of day may also be an important factor. At night, darkness provides cover for attackers. In addition, detection systems may not be operated in some locations at all times.

The tools used by an attacker may include lock picks, ladders, cutting torches, wire cutters, explosives, and many others. Tools may be required to penetrate barriers, to disable detection elements, to jam communications, or to commit sabotage. Weapons, if they are used, range from the very simple to the very powerful. A club, a handgun, an automatic rifle, a shotgun, etc., can be used to combat the response of a physical protection system. These tools can also be used to disable equipment such as lights or cameras.

Information must be collected about the site as well as about the adversary. The types of information needed include plans of buildings, climate, type of construction, site layout, targets, and terrain. The analyst must have this information in order to evaluate the effectiveness of the physical protection system as it interacts with the adversary.

THE ZONE

A defense zone is a space which surrounds but is not necessarily occupied by one or more targets and within which any attack is first detected and ultimately terminated by the physical protection system before an adversary can accomplish his goal. The initial boundary of a zone is the envelope of first potential detection of the adversary. The final boundary of a zone is the envelope of termination of the adversary's attack.

A zone of defense surrounding a site may be visualized as a shell that surrounds and protects the targets. The shell may be thin or thick (the thickness need not be uniform) depending on the space needed to terminate an attack. The zone extends into the air above the site to detect attacks mounted from the air. The zone also extends underground beneath the site to detect tunneling attacks.

An attack by outsiders may require a zone as far removed from the targets as possible. An attack by insiders may require more than one zone very close to the targets, perhaps coinciding with the targets themselves.

FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

In this section, some notes are collected on how the defense zone relates to the four functions (detection, delay, communication, and response) of a physical protection system.

Detection

The zone begins with a detection boundary because the physical protection system cannot begin to oppose an attack until the attack has been detected. Detection might be desired within the zone as well as at a boundary to provide information on the location of the attackers until they are intercepted by a response force. Detection must occur within the zone, but some detection elements may not be located in the zone. An example is monostatic radar which can detect at a distance, and which need not be installed within the zone in order to participate in the detection of intruders within the zone. Outsiders should be detected at the outer boundary of the zone. Some tactics require that detection elements should also operate within the zone. Outsiders attacking by deceit or stealth might not be detected at the outer boundary of the zone, depending on the effectiveness of the detection elements and the adversary's skill.

Delay

Delay must follow detection and occur within the zone. To provide for alarm assessment, attackers must be prevented from moving too quickly away from the place where they caused an alarm. A barrier is necessary to provide this delay.

The time after detection required by the attackers to reach their target must be at least as long as the time required for the physical protection system (1) to communicate with a response force, (2) to mobilize, transport, and deploy the response force, and (3) to intercept and halt the progress of the attackers. One or more barriers may be necessary to slow the attackers sufficiently to give the physical protection system time to respond effectively.*

Communication

Communication is the function which unites all the physical protection elements into a system. Sensors communicate with alarms or displays. The control center communicates with patrol guards, guards in observation posts, and other response forces. The response force has internal communications. Control signals may be communicated to lights, gates, television cameras, etc. The communication network need not lie entirely within the zone. Communication reliability must be very high.

Response

Response is the function of intercepting the attackers and halting their progress before their goal is achieved. The response element (response force) may be stationed inside or outside the zone, but the response force must carry out its function within the zone.

*See the Barrier Technology Handbook, SAND77-0777, for a description of the effectiveness of various barriers against attack.

TYPES OF LOGIC TREES

Thirteen logic trees are available for applying the evaluation technique presented in this section. All of these trees have one characteristic in common. They are all generic logic trees; therefore, each logic tree can be applied to any site. The way in which the generic logic trees are applied to a site is the subject of a later session of this module. For the purpose of this session, it is necessary only to realize that no more than 13 trees are needed for qualitative analysis of any site.

The 13 trees cover 5 kinds of actions that an adversary may perform. Each kind of action is developed on a set of generic logic trees. In each set, there is one tree for each adversary tactic by which the action can be accomplished. The complete list of generic logic trees is given in Table 5-VII.

TABLE 5-VII
Generic Logic Trees

<u>Name (Tactic-Application)</u>	<u>Kind of Action Developed</u>
FORCE-BOUNDARY STEALTH-BOUNDARY DECEIT-BOUNDARY	Penetrate protected boundary
FORCE-AREA STEALTH-AREA DECEIT-AREA	Travel across protected area
FORCE-BUILDING STEALTH-BUILDING	Enter building ^a
FORCE-ACQUIRE SNM ^b STEALTH-ACQUIRE SNM DECEIT-ACQUIRE SNM	Acquire special nuclear materials
FORCE-RELEASE STEALTH-RELEASE	Cause a release of special nuclear materials ^c

^aTo enter a building by deceit, use the DECEIT-BOUNDARY tree.

^bSNM--Special nuclear materials

^cNo known method causes a release of special nuclear materials by deceit.

The five kinds of actions are (1) penetrate a protected boundary, (2) travel across a protected area, (3) enter a building, (4) acquire special nuclear materials, and (5) cause a release of special nuclear materials. Each action, with two exceptions, can be accomplished by the use of deceit, force, or stealth. The exceptions involve deceit. The tree DECEIT-BOUNDARY satisfactorily describes how an adversary might enter a building by deceit; therefore, no DECEIT-BUILDING tree exists. No method has been found to cause a release of special nuclear materials by deceit; therefore, no DECEIT-RELEASE tree exists. Attacks resulting in a release of special nuclear materials must be analyzed with either the FORCE-RELEASE tree or the STEALTH-RELEASE tree.

SELECTION OF LOGIC TREES FOR ZONE ANALYSIS

Since a zone is a space in which the interactions between the adversary and the physical protection system occur, analysis of those interactions by means of generic logic trees requires selection of the correct logic trees to describe the actions which can occur within the zone. Before that can be done, the zone must be described. The description should be done during design when the performance goals for the physical protection system are set. The location of the zone depends on the threat, its tactics, and its objective.

Outsiders must attempt to penetrate the site from the outside, whatever their objective may be. The initial boundary of the zone (the envelope of first potential detection) can reasonably be placed near (at or within) the property line of the site. Detection would be undesirable where the public could not be prohibited since alarms would be generated by innocent bypassers as well as by adversaries. In these circumstances, an adversary could only be identified as such if he were detected while committing an unauthorized act.

The final boundary of the zone (the envelope of termination of the attack) may not exist, i.e., the zone would not be hollow. For example, this can happen when the objective is sabotage. The physical protection system might be designed to accumulate enough delay for a response force to intercept the adversary by requiring the adversary to sequentially disable several targets but not enough to achieve his overall sabotage objective. But if an effective response can more quickly intercept the adversary, it may be reasonable, for example, to prevent him from entering the building that houses his target(s). In this case, the outside of the building may be specified as the final boundary of the zone.

If theft is the object of an attack, the boundary at which the adversary is halted by a response force as he is making his escape with nuclear materials can be the property line of the site which is virtually the same as the boundary for first detection. If the goal of the design of the physical protection system is to prevent the adversary from acquiring nuclear materials, the final boundary may be placed at the outside of any building that houses targets.

Insiders can only be detected as adversaries when they commit an unauthorized act. The initial boundary should be placed where the first unauthorized act could occur.

Once the boundaries of the zone are established for the postulated threat, the generic logic trees needed for analysis can be selected. For the example of sabotage by outsiders, assume that the design of the physical protection system has established the initial boundary of the zone at the property line of the site, rising to a detection "roof" above the ground and descending to a detection "floor" below ground. Assume that the final boundary coincides with the outer walls, roof, and foundation of the hypothetical pressurized water reactor buildings.

The attackers would first penetrate the initial boundary. This action would be analyzed with the three boundary trees. All three boundary trees (DECEIT-BOUNDARY, FORCE-BOUNDARY, and STEALTH-BOUNDARY) must be used since the outsiders have a choice of tactics at this and every step of their attack. Between the initial boundary and the final boundary, the outsiders must travel across open terrain. This action would be analyzed with the three area trees (DECEIT-AREA, FORCE-AREA, and STEALTH-AREA). At the final boundary, it is possible that the delay needed by the physical protection system to interrupt the attack and terminate it will be provided by the barrier of the building structure. The two building trees (FORCE-BUILDING and STEALTH-BUILDING) must be used, and the DECEIT-BOUNDARY tree must be used again, this time to analyze entry into the building.

If the design of the physical protection system is found to be adequate through the use of these trees that describe actions within the zone, there is no need to analyze the release trees. If the design is shown to be inadequate, the analyst might relocate the final boundary. The analyst could use and reuse whatever generic logic trees are needed to describe interactions between the adversary and the physical protection system as the adversary attacks the smaller sets of vital components. The design of the system may prove adequate to protect the facility from a release of nuclear materials even though it could not terminate the attack as quickly as desired. It then becomes an option of the redesign either to move the final boundary of the zone or to improve the physical protection system. Of course, if the release cannot be prevented, there is no choice but to redesign the system.

Assuming that the analyst evaluates the physical protection of the vital components themselves, what additional generic logic trees would be analyzed? For example, assume that the adversary chooses to damage the reactor vessel itself so that adequate cooling to avoid a meltdown is impossible. The adversary must enter the reactor containment to reach the reactor vessel, as shown in Figure 5-11. He might choose to penetrate from the outside directly into the containment through the wall. This would require the use of force, or he might choose to enter the auxiliary building, perhaps by the door close to the personnel hatch of the containment. This might be accomplished by any of the three tactics. Either penetration of the auxiliary building or the containment structure is already subject to analysis with the last trees mentioned above (FORCE-BUILDING, STEALTH-BUILDING, and DECEIT-BOUNDARY). From this point on, new analysis is required. This procedure is as follows. First, trace the adversary through the personnel hatch. After that, his path involves the same trees as he moves to his target within the containment structure. From the door of the auxiliary building to the personnel hatch, the adversary must travel across an area. The generic logic trees, DECEIT-AREA, FORCE-AREA, and STEALTH-AREA, are analyzed again. Their first analysis involved travel outdoors; this time the travel is within a building. Quite different elements of a physical protection system may be involved in the two situations. Nevertheless, the same generic trees are suitable in both situations.

**PRESSURIZED WATER REACTOR
COMPOSITE PLAN GROUND LEVEL**

Figure 5-11.

The adversary's entry into the containment through the personnel hatch (a device designed as an airlock) is analogous to entering a building through a vestibule. This implies that the logic trees to analyze are DECEIT-BOUNDARY, FORCE-BUILDING, and STEALTH-BUILDING. Travel through the containment structure to the location from which the reactor vessel can be sabotaged is analyzed with the DECEIT-AREA, FORCE-AREA, and STEALTH-AREA trees. Finally, the sabotage itself is analyzed with the RELEASE-FORCE and RELEASE-STEALTH trees. Table 5-VIII contains a summary of the trees selected in this example.

TABLE 5-VIII
Generic Logic Trees Used to Analyze an Attack by Outsiders
on a Simplified Pressurized Water Reactor

Action	Trees
WITHIN ZONE	
Penetrate initial boundary	DECEIT-BOUNDARY FORCE-BOUNDARY STEALTH-BOUNDARY
Travel to reactor buildings	DECEIT-AREA FORCE-AREA STEALTH-AREA
Enter auxiliary building or containment	DECEIT-BOUNDARY FORCE-BUILDING STEALTH-BUILDING
OPTIONAL ANALYSIS OF VITAL COMPONENT SABOTAGE	
Travel to personnel hatch	DECEIT-AREA FORCE-AREA STEALTH-AREA
Enter containment through personnel hatch	DECEIT-BOUNDARY FORCE-BUILDING STEALTH-BUILDING
Travel through containment to location for sabotage	DECEIT-AREA FORCE-AREA STEALTH-AREA
Commit sabotage leading to core meltdown and release of nuclear materials	FORCE-RELEASE STEALTH-RELEASE

READING LOGIC TREES

Before the logic trees are used, their content and the method of reading them are presented. Figure 5-12 shows a simplified version of the generic logic tree, STEALTH-BOUNDARY. There are 10 primary events (S3, S5, S8, S9, S10, S11, S12, S22, S97, and S98). These can be divided into two groups. One group concerns the adversary's need to get across the boundary (S5, S8, S9, S10, S11). The other group concerns the adversary's need to remain undetected while the boundary crossing is made (S3, S12, S22, S97, S98).

Physically, crossing a boundary is easy unless one or more barriers are present. Thus, the primary events for boundary crossing relate to barriers that must be overcome. The qualitative question to ask is, "Can the adversary overcome the barrier?" The answer is generally "yes", if the adversary is suitably skilled and equipped. The analyst must have a particular threat in mind if qualitative analysis of these events is to be meaningful.

The quantitative question to ask is, "How much time will the adversary use to overcome the barrier(s)?" This time is the delay provided by the barrier(s). If the adversary is not permanently stopped by some barrier within the zone, it will be necessary to perform a quantitative analysis, using the task times of the data, to estimate whether a response force can intercept the adversary in time to prevent him from achieving his objective. See Session 5.5 for an explanation of Estimate of Adversary Sequence Interruption (EASI).

The logic tree assumes the boundary has two parts. In one part, crossings are made normally, i.e., through a gate or portal (see event S5); in the other, crossings are prohibited, i.e., everywhere other than a gate or portal (see events S8, S9, and S10). These two parts of the boundary should present different problems to the adversary.

The elements of the physical protection system at the gate or portal are not named in event S5. It is the analyst's job to supply these elements from the design which he is evaluating. However, S5 is a developed event; it is further developed on the complete generic logic tree, STEALTH-BOUNDARY. That development is ignored in this discussion.

The generality of these logic trees implies not only their applicability to virtually any nuclear site but also the kind of unspecific event description typified by S5. To enumerate every possible element of a gate or portal and to perform similar enumerations for other events would make the logic trees excessively large and unwieldy. Continuing advances in the technology of physical protection systems would rapidly make an exhaustively developed tree obsolete. If general event descriptions are used and the analyst is relied upon to know the state of the act, the need to alter the generic logic trees should rarely arise and the magnitude of the task is kept relatively small.

GENERIC LOGIC TREE

Penetrate boundary by STEALTH

Figure 5-12. STEALTH-BOUNDARY

Along the boundary elsewhere than at the gates or portals, one kind of element is so frequently used that it is specified by the development of S4. That element is a fence or two fences with a cleared space between them (S8, S9, S10). All other possible kinds of barriers (including any which impede an attack from aboveground or underground) are covered by event S11.

The adversary will remain undetected while crossing the boundary unless detection elements are present. Thus, the primary events for detection relate to detection elements that must be avoided or disabled. The qualitative question to ask is, "Can the adversary almost always avoid or disable the detection elements without an alarm being generated?" To answer "no," the analyst must be convinced that the detection elements are positive features of the physical protection system. The detection elements must operate under virtually any attack that the assumed threat can mount. Data from field tests of performance and vulnerability could provide persuasive support to design claims of effectiveness. To answer "yes," the analyst must find the detection element consistently vulnerable to an attack within the capability of the assumed threat.

The quantitative question to ask is, "What is the probability that the adversary will be detected as he crosses the boundary?" If the adversary is not permanently stopped by some barrier within the zone, it will be necessary to perform a quantitative analysis, using these probabilities of detection among the data.

The logic tree indicates that three kinds of elements detect boundary crossings. One kind is located at entrances (S5, a developed event). No examples are named on the simplified logic tree. One or more guards posted at the entrance would be commonly used. But guards alone may not be a positive feature for detection.

A second kind of element senses along the boundary but not necessarily at entrances (S12, a developed event). No examples of the sensors are named on the simplified logic tree. A combination of sensors may be used. The analyst's job is to evaluate whether the combination produces a positive feature for detection.

The third kind of element operates anywhere along the boundary, both at and away from entrances (S3, S22, S97, S98). Guards on patrol or stationed in observation towers are one example (S97, S98). These would be a trained part of the physical protection system. If they alone could not be positive features for detection, they may reinforce the other kinds of detection elements to produce positive features.

The two events that name guards as detection elements list two ways that an adversary may not be detected. He can avoid being seen by the guards (S97; or, if he is seen, he may be able to prevent the guards from sounding an alarm (S98). While the latter method of avoiding detection may be forceful rather than stealthy, it represents an action required of the adversary if he is to continue his attack by stealth, undetected, after he accidentally confronts a guard. In general, the

adversary will probably be able to see where patrol guards are and cross the boundary when they are absent and unable to see the adversary. It may be difficult for an adversary to know whether or not he is being seen from an observation tower or to prevent the sounding of an alarm if he knows that he has been seen.

Operations personnel may be nearby and see the adversary when he crosses the boundary (S22). The adversary should be able to avoid them. Confrontation would be an unintended complication of an attack by stealth, and it may increase the chance of being seen by a guard in an observation tower.

Reinforcements for the security force (S3) would be called only after detection. The time between notification of the security force and its arrival could be long enough to prevent the force from intercepting the adversary during the boundary crossing that gave rise to the detection. Thus, this event may have no relevance for the crossing of the initial boundary of the zone. It may be meaningful with respect to crossing a boundary within the zone after detection had occurred.

Having examined all primary events on the simplified logic tree, the logic by which the primary events generate the end event is now examined. The adversary must cross the boundary and he must avoid detection while doing so. This is the fundamental logical statement made in the logic tree. All other detail merely elaborates on the possibilities. The fundamental logical statement is made by AND gate S. The input for crossing the boundary comes from event S1. All three other inputs (S2, S3, S22) supply requirements for avoiding detection by the elements that can operate anywhere on the boundary, regardless of where the crossing is made. The elements that detect only at entrances or only away from entrances must be associated with those optional locations for crossing the boundary.

The optional crossing locations are inputs S4 and S5 to OR gate S1. Crossing the boundary at an entrance (S5) is a developed primary event. But crossing the boundary away from an entrance (S4) is generated by an AND gate which repeats the fundamental logical statement of the logic tree. Crossing the boundary away from an entrance requires that four events (S8, S9, S10, S11) be performed. These four events are inputs to AND gate S4. Avoiding detection during the crossing is represented by the single developed event S12, which is an input to AND gate S4.

One other development appears on the tree. Event S2, "Avoid or Confront Guards Undetected," states an option. The necessary logic is an OR gate, S2, with inputs S97 and S98. This same sort of option is implied for S3 and S22, both undeveloped events. Their developments would have the same logical form as the development of S2.

Figures 5-13 through 5-19 are simplified logic trees for crossing boundaries by other tactics (force or deceit), traveling across areas by force or stealth, and entering a building by force or stealth. These trees and all of the complete generic trees can be examined in the same manner as the simplified version of STEALTH-BOUNDARY.

GENERIC LOGIC TREE

Penetrate boundary by FORCE

Figure 5-13

GENERIC LOGIC TREE

Penetrate boundary by DECEIT

Figure 5-14

GENERIC LOGIC TREE

Penetrate boundary by DECEIT

Figure 5-15

GENERIC LOGIC TREE

Cross Area by STEALTH

Figure 5-16

GENERIC LOGIC TREE

Cross area by FORCE

Figure 5-17

GENERIC LOGIC TREE

Enter building by STEALTH

Figure 5-18

GENERIC LOGIC TREE

Enter building by FORCE

Figure 5-19

FITTING A GENERIC LOGIC TREE TO A PARTICULAR FACILITY

Not every event in the generic logic trees will be relevant to the physical protection system for a particular facility. Before the facility can be analyzed, the tree must be modified to accurately reflect the facility and its physical protection system. Using Figure 5-12, assume that the physical protection system design being analyzed includes only one fence. Keep event S8 (outer fence) but delete (cross off) events S9 (inner fence) and S10 (area between fences). Assume that no provision has been made in the design to delay underground or air attacks and that the single fence is the only barrier in the design. Delete S11 (other barriers). The result is that AND gate S4 has only two inputs, S8 (outer fence) and S12 (defeat or bypass sensors). If previous detection cannot be assumed, delete S3 (avoid or confront reinforcements). Modify each logic tree needed to analyze the zone similarly.

EVALUATING A PHYSICAL PROTECTION SYSTEM

Using the logic trees to evaluate a physical protection system is a logically simple procedure. The difficult task for the analyst is deciding whether the design of the physical protection system has positive features that will prevent an adversary from accomplishing a particular event. Making that decision is beyond the scope of this session. The logical evaluation is presented.

Every event in the generic logic trees describes an action which an adversary may perform to achieve the end event of the tree. Qualitatively evaluate each primary event in the tree. The important question is, "Can the adversary accomplish the event, yes or no?" The remaining analysis is done quickly and follows simple rules. Examine all events that input to a gate. If the gate is an OR gate, the adversary need only accomplish one of the input events to accomplish the event generated by the OR gate. If the gate is an AND gate, the adversary must accomplish every input event to accomplish the event generated by the AND gate. To keep track of the adversary's accomplishments and failures, place an "X" on the output line from each event which cannot be accomplished. When all events at the bottom level of the tree have been evaluated, all the necessary information has been generated to apply the logical rules to the gates at the next higher level of the tree. Complete one level before moving up to a higher level. Continue until the gate which generates the end event has been evaluated. The result has been obtained for one tree, the tree for crossing a boundary by stealth.

It is necessary to similarly analyze FORCE-BOUNDARY and DECEIT-BOUNDARY since the adversary has the option of using any tactic. Only if all adversary tactics fail has the physical protection system succeeded.

By countering the threat spectrum the physical protection system meets the defined performance criteria.

VISUALS

NOTES

Physical Protection System Elements and Functions

Function	Example Elements
Detection:	
a. Sensor	Fence disturbance sensor Identity check Metal detector Microwave
b. Assessment (real time)	Guard patrol Television
c. Alarm/display	Television Warning lights/sounds
d. Track	Guard in a tower Radar
Delay	Television Barrier Distance of travel
Communication	Radio Telephone
Response	Guards Police

VISUALS

NOTES

Generic Logic Trees

Name (Tactic-Appliation)	Kind of Action Developed
FORCE-BOUNDARY STEALTH-BOUNDARY DECEIT-BOUNDARY	Penetrate protected boundary
FORCE-AREA STEALTH-AREA DECEIT-AREA	Travel across protected area
FORCE-BUILDING STEALTH-BUILDING	Enter building ^a
FORCE-ACQUIRE SNM ^b STEALTH-ACQUIRE SNM DECEIT-ACQUIRE SNM	Acquire special nuclear materials
FORCE-RELEASE STEALTH-RELEASE	Cause a release of special nuclear materials ^c

^a To enter a building by decont. use the DECEIT-BOUNDARY tree.

^b SNM--Special nuclear materials

^c No known method causes a release of special nuclear materials by decont.

Figure 1-1

Generic Logic Trees Used to Analyze an Attack by Outsiders on a Simplified Pressurized Water Reactor

Action	Trees
WITHIN ZONE	
Penetrate initial boundary	DECEIT-BOUNDARY FORCE-BOUNDARY STEALTH-BOUNDARY
Travel to reactor buildings	DECEIT-AREA FORCE-AREA STEALTH-AREA
Enter auxiliary building or containment	DECEIT-BOUNDARY FORCE-BUILDING STEALTH-BUILDING
OPTIONAL ANALYSIS OF VITAL COMPONENT SABOTAGE	
Travel to personnel hatch	DECEIT-AREA FORCE-AREA STEALTH-AREA
Enter containment through personnel hatch	DECEIT-BOUNDARY FORCE-BUILDING STEALTH-BUILDING
Travel through containment to location for sabotage	DECEIT-AREA FORCE-AREA STEALTH-AREA
Commit sabotage leading to core meltdown and release of nuclear materials	FORCE-RELEASE STEALTH-RELEASE

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

5.0 EVALUATION TECHNIQUES

Session Title: 5.4 Introduction to the EASI Model Date: Thursday, 9 November
Presented By: C. E. Olson, Sandia Laboratories Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. List four advantages and three limitations of the EASI model,
2. Set up input for EASI analysis when given an adversary path into a facility, and
3. List sources of input data required for EASI analysis.

Summary:

This session will present a discussion of the application of EASI to a path-analysis evaluation. It will begin with a method for listing the required input data and proceed through a discussion of the sources of the data and interpretation of the results.

Additional Resource Materials:

SAND78-0506, EASI Program Improvement for HP-67 and TI-59 Calculators

INTRODUCTION TO THE EASI MODEL

THE MODEL

Estimate of Adversary Sequence Interruption (EASI) is a simple, path-level analytical model of physical protection system performance in carrying out the detection, communication, delay, and response functions. Because of the simplified closed-form estimation approach, EASI can be programmed and run on a hand-held programmable calculator.

In order for theft or sabotage attempts to be defeated, the response force must be notified of the attempt while sufficient time remains for that force to respond and interrupt the adversary prior to the completion of the theft or sabotage. An adversary interruption occurs if the adversary is confronted by a response force large enough to prevent the adversary from proceeding further along his path. The physical protection functions of detection, communication, delay, and response, which contribute to the likelihood of adversary interruption, are represented in the EASI model.

Table 5-IX summarizes the relative advantages of EASI compared to other path-level models and to scenario-level models. The advantage of a simple model like EASI in performing sensitivity analyses of component performance and placement should be noted.

TABLE 5-IX
EASI Analysis

ADVANTAGES:	<ul style="list-style-type: none">• Physical protection system interactions and time tradeoffs• Relatively uncomplicated, numeric technique• Illustrates vulnerability quantitatively• Sensitivity analysis
LIMITATIONS:	<ul style="list-style-type: none">• Analyses only single path• Difficult to show lack of vulnerability• Simplified model of detection, assessment communication, time, and response• Neutralization not modeled

THE INPUT

In the EASI model, input parameters representing the physical protection functions of detection, communication, delay, and response are required. Detection, communication, delay, and response are required. Detection and communication inputs are in the form of probabilities that the function will be performed

successfully. Delay and response inputs are in the form of mean times and standard deviations. All inputs refer to a specific adversary path which must be chosen by the analyst.

Detection

The EASI input for the detection function is the probability of detection (P_D) for each sensor encountered by an adversary. P_D is a product of the following three factors:

1. Probability that the detector will sense abnormal or unauthorized activities,
2. Probability that this indication will be transmitted to an evaluation or assessment point, and
3. Probability that a valid signal will be declared valid when processed and evaluated.

In EASI the alarm assessment function is modeled as a part of the detection function. In addition to P_D , the time required for detection and alarm assessment is accumulated as part of the input for response time. Table 5-X suggests several possible sources for realistic input values of P_D . The value of P_D must lie between zero and one.

TABLE 5-X
Detection in the EASI Model

INPUT:	• Probability of detection (P_D)
SOURCES:	• Intrusion Detection Systems Handbook
	• Local tests
	• Data from similar installations
	• Vendor performance specifications
	• Performance requirements
APPLICATION:	• Vary P_D to bracket realistic values

Communication

The communication of an alarm to the response force is represented in EASI by the input parameter probability of communication (P_C). In most physical protection systems, the likelihood of successful communication to the response force increases with time. The time interval corresponding to the value of P_C input to EASI is accumulated as part of response time. Table 5-XI notes potential sources for P_C . As in the case of P_D , it is recommended that a range of values of P_C be used in successive EASI runs to cover all values of P_C that might be obtained under realistic conditions.

TABLE 5-XI

Communication in the EASI Model

INPUT:	• Probability of communication (P_C) (within time limits)
SOURCES:	• Local tests • Data from similar communications systems
APPLICATION:	• Vary P_C to bracket realistic values • Time required is part of response time

Delay

The time required by an adversary to traverse a given path can be thought of as the sum of times required to perform certain tasks or traverse distinct path segments. In general, it is not possible to predict the exact time interval necessary for the adversary to perform these tasks or proceed across these path segments. In EASI these successive times are modeled as random variables possessing an average or mean value and a finite standard deviation. For the sake of simplicity, both task times and traversal times are referred to as adversary task times. The adversary path is divided into segments so that time-consuming tasks and path-segment crossings can be represented by successive time intervals on the adversary time axis. The lengths of each of these successive adversary task times are input to EASI as mean time and standard deviation. The model assumes that the successive adversary task times are independent random variables. Table 5-XII summarizes some possible sources for estimates of the mean and standard deviations of adversary task times.

TABLE 5-XII

Delay Time in the EASI Model

INPUT:	• For each adversary task: Average time (T_i) Standard deviation (σ_{T_i})
SOURCES:	• <u>Barrier Technology Handbook</u> • Limited local tests

Response

Response is modeled in EASI by the time between the generation of an alarm signal by a sensing device and the confrontation of the adversary by a response force adequate to halt the progress of the adversary along the path. This time consists of the following five successive time increments:

1. Time required for alarm assessment,
2. Communication time,

3. Time required for the response force to prepare, e.g., to gather arms, to start vehicles, etc.,
4. Response force travel time, and
5. Time required for the response force to muster and deploy.

Input is in the form of a single mean time and standard deviation representing the sum of the five increments. The model assumes that the response time (T_R) and the adversary task times following receipt of the alarm signal are independent random variables. T_R is assumed to have a Gaussian or normal distribution. Table 5-XIII summarizes T_R inputs.

TABLE 5-XIII

Response Time in the EASI Model

INPUT:	<ul style="list-style-type: none"> • Response time (T_R) • Standard deviation (σ_{T_R})
SOURCES:	<ul style="list-style-type: none"> • Local analysis and tests • Response time includes: <ol style="list-style-type: none"> 1. Alarm assessment time 2. Communication time 3. Guard preparation time 4. Guard travel time 5. Guard muster/deploy time
APPLICATION:	<ul style="list-style-type: none"> • Vary T_R and σ_{T_R} to bracket realistic values

Figure 5-20 shows how the results of response force tests might be presented. The figure presents the results of four hypothetical response exercises, two during normal hours and two during off hours.

A convenient format for organizing the input to EASI is illustrated in Figure 5-21. The inverted triangles on the example adversary time sequence represent points at which the adversary's actions may trigger detection sensors. The symbols $E(t_i)$ and $\sigma(t_i)$ represent the mean and standard deviation of adversary task times. The T_R axis is sometimes an aid in estimating mean response time.

THE OUTPUT

The output of the EASI model is an estimate of the probability that the response force will interrupt the adversary at some point before the adversary completes acts of theft or sabotage. This parameter is referred to as probability of interruption (P_I). It does not include an estimate of the likelihood of adversary neutralization.

Because of the simplifications inherent in the way in which physical protection system functions are modeled in EASI, it is common practice to vary one or more of the EASI input parameters. Through these repeated calculations, it is

Figure 5-20. Example of Response Time Test Results

ADVERSARY TIME-SEQUENCE PATH (EXAMPLE ONLY)

Figure 5-21. EASI Input Organization

possible to estimate the effect on P_I of variations in component performance. An example of the results of such a sensitivity analysis is presented in Figure 5-22. The figure shows P_I versus T_R for two hypothetical systems. The figure also illustrates the usefulness of EASI in estimating the relative performance achievable by major system changes (upgraded system) for a specific adversary path.

Figure 5-22. Sample Plot of the Effect of Component Performance Variation on P_I

Since the EASI model is path-specific, it is difficult to establish the adequacy of system performance in interrupting the adversary using only this model. Conversely, if EASI calculations show a low P_I the physical protection system is likely to be judged vulnerable to adversary attack along the path analyzed.

ESTIMATE OF ADVERSARY SEQUENCE INTERRUPTION (EASI)

• PURPOSE

TO PROVIDE A SIMPLE, EASY TO USE METHOD TO EVALUATE
PHYSICAL PROTECTION SYSTEM PERFORMANCE.

• METHOD

PROBABILISTIC ANALYSIS OF THE INTERACTIONS OF BASIC
PHYSICAL PROTECTION FUNCTIONS WITH GUARD RESPONSE
TIME.

• EQUIPMENT

PROGRAMMABLE CALCULATOR.

EASI ANALYSIS

ADVANTAGES

- PHYSICAL PROTECTION SYSTEM INTERACTIONS AND
TIME TRADEOFFS
- RELATIVELY UNCOMPLICATED, NUMERIC TECHNIQUE
- ILLUSTRATES VULNERABILITY QUANTITATIVELY
- SENSITIVITY ANALYSIS

LIMITATIONS:

- ANALYSES ONLY SINGLE PATH
- DIFFICULT TO SHOW LACK OF VULNERABILITY
- SIMPLIFIED MODEL OF DETECTION, ASSESSMENT
COMMUNICATION, TIME, AND RESPONSE
- NEUTRALIZATION NOT MODELED

ASSUMPTIONS

- Response force is adequate to stop adversary
progress until additional forces arrive to
neutralize the adversary.
- The response time and the time remaining in
the adversary action sequence when the alarm
occurs are independent variables.
- The time to perform each task in the adversary
action sequence is an independent variable.

VISUALS

NOTES

DETECTION

DEFINITION: The discovery of any adversary action.

MEASURES: Probability of Detection.

- (1) Probability that the detector will sense abnormal activities.
- (2) Probability that this indication will be transmitted to an evaluation point.
- (3) Probability that a valid signal will be so declared.

The time delay between detection sensing and communicating the information to the response force.

COMMUNICATIONS

DEFINITION: THE ACT OF INFORMING THE LOCAL SECURITY RESPONSE FORCE OR THE LOCAL LAW ENFORCEMENT AGENCY OR BOTH OF AN ADVERSARY ACTION.

MEASURES: PROBABILITY OF COMMUNICATION.

TIME REQUIRED TO COMMUNICATE.

DELAY

DEFINITION: A MEANS TO IMPEDE ADVERSARY PROGRESS, USUALLY TO BUY TIME TO EFFECT A ...

MEASURES: TIME REQUIRED TO PERFORM EACH ADVERSARY TASK--BARRIER PENETRATIONS, TRANSIT BETWEEN BARRIERS AND OTHER SUCH TASKS.

VISUALS

NOTES

SYSTEM RESPONSE

DEFINITION: ACTION TAKEN BY THE SECURITY FORCES
(ON-SITE AND/OR OFF-SITE) TO PREVENT
ADVERSARY SUCCESS.

MEASURES: TIME REQUIRED TO IMPLEMENT ACTION

- (1) TIME TO RECEIVE A SENSOR WARNING
- (2) TIME TO ASSESS THE WARNING
- (3) TIME TO COMMUNICATE ALARM TO
RESPONSE FORCE
- (4) TIME FOR RESPONSE FORCE TO PREPARE
AND TRAVEL
- (5) TIME TO MUSTER AND DEPLOY

ADVERSARY SEQUENCE INTERRUPTION* -

A CONFRONTATION BETWEEN THE RESPONSE
FORCE AND THE ADVERSARY

NEUTRALIZATION -

RENDERING AN ADVERSARY INEFFECTIVE,
UNABLE TO COMPLETE THE ACTION SEQUENCE

* ASSUMPTION - RESPONSE FORCE IS ADEQUATE TO
DELAY ADVERSARY PROGRESS UNTIL ADDITIONAL
FORCES ARRIVE TO NEUTRALIZE THE ADVERSARY

VISUALS

NOTES

ADVERSARY TIME-SEQUENCE PATH (EXAMPLE ONLY)

SYSTEM RESPONSE TIME

VISUALS

NOTES

EASI TECHNIQUE

THE STEPS IN USING THE EASI MODEL TO EVALUATE A PHYSICAL PROTECTION SYSTEM ARE:

- SELECT AN ADVERSARY ACTION SEQUENCE (BASED ON LOGIC TREE ANALYSIS, CRITICAL JUDGMENT, INSIGHT INTO FACILITY OPERATIONS . . .)
- SELECT A PHYSICAL PATH CORRESPONDING TO THE ACTION SEQUENCE
- DETERMINE LOCATIONS OF SENSORS AND TIME-CONSUMING ADVERSARY TASKS ALONG THE PHYSICAL PATH
- OBTAIN DATA FOR THE PROBABILITIES OF DETECTION AND COMMUNICATIONS AS WELL AS THE MEAN AND STANDARD DEVIATION OF EACH ADVERSARY TASK AND OF THE SECURITY SYSTEM RESPONSE TIME
- PERFORM CALCULATIONS TO OBTAIN PROBABILITY OF INTERRUPTION

5.0 EVALUATION TECHNIQUES

Session Title: 5.5 Hand-Held Calculator Operation

Date: Thursday, 9 November

Presented By: P. Robertson, Sandia Laboratories

Time: 0930 to 1030

Session Objectives:

After the session, the participants will be able to

1. Enter a program from a magnetic card into the calculator memory,
2. Enter data into the operating program, and
3. Run the program and obtain correct results based on the input data.

Summary:

Texas Instruments TI-59 calculators will be distributed along with the Estimate of Adversary Sequence Interruption (EASI) program which is stored on magnetic cards. The participants will be instructed on how to load the program, enter data, and operate the program.

HAND-HELD CALCULATOR OPERATION

Today, hand-held calculators are available which make it easy to use mathematics to handle the problem situations which arise in many professional fields. For example, probability computations can be performed with speed, accuracy, and confidence by means of one of these programmable calculators. The Texas Instruments model TI-59 calculator can be used to compute the probability of interrupting an adversary before the objective is reached. After the calculator has been programmed and certain data entered, the computation is performed automatically. Here is a sample of the procedure used with the TI-59.

SAMPLE PROCEDURE

Power On

The ON/OFF switch is located on the display end of the calculator. When this switch is in the ON position, a "0" should appear in the display. This shows that the battery is charged and that the calculator is ready for operation. If the power switch is turned off and then on again, the calculator is cleared completely.

When the battery is fully charged, the calculator will operate for 2 to 3 hours before recharging is necessary. A weak battery affects all calculator operations adversely. A weak battery is indicated by a dim, erratic, or blank display or by the running of the card drive motor. The alternating current adapter/charger should be connected to the calculator whenever the battery is nearly discharged. The calculator can be operated indefinitely with the adapter/charger connected.

Display Check

After the calculator is turned on, the decimal point $\boxed{.}$ and the change sign $\boxed{+/-}$ keys should be pressed, then the $\boxed{8}$ key should be pressed repeatedly until the display is filled. The minus sign and the decimal point stay to the left of the number in the display. If the display is operating correctly, there will be ten 8's in the display with the decimal point and the minus sign to their left.

Clear Entry Key

If an incorrect entry is made into the keyboard, the entry can be cleared (erased) by pressing the $\boxed{CE}$ key. A flashing display indicates that the calculator has been asked to do a task it cannot perform or that the limits of the display have been exceeded. A flashing display is stopped by pressing the $\boxed{CE}$ key.

General Clear Key

The **CLR** key clears all calculations in process and clears the display, including stopping a flashing display. This key, however, does not affect the program or the memory contents. The **CLR** key does not have to be used after the performance of calculations ending in the **=** key. After using the **=** key, the calculator displays the answer and is ready to start a new problem.

Dual Function Keys

Most of the keys have two functions. The first function is printed on the key. The second function is written immediately above the key. The function shown on the key is performed by pressing the desired key. The second function is performed by pressing the **2ND** key and then pressing the key immediately below the desired second function. For example, to use the **A** key, only the appropriate key is pressed. To use the **A'** key, the **2ND** and then the **A** key are pressed. If the **2ND** key is pressed by mistake, it returns to the first function if it is pressed again.

User Keys

The keys across the top of the calculator labelled A through E and A' through E' are the user keys. These keys are used to enter data into the calculator programs. For example, a program may require the entry of "response time." This entry is made on the display by pressing the keyboard number keys of the desired number. It is entered into the program by pressing the **B'** key, that is, **2ND**, then **B**.

Calculator Memory Partitioning

When the calculator is turned on, there are 60 registers reserved for data storage and 480 locations reserved for program steps. Some programs require different combinations. For example, the Estimate of Adversary Sequence Interruption (EASI) program requires 90 memory locations. Thus, the calculator memory must be repartitioned by pressing **9** **2ND** **OF** **1** **7**. The display will then contain 239.89, which indicates that there are 240 program-step locations and 90 memory registers.

If the calculator memory is not partitioned properly and attempts are made to read a program card that requires a different partitioning, the display will flash. A flashing display after an attempt to read a card means that the card has not been read.

Reading Program Cards

The program to be used with the TI-59 calculator is written on a magnetic card. This program requires that the calculator be repartitioned as indicated in the previous paragraph, i.e., by pressing keys **9** **2ND** **OF** **1** **7**. After the calculator is correctly partitioned, the **CLR** key is pressed. Then, with the program card held by the edges and the magnetic side of the card facing down, the program card is inserted into the card slot on the right side of the calculator. The card is pushed into the slot gently but firmly and released when the drive motor pulls

the card in. The reading program card will pass through the calculator and come out on the left side. If the card has been read, a "1" will appear in the display. If the display is flashing, the **CLR** key should be pressed and card insertion tried again.

Estimate of Adversary Sequence Interruption Program Use

The Estimate of Adversary Sequence Interruption (EASI) program uses all of the user-defined keys. The following inputs or function are performed by the indicated user keys.

- A'** Probability of communication, P_C
- B'** Time required for response, T_R
- C'** Standard deviation of response time, σ_{T_R}
- D'** Number of tasks along path being analyzed
- E'** Program initialization, i.e., reset to begin a new problem
- A** Probability of detection of a task, P_D
- B** Time required for an adversary task, T_i
- C** Standard deviation of an adversary task, σ_{T_i}
- D** Number of a task to be changed
- E** Execution of the computation

The program card is entered into the small window below the display and serves as a memory aid for the entry of data. The lower indication on the card is for the normal function and the upper indication is for the second function. For example, P_D is entered into the **A** key and P_C is entered into the **A'** key (see Figure 5-23).

1		TEXAS INSTRUMENTS		1	
EASI				9 OP 17 (239.89)	
P_C	T_R	σ_{T_R}	NO. TASKS	INITIALIZE	SECOND FUNCTION
P_D	T_i	σ_{T_i}	CHANGE NO.	EXECUTE	
					NORMAL FUNCTION

Figure 5-23. Estimate of Adversary Sequence Interruption (EASI) Program Card

Testing the Program

The program and calculator can be tested for proper functioning by entering the data as shown in Table 5-XIV. If the program is functioning properly, the display should show the indicated number.

TABLE 5-XIV
Testing the Program

Step	Data	Key(s) Pressed (in order)	Display
1	Turn on TI-59 calculator		0
2	Repartition memory	[9] [2ND] [OP] [1] [7]	239.89
3	Enter program card	[CLR]	1
4	Initialize program	[2ND] [E]	0
5	$P_C = 0.9$	[.] [9] [2ND] [A]	0.9
6	$T_R = 2$ minutes	[2] [2ND] [B]	2.
7	$\sigma_{T_R} = 0.2$ minute	[.] [2] [2ND] [C]	0.(4
8	Tasks = 1	[1] [2ND] [D]	1.
9	$P_D = 0.9$	[.] [9] [A]	0.9
10	$T_1 = 5$ minutes	[5] [B]	5.
11	$\sigma_{T_1} = 0.5$ minute	[.] [5] [C]	0.5 momentarily, then 1.
12	Execute computation of the probability of interrup- tion	[E]	.8099375572

Example

The path chosen for analysis is shown in Figure 5-24 and has the following sequence:

1. The adversary penetrates the boundary fence, T_1 , crosses the area between the fence and the main building, T_2 and T_3 , and reaches the locked exterior rear door.
2. While outside, the adversary is subject to surveillance by closed-circuit television sensor 1.
3. After penetrating the exterior door, T_4 , sensor 2, the adversary continues along a corridor to another locked interior door, T_5 .
4. The adversary penetrates this locked door, T_6 , sensor 3, and enters the room containing the vital components, T_7 .

Figure 5-24. Adversary Sequence

The adversary time-sequence path (in minutes) is shown in Figure 5-25.

Figure 5-25. Adversary Time-Sequence Path

The probability of communication, P_C , equals 0.9. The response time, T_R , is 4.0 minutes with a standard deviation, σ_{T_R} , of 0.16 minute.

With the given input information, the estimate of adversary interruption is calculated by following the steps in Table 5-XV.

TABLE 5-XV

Calculation of the Estimate
of Adversary Interruption

Step	Procedure	Key(s) Pressed (in order)	Display
1*	Turn on TI-59 calculator		0
2	Repartition memory	9 2ND OP 1 7	239.89
3	Enter program card	CLR	1
4	Initialize program	2ND E'	0
5	Enter probability of communication, P_C	. 9 2ND A'	0.9
6	Enter expected response time, σ_{TR}	4 2ND B'	4.
7	Enter standard deviation of response time, σ_{TR}	. 1 6 2ND C'	0.0256
8	Enter number of events, No.	7 2ND D'	1.
9	Enter P_D^{**} , for task 1	0 A	0. (No detector)
10	Enter task time of task 1	2 B	2.
11	Enter standard deviation of task 1, σ	. 5 C	0.5 momentarily, then 2.
12	Enter P_D of task 2	0 A	0.
13	Enter task time of task 2, T_2	1 B	1.
14	Enter standard deviation of task 2, σ_2	. 2 C	0.2, then 3.
15	Enter P_D of task 3	. 3 A	0.3
16	Enter task time of task 3, T_3	1 B	1.
17	Enter standard deviation of task 3, σ_3	. 2 C	0.2, then 4.
18	Enter P_D of task 4	0 A	0.
19	Enter task time of task 4, T_4	3 B	3.
20	Enter standard deviation of task 4, σ_4	. 3 C	0.3, then 5.
21	Enter P_D of task 5	. 9 7 A	0.97
22	Enter task time of task 5, T_5	. 5 B	0.5

*If the Estimate of Adversary Sequence Interruption (EASI) program has already been entered, begin with Step 4.

**Probability of detection.

TABLE 5-XV. (Continued)
Calculation of the Estimate
of Adversary Interruption

Step	Procedure	Key(s) Pressed (in order)	Display
23	Enter standard deviation of task 5, σ_5	[.] [1] [C]	0.1, then 6.
24	Enter P_D of task 6	[0] [A]	0.
25	Enter task time of task 6, T_6	[3] [B]	3.
26	Enter standard deviation of task 6, σ_6	[.] [3] [C]	0.3 then 7.
27	Enter P_D of task 7	[.] [5] [7] [A]	0.97
28	Enter task time of task 7, T_7	[.] [1] [B]	0.1
29	Enter standard deviation of task 7, σ_7	[.] [0] [2] [C]	0.2, then 7.
30	Execute computation	[E]	.3517906773

According to the calculations in Table 5-XV, the probability of intercept is 0.35. Momentary, intermediate results are shown which give the contribution of sensor 3 and sensor 2, in that order. If desired, these intermediate calculations can be displayed by pressing the R/S key when they appear in the display. If the R/S key is pressed again, the computation will continue.

Data Changes

If the first sensor were replaced by an improved closed-circuit television system having automatic alarm features with a probability of detection of 0.8, the data changes in Table 5-XVI are made.

TABLE 5-XVI
Data Changes for First Modification

Step	Procedure	Key(s) Pressed (in order)	Display
1	Change desired in task 3	[3] [D]	3.
2	P_D of task 3 to be changed	[0] [.] [8] [A]	0.8
3	Execute computation	[E]	.7513683248

Thus, the change in probability of detection gives a new probability of intercept of 0.75.

Now, if sensor 1 is changed back to the original $P_D = 0.3$ but the response time, T_R , is reduced to 2 minutes with a standard deviation of 0.16 minute, the new solution is found as indicated in Table 5-XVII.

TABLE 5-XVII

Data Changes for Second Modification

Step	Procedure	Key(s) Press (in order)	Display
1	Change in task 3	[3] [D]	3.
2	Change P_D , task 3	[.] [3] [A]	0.3
3	Change T_R to 2	[2] [2ND] [B]	2.
4	Change the standard deviation of T_R to 0.16	[0] [.] [1] [6] [2ND] [C]	0.0256
5	Execute computation	[E]	0.91 (rounded off)

Therefore, changing the system's response time from 4 minutes to 2 minutes increases the probability of adversary interruption from 0.35 to 0.91 along this adversary path.

Data Recall

To display the data currently stored for a particular task (task 7, for example), the steps in Table 5-XVIII are followed.

TABLE 5-XVIII

Recall of Stored Data

Step	Procedure	Key(s) Pressed (in order)	Display
1	Step of data desired	[7] [D]	7
2	Display P_D	[R/S]	0.97
3	Display T_7	[R/S]	0.1
4	Display T_7	[R/S] *	0.02

1. If the [R/S] key is inadvertently pressed again, a flashing zero is displayed. Pressing the [CE] key corrects the error and allows the procedure to be continued.
2. The stored value of P_C can be recalled by pressing [RCL] [0] [7] ; T_R by pressing [RCL] [0] [5] ; and σ_R by pressing [RCL] [0] [6] [√x].

SESSION 5.5

VISUALS

NOTES

<div> <div>1</div> <div> </div> <div>1</div> </div>				
EASI 9 OP 17 (239,89)				
P_C	T_R	σ_{T_R}	NO. TASKS	INITIALIZE
P_D	T_I	σ_{T_I}	CHANGE NO.	EXECUTE
				SECOND FUNCTION
				INTERNAL FUNCTION

6.0 BARRIERS

Session Title: 6.1 Barrier Technology

Date: Wednesday, 8 November

Presented By: M. Madsen, Sandia Laboratories

Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. Define the role of barriers in a physical protection system, and
2. Determine the delay time of individual barriers from the Barrier Technology Handbook.

Summary:

The role of barriers in a physical protection system and the trade-off with guard response time are discussed. A movie of some actual barrier penetration tests is used to demonstrate the rapid penetration times possible for several conventional barriers and to explain some concepts for improvement in barrier delay.

The Barrier Technology Handbook is briefly summarized; emphasis is placed on how the data base was derived and how the data are used.

Additional Resource Materials:

SAND77-0777, Barrier Technology Handbook

MODULE 6

BARRIERS

BARRIER TECHNOLOGY

The foundation of an effective physical protection system is the requirement that any malevolent act, whether theft or sabotage, committed by an adversary (outsider or insider) must be detected so that the response element (security guards, police, etc.) can intercept and neutralize the adversary before his goal can be achieved. Since it is usually not feasible to maintain a sufficient number of guards to provide immediate protection for all sensitive material or equipment, some type of barrier is needed. After an adversary has been detected, this barrier would serve to deter or delay him from completing the malevolent act or delay him until adequate response forces can arrive.

ROLE OF BARRIERS

Figure 6-1 presents a simple graphical illustration of the foundation of a physical protection system and, in particular, the role which barriers play in that system. Although in this example the adversary is considered to be an outsider threat, the logic used also holds true for an insider threat.

Figure 6-1. Role of Barriers

The time required for the adversary to successfully complete his goal is labeled Adversary Task Time. At some point in the adversary scenario, the unauthorized act must be sensed; this point is labeled T_0 . If the adversary merely wishes to occupy a control room or a building, the Adversary Task Time may be very short. If his goal is to accomplish sabotage or theft of sensitive material, the Adversary Task Time will most likely be longer. Following the sensor being triggered at T_0 , some time (several seconds to several minutes) will probably be consumed during which the validity of the alarm and the magnitude of the threat are

assessed. Following a positive assessment, some sort of general response alarm is sounded. Some finite amount of time is then required to muster the appropriate response forces at the desired location to thwart the threat.

The protection objective is to ensure that adequate response forces arrive in time to prevent an adversary from accomplishing his goal. The role of barriers is simply to increase the Adversary Task Time following detection by introducing delay impediments along any path the adversary chooses, thereby providing the needed time for the response forces to arrive and react. Some barriers might deter or, if the adversary is unable to effect penetration, even defeat some threats; however, since the degree to which the barriers are able to fulfill these two roles is uncertain, they can be considered only as obstacles used to delay well-equipped and determined adversaries.

There are other trade-offs for improving the probability of adversary interception which should be considered. Against an outside threat, early detection at the site perimeter rather than inside a building or vault increases Adversary Task Time because of added distance and obstacles the adversary must traverse. Minimization of the amount of time required to complete the assessment decision will improve the total response time. If there is a guard force large enough to immediately intercept, in appropriate force, any perceived threat scenario, then, at least on paper, there would be no need for physical barriers. However, to defend a very large area or facility in this manner, the number of guards required (and hence the cost) would probably be unacceptably high.

Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls, and even many types of vaults are not likely to delay a small group of properly equipped and dedicated adversaries for a significant length of time. Although the role of barriers in a physical protection system is easy to define, the implementation of barriers to ensure the needed delay at typical industrial facilities will probably not be a simple task. Ensuring that the necessary barriers are in effect at all times of the day or night requires special attention.

BARRIER EVALUATION PROGRAM

The ongoing barrier evaluation program being conducted at Sandia Laboratories has two primary objectives:

1. To determine the penetration delays for existing and new barrier designs, and
2. To develop improved barrier design concepts which provide improved penetration delay.

At the present time, five classes of penetration tools are being evaluated:

1. Hand tools (hammers, metal cutters, prybars, etc.),
2. Hand-held power tools (drills, saws, rotohammers, etc.),
3. Thermal tools (oxyacetylene torches),

4. Explosives, and
5. Vehicles used as rams.

The results of this program are published in the Barrier Technology Handbook.¹ The handbook information should be helpful to individuals making effectiveness evaluations of physical protection systems and should also prove of assistance to designers who want to upgrade their physical protection system or to design new facilities which require positive physical protection features. Future updates of the handbook will, hopefully, include more improved barrier design concepts.

Chapter 16: "Penetration Times--Data Base" and Chapter 17: "Rates Information" of the handbook are structured to aid the user in deriving not only specific barrier penetration times but also total adversary scenario task times. Examples of the type of information contained in Chapters 16 and 17 are shown in Figures 6-2 and 6-3, respectively.

Barrier Description	Number of People	Penetration Equipment	Equipment Total	Penetration Time		
			Weight (pounds)	S/N	Mean	Max
<u>FENCE, PERIMETER BARRIER</u>						
9-gauge x 2-inch mesh V-shaped fence	3	Ladder, stepladder	40	0.4	0.8	1.2
	3	Manual boltcutters, tin snips	10.5	1.9	3.8	5.7
<u>DOOR, SHEET METAL</u>						
Standard industrial pedestrian door	1	Lock picking tools	0.5	0.1	2.5	5.0
	1	Pry bar, hammer	5	0.1	0.2	0.3
<u>DOOR, VAULT</u>						
Class 5 vault door	1	Handtools, thermal tools	-	1.1	2.2	3.3
<u>WALL, CONCRETE -- SIX-INCH-THICK -- REINFORCED</u>						
Concrete--3000 psi one layer No. 4 rebar, 8-inch centers	1	Sledge, hand boltcutters	32	3.8	7.6	11.4
	1	Explosives (3) tamper plate, hand bolt- cutters	29	1.2	2.3	3.5

Figure 6-2. Barrier Data Base--Example

The abbreviated examples from Chapter 16, shown in Figure 6-2, are representative of the 300 plus entries in the current data base listing. The entries marked with an asterisk are estimates, i.e., specific penetration tests have not been conducted. In addition to the information shown in these examples, a standard deviation for the probabilistic distributions of penetration times and data sources, along with general explanatory information, are included in the complete listing.

The rate information shown in Figure 6-3 is one of 25 different plots included in the handbook. These plots cover ranges of general activity rather than specific

CUTTING

MATERIAL: REINFORCEMENT BAR

Cutting Rates,
Electrical/
Hydraulic
Boltcutters

Figure 6-3. Rates Information--Example

barrier penetrations. They include rate information on ladder climbing; crawling; cutting rebar, steel plate, fence fabric, and expanded metal; digging with hand tools; explosives set-up, retreat, and wait times; explosives retreat distances; forcing of various materials; running; walking; and use of vehicles. The general rate information plots, along with the specific barrier penetration information on the data base from Chapter 16, should enable the user to develop total unopposed Adversary Task Times for any scenario he chooses at a particular facility. An example of how the data sources can be used is shown in Figure 6-4, which is a graphical sketch of a facility illustrating the impediments along an intruder's path and the mean times necessary to penetrate or traverse these impediments. In this example, the assumed goal of the intruder(s) is to occupy the control room; it is also assumed that detection is made at a point when the intruder crosses the area between the two perimeter fences. Table 6-I lists the sequential barrier elements along the adversary path, the penetration method, the mean time to accomplish the penetration, and the chapter and page in the Barrier Technology Handbook from which the information is taken. It should be apparent that a "worst case" scenario time can also be developed by using the minimum times ($0.5 \times$ mean time) and, conversely, the maximum probable scenario time ($1.5 \times$ mean time). When these scenario times (minimum, mean, or maximum) are compared against the predicted

Figure 6-4. Intruder Path for a Forcible Entry Scenario--Example

TABLE 6-I
Forcible Entry Scenario

Barrier	Method	Mean Time (minutes)	Data Source
Outer fence	Cut fence	0.32	Ch 16, p. 16.3-2
20-metre distance	Run, with tools	0.07	Ch 17, p. 17.1-24
Vehicle barrier	Climb over	0.05	Judgement
10-metre distance	Run, with tools	0.05	Ch 17, p. 17.1-24
Inner fence	Climb fence	0.10	Ch 16, p. 16.3-2
60-metre distance	Run, with tools	0.23	Ch 17, p. 17.1-24
Pedestrian door	Pry door	0.20	Ch 16, p. 16.3-33
Corridor, 15 m	Walk, with tools	0.13	Ch 17, p. 17.1-27
Security door	Cut 40-cm square opening	1.48 front 1.50 channel 1.48 rear	Ch 17, p. 17.1-10 Ch 17, p. 17.1-10 Ch 17, p. 17.1-10
5-metre distance	Walk	0.04	Ch 17, p. 17.1-27

Total Time 5.65
 Minus Outer Fence Penetration -0.32
 5.33

Minus Distance to Sensor -0.03

TOTAL PENETRATION TIME 5.30
 (minutes)

arrival times of an adequate number of guards, an initial judgment of the adequacy of the protection system for that particular scenario can be made. The methods for comprehensively addressing critical facility scenarios and using the penetration times in a completely probabilistic manner are discussed in other modules. The information contained in the handbook (Chapters 16 and 17) should help the user develop credible penetration times for specific barriers similar to barriers presently covered in the data base.

GENERAL OBSERVATIONS

The results of the barrier penetration tests conducted at Sandia Laboratories, coupled with penetration tests conducted by other government agencies, have led to the summary observations and conclusions noted in the remaining discussion of barriers.

Site Perimeter

The standard chain-link fences commonly used as perimeter barriers around industrial facilities cannot be considered a serious deterrent to any dedicated adversary. Fences can be climbed over, crawled under, cut through, or rammed through with a vehicle in just a few seconds. Enhancement of this type of fence with a few rolls of barbed tape obstacle or concertina wire will only increase the delay a nominal amount. In fact, almost any type of perimeter barrier which is a few metres high and on the order of 10 metres wide can be bridged with portable bridging aids in a minute or less. (Many perimeter detection systems would also be vulnerable to bypass by this same technique.) Despite the fact that it is difficult to define a cost-effective perimeter barrier that will delay intruders for a period of several minutes, the merits of upgrading perimeter barriers are significant. First, coupling positive vehicle and personnel barriers into the perimeter, inside and adjacent to the perimeter detection system, will delay the intruder at the point of detection for some finite time, thus enhancing the assessment function. Second, if a meaningful delay of the intruder at the perimeter is achieved and the guards respond promptly to the assessed alarm, the guards could intercept the intruder near the point of the alarm. Without such a delay, it is unlikely that the intruder will still be at the point of the alarm when the guards arrive, and consequently the guard task will be more difficult. Third, when it is necessary to protect a site against an adversary whose target is special nuclear materials stored in a variety of easily penetrated buildings located within the site, a positive protection zone (detection/assessment, delay, and response) at the perimeter may be the most reasonable or attractive option. Finally, as a minimum, a positive vehicle barrier around a site perimeter inside the perimeter sensors that would force an intruder to travel on foot and to carry any needed breaching aids and weapons should be considered.

A complete perimeter protection system concept (except for portals and the response force) is shown in Figure 6-5. Note the guard tower shown. Armed guards in guard towers located at periodic intervals along the perimeter should be capable of detecting intruders approaching the perimeter if these intruders are equipped with bulky bridging aids to bypass detection systems or to bridge barriers. The

tower guards could also perform a primary or secondary assessment role. Warning or lethal fire from the tower guard should slow down or thwart attempts to breach barriers with bridging aids set up in exposed positions and should also provide quick initial guard response to any type of penetration attempt that is detected.

Figure 6-5. Perimeter Detection/Assessment and Barrier System Concept

Buildings

Most building walls and locked doors can be penetrated quickly, either forcibly or surreptitiously. In addition, most buildings include entry points such as windows and ventilation and utility ducts that provide intruders with easy targets for forcible or surreptitious entry or exit. Heavily reinforced, 18-inch-thick concrete walls can be penetrated to provide a crawthrough hole in less than 5 minutes with a few pounds of explosives and rebar cutting tools. Tests show that the concrete is readily removed by the explosive charge; the cutting of the large-diameter (3/4-inch) rebar provides most of the delay. Locked personnel doors can be opened or penetrated within time periods that range from a few seconds to a few tens of seconds. Door or building windows equipped with expanded metal grills offer little delay to determined adversaries.

Hardening a building shell of conventional construction so that it will resist forcible penetration for a minute or two will probably require a significant amount of modification. To harden this type of building shell so that it will provide as much as 5 minutes delay would probably require major modification. Modification to provide any greater delay would not, in most cases, be practical. Hardening the building shell (walls, doors, windows, and all other openings), coupled with hardening of inner rooms or bays, could continue to increase the penetration delay time. However, doors must be opened or unlocked during working hours for operational needs and to serve as rapid emergency exits necessary for personnel safety. Factors such as these tend to limit the structural barrier delays that can be achieved through building hardening.

Activated Barriers

Activated barriers consist of all barriers that are deployed on command or are intruder activated. Examples include mechanisms for door closing and/or locking; filling a tunnel with rubble; the release of chemical obscurants and irritants; rigid and sticky foams; and psychological stressors, such as intense flashing lights, intense sound, etc. For a laboratory or factory-type environment, the dispersal of chemical agents appears to offer a significant potential for increasing adversary delay after the passive, structural barrier options have been exhausted.

CONCLUSIONS

A close examination of the large variety of paths and scenarios an adversary can employ to penetrate a facility presents fairly convincing evidence that existing barriers do not ensure that adversary delay time will be sufficient for an adequate number of guards to respond. Further, if the adversary has not been detected prior to encountering a barrier or unless the barrier is under constant surveillance, the effectiveness of that barrier may approach zero. Most conventional locks, fences, and door and building construction offer only short delays even against attacks which do not use explosives. Against thick, reinforced concrete and other equally impressive-looking barriers, the use of explosives by the adversary for a forcible entry becomes a more likely method of penetration. Ensuring that an adversary will encounter meaningful barriers at all times of the day or night may be very difficult.

On the positive side, a barrier system can be configured or enhanced to provide effective delay times. For instance, the presence of multiple barriers along all possible adversary paths should complicate adversary progress in a manner favorable to the defender by requiring that the adversary be equipped with a number of different attack tools. Colocating barriers along with detection alarms should aid in assessment of and response to alarms. The use of activated barriers, especially chemical dispensables, offers options for deterrence or delay that the existing structures may be incapable of providing.

If the facility to be protected has not yet been constructed, barriers can be incorporated into its design. For example, placing the facility either underground or aboveground with massive overburden is an option that should be strongly considered. Such a facility, if it is equipped with equivalent hardness in entry/exit portals, ventilation and utility ducts, etc., and protected with appropriate detection systems and response forces, could be made highly invulnerable to outsider or insider threats, adversary tactics such as force, stealth, or deceit, and adversary goals of theft or dispersal sabotage, as well as to the method of transportation used by adversaries (foot, land, vehicle, or aircraft), and, to some extent, to the size of a terrorist group.

REFERENCE

1. Barrier Technology Handbook, SAND77-0777, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

VISUALS

NOTES

SESSION 6.1

VISUALS

NOTES

CUTTING

MATERIAL: REINFORCEMENT BAR

VISUALS

NOTES

6.0 BARRIERS

Session Title: 6.2 Locks

Date: Wednesday, 8 November

Presented By: M. Madsen, Sandia Laboratories

Time: 0930 to 1000

Session Objectives:

After the session, the participants will be able to

1. Describe lock vulnerabilities, and
2. Define lock features which increase delay time.

Summary:

The vulnerabilities of specific commercial American locks to surreptitious, forced/surreptitious, and forced entry are described and/or demonstrated.

The locks or lock features that decrease rapid defeat times are described.

LOCKS

Locking devices are necessary to secure the movable portions of barriers, such as doors and gates, which must be opened periodically for authorized entry and exit. For all applications, a lock's resistance to forcible or surreptitious defeat should be equal to the penetration resistance of the barrier which it secures. (Locks, especially padlocks, are probably used as tamper or forcible-entry indicators by some people.)

The following discussion primarily addresses the common vulnerabilities (or defeat techniques) of key locks; the vulnerabilities of some types of combination locks will also be discussed. The discussion will be restricted to the types of locks manufactured or marketed in the United States. Since the lock evaluation program at Sandia Laboratories is still underway, the information presented here will not be comprehensive or in-depth. The first edition of the "Lock Users Handbook," SAND78-0500, soon to be published, will provide a more in-depth treatment of locks.¹ In the interim, Chapter 7 of the Barrier Technology Handbook, SAND77-0777, can be referred to for a basic description of lock mechanisms.² In addition, there are numerous textbooks available on lock mechanisms with surreptitious and forcible defeat techniques described.

GENERAL KEY LOCK VULNERABILITIES

All key locks (padlocks and door locks) are vulnerable to defeat and sometimes even rapid defeat (a few seconds) by the three general methods listed in Table 6-II.

TABLE 6-II

Keylock Defeat Methods

Surreptitious Defeat

- Key duplication
- Picking
- Manipulation
- Shimming

Forcible/Surreptitious Defeat

- Forcing of lock and replacement with new lock
- Core removal and replacement
- Drilling and manipulation of lock and concealment of evidence
- Forcing open and reclosing of lock

Forcible Defeat

- Forcing open
- Cutting and/or drilling of lock
- Use of explosives

A surreptitious defeat method, by definition, leaves no evidence that the lock has been tampered with or opened; that is, the lock can still be opened and closed and subsequent, careful inspection of the lock will probably fail to detect evidence of unauthorized opening. Clearly, if an adversary or malevolent person has access to the appropriate key, he can make an impression of the key and then make a duplicate key. It is probable that all key locks can eventually be picked through manipulation of the internal parts of the lock in a manner that duplicates the action of the correct matching key. The assurance and speed with which picking can be accomplished is a function of the quality and type of lock and the skill of the adversary. There are many professional locksmiths throughout the world who are capable of picking most key locks. In addition, the techniques used are often readily available in publications. The technique identified as manipulation involves bypassing of the basic lock cylinder (tumblers or levers) with a tool which can directly activate that part of the lock mechanism that would be operated by rotation of the key cylinder with the proper key action. Some key locks are vulnerable to this relatively simple technique which takes only a few seconds. Shimming is a defeat method in which a simple shim(s) can be inserted around the shackle of a padlock and rotated in a manner which actuates the detent mechanism (or locking dog) to free the shackle. Also, the locking bolt in a door lock might be shimmed with a thin, stiff material.

Forcible/surreptitious defeat methods include those techniques in which an adversary uses force to open a lock but evidence of this action will probably not be detected by subsequent, casual inspection. Simple removal of a padlock by a variety of forcible means and replacement of the padlock with a duplicate padlock could go undetected until an authorized opening is attempted. Many padlocks (pin-tumbler type) have replaceable cores to facilitate key changes. If the core is accessible, a metal screw can be inserted into the keyhole and used to forcibly extract the core. The lock mechanism can then be activated with a simple tool such as a screwdriver. After it has been opened, the padlock can be reclosed and the core pushed back into the lock; this procedure could go undetected. A small hole can be drilled into some locks (padlocks or mortise locks) and the locking mechanism actuated. After the padlock has been relocked, the evidence of entry can be cosmetically masked. Also, some padlocks can simply be forced open and subsequently forced shut in a manner that casual inspection may fail to detect.

All locks are vulnerable to defeat by force in time periods which range from a few seconds to a few minutes, depending on the lock, locking system, and attack tools used. Locks can simply be forced open or broken. Cutting tools such as metal cutting saws, thermal cutting tools, or drills can be used to open a lock. Most locks can be readily defeated if explosives are used. Clearly, these types of forcible attacks will leave evidence of entry, but speed may be the primary goal of the adversary.

COMBINATION LOCKS (MECHANICAL)

Good quality combination locks are not usually as susceptible to simple, surreptitious defeat methods as key locks. Since only a mechanical control shaft

is required to operate for a combination lock and there is no access hole, the combination lock would appear to be easier to harden against forcible attack when used in a door. This hardening could be accomplished by imbedding the lock mechanism deep in the door system. However, combination locks may be equally vulnerable to rapid defeat by forcible/surreptitious methods. The fact that the combination lock does not have direct access to the lock mechanism, such as a key hole, eliminates most surreptitious options. Also, the large number of combinations possible makes dialing all possible combinations a formidable and time-consuming task.

LOCKING HARDWARE

In addition to the lock mechanism vulnerabilities of padlock and door locks, the auxiliary locking hardware (such as hasps when padlocks are used) and the bolting or linkage mechanism in doors may be more vulnerable to rapid, forcible defeat than the lock itself. For instance, a close examination of some commercial vault doors equipped with high-quality combination locks indicates that the locking pin linkage mechanism can be defeated much more easily than the lock itself.

GENERAL CONCLUSIONS

Although some key locks are not readily vulnerable to manipulation or shimming and picking may be very difficult, all key padlocks (including combination padlocks) can be forcibly defeated in a very short period of time. If the primary concern at a facility is to employ locks that are resistant to surreptitious defeat, combination locks are generally less vulnerable than key locks. However, very careful examination will probably be required to assure that the lock has not been defeated by forcible/surreptitious means.

Selection of a key lock (door or padlock type) that has a positive linkage between the lock cylinder rotation and the actual locking or bolting action should prevent or complicate those surreptitious defeat techniques that allow the adversary to actuate (manipulate) the locking mechanism without operating (rotating) the lock cylinder.

REFERENCES

1. "Lock Users Handbook," SAND78-0500, Sandia Laboratories, Albuquerque, New Mexico, to be published.
2. Barrier Technology Handbook, SAND77-0777, Sandia Laboratories, Albuquerque, New Mexico, April 1978.

7.0 INTRUSION DETECTION SYSTEMS

Session Title: 7.1 Sensors

Date: Wednesday, 8 November

Presented By: J. D. Williams, Sandia Laboratories

Time: 1030 to 1200

Session Objectives:

After the session, the participants will be able to

1. Determine the technological type(s) of sensor(s) and sensor configuration best suited for a particular site, and
2. Identify the information pertinent to the selection, procurement, installation, testing, and maintenance of the elements of an intrusion detection system.

Summary:

Sensor selection consists of identification of the equipment and installation methods which best meet the intrusion detection system objectives of a facility. A consideration of the interaction among equipment, environment, and intruder forces is integral to the selection of the proper technological type of equipment necessary to ensure the desired intrusion detection function. These interrelationships and technological types of both exterior and interior sensors are presented in this session.

Additional Resource Materials:

1. 15-minute film--Exterior Sensor Laboratory
2. 15-minute film--Interior Sensor Laboratory
3. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, Albuquerque, New Mexico, November 1976 (Revised October 1977).

MODULE 7

INTRUSION DETECTION SYSTEMS

SENSORS

Since late 1974, the Department of Energy, Office of Safeguards and Security and its predecessor organizations have provided funds for analysis, modeling, development, implementation, and demonstration of various physical protection system concepts which are appropriate for fixed-site facilities. Emphasis has been placed on Department of Energy type facilities; however, the results of these studies are also applicable to other government agencies and private industry, especially the nuclear power industry (both domestic and foreign).¹⁻¹¹

As part of the nuclear physical protection systems effort sponsored by the Department of Energy, the Fixed Facilities Physical Protection Research and Development program at Sandia Laboratories provides (1) system analysis and evaluation, (2) physical security equipment evaluation and development, and (3) system design and operational testing and evaluation.

The information on exterior and interior sensors presented in this module was obtained from the equipment evaluation and development programs sponsored by the Department of Energy, the Department of Defense, the military services, the Nuclear Regulatory Commission, the Defense Nuclear Agency, and other government agencies, as well as from data provided by commercial security equipment suppliers.¹¹⁻¹⁷

The selection of intrusion detection equipment is based on identification of the equipment and installation methods which best meet the overall intrusion detection system objectives. The objectives take into consideration the purpose of the intrusion detection equipment and the types of assumed threats which this equipment may have to face. The requirements of the intrusion detection system can be divided into three primary areas: (1) the probability of detecting the intruder, (2) the vulnerability to defeat of the equipment, and (3) the false alarm or nuisance alarm rate and causes of the alarms. However, these parameters cannot be represented by single-valued numbers; they are influenced by a large number of variables such as physical environment, weather, threat, maintenance, installation, regulations, procedures, and operating personnel. Therefore, when a high probability of detection and a low false alarm or nuisance alarm rate are required over a wide range of operating conditions, it is necessary to use different types of sensors in combination. Combinations of sensors also play a part in the concept known as "protection-in-depth," which is simply a number of protective measures in series, i.e., an intruder must successfully avoid or defeat each of the protective measures in sequence before access to the protected material or facility can be achieved.

A major design goal is to obtain an intrusion detection system which exhibits low false alarm and nuisance alarm rates and an acceptable probability of detection and is not susceptible to defeat. This goal can be achieved by logically or hierarchically combining the outputs of different types of sensors. No single sensor presently exists that will reliably detect all intruders and still have acceptably low false alarm and nuisance alarm rates for all expected natural and manmade environments. However, the number of sensor types in a system should not be increased and/or logically combined or implemented to change any of the above performance characteristics without consideration of how these changes affect the other performance characteristics. A common assumption is that the system should be adjusted to achieve a value for the probability of detection which is very close to 1 and that any resultant increase in the false alarm and nuisance alarm rates will be tolerated. This assumption is acceptable only if the system false alarm and nuisance alarm rates are equal to or less than the false alarm and nuisance alarm rates which the security force will tolerate while at the same time continuing to treat each alarm as a credible alarm. When these false alarm and nuisance alarm rates are exceeded and the system is turned off or ignored, the actual probability of detection for the system goes to zero.

Figure 7-1 shows a hypothetical site which employs both exterior and interior sensors. In order for theft or sabotage of material (assumed to be stored on the metal shelving shown in the building cutaway) to occur, the following undetected actions by an intruder(s) must be taken:

1. The outer fence must be penetrated by going through, over, or under it. If there are fence sensors, the job is more difficult.
2. The exterior volumetric sensors (assumed to be buried-line, microwave, and electric field sensors) must be gone over or under. This task becomes more difficult as the volume of the detection zone is increased.
3. The inner fence must be gone through, over, or under.
4. The distance from the inner perimeter fence to the building must be traversed.
5. The shell or boundary of the building must be penetrated. If a natural entry is used, door and window switches must be circumvented. If a new opening is made or an unnatural opening used, vibration sensors, ventilation duct sensors, etc., must be circumvented.
6. The motion or volumetric sensors (ultrasonic, sonic, microwave, or infrared) in the building interior must be defeated.
7. The proximity sensors must be defeated.
8. Finally, the entry procedures must be repeated in reverse order if the intruder desires to escape undetected.

Usually, the itemized actions must occur without the intruder being detected by a roving patrol or by closed-circuit television located on the perimeter of the area and in the building. The number of the various sensors shown in Figure 7-1 will vary with the degree of security needed and is influenced by the consequences of any theft or sabotage, available funds, regulations, etc. If buried-line sensors are used, an intruder must dig deeper if he attempts to tunnel under the detection zone.

Figure 7-1. Hypothetical Site Showing a Possible Unauthorized Entry Path

Intrusion detection systems equipment is comprised of (1) sensors, (2) alarm assessment systems, and (3) alarm reporting systems (including alarm communications and information display equipment). The proper operation of an intrusion detection system is influenced by the physical environment, the threat, the type of material to be protected, regulations, procedures, personnel, and the installation and maintenance procedures. Details of these interactions and how these components can be integrated into an operationally effective intrusion detection system are given in the Intrusion Detection Systems Handbook.

The remainder of this module describes the different technological types of sensors, provides guidelines on how to plan an operationally effective intrusion detection system using various sensors, and describes sensor evaluation techniques. A brief summary of the knowledge accumulated to date is also presented.

TECHNOLOGICAL TYPES OF SENSORS

Intrusion detection sensors can be categorized as either exterior or interior sensors. Exterior sensors include fence sensors and free-standing line and buried-line sensors. Interior sensors include boundary penetration sensors, motion (volume) sensors, and proximity sensors. Figure 7-2 illustrates this breakdown.

Figure 7-2. Types of Intrusion Sensors

General Exterior Sensors

Exterior sensors consist of a variety of different technological types of sensors, as Figure 7-3 shows. Most of these categories are covered in the following discussion.

Figure 7-3. Types of Exterior Sensors

Fence-Associated Sensors -- Since it is desirable to sense an intruder as soon as possible, the first type of sensor encountered by an intruder is usually located at the outer perimeter of a facility. Fences, no matter how tall or how elaborate, offer little resistance to a determined intruder. Therefore, fence sensors can only assist in the formation of a viable perimeter system. However, even if a good perimeter system is employed, it is only part of an overall security system and cannot be considered as providing complete protection. Fence-associated systems offer no protection against the intruder who goes over or under the fence or who hides on the premises during a time when he has access to the facility.

Tilt-switch sensors consist of several series or parallel-connected switches coupled to a processor. Sensing is based on the fact that any motion of the switch housing will result in the opening and closure of a contact switch. Switches are mounted on fence posts or chain-link fabric sections so that disturbance to the fence will cause switch action.

Tilt switches sense abnormal motions, shocks, or vibrations which may occur during attempts to climb over the fence, to penetrate the fence by cutting or burning, or to push or pull the fence down. Several different types of transducers are currently in use: mercury switch, pedestal-mounted ball, piezoelectric element, and reed switch. Figure 7-4 shows a tilt-switch sensor installation.

Figure 7-4. Tilt-Switch System

Electret sensor cables are special cables which sense fence movement and sounds. These cables provide sensing along the entire length of the cable. An electret sensor consists of a coaxial sensing cable with a radially polarized dielectric and a processor. Sensing is based on the fact that a small stress applied to the dielectric will produce an electrical output. If the cable is attached to a chain-link fence, any disturbance of the fence will stress the cable and cause a sensor output. The signal generated by the sensing cable is amplified and processed for frequency content, amplitude, and duration in order to allow differentiation between actual intrusions and environmental disturbances. Figure 7-5 shows an electret sensor installation.

Figure 7-5. Electret Sensor

Both the tilt switch and the electret sensor can experience high nuisance alarm rates caused by wind, blowing debris, animals, birds, moving vehicles, snow or ice, earthquakes, electrical storms, adjacent grass or bushes, and the motion of nearby trees. Many of the fence-mounted sensors are designed with variable time-constant adjustments which minimize false and nuisance alarm rates by ignoring a given number of instances (one or more) of fence vibration before producing an alarm. Also, some of the sensors are designed to primarily sense vertical fence motion and to be less sensitive to horizontal motion.

The best countermeasure for the intruder to take against a fence-mounted tilt-switch sensor is to avoid it completely by going over, under, or around the fence without coming in contact with it.

Environmental factors are a primary consideration in the design and installation of fence-associated sensors since these sensors are generally mounted outdoors and thus are exposed to all the inclemencies of the weather. High-quality installation is required; the sensors must be securely mounted and kept clean, dry, and rust-free. Regularly scheduled checks should be used to verify that all mechanical and electrical connections are tight. The fence should be rust-free, the posts set in stable footings, and the fence mesh and other accessories, tight and secure.

Most fence-associated sensors have provisions for line supervision, sensitivity adjustments, and multizone operation. Better rejection of wind-induced alarms and improved self-test features are desired improvements.

The taut-wire sensor or wire-tension sensor consists of a series of wires installed under tension and attached to switch sensors so that deflection of the wires produces an alarm. Various wire configurations are possible, including free-standing and chain-link, fence-mounted configurations.

Commercial equipment built on the taut-wire principle uses barbed wire. The sensor consists of a twisted pair of wires that, when stretched, acts as a spring distributed over the entire fence length. Adequate tension on the wire must be maintained during changes in environmental conditions. The sensor post (Figure 7-6) consists of a number of switches (one switch for each barbed wire) connected in parallel. Each sensor post is centered between anchor posts which can be up to 60 metres apart. Multiple sensor posts can then be wired in parallel to provide a detection zone of any desired length. A wire tension of 35 to 45 kg is necessary for proper operation of the system. Intermediate guide posts are used to guide the horizontal wires through holes to permit unobstructed lengthwise movement. These

Figure 7-6. Taut-Wire Sensor and Sensor Post

posts are usually spaced about 3 metres apart. The sensor switches are clamped to the barbed wire in such a manner that a sideways pull on the switch (which would be induced by a man climbing the wires, pulling the wires apart, or cutting the wires) causes the switches to close. A switch deflection of as little as 2 mm is sufficient to generate an alarm.

A unique feature of the taut-wire switch is its self-adjusting property. This self-adjustment allows for gradual changes in post positions, while short-term changes cause an alarm. The switch actuator is mounted inside a viscous silicone compound which acts as a low-frequency dampener. Slow changes cause the actuator to move through the compound, while faster changes make the compound appear rigid and result in switch closures. This system exhibits a very low false alarm rate. Defeat may be possible by climbover at the anchor posts. Typical taut-wire sensor installations are shown in Figure 7-7.

Figure 7-7. Typical Taut-Wire Sensor

An electric field fence sensor consists of an alternating-current field generator which excites a field wire, one or more sensing wires which couple into the resulting electric field, and an amplifier and signal processor which amplify and detect changes in the signal amplitude of the sensing wires. A signal is generated when a conductive body or a body with a high dielectric constant (such as a human body) distorts the coupling between the field wire and the sensing wires. Such an installation is shown in Figure 7-8. The electric field principle is also employed in free-standing sensors.

Free-Standing Sensors -- Free-standing sensors used for exterior applications include infrared, microwave, and electric field sensors.

Active exterior infrared sensors are free-standing line sensors which consist of infrared transmitters, photodetectors, and appropriate lenses. The effective size of the beam is determined by the size of the lenses.

Figure 7-8. Three-Wire Electric Field Sensor Mounted on Chain-Link Fence

Several transmitters and receivers are usually employed to provide a multiple beam system. The beams are usually configured into a vertical infrared fence. A pulsed synchronous technique is used to reduce interference from and/or defeat by other sources of light.

The significant characteristics of the infrared sensor used for perimeter systems are

1. The sensor is strictly line-of-sight and requires very uniform terrain,
2. Alignment is critical and requires stable mounting to prevent movement,
3. The sensor is subject to high nuisance alarm or false alarm rates and even complete inactivation during heavy fog and snow as well as when wind blows snow lying on the ground into the beam, and
4. The narrow vertical plane does not provide much volume coverage; therefore, the sensor is vulnerable to defeat or bypass.

As a result of these characteristics, the infrared sensors are not well-suited to perform as long-range perimeter sensors. However, they have been used effectively in prisons since the apparatus required to defeat infrared sensors are not usually available to prisoners. These sensors also can be used for short-range,

gap-filling applications, such as the sensing of gates and portals. In general, the preceding discussion also applies to the use of lasers as perimeter sensors.

Microwave sensors used for exterior applications can either be monostatic (transmitter and receiver are located in the same housing) or bistatic (transmitter and receiver are located in two separate housings). Since the bistatic unit is most commonly used in exterior systems, it will be the only type discussed.

A bistatic microwave sensor uses a modulated transmitter and a receiver (usually operating at about 10 GHz) which are separated by a limited (~100-metre) line-of-sight distance. Sensing is based on the fact that an object moving through the beam will cause a signal change in the receiver. The volume of the sensing zone corresponds to a cigar-shaped area between the transmitter and receiver, as shown in Figure 7-9.

Figure 7-9. Various Microwave Sensors

Figure 7-10 shows the effective width and height of the sensing zone as a function of the distance from the transmitter for a typical bistatic system.

Figure 7-10. Sensing Zone for a Bistatic Microwave Sensor

Electric field free-standing sensors are shown in two-wire and three-wire configurations in Figures 7-11 and 7-12, respectively. Not shown are some four-wire systems and other configurations which extend the effective protection volume. This type of sensor can also be mounted on a chain-link fence, as discussed earlier. Desired improvements include better lightning rejection and a provision for allowing small animals to pass under the sensor without being sensed.

Buried-Line Volumetric Sensors -- Buried-line sensors include extended-length cable systems which employ seismic, magnetic, or seismic-magnetic sensing methods. This class of sensors also includes point sensors.

The seismic-magnetic buried-line sensors consist of a cable which is sensitive to both seismic and magnetic disturbances and a processor which evaluates signals generated in the cable. Sensing is based on the fact that seismic disturbances will either move the cable in the earth's magnetic field or strain the flexible magnetic core and by magnetostriction change its permeability. Ferromagnetic material passing near the cable will vary the earth's magnetic field around the cable; this produces a voltage in the sensing coil.

Seismic buried-line sensors include two generic types of seismic buried-line sensors. One type consists of a pair of fluid-filled hoses. When one of the hoses receives more pressure than the other, a differential signal is produced. The second system consists of piezoelectric ceramic discs located at various intervals along a cable. Stressing the ceramic disc creates a signal.

Figure 7-11. Two-Wire Electric Field Sensor

Figure 7-12. Three-Wire Electric Field Sensor

The magnetic buried-line sensor consists of a wire loop which is coplanar to the earth's surface. As an intruder with ferromagnetic material crosses the loop, an electrical signal is generated in the wire. This type of sensor will not sense a "magnetically clean" intruder.

Point Sensors are those sensors which provide a small zone of coverage and can be used as "gap fillers" and as tamper or "weak-link" sensing devices. Point sensors can be geophones, electromagnetic point sensors, or Doppler radar sensors.

Interior Sensors

Sensors which monitor intrusions into buildings or enclosed structures have been available for a number of years. Recently, however, some significant improvements in the performance characteristics of these sensors, test techniques, and application understanding have been realized.

Figure 7-13 shows a general breakdown of the technological types of interior sensors available.

Figure 7-13. Types of Interior Sensors

Boundary Penetration Sensors -- Boundary penetration sensors are designed to sense penetration of the boundary of a protected area. Included in this class of sensors are vibration sensors and door and window sensors. Vibration sensors are passive devices which are mounted on the wall and sense vibrations. They use a piezoelectric crystal or a moving-coil transducer. The transducer converts mechanical or acoustical signals into electrical signals. These transducers can be mounted on or within walls, and can be adjusted to sense attempts to penetrate walls. Door and window sensors are usually balanced magnetic switches. Other boundary penetration sensors exist but are not included in this discussion. These include passive ultrasonic sensors, wire grid sensors, and metal foil sensors.

Motion (or Volume) Sensors -- These types of sensors are designed to sense the motion of an intruder within a confined interior protected area. Several different technological types of sensors fall into this category of motion sensors:

1. Ultrasonic sensors are active sensors which operate in the frequency range of 19 to 40 kHz. Sensing is provided by observing the Doppler frequency shift associated with motion.
2. Microwave sensors are active sensors which operate at a frequency of approximately 10.5 GHz. Sensing is provided by observation of the Doppler frequency shift associated with motion.
3. Infrared sensors can be active or passive sensors and can be designed to sense heat and/or motion.
4. Audio (sonic) sensors can be active or passive sensors. They operate at frequencies in the audio range and sense both Doppler frequency shift and phase shift associated with motion. In their simplest form, passive systems employ a microphone and amplifier to detect sound caused by an intruder.

Other motion sensors exist but are not included in this discussion. The electric field sensor, designed for interior use, is an example of such a sensor.

Ultrasonic sensors sense acoustic wave changes caused by target motion. When a target moves, the Doppler frequency shift causes the reflected energy to appear at a frequency which is different from that of the transmitted energy. Figure 7-14 illustrates how movement in a room produces a Doppler frequency shift. Examples of the types of data that are important for this sensor are presented in Figures 7-15, 7-16, and 7-17.

Microwave sensors for interior use are typically monostatic. Monostatic microwave sensors employ a single antenna for both the transmit and receive functions. Sensing is based on the Doppler frequency shift; typical units operate at a frequency of about 10.5 GHz. The Doppler frequency shift is produced by movement similar to that illustrated in Figure 7-14 for ultrasonic sensors.

An active infrared sensor system is basically a beam-breaking system. Passive systems, on the other hand, respond to the energy emitted from a moving intruder by employing special optical and electronic techniques. The sensing pattern for a passive infrared system is shown in Figure 7-18.

ULTRASONIC SENSORS

DOPPLER SHIFT

$$\Delta f = 2V/\lambda$$

$f = 18 \text{ KHZ TO } 40 \text{ KHZ}$

$\lambda = 16 \text{ MM TO } 8 \text{ MM}$

Figure 7-14. Operational Principle of an Ultrasonic Sensor

Figure 7-15. Sensing Pattern for a Ultrasonic Sensor

Figure 7-16.. Intruder Velocity Range Multiplication Factor for an Ultrasonic Sensor

Figure 7-17. Sensitivity Setting Range Multiplication Factor for an Ultrasonic Sensor

Figure 7-18. Sensor Pattern for a Passive Infrared Sensor

The active sonic (audio) sensor is similar to the ultrasonic and microwave sensors except that its operating frequency is about 1 kHz.

Proximity Sensors -- Proximity sensors are designed to provide an indication if a person attempts to touch or actually does touch a metallic object. Capacitance point sensors or capacitance proximity sensors are included in this category of interior sensors.

The interior capacitance proximity sensor can be used to sense unauthorized access to metal objects. It is sensitive to changes in capacitance between the protected object and ground caused by the approach of an intruder or another object. This change in capacitance is sensed by a tuned circuit located in the control unit.

PLANNING AN OPERATIONALLY EFFECTIVE INTRUSION DETECTION SYSTEM

The expression "operationally effective" is used to describe intrusion detection systems which have achieved a reasonable balance between (1) optimization of system hardware, (2) comprehension, acceptance, and efficient utilization of the system by security personnel, and (3) a sufficient degree of detection capability at the facility.

It is essential that any new intrusion detection system be carefully planned and analyzed to ensure that it will perform its function reliably and that its strengths and weaknesses are identified and understood. The same care should be used when improvements are incorporated into existing systems. Included in the planning and analysis is the development of (1) a system philosophy, (2) a preliminary system design, (3) on-site experiments and evaluation, (4) final

system design, (5) construction and installation considerations, (6) a program schedule, (7) cost considerations, and (8) procurement.

Intrusion detection systems hardware comprises sensors, alarm assessment systems, and alarm reporting systems (including alarm communications and information display equipment). The performance of the sensing and assessment equipment is heavily influenced by the physical environment in which it must operate as well as by installation and maintenance. Since present-day knowledge of the correlation between sensor operation and the physical environment is limited, some on-site evaluation will be required before, during, and after installation. An operationally effective intrusion detection system is also influenced by facility regulations, procedures, and personnel. All of these items, coupled with the type of facility or material to be protected and the threat spectrum (including some intruder attributes), influence the final system selection.

Intrusion detection systems are generally used in association with a barrier system so that attempts to penetrate the barrier will result in an alarm. Intrusion detection systems interface with entry-control systems to allow authorized activity at a facility.

Considerations for Sensor Selection

Sensor selection consists of identification of the equipment and installation methods which best meet the intrusion detection system objectives for a facility. A consideration of the interaction among equipment, environment, and intruder forces is integral to the selection of the proper technological type of equipment necessary to ensure the desired intrusion detection functions. These interrelationships and various technological types of both exterior and interior sensors are discussed.

Exterior Detection -- The physical and environmental conditions that can affect exterior detection systems include topography, vegetation, wildlife, background noise, meteorological conditions, and soil and pavement. It is important to recognize that there is no "typical" site since combinations of conditions are site specific. Topographical concerns include slopes and hills, gullies and ditches, lakes, rivers and streams, swamps and temporary surface water, perimeter access points, and manmade structures. Vegetation includes all plant life such as trees, weeds, grass, bushes, and crop foliage. The vibration of the root systems of this vegetation as well as the aboveground motion of foliage can affect sensor performance. Wildlife of concern includes large and small animals, burrowing animals, and birds and insects. Background noise such as traffic, wind, natural and manmade seismic sources, and electromagnetic interference all must be taken into account. The specific type of meteorological information which may prove useful in the design and operation of sensor systems includes wind, temperature, rain, snow, hail, visibility, airborne corrosives, and electrical storms. Soil and pavement conditions primarily affect buried sensors.

The major characteristics of several types of exterior sensors suitable for fixed-site applications are shown in Table 7-I. The relative individual adversary detection coverage provided by these sensors is depicted in Figure 7-19.

TABLE 7-1
Exterior Sensors Suitable for Fixed-Site Applications

APPLICATION	OPERATING PRINCIPLE	AVAILABILITY	DETECTION					CONDITIONS FOR UNRELIABLE DETECTION	TYPICAL DEFEAT METHODS	MAJOR CAUSES OF FALSE ALARMS										
			NONMAGNETIC	WALK, RUN, & CRAWL	TUNNEL	CLIMB FENCE	CUT FENCE			HIGH WINDS	HEAVY RAIN	HEAVY SNOW	HEAVY FOG	BIRDS	SMALL ANIMALS	LARGE ANIMALS	SEISMIC ACTIVITY	THUNDER AND LIGHTNING	ELECTRICAL TRANSIENTS	RADIOFREQUENCY INTERFERENCE
BURIED-LINE	SEISMIC-MAGNETIC	MILITARY PRODUCTION	X	X	X				BRIDGE AND CARRY NO FERROMAGNETIC MATERIAL	X						X	X	X	X	X
	SEISMIC	PRODUCTION	X	X	X			FROZEN GROUND	LOW BRIDGE	X						X	X	X		
	MAGNETIC	PRODUCTION		X	X				CARRY NO FERROMAGNETIC MATERIAL									X	X	X
FENCE-ASSOCIATED	ELECTRET CABLE	PRODUCTION	X			X			LADDER OR SHORT TUNNEL	X						X		X	X	
	TILT SWITCH	PRODUCTION	X			X			LADDER OR SHORT TUNNEL	X						X				
	TAUT-WIRE	PRODUCTION	X			X	X		LADDER OR SHORT TUNNEL							X				
FREE STANDING LINE	E-FIELD (CAN BE FENCE-ASSOCIATED)	PRODUCTION	X	X		X	X		TUNNEL OR HIGH BRIDGE					X	X	X		X	X	X
	MICROWAVE	PRODUCTION	X	X				IRREGULAR TERRAIN, HIGH GRASS	TUNNEL OR HIGH BRIDGE					X	X	X				
	INFRARED	PRODUCTION	X	X				IRREGULAR TERRAIN, HIGH GRASS, OR SNOW DRIFTS	LADDER, SHORT TUNNEL, OR REDIRECT LOW BEAM		X	X	X		X	X				
POINT	SEISMIC OR ELECTROMAGNETIC	DEVELOPMENT	X	X					TUNNEL					X	X	X		X		X

As mentioned earlier, no single sensor exists that will detect all types of intrusions and have an acceptably low false alarm rate in normal outdoor environments. Single sensors can be employed to reliably sense the casual intruder who might simply climb a fence and walk through an area. However, in order to sense determined intruders while maintaining an acceptably low false alarm or nuisance alarm rate, an appropriate combination of sensors is required.

Interior Detection -- In general, three classes of interior sensors are of interest: (1) boundary penetration sensors which are designed to detect

Figure 7-19. Sensor Coverage Provided by Various Sensors

penetration of the perimeter of the area to be protected, (2) motion (or volume) sensors which are designed to detect the motion of an intruder within a confined interior protected area, and (3) proximity (hands-on) sensors which are designed to protect a metallic object and indicate if any attempted or actual contact with the object has occurred. Environmental conditions which may affect interior sensors can be electromagnetic, radioactive, acoustical, thermal, optical, seismic, or meteorological in nature. Two important physical conditions which affect sensor performance are the building or room construction and the various equipment or objects that occupy the area or room to be monitored.

Selection of particular technological types of sensors depends upon (1) the level of security required and (2) the physical and environmental conditions that exist within the volume to be detected. An intrusion detection system consistent with the three classes of interior sensors can be designed which provides three levels of detection, i.e., at the boundary, within the room, and at the object to be protected. This philosophy is followed in the Joint-Services Interior Intrusion Detection System program (see Reference 18).

It is usually possible to identify appropriate technological sensors which will perform acceptably in the environment in question since the environment associated with interior areas is normally controlled and is usually predictable and measurable. However, correct sensor choice requires that the particular false or nuisance alarm stimuli to which it is susceptible be known, as well as whether these stimuli are contained in the environment in question. This is particularly true of the volume detectors (ultrasonic, microwave, infrared, and sonic), all of which can be installed to provide acceptable detection coverage and which typically false or nuisance alarm from different stimuli. However, as is the case with exterior sensors, acceptable operation can best be achieved by an appropriate combination of sensors.

Sensor Characterization

Although it is difficult to assign specific numbers for probability of detection, false and nuisance alarm rates, and vulnerability to defeat, performance characteristics are still important considerations. This realization guides most evaluation programs. Instead of attempting to identify or assign a probability-of-detection number to a sensor, the Sandia Laboratories evaluation program is designed to identify the sensing capabilities and limitations of sensors. For example, how does a sensor pattern vary as a function of intruder velocity, how does the sensor sensitivity vary with background noise, or how does the weather affect the performance characteristics? Instead of assigning false or nuisance alarm rate numbers, the causes of false or nuisance alarms are identified; this identification evolves from an understanding of the operational principles of the sensor, including any signal processing, and the ascertainment of what stimuli will cause alarms. A complete evaluation program must also identify the methods which an adversary can employ to render a sensor useless.

Exterior Sensor Testing -- An extensive exterior sensor evaluation laboratory exists at Sandia Laboratories, Albuquerque, New Mexico. It is at this site that evaluations of the various types of exterior sensors which have been discussed are conducted. The site is equipped with a complete meteorological station, analog, digital and video signal recording capability, and closed-circuit television. Fences can be climbed, cut, or given calibrated impact forces. The buried-line sensors also receive calibrated impact forces, and both the buried-line and volumetric sensors require run, walk, and crawl tests.

In addition to human test targets, trained dogs and a number of simulators have also been used. One technique uses aluminum spheres of various sizes to provide

a human intruder simulation which is used to quantize bistatic microwave sensor performance. (The data in Figure 7-10 were generated by this technique.) Figure 7-20 shows the equipment designed to move the spherical targets through the beam at preselected heights and velocities.

In addition to the tests conducted at Sandia, a site near Denver, Colorado has also been utilized to evaluate and validate the installation, alignment adjustment, and test procedures which have been developed for exterior sensors. In order to determine the effect of exceptionally high electromagnetic field intensities and transients on the operation of microwave, electric-field, and piezoelectric buried-line sensors, a joint evaluation program is being conducted with the Bonneville Power Administration.

Figure 7-20. Apparatus for Moving Spherical Test Ball

Interior Sensor Testing -- A detailed paper on the Sandia interior sensor evaluation capability has recently been presented.¹⁹ A few of the highlights of that paper are repeated here.

Motion sensors have been evaluated by individualized test scenarios which address the most sensitive capabilities of each of these sensors. They have also been evaluated with one universal test procedure that is applicable to all of the different types of sensors. It is believed that both types of evaluations are necessary.

The former testing procedures, which address the sensor's most sensitive capabilities, must be performed during the initial stages of the evaluation in order to develop a basic understanding of sensor operation. The latter procedure has to be performed afterwards in order to determine the strength and weakness of each type of sensor so that the experimenter can identify those combinations of sensors which will successfully provide the desired sensing coverage. For example, a monostatic ultrasonic sensor is most sensitive to motion directed radially toward or away from it; infrared sensors are most sensitive to intruders azimuthally crossing the sensor field of view. A knowledge of the azimuthal-motion response of ultrasonic sensors and the radial-motion response of infrared sensors is extremely beneficial to the system designer.

In addition to the patterns for radial intruder motion (such as those shown in Figure 7-15), patterns have also been determined for movement normal and parallel to the centerline of the sensor field of view. Figure 7-21 is a composite for an ultrasonic sensor which shows the plus and minus radial directions on the left of the centerline and the plus 45° directions parallel to the line and the minus 135° directions parallel to the line on the right of the centerline. For this sensor,

Figure 7-21. Sensing Pattern Along Radial Directions

the patterns are symmetrical about the centerline; however, recent data have shown that this symmetry does not always exist. The arrows indicate intruder direction and the dots on the arrows indicate the position where sensing occurred. The patterns in Figures 7-22 and 7-23 are for the plus and minus directions parallel to the centerline and plus and minus directions parallel to the base line, respectively. Figure 7-24 shows a composite of all 10 movement directions. Movement by an intruder in any direction in this composite would generate an alarm. In all cases, the composite is smaller than the radial patterns and, in a few cases, it is much smaller. These facts coupled with the basic differences in direction of movement for greatest sensitivity for different technological types of sensors must be considered when operational systems and performance tests for those systems are planned.

Figure 7-22. Sensing Pattern for Movement Parallel to Centerline

Figure 7-23. Sensing Pattern for Movement Parallel to the Base Line

Figure 7-24. Composite of all 10 Movement Directions

Another important aspect in the development of sensor evaluation techniques involves the elimination, when possible, of the human factor from the test procedures. This is desirable for several reasons: (1) some test procedures are rather redundant and hence are better achieved electronically and/or mechanically, (2) if the simulation techniques are appropriately defined, then accurate repetition of experiments is possible, (3) error due to human judgment is minimized, and (4) greater flexibility in experimentation is achieved.

A floor plan of the interior sensor evaluation laboratory is shown in Figure 7-25. A picture of an aid developed to regulate the velocity of a human test target is shown in Figure 7-26; a picture of a motor-driven mannequin used to replace human targets is shown in Figure 7-27.

Figure 7-25. Interior Sensor Evaluation Laboratory

Figure 7-26. Human Test Target Holding onto a Constant-Velocity String Controller

Figure 7-27. Motor-Driven Mannequin Used in Evaluation Programs

Electronic simulators have also been developed to test ultrasonic and microwave sensors which operate on the Doppler principle. These electronic simulators can be used to determine detection pattern variations as a function of intruder velocity. They have also been programmed, in conjunction with temperature controls for the refrigerated rooms, for use in temperature testing of sensors. It now appears feasible to automatically achieve the time-consuming, cold-temperature testing totally within a refrigerated room without the necessity of opening the

door or using a human target. Warm temperature testing can be conducted in a hot room in a similar manner. Some recent results indicate that the performance of some sensors varies by a factor of three over a temperature range of -18° to 49° C.

SUMMARY AND CONCLUSIONS

This discussion has provided a brief review of some intrusion sensors which have been characterized by Sandia Laboratories through work sponsored by the Department of Energy, Office of Safeguards and Security. Other types of sensors exist. Some of them have been characterized by other laboratories and some have yet to be characterized. Sensor inclusion or noninclusion in this discussion does not reflect on the usefulness of any type of sensor.

The key concepts which must be considered in planning a sensor system and the site characteristics which affect the performance of both exterior and interior sensors were mentioned. A characterization will be required for each site since each is unique. Performance characteristics (probability-of-detection, false or nuisance alarm rates, and vulnerability to defeat) of the total physical protection system, rather than of the individual sensor, should be optimized. Weaknesses of individual sensor types can be compensated for by employment of combinations of more than one technological type of sensor. The outputs of these sensors can be combined with other pertinent systems (1) to produce an "operationally effective" physical protection system and (2) to achieve "protection-in-depth."

The ability to assess the cause of an alarm (a topic not specifically discussed in this section) is part of the pertinent system information and must be included in the overall system planning.

Various sensor characterization and evaluation techniques were mentioned. Some of these are applicable for field use and others are limited to laboratory use. More complete information on the sensors discussed can be found in References 12 through 21.

REFERENCES

1. H. E. Lyon, "The Role of Material Control and Development in ERDA's Safeguards Program," Journal of the Institute of Nuclear Materials Management, V, No. 111 (Fall 1976), 57-64.
 2. Orval E. Jones, "Advanced Physical Protection Systems for Facilities and Transportation," Journal of the Institute of Nuclear Materials Management, V, No. 111 (Fall 1976), 211-225.
 3. L. M. Brenner and S. C. T. McDowell, "ERDA's Integrated Safeguards System Program," Journal of the Institute of Nuclear Materials Management, V, No. 111 (Fall 1976), 292-301.
 4. T. R. Canada, J. L. Parker, and J. W. Tape, "The U.S. ERDA Safeguards Technology Training Program," Journal of the Institute of Nuclear Materials Management, V, No. 11 (Summer 1977), 54-59.
 5. Nuclear Proliferation and Safeguards, Congress of the United States, Office of Technology Assessment, Washington, D.C. (New York: Praeger Publishers).
- and also
- Appendix, Volume II, Part 2 to Nuclear Proliferation and Safeguards, Appendix VIII, Section 4.1, VIII-34 (OTA-E-50), June 1977.

6. H. E. Lyons, "The Many Faces of Safeguards," Journal of the Institute of Nuclear Materials Management, VI, No. 111 (Fall 1977), 37-43.
7. L. M. Brenner, "The Role of Containment and Surveillance in Integrated Safeguards Systems," Journal of the Institute of Nuclear Materials Management, VI, No. 111 (Fall 1977), 94-100.
8. Nuclear Safeguards Technology Handbook, HCP/D6540-01, U.S. Department of Energy, December 1977.
9. Measurement Reliability for Nuclear Material Assay, LA-6574, Los Alamos Scientific Laboratory of the University of California, January 1977.
10. Diversion Path Analysis Handbook, Vols. I and II, U.S. Department of Energy, Safeguards and Security, October 1976.
11. James D. Williams, "DOE/SS Handbooks--A Means of Disseminating Physical Security Equipment Information," Journal of the Institute of Nuclear Management, VIII, No. 1 (Spring 1978) 65-76.
12. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, Albuquerque, New Mexico, November 1976 (Revised October 1977).
13. Sigmund Scala, "Generic Data Base for Modeling Safeguards Security Equipment Interim Report," Stanford Research Institute, prepared for Sandia Laboratories on Contract No. 05-8748, September 1977. (To be used in safeguards programs under the jurisdiction of the Nuclear Regulatory Commission (NRC))
14. Catalog of Physical Protection Equipment (NUREG-0272) and Guide for the Evaluation of Physical Protection Equipment (NUREG-0273), U.S. Nuclear Regulatory Commission, January 1978.
15. R. A. Fite, Interim Report: Commercial Sensor Evaluation, MERADCOM, Ft. Belvoir, Virginia, August 7, 1975.
16. Siting Criteria for SAFE Programs, (SAFE-SIT-0001), Deputy for Command and Management Systems, Base and Installation Security System Program Office, July 1976 and Master Development Plan for the DOD Base and Installation Security Systems, April 1976.
17. Report on Sensor Technology for Battlefield and Physical Security Applications, MERADCOM, Ft. Belvoir, Virginia, July 1977.
18. "Selection and Application of Joint Services Interior Intrusion Detection System," Department of Army Technical Bulletin TB 5-6350-262, Department of Air Force T031S9-1-101, Department of Navy Navelex 0967, 464-9010, February 1974.
19. Dennis L. Mangan, "DOE-Sponsored Evaluations of Interior Intrusion Detection Systems," 1978 Carnahan Conference on Crime Countermeasures Proceedings, May 15-19, 1978.
20. W. C. Garrett, Infrared Motion Sensor Evaluation, No. 2237, U.S. Army Mobility Equipment Research and Development Command, Ft. Belvoir, Virginia, March 1978.
21. Dennis L. Mangan, "The DOE Handbook on Intrusion Detection Systems," scheduled for publication in the January-February 1979 issue of Nuclear Safety.

MODULE 7

SESSION 7.1

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

7.0 INTRUSION DETECTION SYSTEMS

Session Title: 7.2 Alarm Assessment and Reporting Systems

Date: Friday, 10 November

Presented By: J. D. Williams, Sandia Laboratories

Time: 0830 to 1000

Session Objectives:

After the session, the participants will be able to

1. Identify the pertinent parameters of alarm assessment and alarm reporting systems, and
2. Discuss the process of integrating and interfacing the various individual elements, procedures, and personnel involved in intrusion detection into a single operationally effective system.

Summary:

Alarm assessment is the process of determining what activated a particular sensor. Accurate and rapid assessment is essential to prevent the commitment of response forces as a result of nuisance alarms, false alarms, or diversionary action by intruders. Alarm reporting systems include a wide variety of equipment which is used to communicate and display alarm information gathered from intrusion detection sensors and assessment equipment to security personnel.

It is essential that any new or to-be-improved intrusion detection system be carefully planned and analyzed to ensure that it will reliably perform its function and that its strengths and weaknesses are identified and understood. Planning and analysis include development in the following areas: (1) general physical protection system design philosophy, (2) preliminary intrusion detection system design considerations, (3) experiments and evaluation, (4) final intrusion detection system design consideration, (5) construction and installation, (6) program scheduling, (7) cost considerations, and (8) system procurement guidelines.

Additional Resource Materials:

30-minute film--Lighting Systems, Video Motion Sensors, and Thermal Imaging Devices.
Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, Albuquerque, New Mexico, November 1976 (Revised October 1977).

ALARM ASSESSMENT AND REPORTING SYSTEMS

CLOSED-CIRCUIT TELEVISION ASSESSMENT SYSTEM

A video alarm assessment system provides security force personnel with a means of rapidly assessing alarms from locations physically remote from the sensors. In addition to real-time observation, a video alarm assessment system has the capability of event recording and storage. This capability permits subsequent video replay of recorded activity which occurred within the protected zone, even when the activity took place under conditions of multiple simultaneous alarms or delayed security personnel attention.

A basic closed-circuit television system (including proper lighting) is illustrated in Figure 7-28. The video system is composed of one or more cameras and lenses at the remote end, a display monitor at the local end, and various transmission, switching, and recording systems which connect the cameras to the display

Figure 7-28. Basic Closed-Circuit Television Alarm Assessment System

monitor. The camera and lens convert the optical sense to a video signal which is passed over a transmission system to a video switcher at the control location. The switcher can distribute the video signal to one of several monitors for display. A selected signal may also pass through a video recorder for delayed display or permanent retention.

Auxiliary camera equipment which provides extra control of the camera and lens system is also available. System display or recording may be dependent on the method of synchronization employed. The output display may be augmented by the addition of alphanumeric data which use information display equipment. Finally, through installation of a video motion detector, the assessment system may be used as an intrusion detection sensor.

Camera/Illumination Systems

The primary goal in the design of a closed-circuit television assessment system is to minimize overall cost while maintaining adequate system performance. Adequate performance can be achieved with the following camera/illumination systems:

1. Inexpensive, low sensitivity cameras and expensive intense illumination,
2. Medium sensitivity low-light-level cameras and moderate illumination, or
3. Expensive, high sensitivity, very low-light-level (intensified) cameras and low-level illumination.

Energy considerations as well as initial installation costs make the first option unattractive. The use of low-light-level cameras coupled with night-time artificial lighting is a more frequently chosen alternative than the use of extremely low-light-level cameras for a variety of reasons: (1) significantly reduced camera procurement and maintenance costs, (2) reduced possibility of camera damage under high (full sun) scene illumination conditions with the resultant increase in resolution, (3) the psychological deterrent effects of night-time area illumination, (4) increased probability of intruder detection (due to projected shadows in the clear zone), and (5) implementation of security countermeasures (improved visibility conditions).

Camera tubes which fall into the low-light-level category are the silicon diode array vidicon and the Newvicon. Regardless of the system chosen, the lighting spectrum must be closely matched to the camera response to ensure an efficient system.

Closed-Circuit Television Cameras

Selection of a closed-circuit television camera should take into account the following desirable characteristics:

1. High sensitivity (to best utilize available light),
2. Low lag (to retain picture clarity at all points in the scene),
3. Long life (for resistance to burnout),
4. High resolution (for good picture definition), and
5. Low blooming (to maintain an adequate picture in the presence of bright sources).

Table 7-II can be used to obtain a rough idea of how various popular camera tubes compare with respect to these characteristics. A rating of 1 indicates superior performance; a rating of 3 or 4 indicates relatively poor performance. Table 7-II is only meant to give an overview of common tube types. It should not, in itself, be used for design purposes.

TABLE 7-II
Camera Tube Types

<u>Camera Tubes</u>	<u>Sensitivity</u>	<u>Lag</u>	<u>Life</u>	<u>Resolution</u>	<u>Blooming</u>
Standard Vidicon	4	3	2	1	1
Silicon Diode Array Vidicon	3	1	1	3	3
Newvicon	2	2	1	2	2
Silicon Intensified Target Vidicon	1	1	3	4	4

Lenses

The basic function of the lens in a video camera system is to focus the light energy which is reflected off the object and enters the lens onto the image tube target where it is converted into an electronic video signal. An important lens parameter is the focal ratio or f number, which is a measure of the light-gathering power of the lens. A small f number (1 to 2) is desirable. Other important parameters include focal length, which determines magnification, and field-of-view, which determines how much of the actual scene is viewed by the camera.

As a general rule, a short focal length lens will not resolve the detail that a longer focal length lens will. As a result, for a desired minimum resolution, the range (length of the coverage) of the short focal length lens will be less than that of the long one, as Figure 7-29 illustrates. The sectors indicate the usable camera coverage.

Figure 7-29. Practical Field-of-View versus Focal Length of Lens

Choosing the correct lens to fit the application is very important. The selection procedure is detailed in Section 6.2.3 of the Intrusion Detection Systems Handbook.¹

Lighting

The two most important parameters that characterize a closed-circuit television lighting system are its minimum intensity and its evenness of illumination. The intensity must be great enough to ensure adequate performance of the chosen camera system. Of equal importance is the evenness of illumination, which is characterized by the light-to-dark ratio (maximum intensity/minimum intensity). A light-to-dark ratio of greater than 10:1 will produce unacceptable pictures in which the bright areas appear washed out and the darker areas appear black due to lack of light. A ratio of 6:1 or even 4:1 is preferable.

Table 7-III characterizes the popular lamp types. The left-hand column lists some of the more important lamp parameters. In general, the sodium vapor lamps are a good choice for exterior illumination due to their energy efficiency.

TABLE 7-III
Lamp Characteristics

	Incandescent	Quartz Iodine	Mercury Vapor	Metal Halide	High Pressure Sodium	Low Pressure Sodium
Efficiency (lumens/watt)	12-20	20-23	40-65	80-100	95-130	131-163
Spectrum	Broad, high in infrared	Broad, high in infrared	Blue Green	Broad	Gold-Yellow	Mono- Chromatic Yellow
Restrike Time	Immediate	Immediate	3-6 Minutes	10-20 Minutes	2 Minutes or less	Immediate to 2 Mins.
Time to Full Output (Initial or restrike)	Immediate	Immediate	3-7 Minutes	3-5 Minutes	3-4 Minutes	8-15 Minutes (immediate) 5 Minutes (restrike)
Lamp Life (hours for size)	750 (100W)	2000 (1500W)	24000 (100-400W)	15000 (400W)	20000 (400W)	18000 (180W)
Voltages Available	5-5000	45-5000	175-3000	175-1500	50-1000	35-180

Transmission Systems

The overall function of a video transmission system is to interconnect the remote cameras to the local video monitors in such a way that no undesirable effects are introduced to the video signal. Video transmission may be accomplished in a number of ways. One of the most widely used techniques for multiple-camera alarm assessment purposes is cable transmission, which may be base-band video or video-modulated radiofrequency. Microwave links and optical (e.g., infrared) systems are also employed in some installations.

Video Cable--The level of performance demanded from a video cable is typically based upon (1) the frequency content of the particular video signal transmitted through it, and (2) the physical and/or electrical environment in which it will be used.

All transmission lines, including video cables, will have resistive and/or reactive losses associated with them. With video cable, this loss is primarily a function of the distributed interconductor capacitance and core resistance. This loss is normally expressed in decibels per unit length (at various operating frequencies) and/or capacitance per unit length. Attenuation increases with both frequency and section length and varies widely with the particular cable type in use.

To compensate for these inherent signal degradations, conditioning of the video signal must be accomplished at one or more points between the camera and the display monitor. A wide range of commercial signal-conditioning equipment capable of satisfying most video cable transmission objectives is available.

Signal-Conditioning Equipment--All video cable will impart a finite amount of degradation to the video signal. This loss of signal quality, which can take the form of high-frequency attenuation, superimposed noise, and phase addition, can radically alter the amount of useful information contained in the resulting monitor image. High-frequency attenuation reduces image detail (resolution), while phase addition (in its undesirable form) causes image "smear," which is similar to ghosting, due to the vector addition of incident and reflected signals at cable and/or equipment impedance discontinuities. Superimposed noise can be observed on the monitor in two forms: (1) high-frequency (random) noise, which manifests itself visually as "snow," and (2) powerline frequency (60-Hz) noise, which manifests itself as black or white horizontal bands ("hum-bars") on the monitor screen. Both forms of noise partially obscure the desired image on the monitor screen, effectively reducing system resolution.

Video equalizers restore the signal to the same amplitude versus frequency relationship as the original (camera-output) signal. Hum clampers and isolation transformers can be used to remove powerline frequency hum that often combines with the video signal on long cable runs. Balanced line transformers will improve the noise introduced into the video signal under the conditions of extreme electromagnetic interference and long cable runs. Various amplification systems can be used to bring a video signal to the correct amplitude.

Radiofrequency Transmission Equipment--If a large number of cameras which require video signal transmission over relatively great distances are incorporated into an alarm assessment system, video cable installation and transmission equipment for each camera can be excessively expensive. In such instances, transmission of radiofrequency multiplexed video signals over a single cable or over a microwave link may be a cost-effective alternative. This type of video transmission is characteristic of commercial cable television systems.

The radiofrequency modulator, which is located at the remote camera site, converts the base-band video output from the camera to an amplitude modulated or vestigial side band signal in a unique channel between 5 MHz and 300 MHz. A number of channels can thus be combined (by frequency division multiplexing) into a composite, single radiofrequency signal. Once the video signals have been modulated into the radiofrequency band, the signal can be amplified and transmitted directly over hard wire to interconnect the remote radiofrequency transmitter and the local radiofrequency receiver. Alternately, the radiofrequency signal can be used to modulate a microwave transmitter which operates at a carrier frequency between 2 and 40 GHz. The remote microwave transmitter links to an associated local microwave receiver over a line-of-site path of up to 80 km. (Radiofrequency cable is normally used when multiplexed transmission distances do not exceed 8 km.)

At the local (control) site, a compatible radiofrequency receiver demultiplexes (demodulates) the remote frequency modulation transmitter output to recover the individual (base-band) video signals for subsequent routing and/or display.

Synchronization Generation

In an ideal closed-circuit television system, the scanning electron beam which generates the video signal and the electron beam which generates the picture on the display monitor are at identical places at identical times. Synchronization pulses control this time/position relationship by controlling the oscillators driving horizontal retrace blanking and vertical blanking between fields.

Two sources exist for synchronization signals. In the first, local oscillators in the cameras provide synchronization which is often individually phase-locked to the alternating-current line frequency. Each camera generates its own synchronization pulses, which may differ in timing and frequency from the pulses of all the other cameras. In the second, a master synchronization generator can be used to provide a consistent signal to all cameras. In this method, the synchronization pulses are transmitted to each camera, thus controlling the camera oscillators. Pulses are distributed through delay amplifiers so that all video signals arrive precisely in phase at the display location regardless of transmission line length. Synchronization signals can also be distributed to auxiliary equipment such as monitors or recording devices. The master synchronization phase may be arbitrary or phase-locked (gen-locked) to an external source.

Under some circumstances, vertical roll can be considered as objectionable due to loss of information during the interval in which the roll occurs. A master synchronization system should be employed to ensure clean switching and recording which is free of vertical roll.

Video-Switching Equipment

Most alarm assessment systems employ more cameras than display monitors since there will seldom be instances when all camera sectors simultaneously require viewing. For this reason, video-switching equipment may be utilized between a large number of camera signal lines and a relatively small number of display monitors. The associated alarm sensor system generally interfaces with the switching system in such a way that an alarm in any sector causes the associated camera output to be automatically displayed on a local monitor. Multiple alarms are processed in a similar manner but may require additional monitors and/or priority-sensitive, camera-switching control equipment. However, the basic function of all video switchers is the same, i.e., to effectively interface multiple video signals (cameras) with one or more monitoring devices (monitors and/or video recorders).

Switcher Types--The simplest type of switcher connects one of a number of inputs to a single output buss. Only one input can be connected at a time. Multiple output switchers can switch one or more inputs to any combination of output busses. In a fully connected switcher, any input can appear on any output, one input can go to all outputs, or different inputs can go to each output.

Switching can be either passive or active. In a passive switcher, control is by manual input. The actual switching is performed by pushbutton contacts and the video signal is routed through the switcher with no electronic conditioning or timing. Active switchers typically may include input and output amplifiers which provide signal isolation, impedance matching, and amplitude control. Electronic processing of the video signal can be included to control the timing of switching between video signals. The switching path for the video signal is through relay contacts of semiconductors.

Some widely used switching systems include

1. Manual switching (passive system),
2. Sequential switching (all camera outputs are sequentially scanned),
3. Alarm-activated switching (alarmed-sector camera information is automatically presented to the output regardless of the selected input before alarm activation), and
4. Remote switching (some switching is done prior to entry of the signals into the security command center).

Video Recording

The purpose of the video recording system is to produce a permanent record of an event on a magnetic-coated medium. In addition to providing historical information for subsequent study, it provides an aid to the real-time assessment framework

by adding instant replay and stop-action capabilities into the system. The most prevalent system in use for closed-circuit television applications is the helical scan system (video tape). This system has a relatively simple design and is inexpensive, reliable, and easy to operate and maintain. Another important system is the disc system. While considerably more expensive than the helical scan method, the disc system provides virtually instantaneous recording capability--a feature vital to some assessment systems and desirable in almost all systems.

Disc/Tape Usage Characteristics---Although video discs and video tape recorders both have the same basic function, i.e., storing video data, their usage characteristics are entirely different.

Video tape recorders provide long-term storage of large quantities of video data, are able to store up to several hours of real-time video data, and are readily removable for later use or observation on other machines. The mechanical components and tape interface of video tape recorders do not, however, support continuous instantaneous recording capabilities. Component and head tape wear requires daily maintenance to preserve recording capabilities if the machine is set in a ready-to-record mode. In addition, major repairs can be expected every several months.

Video disc machines can provide near instantaneous recording since the low mass head can be retracted from the disc surface when not in use. The only moving part is a high mass disc driven by a motor which is rated for continuous operation. When a command to record is given, the head can be positioned in a few milliseconds and start recording as soon as the next video field appears. However, video discs can store only about 200 frames (400 fields) of video data and often cannot be changed from one machine to another.

The choice of whether to use a disc or tape recorder (or both) depends on whether the capability for instantaneous recording is required. Discs will be required if (1) the assessment area is small or contains no barriers or other delay elements, allowing an intruder to pass through quickly (i.e., in less than 15 seconds), (2) multiple simultaneous alarms can be expected, requiring successive observation and assessment, or (3) the system operator is required to perform other functions which may prevent him from assessing alarms within a very short time after he has received notification of their occurrence.

Video Monitors

Video monitors work in a manner opposite to the working of a video camera in that a scanning beam generates a visual scene on the face of the output tube. Monitors are similar to home television receivers in function but generally have wider bandwidths and do not have radiofrequency tuning. Low impedance (75-ohm) or high impedance (looping) inputs are normally provided. High impedance looping allows a single video signal to drive multiple inputs (loads). In addition, the video monitors have a provision for accepting an external synchronization input in place of the synchronization contained in the composite video signal.

Since the video picture monitor is the final output transducer in most assessment systems, a level of performance compatible with other system components is an important concern. Monitors utilize the same dimensions for resolution as video cameras, namely television lines (horizontal resolution). The vertical resolution of both monitors and cameras is limited by the number of "active" scan lines, i.e., those lines containing picture information. There are commonly 340 television lines for a 525 scan line system; hence, the horizontal resolution alone may be specified. Monitor resolution is frequently expressed in conjunction with a certain level of screen brightness or illuminance; separate degrees of resolution are specified for the center (where resolution is normally highest) and corners of the screen. Monitors having 700 to 800 television lines of horizontal resolution are often employed in 525 line scan rate systems operating at up to 10 MHz of horizontal system bandwidth.

An ideal monitor would be capable of displaying white, black, and an infinite number of shades in between; whereas, a worst-case (bistable) monitor could display only white or black regardless of video input. Monitors capable of 10 discernible shades of gray or better have produced acceptable results in existing assessment systems.

Video Motion Detectors

Intrusion in an area assessed by a video system may be directly indicated by a change in the video scene during the intrusion attempt. This change may be sensed by a video motion detector to provide an alternate intrusion sensor. Changes in a video scene are sensed by comparison of the present scene with a view of the scene during a nonintrusion period. Significant changes in brightness or contrast cause an alarm to be issued. The reference scene is periodically updated so that slow changes in overall light level do not cause alarms.

The main differences among video motion detectors derive from the method used to process and compare video signals. There are two primary types of comparison methods: fine grain comparison and integrated comparison.

In fine grain comparison, the details of a video scene are essentially compared element by element. Signals may be in analog form or in digital form. In analog form, the video scan lines are compared; in digital form, a number of discrete points are compared.

Analog analysis requires a complex signal storage medium such as video disc or tape for preservation of reference signals. The present scene is then processed by a real-time comparison to the reference scene. In digital analysis, the reference signal is digitized and stored in a computer-like memory. This reference is then compared with corresponding points of the present scene after it has been digitized.

In integrated comparison, an average value for scene illumination is measured for comparison with the averaged reference scene. Integrated comparison video motion detectors are almost strictly analog devices and are usually much less expensive than fine grain comparison hardware.

SYSTEM DESIGN EXAMPLE

This section provides an example of how a video alarm assessment system is applied to a sensor-alarmed perimeter. This example is developed to indicate the major factors in the system design. It is intended merely to serve as an overview and therefore does not give a detailed description of the design of an actual system. For the purposes of this discussion, assumptions are made which require specific hardware applications but, in reality, there are many alternate configurations and solutions to the problems posed which should be considered for application to an actual system.

Site Description

The site considered in this example is illustrated in Figure 7-30. The 10-metre-wide clear zone is divided into six sensor sectors; the sensors are located midway between fences. The function of the area enclosed by the site need not be specified; it is simply assumed that it presents an attractive target for theft or sabotage. The site is assumed to be part of a larger facility which contains the security control center, which is located approximately 1 km from the example site. Two guards are permanently stationed at the site, primarily for access control.

Objectives

The first step in the design of a closed-circuit television assessment system is the establishment of system objectives and restraints.

1. Coverage--For the example, the video assessment system interfaces with a perimeter alarm system and no observation towers are present; therefore, video provides the only means of rapid assessment. The video system must provide complete coverage of the area between the fences around the entire perimeter. (Note that video coverage is fixed to the perimeter. A manned observation tower provides coverage of the entire area.)
2. Resolution--Recognition of humans and detection of small animals is required for this example. For animals no smaller than 20 cm, this translates to a maximum horizontal field-of-view of 27 metres (as calculated in the Intrusion Detection Systems Handbook, Sec. 6.8.2). This development of field-of-view assumes a high resolution wideband video system. Equipment must be procured which can meet these requirements.
3. Operations--Only a single guard position, with no technical training requirements, is available for system operation. The operator must perform other security duties in addition to having responsibility for assessment of this system.
4. Assessment Delay--Two factors enter into the consideration of assessment delay. First, the distance from the sensor line to the interior of the protected area can be crossed in approximately 6 seconds (1 second to

Figure 7-30. Perimeter Assessment System Example Site

cover 5 metres, 4 seconds to scale the fence, and 1 second to get well inside the protected area). Second, due to his other responsibilities, the operator may not be available to immediately assess incoming alarms. Four actions are possible to preclude loss of video intrusion assessment due to delay:

- a. Increase the time required to traverse the assessed area. This may be accomplished in a number of ways: (1) by enlarging the area (consistent with limitations on resolution requirements), (2) by

- moving the sensors to the outer fence (consistent with increased false alarm rate due to small animals, blowing debris, fence motion, uncleared personnel access, etc.), and (3) by improving the barriers through installation of more fences, obstacles, etc.
- b. Record video scenes at less than 5-second intervals. This may be accomplished by time-lapse video tape or disc recorders. Alarms would freeze the recorder at the nearest picture after alarm.
 - c. Provide nearly instantaneous recording. This would require the use of a video disc with the attendant need for computer-controlled switching, disc operations, and master sync for all cameras.
 - d. Reduce human delay times. This may be accomplished by assigning one security operator to do nothing but operate the alarm system.

The example used assumes that choice of action c, above, is available, e.g., video disc recording. Note that this is done in order to allow the requirements of a complex video assessment system, which is more suited to a large intrusion detection system than to the relatively simple example presented here, to be illustrated. If a design for an actual system were based on this site layout, a combination of action a (increased traverse time) and action b (time-lapse recording) could be the most cost-effective system.

5. Display--Video display will be installed in the security control center. Two monitors will be provided, one for viewing real-time scenes and one for display of recorded scenes. (Note that for a six-camera system, two monitors provide real-time coverage of one-third of the entire perimeter. This might be adequate for strictly real-time assessment if operator delay is not excessive.)

Site Survey

With the objectives completed, a detailed site survey should be performed, with particular attention paid to the following six items:

1. Terrain--The ideal terrain would be smooth, flat, and free of vegetation. (This condition is assumed to exist for this example.) Any deviation from these conditions may require additional cameras and lighting.
2. Fencing--To be cost-effective, inner and outer perimeter fences should be straight and equidistant from each other. Deviations will complicate camera field-of-view layout.
3. Obstructions--The presence of obstructions in the area between fences will create "shadows" where camera vision is blocked. The problems introduced by obstructions in the cleared area can be seen by the following example. Assume that a guard house is situated between the fences at the road entering the area. Camera coverage of Sector 2 must be provided by a camera north of the sector (looking south) since the view of a camera south of the area (looking north) will be blocked. Likewise, a major obstruction in the middle of a sector will preclude total sector coverage by a single camera. Sensor layout should be done in conjunction with camera layout so that assessment is not unduly complicated.

4. Transmission Routing--For hard-wire systems, determination of cable layout paths and total cable length from camera to control room is needed to ascertain equalization, clamping, gain, and isolation requirements. For wireless systems (e.g., optical or microwave), straight or mirror-reflected path measurements must be made to aid in the determination of system power requirements. Routing is also dependent upon weather conditions.
5. Manmade Interference--The transmission routing path should be scrutinized for any possible sources of interference such as high-voltage lines, buried powerlines, power transformers, ignition noise, and commercial radiofrequency transmission sources (assumed not to exist in this example). Whenever practical, paths should be routed to avoid these interference sources. It is, for example, less expensive and easier to compensate for an additional 30-metre length of cable than it is to add special cabling formats and isolation transformers to compensate for a strong induced 60-Hz signal from a nearby powerline. In addition to visual observation, measurements should be taken if any doubt exists as to the influence of a potential noise source on the transmission system.
6. Weather--Temperature extremes, humidity, hail, wind, rain, snow, and lightning all place requirements on the assessment system. For this example, it is assumed that wind and rain occur frequently enough to require camera faceplate windshield wipers.

Camera Layout

The camera layout for Sectors 2, 3, 5, and 6 is shown in Figure 7-31. The cameras are assumed to use 100-mm focal length lenses. (The choice is taken from Section 6.8 of the Intrusion Detection Systems Handbook.) Note that each camera allows assessment of the sector (including fences) between 100 metres and 200 metres from the camera. Mounting height and tilt will be considered later.

The layout for Sectors 1 and 4 requires more thought. A 100-mm lens can be used but the camera must be placed outside the secured area (and thus outside the sensor-alarmed perimeter), as illustrated in Figure 7-32. Alternatively, two cameras, equipped with 50-mm lenses, can be used as shown in Figure 7-33. However, neither layout is totally satisfactory. Either a camera is placed in an unprotected area (and cables must then cross the sensor field) or two cameras must be turned on for one alarm. The two-camera system is workable (in the context of this example) only if two disc recorders are available to record both signals simultaneously or assessment delay objectives are relaxed. A better solution, perhaps, would be to divide Sectors 1 and 4 into two alarm areas, preserving the one-to-one relationship between cameras and sectors.

For this example, the option of single-camera coverage is chosen. Since the site is remote from the command center, some cable crossing of the exclusion zone is required; therefore, the camera cables will not present an additional problem. Camera housings and junction boxes will have to be equipped with tamper switches, and the camera signal should be continuously monitored by a video presence

Figure 7-31. Camera Layout for Sectors 2, 3, 5, and 6

detector. An auxiliary operator-controlled pan/tilt and zoom-equipped camera might also be installed to allow remote inspection of the cameras covering Sectors 1 and 4.

Figure 7-32. Sector 1 Layout Option 1

Figure 7-33. Sector 1 Layout Option 2

Lighting

Given the initial choice of camera lens focal length, lighting requirements can be established and lens speed (f number) chosen. Fast (f 1.4) 100-mm lenses can be obtained, minimizing light-level requirements. In this example, based on information contained in the Intrusion Detection Systems Handbook, calculations indicate a need for an illumination of at least 8 lumens/m^2 for this lens mounted on a low-light-level (silicon diode array tube) camera. This is fairly easy to achieve over the 10-metre-wide clear zone. (Note that if lighting requirements are excessive due to the unavailability of a lens with a small enough f number, the area coverage and camera positioning might have to be adjusted.)

Equipment Selection

Once the number and placement of cameras are completed, the remainder of the video assessment system can be designed. The camera video outputs can be transmitted directly to the security control center or can be wired to a remote switcher. The maximum cable run at this site for direct wiring is nominally 1500 metres. This is sufficiently short that commercial video equalizers at the receiving end can compensate for cable losses. If the distance were greater, placing a six input/two output switcher at the site might be more economical since fewer video cables would need the more involved signal conditioning to run beyond 1500 metres.

Selection of the remainder of the equipment is straightforward. Once all the equipment has been chosen, the video assessment system is then assembled as shown in Figure 7-34. Components are required for the specific reasons outlined below:

1. The environmental housing is necessary since blowing rain conditions require the use of windshield wipers.
2. The equalizer and clamper correct high-frequency attenuation in the cable and control induced hum.
3. The presence detector provides continuous monitoring of the video signal of the cameras located outside of the secured area and of the cables, all of which run through an unsecured area.
4. The video disc recorder provides the instantaneous disc recording

Figure 7-34. Video Assessment System Layout Example

required by the short assessment time windows and the uncontrolled delay in assessment time.

5. The time/date generator is necessary since assessment from the recorded scene may require knowledge of time of the alarm.
6. A 10 x 10 switcher to match manufacturer specifications may be required for the eight inputs directed to two outputs (monitor and video disc recorder).
7. The switcher and disc automatic control provides switching between input, recorder, display, and control of disc functions required by disc use. This is typically done by a microprocessor, minicomputer, or other logic interface which will be custom-designed for the site.
8. The switcher manual control is necessary for certain specific operational requirements and, in case of computer failure, allows video assessment.
9. The master sync, sync delay amp provides the means for identical timing of disc recordings.

The total system cost is approximately \$83,000, exclusive of construction and lighting costs.

ALARM REPORTING SYSTEMS

The term "alarm reporting system" encompasses a wide variety of equipment used to communicate alarm information from intrusion sensors to security personnel and includes both alarm communication systems and display/console systems. The various commercially available alarm reporting systems differ substantially. Some notable differences include

1. The geographical distribution of the alarm communication hardware,
2. The degree of security, e.g., line supervision, which is provided by the alarm communication system,
3. System capacity with regard to the number of points or zones which can be monitored,
4. The quality of information which is presented to the security personnel (or operator/guard),
5. The degree of control which the operator/guard can exercise over the information presented,
6. The clarity of the information presented,
7. Ease of operation, and
8. Overall system cost.

Alarm Communication System

An essential part of an intrusion detection system is the alarm communication link which transmits information from the intrusion detectors to the alarm display equipment. Two principal considerations in alarm communication links are (1) the basic economic and technical aspects of the technique used to transmit the alarm information and (2) the degree of security provided for the communication system. An intrusion detection system is of little value if the communication link from the sensor to the control center fails to report alarms because of accidental damage or malevolent attack.

A number of techniques are available for the transmission of alarm signals, e.g., landlines, radio links, dedicated point-to-point circuits, and shared multiplexed circuits. Each of these techniques offers unique cost and performance advantages and each technique is usually best suited to a specific set of conditions.

Communication links can be divided into two broad categories: (1) passive links (i.e., a signal is sent over the link only when an alarm occurs) and (2) active links (i.e., some type of signal is continually sent across the link). The most common security measures for passive communication links physically protect the link from an attack. Supervisory systems have been developed to detect unauthorized monitoring of active communication links. Physical protection techniques include the use of conduit, cable burial (and camouflage), the use of asphalt and concrete, etc. Supervisory systems include (1) static in which the "no-alarm" condition is always represented by the same signal, e.g., direct-current and alternate-current end-of-line resistor systems, and (2) dynamic systems in which the "no-alarm" condition is a signal which continually changes with time via random encoding, pseudorandom sequences, and cipher-text-auto-key. Dynamic systems typically provide more security than static systems. The system designer has to recognize the advantages and disadvantages of each of the various techniques to avoid an overkill system.

Display/Console Considerations

A wide variety of systems is available for presenting information to security personnel. The various types of equipment include

1. Annunciator panels, which provide individual lights to simultaneously display the status of every alarm circuit,
2. Numeric readouts, which use a single digital display to report alarm information from one alarm circuit at a time, and
3. Computer-driven cathode ray tube displays, which simultaneously present a wide variety of alarm circuit information.

These various approaches to the alarm display problem offer a wide range of capabilities but also present a number of distinct limitations and disadvantages. Specific aspects of alarm reporting systems which must be considered in determining the appropriate type of display/console include (1) compatibility with operational procedures, (2) human factors, (3) selection of information to be displayed, (4) display techniques, (5) organization of the display, (6) operator interaction, (7) possible report generation, and (8) backup considerations.

INTRUSION DETECTION SYSTEM INTEGRATION

This section contains general information relevant to intrusion detection system integration, which is the process of completely integrating and interfacing the various individual elements, procedures, and personnel involved in intrusion detection into a single operationally effective intrusion detection system. The expression "operationally effective" describes systems which have achieved a reasonable balance among (1) optimization of the system, (2) understanding, acceptance, and efficient use of the system by security personnel, and (3) a sufficient degree of detection capability at the facility.

It is essential that any new or to-be-improved intrusion detection system be carefully planned and analyzed to ensure that it will reliably perform its function and that its strengths and weaknesses are identified and understood. Planning and analysis include development in the following areas:

1. General physical protection system design philosophy--In the design of a physical protection system, the general concepts that need to be addressed include the postulation of threat, the interplay of detection, delay, and response, the concept of protection-in-depth, which involves the use of a number of distinct safeguards measures which the adversary must defeat in sequence in order to be successful, and system design methodologies, which include analyses and evaluations to determine the effectiveness of the design.
2. Preliminary intrusion detection system design considerations--The major considerations that influence the preliminary design of an intrusion detection system include site-specific items, e.g., procedures, personnel, and environment, and initial equipment identification for the main elements of the system, i.e., the sensors, alarm assessment equipment, and alarm reporting equipment.

3. Experiments and evaluation--In almost every instance, some on-site experiments and evaluations will be required in order to identify the correct equipment for the system. Although one of the intents of this discussion is to provide guidance for the selection of equipment, the state-of-the-art, particularly with regard to sensors, requires that this guidance be supplemented by on-site evaluation. Once the system designer has determined the intrusion detection system equipment appropriate for his site, his next step is to procure and subsequently evaluate this equipment. All in all, thought should first be given to the types of experiments and evaluations which need to be conducted. Candidate equipment should then be procured and evaluated. Finally, specific equipment should be selected.
4. Final intrusion detection system design considerations--The knowledge of site-specific factors involving procedures and personnel and the information provided by on-site evaluations should place the designer in a position to finalize a design that ought to result in an operationally effective system. To achieve a design in which all the elements combine to form one integral unit, the following final objectives must be implemented: (1) a simplistic design, complicated only to the extent necessary to achieve effectiveness, (2) standardized equipment that does not compromise effectiveness, and (3) a modular design which facilitates maintainability yet allows attendant effectiveness.
5. Construction and installation--During installation, the intrusion detection system is highly vulnerable to compromise. Protection against such compromise should be maintained.
6. Program scheduling--Good program scheduling has to be realized to efficiently achieve the final intrusion detection system.
7. Cost considerations--Cost estimates on equipment, construction, and installation must be established for budgetary reasons and to aid in the definition of the ultimate system.
8. Procurement guidelines--In addition to the procurement guidelines previously mentioned, assurance must be made that the equipment selected is available within the required time scales, that maintenance and troubleshooting manuals are available, and that all miscellaneous items have been identified and are available.

REFERENCE

1. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, Albuquerque, New Mexico, November 1976 (Revised October 1977).

VISUALS

Camera Tube Types

Camera Tubes	Sensitivity	Len	Life	Resolution	Blooming
Imageicon	4	1	2	1	1
Silicon Imageicon	3	1	1	3	3
Imageicon	2	2	1	2	2
Silicon Imageicon	1	1	3	4	4

VISUALS

NOTES

	Seamless	Shrink Tulle	Wetweave Canvas	Netal Balis	High Pressure Sodium	Low Pressure Sodium
Efficiency (lumens/watt)	12-20	20-25	40-65	80-100	75-110	110-140
Spectrum	Warm, little or infrared in infrared	Warm, little or infrared in infrared	Blue Green	Warm	Yellow-Red	Warm Yellow-Red
Service Time	Immediate	Immediate	1-2 Months	1-2-20 Months	2 Minutes or less	Immediate for 2 Min.
Time to Full Output (Initial or replace)	Immediate	Immediate	1-2 Months	1-5 Months	1-2 Min	1-15 Minutes (Immediate 5 Minutes (replace))
Lamp life (hours in use)	750 (1000)	2500 (15000)	10000 (15000-20000)	15000 (10000)	25000 (10000)	10000 (10000)
Voltage Available	4-5000	45-5000	175-1000	175-1500	50-1000	15-180

Security
Control
Center

Located Approx.
1000 Meters
From Site

VISUALS

NOTES

VISUALS

NOTES

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

8.0 ENTRY-CONTROL SYSTEMS

Session Title: 8.0 Entry-Control Systems

Date: Friday, 10 November

Presented By: V. K. Smith, Sandia Laboratories

Time: 1030 to 1200

Session Objectives:

After the session, the participants will be able to

1. State the role of an entry-control system in a physical protection system,
2. List the elements which may be applied in an entry-control system,
3. Discuss the philosophy of entry control, including psychological deterrents,
4. Discuss the trade-offs between manual, machine-aided manual, and automated entry-control systems, and
5. With the aid of the Entry-Control Systems Handbook, interpret the equipment evaluations, list equipment maintenance and installation precautions, and list equipment vulnerabilities.

Summary:

The Entry-Control Systems Handbook is discussed with an overview given of the applicable equipment. The three types of entry-control systems are compared and the equipment which is available for implementation is listed. A movie is shown which demonstrates the use of an entry-control system, and some entry-control system equipment is demonstrated.

Additional Resource Materials:

SAND77-1033, Entry-Control Systems Handbook

SAND78-1066C, Design Features of an Automated Entry-Control System

SAND78-1108C, Progress in the Development of Explosives Materials Detectors

MODULE 8

ENTRY-CONTROL SYSTEMS

An entry-control system functions in a physical protection system to allow the movement of authorized personnel and material through normal access routes, yet detect and delay unauthorized movement of personnel and contraband. Protected areas could contain special nuclear materials, vital equipment, and/or classified matter.

Four elements, which must react in a timely manner, form the foundation for an effective physical protection system.

1. Detection systems must detect and verify any unauthorized intrusion attempt by outsiders or any serious malevolent acts by insiders or outsiders.
2. Communication systems must ensure that all pertinent information is transferred to the point(s) where appropriate action can be taken.
3. Delay systems must impede continued adversary penetration into, or exit from, the area being protected.
4. Response systems, or forces, must counteract adversary activity and neutralize the threat.

These elements are equally important and none of them can be eliminated or compromised if an effective physical protection system is to be achieved. Detection, which encompasses not only entry control but also intrusion detection, is an important function since any delay scheme can eventually be penetrated, and without detection the response force would not be alerted. Delay elements must provide sufficient time after detection to allow the response force to arrive. Finally, the response force must be adequately prepared to neutralize the adversary actions.

Objectives

The objectives of an entry-control system to be used in a physical protection system at a nuclear facility are

1. To permit only authorized persons to enter and exit,
2. To detect the attempted entry of contraband material (weapons, explosives, and unauthorized tools),
3. To detect the attempted unauthorized removal of nuclear materials, and
4. To provide information to the guard control center to facilitate assessment and response.

In these systems, an alarm occurs when an entering individual is not properly identified or when contraband is detected. Upon receipt of an alarm at the control center, the problem is assessed, a determination is made of whether the alarm is false or real, and, if necessary a preplanned response is initiated. It is expected that all personnel and material would be examined for contraband where entry is controlled. This search should include maintenance tools, food, instruments, building materials, and operating supplies. Upon exit, all personnel and materials (such as operating and construction residue, materials for reclamation, equipment to be repaired, and sewage) should be examined for nuclear materials. Since vehicles are generally difficult to search, some facilities might find it advantageous to maintain vehicles captive to the controlled area.

Entry-control systems are considered for use in two specific areas: (1) protected area, and (2) material-access area. These areas are illustrated in Figure 8-1. The primary concerns addressed by an entry-control system are to detect the entry of unauthorized personnel and to detect contraband covertly carried by authorized personnel. Once detected, the unauthorized person becomes an adversary and any further penetration becomes an overt act and is not considered an entry-control problem.

Figure 8-1. Schematic of Areas to be Protected

Applicable entry-control equipment and systems are described in the Entry-Control Systems Handbook.¹ Some of the equipment that is described may not be suitable for use at all facilities; consequently, each facility should decide which equipment is appropriate for use. Users should not assume just because a piece of equipment is listed that it would be effective in a physical protection system.

ACCESS CONTROL

Personnel Authorization

Personnel authorized to enter a facility can utilize photo identification (ID) badges, coded badges, stored images, or memorized numbers. These credentials are used for authorization, not identification, and certify that a person has authority to enter a controlled area.

Credentials

The photo identification badge is the most common credential used for access control. However, the photo identification badge can be falsified. Even if the badge is not falsified, an individual can make up his face to match that on a stolen badge in an effort to gain unauthorized access.

A badge exchange system minimizes the possibility of a badge being counterfeited, lost, or stolen. Under this procedure, duplicate badges are held at each entry-control point. When an employee requests entry, a guard matches the individual to the photo on the corresponding exchange badge held at the entry-control point. If the comparison matches, the guard exchanges the badges and grants access. The employee's badge is held at the entry-control point until the employee leaves the area, at which time, the badges are again exchanged. In this way, the exchange badge worn within the protected area is never allowed to leave the area. The badge exchange system does not, however, prevent someone from making up his face to match the image on a stolen badge in order to gain unauthorized access.

The use of a stored image (video comparator) system requires a guard to verify an individual's identity based on visual characteristics; however, a securely stored image is used for comparison with a real-time image of the individual requesting entry. Although stored image systems are not positive personnel identity verification systems, they have an advantage over manual photo identification systems in that it is difficult to tamper with the stored image. In this sense, the stored image system is comparable to badge exchange systems. Two of the most important features of such a system are enrollment capability and access time. Enrollment capability is the maximum number of images that can be stored by the system. The access time is the time elapsed from entry of the identification number until the stored image is displayed for viewing. Stored image systems which are commercially available include

1. The television video comparator (video tape recorder),
2. The microfiche video carousel, and
3. The photograph/video carousel.

These systems utilize a coded badge or keyboard to call up the stored image for projection and visual comparison by the guard.

Coded-credential systems, also called key-card systems, are commercially available with a wide range of capabilities. These include the following capabilities:

1. Maintenance of access authorization records for each coded credential,
2. Provision of unique identification code numbers which can be read by a machine,
3. Accommodation for 500 or more badges,
4. Termination of access authorization for an individual without the necessity of recovering that individual's badge, and
5. Provision for several levels of access authorization, such as access only at selected access-control points or only at certain times of the day.

The access authorization records could be checked each time access is requested. Each access action and its time of occurrence, access location, and the coded-credential identification number could be logged to provide a record of all entries.

The optical-coded badge contains a geometric array of spots printed on an insert laminated into the badge. Photodetectors in the badge reader detect the relative optical transmission of the spots and hence the code. To make this coded badge more tamper resistant, the pattern of spots can be concealed by making the badge opaque to visible light but transparent to infrared light. The spots are printed with ink which is opaque to infrared light. This technique offers good tamper protection and badges are reasonably difficult to counterfeit. The badge can be made completely nonmagnetic and nonmetallic so as not to interfere with sensitive metal detectors.

The electric-circuit-coded badge is a plastic-laminated badge containing a printed circuit pattern that selectively closes electrical circuits when inserted into a badge reader. For this credential, the badge reader is simply a card-edge connector for a printed circuit board. The badge, however, can be decoded with a simple electrical continuity tester and, consequently, counterfeit badges can be easily fabricated.

Several magnetic-coded badge systems are presently in wide use. This badge contains a sheet of flexible magnetic material on which an array of spots has been permanently magnetized. The code is determined by the polarity of the magnetized spots. The badge reader contains either magnetic sensors which are interrogated electrically or magnetic reed switches which are mechanically actuated when a magnetic spot with the proper polarity is located adjacent to the reed. The magnetic spots can be accidentally erased if the badge is placed in a sufficiently strong magnetic field. However, field experience has shown that this is not a significant problem. The amount of data which can be encoded on this type of badge is limited to approximately 60 bits. Since it is possible to build equipment to

recode or duplicate the pattern of magnetic spots, fabrication of a false credential is possible. It is more difficult, however, to falsify this type of credential than to fabricate an electric-circuit-coded badge.

Magnetic-stripe encoding is widely used in commercial credit card systems. For the magnetic-stripe-coded badge, a stripe of magnetic material located along one edge of the badge is encoded with badge data. These data are then read as the magnetic stripe is moved past a magnetic read head. Three materials have been utilized as the magnetic-stripe medium. The most common material, a single-layer, 300-oersted magnetic stripe, has proven more susceptible to accidental erasure than other magnetic badge types. The second material, a dual-layer, 300/4000-oersted tape provides erasure protection on the 4000-oersted layer; however, accidental writing on the 300-oersted layer may present a problem. The third material, a single-layer, 4000-oersted tape, cannot be accidentally erased. The use of alpha-numeric coding allows the badge holder's name to be included in addition to a badge number. Credential forgery is relatively easy since data from the magnetic stripe can be decoded or duplicate badges encoded by the use of parts from a common magnetic tape recorder.

The passive-electronic-coded badge is a badge into which electrically tuned circuits are laminated. In order for the badge and the code to be read, a swept-frequency radiofrequency field is generated and then the frequencies at which significant energy is absorbed are detected. These frequencies correspond to the resonant frequencies of the tuned circuits and are decoded to give a unique badge number or code. An important advantage of this technique is that the badge does not need to be inserted into a reader mechanism but can simply be placed near the antenna which serves as the read station. The disadvantages are (1) the badges can be decoded with common radiofrequency test instruments, allowing the counterfeit badges to be fabricated, and (2) the number of unique code combinations is limited to a few thousand.

The active-electronic badge system consists of a portable, electrically-coded badge and a stationary interrogation unit. The interrogation unit supplies power to the badge by magnetic induction and receives and decodes the credential number transmitted from the badge. When the interrogation unit is placed at strategic locations, such as corridors or doorways leading to protected areas, the system can automatically monitor, identify, and log the individual badge entering or leaving that particular area. The employee is not required to take any action whatsoever to accomplish the badge reading since the badge is read automatically when the employee passes through the radiofrequency field set up by the interrogation unit.

The capacitance-coded badge is a badge into which an array of small conducting plates is laminated. Selected plates are connected together and the code is read from the badge by an electronic reader which measures the capacitance of the plates and distinguishes which plates are isolated and which are connected.

The metallic-strip-coded badge utilizes rows of copper strips which are laminated in the badge. The presence or absence of strips in the rows determines

the code pattern, which is read from the badge as it passes through an eddy-current sensor.

There are many other methods of encoding badges but, in general, these badges can all be duplicated or forged. This fact should be considered (easy to duplicate or forge) before using a coded badge to grant access. However, coded badges are useful in conjunction with other systems to call up an identification such as the stored image, the memorized number, or the positive personnel identification information (discussed later).

Systems are available in which a memorized number is utilized to gain access. These systems use a coded credential to call the reference file associated with that badge number. An individual requesting access first inserts his coded credential and then enters his memorized number via a keyboard. A comparison is made of this number with the one with which the person enrolled and which is, therefore, stored in the reference file. If the numbers are the same, the person is granted access. The memorized number may be selected by the individual enrolling or it may be assigned. A five-digit number is usually used.

The memorized number is considered to be the most secure of the authorization systems. It does have vulnerabilities because an individual could pass the memorized number and credential used to call the reference file to an unauthorized individual or the memorized number could be obtained by coercion. Vulnerability can be reduced by an antipassback feature. This feature prevents a badge from being used for two successive entries or exits. Thus, for example, an employee cannot use his badge to gain entry through a portal then pass it back (for instance, over a fence or out a window) to another individual. This feature also applies to duplicate credentials.

POSITIVE PERSONNEL IDENTITY VERIFICATION

Positive personnel identity verification systems verify identity based on some unique physical characteristic(s) of the individual. Commercial equipment is available or prototype systems have been developed which utilize fingerprints, speech, handwriting, hand geometry, and various other individual physical characteristics. Problems common to all positive personnel identity verification systems are

1. The lack of uniqueness of the feature used for identification,
2. The variability of the characteristic, and
3. The difficulty of implementing the system which processes the characteristic.

Hand Geometry

The hand-geometry system is commercially available in the United States and will be discussed in detail. It is manufactured by the Identimat Corporation.

The Identimat hand-geometry system verifies identity based on the measurements (M1 through M4) shown in Figure 8-2. The measurements are made by

photodetector devices located beneath a top-lighted plate on which the hand is positioned. The hand is positioned on the plate by means of a peg which projects between the middle and ring fingers. The hand-positioning is not critical; however, the fingers must be placed firmly in each slot to block the light entering the photo detector that scans each slot. A capacitive switch must sense the presence of a hand to initialize the scan.

During enrollment, data on both hands are accumulated for the reference file. Twenty 16-bit words of template data (including identification, name, and status) are stored on a mass storage device for each individual who is enrolled. Enrollment time is less than 2 minutes.

Figure 8-2. Measurements used by Identimat

When an individual wishes to use the Identimat, he enters his reference file number (through either a badge reader or keyboard). A central controller randomly selects either the right or left hand and transmits the necessary reference file data from the mass storage devices to the Identimat. The Identimat processor informs the individual, by lights located on the hand scanner, which hand is to be scanned. The individual places the selected hand on the scanner as shown in Figure 8-3 and, after the capacitive switch has been closed for 1 second, the scanning process begins. The scan data are compared to the reference file data and, if the scan and file data match within a predetermined tolerance, access is allowed. A maximum of three scans is allowed for verification.

Figure 8-3. Identimat Hand Scanner

An Identimat hand-geometry scanner was tested in the Sandia Computer Annex. The test subjects comprised second- and third-shift operations personnel. Scanning was initiated by a pressure switch rather than by a capacitive switch. The preliminary results indicate that it is possible to achieve Type I and Type II error rates* of less than 2 percent with a throughput of 10 per minute, as shown by Figure 8-4. The throughput of 10 per minute does not include the identification entry time. The Type I and Type II error rates resulting from the Sandia tests may be inflated because, when the tests were monitored, some deviations from the required test procedures were observed.

Figure 8-4. Plot of Error Rates Versus Tolerance

*Type I error--Rejection of a claimed identity when, in fact, the identity claimed was true.

Type II error--Acceptance of a claimed identity when, in fact, the claimed identity was false.

The receiver coils are mounted on each side of the passageway perpendicular to the transmitter coil. Metal passing through the passageway disturbs the field; this change is sensed by the receiver coils as a voltage variation and is sent to the detection circuitry. The signal is amplified, the phase detected, and an alarm activated if the signal exceeds a threshold voltage. Phase detection techniques permit some optimization of detection for either ferrous or nonferrous metals.

When a metal detector is used as a shielding detector, it must be able to detect small quantities of lead; therefore, both the frequency and sensitivity are usually increased. Because of the high sensitivity, a "change" room is required where personnel using the shielding detector can remove all metal from their bodies. These detectors will only detect metallic materials such as lead; they will not detect composite materials such as lead-loaded paraffin.

Metal detectors are especially sensitive to metal moving outside of the detector field, either in front of or to the side of the detector; therefore, care must be exercised in detector placement. Any movable metallic objects such as doors, metal cabinets, forklifts, etc., near a metal or shielding detector can cause false alarms. Areas on the side of a wall opposite the side on which a detector is located should be carefully examined for movable metal objects. Radio transmitters, powerline transients, and flickering fluorescent lighting fixtures can also affect detector operation and can result in false alarms.

Far infrared detection techniques are being developed which can be used to detect contraband material carried by an individual. Such a system uses Schottky diode detectors that are sensitive to 0.50-mm and 1.2-mm infrared wavelengths. The use of these detectors in a passive mode appears feasible. The detection technique used is based on the difference in emissivity between cloth, leather, and any contraband material, such as metallic items, that can be carried on a person. It appears that small quantities of material, for instance, shielding material for special nuclear materials, weapons, and any kind of metallic object that is external to an individual's body can be detected by far infrared techniques. Since this work is still in the developmental stage, it will probably be 1 to 2 years before a prototype system will be available. This type of system may provide a more effective means of searching people for contraband than is provided by either the metal detector or the shielding detector.

Package Search

Packages may be searched for contraband manually or by active detection. Active detection methods used to detect various metal objects that are considered contraband include X-ray, multiple-energy X-ray, gamma-ray, and neutron activation. In general, these methods are not safe for use on personnel.

A conventional X-ray package search system such as the systems used by the airlines in the United States may not be adequate for use in nuclear facilities even though they are effective for airline use. The X-rays may not penetrate larger or more dense materials and shipping containers. Therefore, high-energy X-rays or multiple-energy X-rays are needed which penetrate the package being

examined. It has been demonstrated that a few centimeters of lead can be detected behind 10 cm of iron if 320-kV and 530-kV X-rays are used for detection. Based on the characteristics of different densities and different atomic numbers of materials and the use of dual energy X-rays, an automated system is being developed that uses computer image processing and pattern recognition equipment. Such a system will not be available for 3 to 5 years.

Explosives Detectors

Passive detectors detect the vapors emitted from explosives and can be safely used to search personnel. Some explosives cannot be detected because of the extremely low vapor pressures of these explosives. However, five commercially available detectors have been evaluated. Passive methods of detection are

1. Electron capture,
2. Olfactory,
3. Mass spectrometry, and
4. Plasma chromatography.

Active detectors use a source of radiation (X-rays, gamma rays, neutrons, or radiofrequency or magnetic fields) to stimulate the bulk of the explosive. These techniques may not be usable to search personnel but can be effectively used to search packages. Active methods include

1. Nuclear quadrupole resonance,
2. Nuclear magnetic resonance,
3. Thermal neutron activation, and
4. Computerized tomography.

All of these methods are described in the paper, Progress in the Development of Explosives Materials Detectors, which is appended to this module.²

Nuclear Materials Detection

The purpose of nuclear materials monitors used for entry control is to detect the unauthorized concealment of nuclear materials on persons, in packages, or in vehicles exiting from a protected area. Concealed nuclear materials can be detected by both passive and active methods. Passive methods use gamma-ray and neutron detection techniques to detect the natural radiations and emissions from nuclear materials. These methods can be defeated by shielding with a small thickness of metallic lead, composite lead materials, or organic shields if the quantity of concealed material is less than a few hundred grams. Active methods utilize neutron activation or X-ray techniques.

Passive Gamma-Ray Detectors -- The block diagram in Figure 8-6 shows the elements of a typical nuclear materials detection system. Special nuclear materials monitors contain scintillators which detect gamma rays from the radioactive decay of special nuclear materials. Scintillation is the process by which photons are produced as a result of the absorption of ionizing radiation in scintillator material. Typically, the detectors are crystal scintillators, or liquid organic scintillators.

The detection system uses a photomultiplier tube to convert the photons from the scintillator to charge pulses. Signal-conditioning electronics drive the pulse height analyzer that counts only the pulses between 50 keV and 250 keV. This range covers the normal gamma ray emission energies from both uranium and plutonium.

Figure 8-6. Block Diagram of a "Typical" Nuclear Materials Monitor

Alarms are generated by alarm circuitry that monitors the output pulses from a single-channel analyzer and detects when a statistically significant increase of the normal background reading has occurred. Detecting radiation from nuclear materials in the presence of natural background radiation involves selection of an alarm threshold close to the normal background level but not so close as to cause a large number of false alarms. A counting time interval is first selected. Optimum detection is obtained when the counting time interval closely matches the time that the nuclear materials are located near the detectors. The signal count is compared to an alarm level derived from an average background count. The background level is established by making counts over a number of signal time intervals. This reference background count is continuously being accumulated, updated, and averaged.

To reduce false alarms in some commercial walkthrough models, the signal count is only accumulated during occupancy. Each time the signal count is updated, it is compared to the alarm level count and an alarm occurs if the signal count exceeds the alarm level. Other alarms detect powerline failure, equipment failure, or equipment tampering.

Far infrared techniques (described earlier) can also be used to detect shielded nuclear materials. These techniques are probably the best method of detecting small quantities (less than 500 grams) of special nuclear materials.

ENTRY-CONTROL SYSTEMS

Entry-control systems can be grouped into three categories: manual, machine-aided manual, and automated. Manual systems involve the use of a guard to examine a credential, such as a photo identification badge, and compare the image to the physical appearance of the person requesting access. The machine-aided manual system uses equipment such as closed-circuit television, or the contraband detector used by airlines to supplement the guard force. Automated systems utilize equipment (detectors) microprocessors, and computers to control access. They function independently of the guard force and interface with it only when assessment of an alarm and guard force response are required. In general, the machine-aided manual system is considered to provide better security than the manual system, although this may not be true for very small facilities (less than 50 people).

Manual Systems

Manual systems utilize personnel (normally members of the protective force) to control access based on some identification criteria. These criteria may vary from a simple check for an authorized credential to a badge exchange procedure. Intermittent personnel and package searches for contraband are also performed. Specific advantages and disadvantages of manual systems depend on the criteria used for determining access approval. In order to increase the security level and maintain the same throughput in a manual system, the number of persons required for conducting entry control must be increased.

Machine-Aided Manual Systems

Machine-aided manual entry-control systems utilize one or more entry-control elements to assist a guard in making decisions on whether to allow or deny entry to or exit from a controlled area. When this type of entry-control system is used, the final decision to allow or deny entry or exit is made by one or more guards. Although security is enhanced by the use of entry-control subsystems, machine-aided manual systems retain some of the disadvantages of purely manual systems in that protective force effectiveness can be highly variable.

All airports within the United States which have scheduled airline service utilize either hand-held or walkthrough metal detectors. Many of these airports also use an X-ray package search system. One entry-control system which can now be installed at nuclear facilities is a component-type system similar to that used

in airports where all entry-control elements are stand-alone subsystems. The major disadvantage of this type of system is that, to maintain throughput and effectiveness, the number of personnel required for conducting entry control must be increased; however, the number required will be less than for a manual system. An example of the application for a conceptual component-type entry-control portal positioned within a double fence line is shown in Figure 8-7. Many configurations of this system are possible; however, in general, all the subsystems shown are necessary for effective, comprehensive entry control. In the system shown, the equipment could be mounted in the hallway of a building; guards located in the hallway could assess detector alarms by using hand-held detectors to examine entering personnel.

Figure 8-7. A Conceptual Machine-Aided Manual Entry-Control System

Even though a system may be composed of individual stand-alone subsystems, care must be taken to prevent the subsystems from interfering with one another. Some of the more common problems which could occur are

1. Metal detector performance is degraded when operated in the vicinity of another metal detector if the two detectors are not shielded from each other.
2. Metal detector false alarm rates can increase when the detector is operated in the vicinity of a pulsed X-ray package search system if the

power for each system is not isolated. Normally, the shielding around the X-ray system is sufficient to prevent X-rays from the package search system from producing false alarms in the nuclear materials monitor, although this may also represent a problem.

3. The false alarm rate for metal detectors will increase when operated in the vicinity of equipment with moving metal parts, e.g., the conveyor belt of an X-ray baggage detector.

Automated Systems

Automated systems allow personnel to enter and exit a controlled area without guard intervention unless an alarm occurs. When an alarm occurs, the protective force assesses the alarm and initiates proper response action. The advantages of an automated system are decreased reliance on human control, with its attendant potential vulnerability to deceit, and the capability to function continuously at a high level of effectiveness. Its disadvantages include higher installation and maintenance costs and increased installation time. An automated entry-control portal system is being developed. This system is fully described in the paper, Design Features of an Automated Entry-Control System, which is appended in this module.

CONCLUSIONS

The entry-control systems and equipment that have been described meet the objective of allowing the movement of authorized personnel and material through normal access routes while detecting and delaying unauthorized movement of personnel and material into and out of protected areas. The equipment described does have limitations, some of which have been described; however, these limitations will be reduced as equipment development continues and new and better equipment becomes available.

Although entry control effectiveness has been discussed in terms of acceptance/rejection rates and throughput, additional effectiveness may be obtained in the form of deterrents. In order to maintain the confidence of the personnel who respond to alarms and of the employees who use the entry-control systems, the systems must be designed to minimize the number of false alarms. However, the infrequent occurrence of a false alarm is acceptable since it helps create the impression that the detectors are effective. In addition, occasional false alarms provide a chance to exercise the procedure to be followed for assessment and response.

REFERENCES

1. Entry-Control Systems Handbook, SAND77-1033, Sandia Laboratories, Albuquerque New Mexico, October 1978.
2. W. David Williams, et al., Progress in the Development of Explosives Materials Detectors, SAND78-1108C, Sandia Laboratories, Albuquerque, New Mexico, June 1978.

MODULE 8

VISUALS

NOTES

ENTRY CONTROL

- OBJECTIVES
- ACCESS CONTROL
PERSONNEL AUTHORIZATION AND IDENTIFICATION
- CONTRABAND DETECTION
- ENTRY CONTROL SYSTEMS
- CONCLUSIONS

OBJECTIVES

- TO PERMIT ONLY AUTHORIZED PERSONS TO
ENTER OR EXIT
- TO DETECT AND PREVENT THE ENTRY OF CONTRABAND
MATERIAL
- TO DETECT AND PREVENT THE UNAUTHORIZED REMOVAL
OR DISPERSAL OF NUCLEAR MATERIAL
- TO PROVIDE INFORMATION TO THE GUARD CONTROL
CENTER

VISUALS

NOTES

Schematic of Areas to be Protected

CONCERNS ADDRESSED BY ENTRY CONTROL

- IDENTIFY AND ADMIT AUTHORIZED PERSON
- AUTHORIZED PERSONNEL - COVERT ACTIVITY
- UNAUTHORIZED PERSONNEL - OVERT ACTIVITY

VISUALS

NOTES

ACCESS CONTROL - AUTHORIZATION

- CREDENTIALS
 - PHOTO BADGES
 - BADGE EXCHANGE
 - STORED IMAGE
- CODED BADGES
 - ACCESS RECORDS
 - UNIQUE CODE NUMBERS
 - 500 OR MORE BADGES
 - ACCESS TERMINATION
 - SEVERAL LEVELS OF ACCESS

TYPES OF CODED BADGES

OPTICAL
ELECTRIC CIRCUIT
MAGNETIC
MAGNETIC STRIPE
PASSIVE ELECTRONIC
ACTIVE ELECTRONIC
CAPACITANCE
METALLIC STRIP

CODED BADGE VULNERABILITY AND USE

VISUALS

NOTES

MEMORIZED NUMBER SYSTEMS

REFERENCE FILE - ENROLLMENT

CODED BADGE

NUMBER ASSIGNED OR SELECTED BY THE
INDIVIDUAL

VULNERABILITIES

ANTI PASSBACK

ACCESS CONTROL - POSITIVE IDENTIFICATION

HAND GEOMETRY

HANDWRITING

FINGERPRINTS

SPEECH

VISUALS

NOTES

Identification by hand geometry depends on the unique dimensions and configurations of each person's hand. A computerized scale has been constructed for adequate applications determines the four hand dimensions illustrated and compares their data with values of the corresponding measurements previously encoded on a special card or stored in a computer memory. Measurement of the dimensions depends on finger length. Identification is achieved if the measurements of the presented hand agree with the stored dimensions for that individual.

HAND GEOMETRY

VISUALS

NOTES

IDENTIPAT HAND-GEOMETRY

MAXIMUM NO. OF ATTEMPTS/USE = 3

AVERAGE NO. OF ATTEMPTS/USE = 1.17

PLOT OF ERROR RATES VERSUS TOLERANCE

VISUALS

NOTES

CONTRABAND DETECTION

• CONTRABAND INCLUDES UNAUTHORIZED

WEAPONS

EXPLOSIVES

SHIELDING MATERIALS

NUCLEAR MATERIALS

METAL AND SHIELDING DETECTORS

COIL GEOMETRY FOR SOLCO MODEL XI METAL DETECTOR

- 100 Hz TO 25 kHz CW
- PULSED FREQUENCIES OF 400 - 500 Hz
- RESPONSE TO METALLIC OBJECTS
 - TYPE OF METAL
 - MASS
 - SHAPE
 - ORIENTATION

VISUALS

NOTES

METAL AND SHIELDING DETECTORS

- SHIELDING DETECTORS - METAL TYPE
 - SHIELDED NUCLEAR MATERIAL
 - LEAD
 - LEAD LOADED PARAFFIN/PLASTICS
- SHIELDING DETECTORS - FAR INFRARED TYPE
 - 0.5 MM TO 1.2 MM WAVELENGTH
 - SCHOTTKY DIODE DETECTORS
 - PASSIVE DETECTION
 - NOT AVAILABLE - UNDER DEVELOPMENT

METAL AND SHIELDING DETECTOR

PROBLEMS

- FALSE ALARMS CAN BE PRODUCED BY:
 - SENSITIVITY SETTING
 - MOVING METAL
 - RADIO TRANSMITTER
 - POWER TRANSIENTS
 - FLUORESCENT LIGHTS
- VELOCITY SENSITIVITY
 - SHOULD BE UNDER GUARD
 - OR TV OBSERVATION
 - VOLUME TYPE

VISUALS

NOTES

EXPLOSIVES DETECTORS

• PASSIVE DETECTION - VAPOR DETECTORS

ELECTRON CAPTURE

ION MOBILITY

OLFACTORY

PLASMA CHROMATOGRAPH

MASS SPECTROMETER

VAPOR PRECONCENTRATOR

VULNERABILITIES

FALSE ALARMS

PACKAGING

VISUALS

NOTES

EXPLOSIVES DETECTORS

- ACTIVE DETECTION

- NUCLEAR QUADRUPOLE RESONANCE

- NUCLEAR MAGNETIC RESONANCE

- NEUTRON ACTIVATION

- COMPUTER TOMOGRAPHY

PACKAGE SEARCH

- MANUAL SEARCH

- ACTIVE DETECTION (NOT FOR PERSONNEL SEARCH)

- X-RAY

- MULTIPLE ENERGY X- OR GAMMA-RAY

- NEUTRON ACTIVATION

- AUTOMATED SYSTEMS

- COMPUTER IMAGE PROCESSING

- PATTERN RECOGNITION

- NOT AVAILABLE FOR THREE TO FIVE YEARS

VISUALS

NOTES

NUCLEAR MATERIALS DETECTION

- DETECT CONCEALMENT OF NUCLEAR MATERIALS ON PERSONS, IN PACKAGES, OR VEHICLES
- PASSIVE METHOD
- ACTIVE METHOD
- SHIELDING PROBLEM

BLOCK DIAGRAM OF A "TYPICAL"
NUCLEAR MATERIALS MONITOR

NOTES

- MANUAL
- MACHINE-AIDED MANUAL
- AUTOMATED

- 9 U. S. AIRPORT TYPE
- 8 NUMBERS OF GUARDS
- 6 LEVEL OF SECURITY
- 4 PROBLEM AREAS

INTERACTION OF DETECTIONS
X-RAY PACKAGE SEARCH-SHIPPED MATERIAL

VISUALS

NOTES

ENTRY CONTROL SYSTEMS

AUTOMATED SYSTEMS

- GUARD REQUIREMENTS
- LEVEL OF SECURITY
- ALARM ASSESSMENT

VISUALS

NOTES

VISUALS

NOTES

SANDIA RESEARCH REACTOR AUTOMATED SYSTEM

IDENTIFICATION FUNCTION

IDENTITY VERIFICATION - MEMORIZED NUMBER
CREDENTIAL - MAGNETIC STRIPE BADGE

CONTRABAND DETECTION FUNCTION

SNM DETECTION (PERSONNEL AND PACKAGE)

CONCLUSIONS

- EQUIPMENT IS AVAILABLE THAT WILL ALLOW THE MOVEMENT OF AUTHORIZED PERSONNEL AND MATERIAL THROUGH NORMAL ACCESS ROUTES, YET DETECT AND DELAY ANY UNAUTHORIZED MOVEMENT
- SOME EQUIPMENT VULNERABILITY
- VEHICLE ACCESS
- EMERGENCY EXITS
- PSYCHOLOGICAL DETERRENTS

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

9.0 COMMUNICATIONS

Session Title: 9.0 Communications

Date: Monday, 13 November

Presented By: W. D. Lyle, Sandia Laboratories

Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. Describe two vulnerabilities of a communication system and
2. Define at least two methods of emergency communication.

Summary:

The importance of the internal and external communication system in relation to total response time is discussed, and the vulnerability of the system to sabotage by jamming or power failure is described.

A description of emergency communication techniques is given; emphasis is placed on secondary systems and multiple frequency systems.

MODULE 9 COMMUNICATIONS

An important factor in the effectiveness of a physical protection system is the speed and reliability with which information can be transferred between components of the system. This information transfer is used to monitor the state of the system and is necessary to provide rapid response in the event of attempted theft or sabotage.

Transfer of information requires some type of communication system and there is a vast variety of systems available, including everything from drums to satellites. Among the most important and most common methods of communication are electrical systems. Electrical systems can be defined as those systems that provide the information link between source and destination primarily, but not exclusively, through the use of electrical devices and phenomena. The functional elements of such a system are shown in Figure 9-1.

Figure 9-1. Components of a Communication System

The first element in the system is the source which produces the message that is to be communicated to the destination. For example, one source for a radio system would be the voice; a source for a sensor system would be environmental disturbances. In general, the message produced by a source is not electrical. A device known as an input transducer converts the source message to an electrical signal, a form well-suited for transmission. Likewise, the output transducer converts the received electrical signal back into the desired form, such as voice.

The electrical signal from the input transducer is usually coupled onto the transmission channel by the transmitter. In some systems, the transmitter may not be present. In this case, the input transducer is designed to deliver a signal matched to the channel. However, in most cases, additional signal processing is necessary to provide a signal that can be propagated over the available channel. This signal processing operation is known as modulation. The receiver performs the inverse operation known as demodulation and delivers a replica of the transmitted signal to the output transducer.

The transmitter and receiver are connected by the medium over which the signal must propagate; this medium is known as the channel. Physically, the channel may consist of wires, coaxial cable, waveguides, or, in the case of a radiating electromagnetic wave, the atmosphere. Regardless of the type of channel used, there are two factors associated with the channel that impose limitations on reliable communication. The first is attenuation or the decrease in signal power with increasing distance between transmitter and receiver. A well-designed communication system makes allowance for this loss by ensuring that the transmitter has sufficient power. The channel, as well as other components of the system, may degrade with age. In particular, the channel attenuation may increase with age unless periodic corrective maintenance is performed.

The second limitation on reliable communications is the interference caused by noise sources, as Figure 9-1 indicates. Noise is always present in a communication system. Elimination of all noise is not even theoretically possible; however, the amount of noise interference and its effects can be minimized. Noise is generated by natural causes both internal and external to the system as well as by manmade sources. Examples of natural noise generating mechanisms are electron motion and lightning. Manmade noise sources include signals, similar in form to the desired signals, which are transmitted over one channel and accidentally coupled into an adjacent channel, signals intentionally introduced into a channel for the purpose of masking or obliterating the true signal, and signals intentionally introduced into a channel for the purpose of deceiving the system user. These three types of noise are commonly known as crosstalk, jamming, and deception, respectively. Control of crosstalk should be accomplished during the design, installation, and checkout of a new system. Keeping levels of crosstalk acceptably low requires preventive and corrective maintenance on a continual basis. Jamming and deception are discussed later.

The remainder of this module is devoted to a discussion of communications requirements at a fixed site, communication system vulnerabilities with particular emphasis on channel vulnerabilities, and emergency procedures.

COMMUNICATIONS CONSIDERATIONS AT A FIXED SITE

There are two general classes of communication systems required at a fixed site. The first class consists of the systems necessary to connect the intrusion detectors to the central alarm station; the second class consists of the voice systems used by members of the protective force.

Alarm Communication System

An alarm communication system is designed to transmit information from the intrusion detectors or sensors to the alarm display equipment. The source in such a system is the environmental disturbance which the system is designed to detect. The destination is the assessment center. The medium which connects these two components is the channel, which may be the most expensive component as well as the most vulnerable. Therefore, the channel occupies a position of critical importance in the alarm system and warrants careful study. There are two types of

channels commonly used for transmission of alarm signals: land lines and radio links. Each of these channels has advantages and limitations that need to be understood.

One basis of comparison between land lines and radio links is relative cost. Figure 9-2 shows relative cost curves for each channel as a function of the distance between the detector and the alarm display equipment. As shown in Figure 9-2, the cost of land lines increases at a constant rate with increasing distance. In contrast, the use of radio links requires a large initial investment but the cost after this initial investment is relatively independent of distance. The reason for this difference is that the major cost of a land line is for purchase and installation of the wire, an expense which obviously increases with increasing distance. The large initial investment required for radio links covers the purchase and installation of transmitters, antenna, and receivers, the cost of which is relatively independent of distance. The exact cost crossover point is a function of the terrain and distance. However, a general rule of thumb in the U.S.A. is that land lines are less expensive for distances of less than 2 km and radio links are less expensive for distances on the order of 5 to 10 km.

Figure 9-2. Relative Channel Cost

If cost were the only consideration, it would be a simple matter to determine the best channel type. Unfortunately, this is not the case since channel security is also an important consideration. Again, as with cost, each channel has advantages and limitations with regard to security. Land lines are usually placed inside a protected area so that an adversary must gain physical access to the line in order to successfully attack the system or to monitor the transmission in order to gain information about the alarm system. Radio transmissions, on the other hand, propagate through the air and can be monitored by adversaries at remote locations; however, the radio channel itself, unlike land lines, cannot be destroyed.

Radio links are subject to climatic disturbances such as strong electrical interference from lightning. Land lines can be protected against this sort of disruption by being enclosed in metal conduit and then buried. Burial of

conduit-enclosed lines also provides additional physical protection of the channel. A large number of land line channels are presently in use, and proliferation of such channels can be anticipated for short distance systems. Special transmission techniques have been developed to provide additional security for these systems. These techniques are presented next.

Land Line Alarm Transmission Techniques -- Alarm communication systems can be broadly categorized as either passive or active systems. Passive systems are characterized by the fact that a signal is sent over the channel only when an alarm occurs. Consequently, any break in the channel will prevent alarms from being reported. The break will not be discovered unless a system test is performed. Thus, this system relies exclusively on physical protection measures to ensure alarm transmission system integrity.

Active (or supervised) links utilize a signal which is continually present in the channel. Therefore, simple breaks in the channel are readily detected, and sophisticated supervision techniques can detect line tampering even when a break in the line has not occurred. Attacks that require line tampering are attacks of deception and to be successful require that the adversary first learn the characteristics of the signal for the "no alarm" or "all clear" condition. The adversary can gain this knowledge either by obtaining system documentation or by actually observing the signal on the line. Next, hardware must be constructed that will generate either the "no alarm" or "alarm" signal. After the hardware is constructed, the adversary must then gain access to the appropriate channel for an amount of time sufficient to install the hardware. If this is accomplished, the adversary can then do one of two things. He can substitute the bogus "no alarm" signal on the channel which connects the sensor at the point of intrusion to the alarm monitoring equipment, and thereby disable the system, or he can substitute a bogus "alarm" signal on this or another channel to deliberately induce what appear to be false alarms so that the intrusion detector or line supervision system will appear to be faulty.

In order to protect the system, one or more of these steps must be prevented or detected. The function of supervisory systems is to protect active systems by monitoring the system to assure that it is operating correctly and that data have not been altered during transmission. These systems can be divided into two categories: static and dynamic.

Static systems are those in which the "no alarm" condition is always represented by the same signal. These systems are the easier of the two to defeat since the nature of the "no alarm" signal can be determined without causing an alarm by measurement of the signal parameters. Generation and substitution of the bogus signal completes the attack.

Dynamic systems are those in which the "no alarm" signal continually changes with time. These systems are inherently more secure than either passive systems or active static systems since learning how the "no alarm" signal changes with time

may be a formidable task. Details on dynamic systems can be found in an article by A. Zushin on line supervision¹ and in a report by J. Ahrens on alarm communication systems.²

Voice Systems

Effective control over members of the protective force at locations remote from the central alarm station requires some type of communication system. The most common system used for this purpose consists of low-power, battery-operated, hand-held transceivers.* These units are small, lightweight devices that allow for rapid reporting of unusual conditions encountered during routine patrols and for rapid deployment of the response force during emergencies.

The channel for transceivers is the atmosphere. A precise description of the channel is given by the center frequency of the band of frequencies occupied by the channel. Typically, a transceiver is capable of operating on any one of two to six preset channels. The maximum range for reliable communication between two transceivers is on the order of 2 to 5 km; however, the maximum range for reliable communication between a transceiver and fixed installation equipment with a more powerful transmitter and a better receiver may be in excess of 20 km. Normally, a fixed installation would be found in the security control center.

The advantages of this system are its ease of system operation, multichannel capability, and self-contained power supply. The disadvantages of the system are the ease with which transmissions can be monitored at locations remote from the site (standoff channel access), the ease with which the system can be jammed, and the ease with which deception can be introduced into the system. The disadvantages of the system will be more fully explored when system vulnerabilities are discussed, but it should be pointed out that, in spite of its vulnerabilities, no system of comparable versatility and operational simplicity has been suggested as a replacement.

An easily obtainable backup system for the transceivers consists of a network of telephones located at critical points within the facility and connected to the security control center via land lines which are used as the system channels. Such a system should be kept separate and distinct from all other internal communication lines so that the lines for this system would be dedicated to the protective force. The advantage of such a system is that the lines are interior to the site and can be buried to provide channel security. The primary disadvantage is that the number of terminals is limited and the location of the terminals is fixed at the time of installation. Nevertheless, such a backup system should be carefully considered since failure of the transceiver system would otherwise leave the guard force without voice communications.

Hand-held transceivers provide a means of communication between members of the protective force but are not an adequate means of emergency communication such as requesting assistance from local law enforcement agencies in the case of extreme

*A transceiver is a device having both a transmitter and receiver mounted in a single unit.

situations. The most natural system for requesting local law enforcement agency assistance is the conventional telephone system. This system normally consists of land lines that may extend for several kilometers over unguarded territory and is, therefore, vulnerable to destruction by an adversary. Hence, a backup radio system connecting the site and law enforcement headquarters is strongly recommended; the on-site terminal of the system should be located in the security control center. As with all unciphered radio systems, this system can be monitored and jammed by an attack force. However, telephone and backup radio appear to be the only viable candidates at the present time.

So far, the discussion has centered on system hardware. There are, however, additional factors that influence the effectiveness of communication systems. Two of these factors are (1) the training given to personnel who use the system and (2) established procedures which the system user can implement in the event of an emergency. The importance of these factors can be seen in the following example. Assume that either deception or jamming is being used against the primary transmitter channel. Based on previous training, the system user can recognize this type attack, and the procedures established for such a situation tell the user what to do. In this case, standard procedure would be to switch to one of the alternate channels. The importance of user training and the use of established procedures cannot be overemphasized since complete chaos can result if these two areas are overlooked.

Voice network discipline is one item that overlaps both training and procedures and, as such, deserves special mention. One aspect of network discipline is the effort required by the system users to keep the number of transmissions to a minimum and also to transmit no more information than is required to complete an assigned task. Unless the number of transmissions is kept to a minimum, a skillful adversary could obtain a surprisingly large amount of information related to response force disposition, emergency procedures, and even the state of the physical protection system simply by monitoring transmissions.

A final procedure note concerns the interface and coordination between on-site personnel and the local law enforcement agency personnel who would respond in the event of an emergency. The security control station and law enforcement headquarters are each provided with a communication link, but this does not necessarily imply that effective communication will exist between the responding officers and the on-site personnel. To ensure that on-site and law enforcement personnel can communicate, prior arrangements and procedures governing their communication must be established.

Maintenance

In addition to hardware, training, and established procedures, a preventive maintenance program is essential to ensure continuous operation for all the communication systems. Preventive maintenance procedures should be written for every new installation and updated as required. Such procedures should contain acceptable system performance measures along with a schedule for periodic checking of the system and its components to ensure that the required performance measures are

satisfied. Whenever the system is found to be operating at a level less than the level required, corrective maintenance is necessary. Furthermore, if repairs cannot be immediately undertaken to remedy a deficiency, the system user should be made aware of any system degradation that might result.

SYSTEM VULNERABILITIES AND COUNTERMEASURES

Loss of Power

Except for the battery-powered transceivers, all communication systems require emergency power systems to serve as backup in the event of power failure. Therefore, an emergency power source is absolutely essential for each system.

Physical Destruction

Any communication system can be rendered inoperative by the destruction of some key system component such as the channel. Whether or not a system is vulnerable to this sort of attack depends on the degree to which the system is physically protected. The next section of the discussion concerns the degree to which the systems previously described are vulnerable to physical destruction.

There are three key components of the alarm communication system that are vulnerable to physical destruction: the sensor itself, the channel, and the alarm indicators. Destruction of the sensor should automatically produce an alarm; therefore, this act would not lead to a successful attack on the system. Destruction of the alarm indicators implies that the adversary has gained access to the central alarm station and, if this indeed has occurred, problems more serious than loss of the alarm system may exist.

The channels for radio communication systems cannot be physically destroyed unless there is a repeater between the sensor and the central alarm station. Normally, alarm system radio repeaters are not required at a site. However, if such repeaters were required, they would be vulnerable to physical destruction and would, therefore, require protection.

Channels for active land line systems cannot be successfully attacked by physical destruction since cutting the lines would cause loss of the continuous signal and would be immediately detected. In contrast to this, physical destruction of a passive land line channel would constitute a successful attack since the destruction would only be discovered when a system check was performed. Effective countermeasures against such an attack include burial of the line and camouflage of the line location. Careful replacement of soil and either replanting or clearing of the area will hinder potential attackers. Additional techniques include planting of parallel cables, one of which is a fake, and encasing the cable in concrete. These techniques make the attackers' problem more difficult. The final security option would be for a security force to patrol the areas which contain buried cables often enough to ensure that an attack on the system could be detected before it could be completed.

The channel for the internal telephone system is similar to the passive alarm system. Consequently, the channel vulnerabilities and countermeasures for the two systems are identical. Additionally, if each terminal contains a handset, the handset can be rendered inoperative. One remedy for handset vulnerability is to equip the terminals with jacks into which the guard can plug a small telephone handset which he carries.

The channel for the external telephone system is the most vulnerable component since the lines extend outside the protected perimeter. Generally, such lines are not controlled or maintained by site personnel. Therefore, any physical protection features provided for these lines must be mutually agreed upon in negotiations between site personnel and the telephone company. In any event, the lines are vulnerable to physical destruction if they can be located by the adversary. Very little can be done to prevent destruction of these lines once their locations are known. Consequently, this system should be regarded as extremely vulnerable to physical attack.

The channel for voice radio systems is the atmosphere and therefore is not vulnerable to physical attack. The only exception would be if a repeater were necessary at the link between the site and the law enforcement agencies. If this were the case, the system would be vulnerable to physical attack. The transmitter and receivers for these systems are normally located in the vicinities where armed personnel are stationed. Consequently, these systems are not particularly vulnerable to physical attack except for the special case in which a repeater is used at an isolated location.

Jamming

Intentional introduction of unwanted signals into the channel of a communication system for the purpose of masking or obliterating the true signal is known as jamming. Systems such as radio that use the atmosphere for a channel are the most vulnerable to attacks by jamming since the attacker has access to the channel from a remote location. Systems using land line channels are vulnerable to jamming but, for the attacker to have access to these channels, he must be physically present at some point along the land line. Hence, a jamming attack on a land line system is unlikely since a more effective attack would be either to physically destroy the system (as discussed earlier) or to use methods of deception. (This latter option will be discussed later.) Therefore, jamming attacks directed against systems which employ land lines will not be considered as a serious threat.

Voice radio systems are the most vulnerable to attack by jamming since the adversary has access to the channel from a remote location and since this form of attack is known to be effective against voice systems. The adversary can obtain the system operating frequencies by either monitoring transmissions or by obtaining the system documentation. Once the operating frequencies are known, it is a simple matter to tune a transmitter(s) to the proper frequency(s) and commence jamming. If the jamming signal is of sufficient power, the true signal will be obliterated or masked to such an extent that effective communication will be severely degraded.

An appreciation of the effect of jamming on the intelligibility of speech is illustrated by the curves shown in Figures 9-3 and 9-4. In each figure, the vertical axis, in essence, represents the probability that a listener will correctly identify the test item, e.g., digits or words. This probability is plotted as a function of the signal-to-noise ratio on the horizontal axis. As the name implies, the signal-to-noise ratio is defined as the ratio of signal power to noise power and is obtained by multiplying the base 10 logarithm of the signal-to-noise ratio by the quantity 10; the value obtained is in decibels. Mathematically, the expression for signal-to-noise ratio in decibels (denoted by SNR_{dB}) is given by $SNR_{dB} = 10 \log (\text{signal power/noise power})$.

Figure 9-3. Intelligibility Scores as a Function of Signal-to-Noise Ratio

In general, the signal-to-noise ratio at the receiver output is an important quantity for most communication systems. Whenever the effects of jamming are being discussed, this quantity is particularly important since the purpose of jamming is to decrease the signal-to-noise ratio and consequently mask or obliterate the true signal or message.

The three curves of Figure 9-3 show the probability that a listener will correctly identify digits, words in a sentence, and nonsense syllables as the signal-to-noise ratio is varied. Note that the probability of a listener correctly identifying words in sentences rapidly decreases toward zero as the signal-to-noise ratio decreases. The intelligibility of digits also decreases as the signal-to-noise ratio decreases but not as much as does the intelligibility of words. The intelligibility of nonsense syllables decreases more rapidly than the intelligibility of words. The conclusion reached from observation of this behavior is that,

for a given signal-to-noise ratio, the intelligibility of speech is higher when the number of possible messages (digits) is small than when the number of possible messages (words and nonsense syllables) is large.

Figure 9-4. Effects of Vocabulary Size Upon the Intelligibility of Monosyllabic Words

Further evidence of this behavior is illustrated by the curves shown in Figure 9-4, which graphs the results of tests based on message sets containing 2, 4, 8, 16, 32, 256, or an unspecified number of monosyllabic words. Here again, for a fixed signal-to-noise ratio, the probability that a listener will correctly identify a word increases as the number of words decreases.

It has been pointed out that communication procedures should attempt to minimize the number of transmissions which take place and to restrict the information content of each transmission to only that which is absolutely necessary. The intelligibility results presented in this section indicate that the jamming problem becomes more difficult if the procedures also require the use of a vocabulary which has as small a number of words as possible. For instance, formatted voice messages can be used so that the recipient has some prior knowledge of what to expect when the transmission begins. Such formatted messages can be used for both routine and emergency reporting.

The most effective countermeasure against a jamming attack is a frequency shift to another channel. Most protective force transceivers have this frequency shift capability, and the protective force/law enforcement agency link should be provided with one or more emergency frequencies for this purpose. It should again be emphasized that user training and established procedures are necessary if frequency shifting is to be effective. All system users must know when to shift and to what new frequency the shift should be made; otherwise, the multifrequency system is of little use.

Deception

Intentional introduction of unwanted signals into the channel of a communication system for the purpose of deceiving or confusing the system user is known as deception. Deception is, in some respects, the most insidious form of attack due to the fact that the system user may be unaware that the attack is taking place. Various systems are susceptible to this type of attack.

Both passive and active alarm systems are vulnerable to attack by deception. For example, deception can be used against passive systems to generate false alarms in an attempt to destroy confidence in the alarm system. In the case of active systems, deception can be used either to generate false alarms or to simulate a "no alarm" condition. The most effective countermeasure for passive systems against this attack is physical protection of the channel. For active systems, physical protection of the channel coupled with line supervision are effective countermeasures.

A deceptive attack against a telephone system is possible; however, physical destruction of the line would be a more effective method of attack once channel access is gained and hence is more likely. The voice radio system is the most vulnerable to attack by deception. The adversary can gain easy remote access to the channel. The only equipment that is needed consists of a transmitter and receiver similar to the equipment which is under attack. A typical deception attack might involve adversary transmission of false reports or false protective force deployment instructions.

An effective countermeasure to such an attack against a voice radio system would be to shift to an alternate channel. If the adversary is capable of following this shift, protective force training coupled with rigid adherence to established procedures would be the most effective countermeasure. If these techniques fail, it would be necessary to use the telephone systems.

Summary of System Vulnerabilities and Countermeasures

Table 9-I summarizes the communication system vulnerabilities and the countermeasures which can be employed against the various possible forms of system attack. It should be noted that every communication system is vulnerable to some form of attack. A well-designed communication system is one in which inherent system vulnerabilities have been recognized and for which adequate countermeasures are provided, if possible. Whenever there is some doubt as to the adequacy of the countermeasures, an alternate backup system is required. The overall effectiveness and vulnerability of a site's communication systems should be a subject of continual study by the personnel at the site; otherwise, what is, at present, an adequate system could quickly become, at a future time, an inadequate system due to technological changes or to changes in the nature of the threat posed to the system.

TABLE 9-I
Communication System Vulnerabilities

System	Physical Destruction	Jamming	Deception	Countermeasures
Hand-held transceiver	No	Yes	Yes	Multiple-channel capability along with user training and established procedures
Passive alarm systems	Yes	No	Yes	Physical protection of the channel
Active alarm systems	Not likely	No	Yes	Physical protection of the channel and line supervision
Telephone	Yes	Not likely	Not likely	Alternate system
Voice protective force/ local law enforcement agency	No	Yes	Yes	Multiple channel capability along with user training and established procedures

SUMMARY AND CONCLUSIONS

Various communication systems are required for fixed-site protection. However, every system is vulnerable in some way to attack. The communication system design problem is to provide for prompt and reliable communications and to minimize the system's vulnerability to attack. One of the primary means of accomplishing this is physical protection of the channels; if this is inadequate, an alternate communication system is required. In particular, voice radio and telephone systems can be used for alternate systems. This dual capability can be provided at a reasonable cost.

Effective communications involve more than just hardware. Three important factors in system effectiveness include system maintenance, user training, and established procedures. If any of these elements of the total system are neglected, system performance will be degraded and, in extreme cases, the neglect of any one of these factors can cause the system to fail at a critical time.

A final point concerning communications requirements is worth noting. This point is that virtually any communication system can be defeated if the attacker devotes sufficient resources to the attack. However, the primary target of an attack force is not the communication system but the facility which it serves. Thus, the degree of vulnerability of the system depends on the resources which the attack force devotes to defeating the system. Hence, a certain type of system may be known to be vulnerable to a sophisticated attack, but an analysis of the threat could indicate that the attackers do not have the required capability. In this case, the conclusion would be that the system is not vulnerable, relative to the threat. This sort of reasoning is always necessary because the cost and complexity of the system grow without bounds if attempts are made to protect the system against every conceivable threat.

REFERENCES

1. Albert R. Zushin, "Line Supervision Techniques," 1974 Carnahan and International Crime Countermeasures Conference, April 1974.
2. Janet Ahrens, A Survey of Secure Alarm Communication Systems, SAND76-0550, Sandia Laboratories, Albuquerque, New Mexico, December 1976.

MODULE 9

VISUALS

NOTES

VISUALS

NOTES

VISUALS

NOTES

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

10.0 TRANSPORTATION

Session Title: 10.1 Transportation Regulations of
the U.S. Nuclear Regulatory
Commission

Date: Friday, 3 November

Time: 0830 to 1000

Presented By: G. W. McCorkle, Nuclear Regulatory
Commission

Session Objectives:

After the session, the participants will be able to list the four key elements of an effective transportation protective system.

Summary:

A brief history of the evolution of in-transit protection requirements, a summary of requirements as they exist today, and an indication of the direction of future in-transit protection programs are discussed.

Additional Resource Materials:

U.S. Nuclear Regulatory Commission Regulations, Part 73, Paragraphs 73.30 to 73.36
(10CFR73.30-73.36)

MODULE 10

TRANSPORTATION

TRANSPORTATION REGULATIONS OF THE U.S. REGULATORY COMMISSION

The past several years have seen a marked upgrading of transportation physical protection requirements. The evaluation of in-transit protective requirements is outlined in Table 10-I. Until 1969, there were no regulatory requirements in the United States for physical protection of special nuclear materials in transit. Early in 1969, a strategic shipment of highly enriched uranium was misrouted and not located for several days. As a result of this incident and an ensuing staff study, it was decided to issue requirements to assure against the recurrence of a similar incident. Accordingly, in April 1969, the U.S. Atomic Energy Commission (now the U.S. Department of Energy) published effective regulations which required (1) the use of carriers which employ established systems for the protection of valuable materials and (2) the exchange of hand-to-hand receipts or continuous personal custody of the shipment by an authorized individual. No additional changes were made in the regulations governing the protection of special nuclear materials in transit until 1973. Because of the large number of aircraft hijackings, in February 1973 the Atomic Energy Commission amended the regulations to prohibit the shipment by passenger aircraft of plutonium or U^{233} in amounts exceeding 20 grams or 20 curies, whichever is smaller.

TABLE 10-I

Evolution of In-Transit Protective Requirements

Prior to 1969	1969 to 1972	February 1973	November 1973
None	<ol style="list-style-type: none"> Carrier must have established system for protection of valuable material Exchange of hand-to-hand receipts or continuous personal custody 	Prohibition of shipment by passenger aircraft of amounts exceeding 20 grams or 20 curies, whichever is smaller	<ol style="list-style-type: none"> Strengthen protective measures Reduce amounts of plutonium requiring protection from 5 to 2 kg

Significant new transportation requirements were published in November 1973, with an effective date of March 1974. In addition to strengthening protective measures, these regulatory changes also reduced the threshold amount for plutonium requiring protection from 5 to 2 kg. The new requirements were issued in recognition of increased terrorist activities and in anticipation of increased numbers of strategic shipments of these materials.

Details of the transportation requirements contained in paragraphs 73.30 through 73.36 of the U.S. Nuclear Regulatory Commission Regulations, Part 73, are discussed in the following paragraphs.

Each person who is licensed or applies for a license to possess special nuclear materials must submit plans to the Nuclear Regulatory Commission for review and approval. These plans should outline the methods to be used in meeting the requirements of Part 73. This includes a separate plan for transportation of special nuclear materials. No changes may be made to either plan which would decrease its effectiveness without prior approval of the Nuclear Regulatory Commission. In transporting privately owned special nuclear materials, licensees may use their own transport equipment and personnel or, if they so choose, they may make arrangements for shipment by common or contract carrier. If a common or contract carrier is used, the carrier must have a plan which has been approved by the Nuclear Regulatory Commission and the licensee's plan must reflect how he will interface with the carrier.

There are a number of general requirements which apply in all cases. These requirements include the previously mentioned requirements that the carrier have an established system for the protection of valuable material and that there be an exchange of hand-to-hand receipts at both origin and destination. In addition, there are other requirements which involve detailed preplanning: (1) to minimize transit times by selection of the most direct route, (2) to select routes which will avoid areas where natural disasters have occurred or where civil disorders have or are likely to occur, (3) to ensure that the consignee is available upon arrival to accept the shipment, (4) to ensure that containers are sealed with tamper-indicating seals, (5) to ensure that either the containers or vehicle itself is locked, and (6) to ensure that guards, when used, have received training and have demonstrated an understanding of their duties and responsibilities. The general thrust of these requirements is to protect the integrity of the shipment.

At this point, it would perhaps be appropriate to discuss a few of these elements and to stress their importance. For example, the use of hand-to-hand receipts is of little value unless each custodian confirms the accuracy of the receipt by cross-checking it against the shipment, and the use of tamper-indicating seals is meaningless if they are not inspected to ensure they have not, in fact, been tampered with. The preplanning of shipments deserves more than just a routine check of the road maps and development of what could be unrealistic schedules. The key role played by all individuals participating in the shipment process, whether they are drivers, guards, shippers, receivers, or whatever, should be emphasized.

Unless each person responsible for his portion of the shipping process understands his duties and carries them out conscientiously, the desired level of protection is not going to be achieved.

The specific requirements for shipments by road are: (1) that no scheduled intermediate stops to transfer cargo between the points of origin and destination be permitted, (2) that the transport and escort vehicles be equipped with radio telephones, (3) that position reporting via communications be made at predetermined intervals (not to exceed 2 hours) to a central point with overall control of the shipment, and (4) that an automatic response be made when reports are not received on schedule. The effectiveness of these controls is dependent on the individuals involved knowing what to do and when to do it.

Present requirements for shipments by air are relatively basic. First, shipments of plutonium and U^{233} which consist of quantities in excess of 20 grams or 20 curies, whichever is less, are prohibited on passenger aircraft. Preplanning is an important factor for movements by cargo aircraft to assure (1) that needless transfers are avoided, (2) that all transfers are protected by four armed guards, and (3) that all export shipments are monitored by a courier who may also be a member of the air crew. For air shipments, the courier's duties extend from the time of departure at the last terminal in the United States until the shipment is unloaded at a terminal of another State. Also included are monitoring duties at the port of entry of another State. All air shipments outside of the United States must be nonstop from the last port in the United States to the first port outside the United States.

As in the case of road shipments, escorts are required to maintain radio-telephone communications with the licensee or his agent at intervals not exceeding 2 hours. When radiotelephone reporting is not possible for periods up to 5 hours due to the local conditions, position reports must be given by conventional telephone. During the planning stage for any shipment, the licensee or his agent with whom the escorts are to maintain contact should be predesignated. When a scheduled call providing shipment status and location is not received, the licensee or his agent must immediately notify appropriate law enforcement agencies and the Nuclear Regulatory Commission. These responses must be immediate and automatic.

Physical protection requirements for shipments by sea include the same basic ingredients which apply to other modes of transportation. First, they must be scheduled to assure that the minimum number of ports of call are involved and that no transfers to other ships are permitted. At domestic ports where transfers to other modes of transportation are involved, suitable arrangements to safeguard such transfers must be made. All shipments must be placed in locked and sealed compartments. Locks and seals must be periodically inspected by the courier, who may be a crew member, to assure their integrity. Sea shipments must be accompanied by an individual who serves as the courier; this person may be a designated member of the crew. Courier duties extend from the last port in the United States until the shipment is off-loaded at a port of another State. The courier's duties also include monitoring the shipment at the port of another State.

Ship-to-shore communications must be made at least once in every 24-hour period. These status reports will include position information and any pertinent data concerning the shipment as determined from daily inspections. This information is, in turn, to be passed on to either the licensee or his agent who made the arrangements for the protection of the shipment.

One important element that is common to all shipments, regardless of the mode of transportation, is the monitoring of transfers. The importance of this function cannot be overemphasized and is therefore deserving of special mention.

There are a number of miscellaneous requirements for protection of special nuclear materials in transit. First, each licensee who takes delivery of special nuclear materials is responsible for making the protection arrangements.

Whenever a licensee (consignor) delivers special nuclear materials to a carrier for transport, he is required to immediately notify the consignee (licensee for whom the shipment is intended) by telephone or other expeditious means of the time of departure, the method of transportation, the name of the carrier, and the estimated time of arrival. In all cases, the consignor should make advance arrangements with the consignee to be notified as soon as the shipment arrives.

Licensees who import shipments are responsible for making in-transit protection arrangements. Either the licensee's designated representative or agent is required to confirm the container count and to inspect locks and seals for evidence of tampering at the first point in the United States where the shipment is discharged from the inbound carrier. It is the responsibility of the importer to ensure that the requirements for domestic shipments are met.

In the case of export shipments, the licensees are responsible for making all protection arrangements for the various modes of transportation involved from the time of initial delivery to a carrier until such time as the shipment is off-loaded at the first port of another State. The responsibility of the licensee extends to his arranging to be notified by the consignee that the shipment has or has not arrived.

When a shipment fails to arrive at its destination on schedule, the person responsible for its protection must immediately notify the Nuclear Regulatory Commission and advise them of the action being taken to trace the shipment. The trace investigation must be initiated immediately and the Nuclear Regulatory Commission must be informed of its progress.

A brief history of the evolution of in-transit protection requirements and a detailed discussion of present regulations has been given. It is believed that significant strides have been made in the protection of special nuclear materials since the initial requirements were levied in 1969. However, in order to ensure that special nuclear materials are protected during transportation, further protective measures are being included in a forthcoming upgrade rule. In all likelihood,

the additional transport protection requirements being proposed will be adopted. Some of the proposed requirements are listed in Tables 10-II and 10-III.

TABLE 10-II

Proposed Physical Security Requirements

Road Shipments

- Shipment in (1) Armored car with three separate armored escort vehicles and a total of nine armed guards or,
(2) Special vehicle with armored cab, penetration-resistant cargo compartment, immobilization features with two separate armored escort vehicles and nine armed guards.
- Improved communications in transit
- Minimum of nine armed guards to protect transfer points
- Upgraded guard-training requirements
- Armament
- Improved access controls
- Formal procedures for identification of personnel at transfer points
- Personnel clearance program
- Classification program
- Formal procedures for advance plan review

TABLE 10-III

Proposed Requirements

Air Shipments

- Cargo aircraft only--last on, first off
- Nine armed guards to protect cargo when aircraft is on the ground
- Preflight search of aircraft
- Escort by two armed guards
- Nonstop flights
- Personnel clearances
- Communications
- Transfer monitoring the same as for road shipments

In addition to the foregoing points which apply to specific portions of in-transit protection requirements, another important matter under consideration is a clearance program for certain individuals involved with the transportation of

special nuclear materials. Those individuals who are responsible for the preplanning of shipments and who have a detailed knowledge of schedules, transfers, and other important facts would be particularly involved.

The important role that all personnel concerned with the transportation cycle play in assuring that each shipment is afforded the required degree of protection has been indicated. The key elements of an effective transportation protection system can be stated simply as (1) a clear-cut understanding of responsibility, (2) sound preplanning procedures, (3) well-trained and qualified guards, and (4) good communications equipment and procedures. All of the other requirements which have been discussed are interrelated to these basic points and are dependent on personnel performance.

The development of security measures related to the transportation of special nuclear materials, a summary of requirements as they exist today, and some indication of the direction of future in-transit protection programs have been discussed. The significant progress realized in transportation security has resulted from the involvement and cooperation of all those concerned in the transportation process. The future course of transportation of special nuclear materials will be dependent upon continued assistance and understanding of objectives.

MODULE 10

SESSION 10.1

VISUALS

NOTES

NUCLEAR REGULATORY COMMISSION

NUCLEAR MATERIAL SAFETY AND SAFEGUARDS

VISUALS

NOTES

PROTECTION OBJECTIVES

- PROTECT MATERIALS AND VITAL EQUIPMENT AGAINST SABOTAGE
- PROTECT SSNM AGAINST THEFT

PROTECTION AGAINST THEFT OF SSNM IN TRANSIT

- PROTECTION REQUIREMENTS APPLY FOR SHIPMENTS OF > 5000 FORMULA GRAMS
- IRRADIATED SHIPMENTS EXEMPTED

SIGNIFICANT QUANTITIES OF SSNM

Pu: ≥ 2000 GMS

U-233: ≥ 2000 GMS

HEU: ≥ 5000 GMS CONTAINED U-235

OR ANY COMBINATION OF THE ABOVE MATERIALS THAT IS 5000 GMS OR MORE
COMPUTED BY THE FORMULA: $\text{GRAMS} = (\text{GRAMS CONTAINED U-235})$
 $+ 2.5 (\text{GRAMS U-233} + \text{GRAMS Pu})$

TRANSPORTATION PROTECTION PLAN

- SSNM SHIPMENTS MADE ONLY IN ACCORDANCE WITH APPROVED TRANSPORTATION PLAN
- PLAN MUST DESCRIBE HOW REQUIREMENTS WILL BE MET
- ANY ORGANIZATION--NOT RESTRICTED TO LICENSEES--WHICH CAN SATISFY PROTECTION REQUIREMENTS CAN APPLY FOR AND OBTAIN AUTHORITY TO PROTECT SSNM IN TRANSIT

VISUALS

NOTES

KEY ELEMENTS OF IN-TRANSIT SECURITY

- UNDERSTANDING OF RESPONSIBILITY
- SOUND PLANNING PROCEDURES
- WELL TRAINED AND QUALIFIED GUARDS
- GOOD COMMUNICATIONS EQUIPMENT AND PROCEDURES

EXISTING PHYSICAL PROTECTION REQUIREMENTS ROAD SHIPMENTS

- SHIPMENT IN () : ARMORED CAR OR
 () : VEHICLE WITH ARMORED CAB AND PENETRATION
 RESISTANT CARGO COMPARTMENT
- SEPARATE ESCORT VEHICLE (2 AT NIGHT)
- MINIMUM OF 5 ARMED GUARDS (7 AT NIGHT)
- TRAVEL ON MAJOR HIGHWAYS
- COMMUNICATIONS IN TRANSIT
- MINIMUM OF 4 ARMED GUARDS TO PROTECT CARGO AT TRANSFER POINTS
- ADVANCE PLAN REVIEW BY NRC FOR IMPORT/EXPORT

VISUALS

NOTES

EXISTING REQUIREMENTS AIR SHIPMENTS

- CARGO AIRCRAFT ONLY*
- FOUR (4) ARMED GUARDS PROTECT CARGO WHEN AIRCRAFT IS ON GROUND
- NON-STOP FROM U. S. TO FOREIGN TERMINAL
- UNARMED ESCORT

*NO PU SHIPMENTS BY AIR

SEA SHIPMENTS

- SECURE COMPARTMENT LOCKED AND SEALED
- UNARMED ESCORT
- MONITORING SAME AS FOR ROAD
- SHIP TO SHORE COMMUNICATIONS

NEW RULES RELATED TO PHYSICAL PROTECTION

- SAFEGUARDS CONTINGENCY PLANS (APPROVED)
- UPGRADED PROTECTION REQUIREMENTS -- STRATEGIC SNM AT FUEL FACILITIES AND DURING TRANSPORT (PUBLIC COMMENT STAGE)
- IMPROVED GUARD TRAINING AND QUALIFICATION CRITERIA (PUBLIC COMMENT STAGE)
- ACCESS AUTHORIZATION (CLEARANCE) PROGRAM (PUBLIC COMMENT AND HEARING STAGE)

RULES IN PREPARATION RELATED PHYSICAL PROTECTION

- PHYSICAL PROTECTION OF NON-STRATEGIC QUALITIES AND TYPES OF SNM (CATEGORY II AND III MATERIALS)
- SPECIFIC REQUIREMENTS FOR RESEARCH REACTOR PHYSICAL PROTECTION
- REQUIREMENTS FOR DETERMINING ACCEPTABILITY OF FOREIGN PHYSICAL PROTECTION PROGRAMS (U.S. EXPORTED NUCLEAR MATERIALS AND FACILITIES)

VISUALS

NOTES

PROPOSED PHYSICAL SECURITY REQUIREMENTS ROAD SHIPMENTS

- SHIPMENT 1: (1) 1 ARMORED CAR WITH 3 SEPARATE ARMORED ESCORT VEHICLES AND A TOTAL OF 9 ARMED GUARDS, OR
- SHIPMENT 2: (1) 1 SPECIAL VEHICLE WITH ARMORED CAB, PENETRATION RESISTANT CARGO COMPARTMENT, IMMOBILIZATION FEATURES WITH 2 SEPARATE ARMORED ESCORT VEHICLES AND 9 ARMED GUARDS
- IMPROVED COMMUNICATIONS IN TRANSIT
- HARDENED SHIPPING CONTAINER FOR PU
- MINIMUM OF 9 ARMED GUARDS TO PROTECT TRANSFER POINTS
- UPGRADED GUARD TRAINING REQUIREMENTS
- ARMAMENT
- IMPROVED ACCESS CONTROL'S
- FORMAL PROCEDURES FOR ID OF PERSONNEL AT TRANSFER POINTS
- PERSONNEL CLEARANCE PROGRAM
- CLASSIFICATION PROGRAM
- FORMAL PROCEDURES FOR ADVANCE PLAN REVIEW

PROPOSED REQUIREMENTS AIR SHIPMENTS

- CARGO AIRCRAFT ONLY, LAST ON FIRST OFF
- NINE (9) ARMED GUARDS PROTECT CARGO WHEN AIRCRAFT IS ON GROUND
- PRE-FLIGHT SEARCH OF AIRCRAFT
- ESCORT BY 3 ARMED GUARDS
- NON-STOP FLIGHTS
- PERSONNEL CLEARANCES

VISUALS

NOTES

POTENTIAL FOR MISUSE

SPENT FUEL CASKS PROTECT AGAINST

- SMALL ARMS FIRE
- ANTI-TANK WEAPONS, SURFACE TO AIR MISSILES, ETC.
- TRAIN AND TRUCK CRASHES
- DROPPING FROM BRIDGES OR INTO DEEP WATER
- MECHANICAL OPENING BY TOOLS OR BURNING BARS
- CASUAL USE OF LARGE AMOUNTS OF HIGH EXPLOSIVES
- EXPERT USE OF CAREFULLY DESIGNED EXPLOSIVE CHARGES

NOTE THAT A NATIONAL EFFORT WOULD BE REQUIRED TO SEPARATE THE PLUTONIUM FROM THE FISSION PRODUCTS.

VISUALS

NOTES

ALTERNATIVES FOR PROTECTING SSNM

- FEDERAL GUARD FORCE
- DOE TRANSPORT SYSTEM
- DEPARTMENT OF DEFENSE EQUIPMENT AND FACILITIES
- USE OF FOREIGN MILITARY AIRCRAFT FOR IMPORT/EXPORT
- RESTRICTING TRANSPORT TO A PARTICULAR MODE

CONCLUSIONS

- SHIPMENTS NOT NOW COVERED BY NRC PHYSICAL PROTECTION REQUIREMENTS NOT A THREAT TO PH&S
- EXISTING PHYSICAL SECURITY REQUIREMENTS FOR SSNM ARE ADEQUATE TO PROTECT AGAINST AN ASSAULT BY A SMALL GROUP WITH INSIDE ASSISTANCE
- EVEN THOUGH THERE IS NO EVIDENCE OF AN ACTIVE TERRORIST THREAT IN THE U.S., PRUDENCE DICTATES THAT OUR SAFEGUARDS POLICY BY SUBJECT TO CONTINUING REVIEW
- USE OF ALTERNATIVE METHODS NOT NOW CONSIDERED NECESSARY

Physical Protection of Nuclear Facilities and Materials

10.0 TRANSPORTATION

Session Title: 10.2 Transportation Technology

Date: Monday, 13 November

Presented By: F. O. Luetters, Sandia
Laboratories, and
D. P. Dickason, Department
of Energy

Time: 0930 to 1030

Session Objectives:

After the session, the participants will be able to discuss the unique problems associated with transportation security and identify some procedural and technological solutions which can be applied to the major transportation system elements.

Summary:

The experiences gained by Sandia Laboratories while assisting the Department of Energy during the development and upgrading of its Transportation Safeguards System are applied broadly to the unique problems encountered in the transportation of nuclear materials. Specific technology applications are presented which enhance transportation security. Overall system design must consider the balance of major system elements to provide in-depth defense in a cost-effective manner.

TRANSPORTATION TECHNOLOGY

In the United States, nuclear materials are moved by transportation systems which meet safety regulations and insure positive, continuous control of the nuclear materials. The inherent characteristics of transportation systems create unique control problems, such as extensive exposure of the vehicles to danger, the remoteness of the vehicles from communications and assistance, and limitations on the amount of protection which can be physically carried by the vehicles. Therefore, an effective system should be comprised of complementary system elements, balanced to provide comprehensive coverage while also providing in-depth defense. This discussion describes technologies and methodologies used in the development of a domestic operational transportation system by the United States Department of Energy and examines unique problems associated with transportation security. It also describes the major elements of the transportation system and their roles, discusses transporter barrier technology, and describes approaches for evaluating system effectiveness.

UNITED STATES DEPARTMENT OF ENERGY TRANSPORTATION SAFEGUARDS SYSTEM

The Department of Energy, recognizing that many of its nuclear materials routing requirements result in the necessity to transport by land, has developed a nationwide road transportation network. Security is provided by specially designed transporters and trained, well-equipped couriers (Figure 10-1). This system either meets or exceeds the current and proposed requirements of the Nuclear Regulatory Commission. The requirements are often exceeded because national defense shipments are part of the mission, and more stringent regulations apply.

The transporter and courier escort vehicles travel throughout the United States in convoys and are linked to a central control station by means of a special communication network. Problems with the shipment can be detected promptly and requests for assistance can be quickly retransmitted to response forces.

The transporter vehicle, called the Safe-Secure Trailer (SST), provides defense against security threats to the cargo and also assumes the burden of safety for the system. Safety is provided by (1) vehicle design features, (2) traveling only when conditions are not hazardous, and (3) a thorough preventative maintenance program. In addition, accident protection for the nuclear materials is provided by the container design and construction. Security is provided by (1) vehicle design features, (2) immobilization features, and (3) container design features which make removal of the cargo from the vehicle very difficult. A safe-secure rail system similar to the road system will soon be implemented.

Couriers are specially trained and equipped to respond effectively to any attempts to subvert shipments. Couriers have appropriate weapons and protective

Figure 10-1. Department of Energy Transportation Safeguards System.

equipment and are trained and drilled regularly in emergency procedures. Courier vehicles provide for the rest and alertness of the occupants over extended periods of time and are properly equipped to reduce the courier's vulnerabilities.

Communications is a key link in transportation system effectiveness. The convoys are centrally controlled by means of a nationwide high-frequency communications network called Security Communications System (SECOM) which has proven to be highly reliable and comprehensive in its nationwide coverage (Figure 10-2).

Figure 10-2. Security Communications System

The system utilizes digital messages for routine reports but has the capability of utilizing voice for emergency situations when additional detail is required. The convoys also use very high frequency (VHF) radios for reliable communications within a convoy.

TRANSPORTATION PROTECTION SYSTEMS AND TECHNOLOGIES

A number of problems are unique to transportation systems, and these problems influence design approaches. Some of these security problems are outlined in Table 10-IV. For transportation involving lengthy trips, control tends to be decentralized. Special attention must then be focused on the reliability of communications, the thoroughness of procedures, and the quality of personnel training. Good communications allow the convoy to be monitored, to be provided with guidance and special instructions, and, should the need arise, to be supplemented quickly with additional resources. Well-defined procedures and special training provide confidence that the escorts will act in a predictable and acceptable manner.

TABLE 10-IV

Unique Transportation Security Problems

Decentralized Control

Extensive Exposure

- Changing Terrain and Surroundings
- Vulnerable to Ambush
- Terrorist Choice

Communications

- Atmospheric Conditions
- Frequent Communications

Response Forces

- Varied Organizations
- Jurisdictional Problems
- Personnel Recognition
- Utilization

Public Involvement

- Traffic Proximity
- Hostages

Equipment Maintenance

Transportation systems employed over extensive distances are typically exposed to changing terrain and surroundings. For this reason, shipments are vulnerable to ambushes at locations which may possibly benefit the adversary. Although, as noted earlier, very reliable communications can be designed, these systems are sometimes affected by atmospheric disturbances. Frequent communications with the convoy are necessary to assure that emergencies are acknowledged and responded to quickly.

For some scenarios, analyses and tests suggest that even very complete transportation security systems can be overcome if the resources are limited to those which are inherently part of the system. For this reason, the dispatch of

nondedicated response forces from local law enforcement agencies becomes a meaningful factor. In the United States, effective use of state and local law enforcement agencies is accomplished only when the organizational, jurisdictional, and capability differences among the various agencies are completely understood.

Possible public involvement in a security-related incident is of continuing concern. The proximity of the public to the transportation system opens up the possibility of injury to bystanders or their use as hostages by the adversary. No clear-cut solutions to this type of problem have been identified. Escort training, tactics, and procedures, however, are designed to minimize hazards to the public.

Since technology plays an important role in an effective transportation security system, equipment tends to become more and more sophisticated. In order to achieve system cost-effectiveness, this sophistication requires routine preventative maintenance programs which are significantly better than those programs for normal "over-the-road" equipment.

The experience gained by Sandia Laboratories suggests that a typical system for nationwide utilization has four significant elements: (1) the guards (or escorts), (2) the transporter, (3) communications, and (4) response. These elements are shown in Table 10-V. The emphasis which should be placed upon a given element is strongly influenced by the mission of the system, the environment in which it

TABLE 10-V
Major System Elements

	<u>Guards (Escorts)</u>	<u>Transporter</u>	<u>Communications</u>	<u>Response</u>
Roles	Material Custody	Guard Protection	Facilitate Operations	Incident Containment
	Vehicle Operation	Assessment Time	Convoy Coordination and Progress	Defense
	Detection, Assessment, and Communication	Long Access	Distress Call	
	Defense and Access Denial	Delay		
Desirable Attributes	Protection	Active & Passive Barriers	Range	Numbers
	Training	Armor	Reliability	Arrival Time
	Weapons	Immobilization	Frequency of Communications	Weapons
	Equipment	Structural Integrity	Privacy	Equipment
	Motivation	Formidable Appearance		Training Motivation Allocation

operates, and trade-offs among elements for cost-effectiveness. The roles of these four elements and some of the attributes of each are discussed next.

Guards (or escorts) have many routine responsibilities but their primary security responsibilities should be (1) to detect that an incident is about to occur, (2) to assess the situation, (3) to communicate with central control, and (4) to take appropriate action to protect the shipment and deny unauthorized access to the cargo. These responsibilities suggest that specialized training should be emphasized and that appropriate equipment, including armament, should be provided. Special attention should be given to keeping the guards motivated since the routine operation of the system can lead to a relaxed attitude which may cause the guards to be unprepared if an emergency arises.

The role of the transporter includes (1) offering sufficient protection to the guards (such as armor) so that they are not completely vulnerable to an ambush, (2) providing sufficient protection against easy access to the cargo so that guard assessment of the situation can occur before application of lethal force becomes necessary, and (3) supplementing the access-denying capability of the guards by providing penetration resistance to the cargo compartment, hopefully for extended periods of time. These three characteristics can be provided by transparent and opaque armor for personnel protection and active and passive barriers which surround the cargo.

A reliable communications system is necessary to provide operational and logistical control as well as to inform the control center of emergency situations which may arise. As indicated previously, if the transportation system is operated over large geographical areas, attributes such as reliability, range, privacy, and frequency of use become important design parameters.

Response forces are essential to the system in order to help contain security incidents and to provide defense against ultimate loss of nuclear materials. In the United States, arrangements have been made to involve state and local law enforcement agencies should a security incident occur. This is accomplished via the communication system described previously. Assessment of the contribution which such a response force can make has required a rather thorough understanding of these agencies. Attributes of the agencies have been documented and predictions of the potential contributions have been carefully analyzed. Where deficiencies exist in a particular geographical area, other security-oriented steps, such as additional guards and more frequent communications, are taken.

Most of the Sandia Laboratories recent involvement with transportation systems has been in the design and evaluation of penetration-resistant barriers which make up the transporter walls. This activity has been undertaken in response to the regulations of the Nuclear Regulatory Commission. The penetration-resistant features of a vehicle are influenced by several factors, among which are

1. The addressed level of threat, which typically requires an explosive-resistant structure. This implies, among other things, (1) a thick-walled structure and (2) a cargo hold with limited free volume which impedes removal of the cargo if access to the hold is gained.
2. State and Federal regulations which limit the total vehicle weight and weight distribution.

A cross section of a typical wall section which shows promise and attempts to meet these criteria is shown in Figure 10-3. The 6.4-mm outer steel skin of the

Figure 10-3. Typical Wall Construction

wall is unprotected and offers little resistance to attack, but it does conceal the structure of the channel array to any attacker. Beneath the skin is a 600-mm-thick matrix of welded crisscrossed layers of steel channel. The gaps between channels are filled with polyurethane foam which can serve several purposes. The channel array reduces the effectiveness of shaped charges by preventing the optimum standoff distance from being used. The structure also tends to disrupt the shaped-charge jet as it passes through the multiple layers of the panel. A flyer plate may still be fired from its optimum standoff distance but the array will tend to reduce the flyer-plate velocity and, consequently, its effectiveness. The channel array is very effective against hand-tool attack largely because of the welded construction

of the array. The inner layer of the panel, a 13-mm steel liner, is intended to deform and "lock in" the cargo if violent penetration methods are used. The total matrix has an areal density of about 83 kg/m^2 .

Implementation of this wall-construction concept into a vehicle is shown in Figure 10-4. This conceptual vehicle has a gross vehicle weight of 33,000 kg, a cargo capacity of 3630 kg, and a volume of 7.25 m^3 . The cargo hold has dimensions of 1.2 metres by 1.2 metres by 4.9 metres. These dimensions are compatible with the cylindrical packages typically used for United States domestic shipments of special nuclear materials. Transparent and opaque armor provides crew protection, and a command-activated immobilization system provides the capability for locking all wheels to prevent easy removal of the vehicle from the incident scene.

Although the penetration-resistant features of the vehicle are the major factors contributing to the overall effectiveness of the system, in the end, the system is only as effective as the doors which allow access to the cargo shipment. The cargo compartment doors must be successfully integrated with the cargo compartment walls, as shown in Figure 10-5, for example. The vault-type construction incorporates a "dead-bolt" feature which prevents removal of the doors by cutting off the hinges. In addition to the dead-bolt feature, the doors overlap in the center and close with internal blades driven through a mechanical linkage. Only one door requires a locking mechanism. An electronic coded switch controls power to the locking/unlocking mechanism, and code knowledge is required for operation.

Another concept is shown in Figure 10-6. This arrangement takes better advantage of a close "nesting" of the cargo to the inner barrier wall, thus increasing the likelihood that an explosive attack will "lock in" the cargo. The basic shipping container, which becomes the cargo, is 440 mm in diameter and 1.6 metres long and weighs about 810 kg (Figure 10-7). Each shipping container contains four 8-kg canisters of plutonium oxide. The canisters are contained within a primary pressure vessel, a secondary pressure vessel, and appropriate shielding and heat-transfer materials. The transporter accommodates eight shipping containers.

The vehicle physical security features (Figure 10-8) include guard armor protection, a brake-locking system for emergency situations and, in conjunction with the brake-locking system, an emergency dead-bolt mechanism system surrounding the individual shipping containers that firmly locks the containers into the cargo structure when an emergency signal is received. This system latches dead bolts into the actuated positions so that unusual physical access is required to disengage the dead bolts from the shipping container. Actuation of the emergency dead-bolt system could be accomplished by a hard-wire connection from the vehicle tractor, a radio-frequency link, intrusion sensors, or any combination of these.

For access denial, the shipping containers are completely surrounded (sides, top, and bottom) by about 700 mm of welded, crisscrossed steel channels; the gaps are filled with a suitable foam or plastic material. This material, in addition to its security and safety benefits, could provide further neutron shielding, if

Figure 10-4. Conceptual Design of a Special Nuclear Materials Vehicle

Figure 10-5. Vault Door Concept

needed. Other materials that could increase the difficulty of cargo structure penetration, such as irritants and disabling chemicals, could also be incorporated into the channel matrix.

To gain access to the plutonium-oxide powder through means other than normal access would require the penetration of a number of materials. These include the outer cargo compartment wall, the channel matrix with its associated foam and penetration-resistant materials, the inner cargo compartment wall, and the various materials of the shipping container. Penetration of all of these materials would require the use of multiple, contrasting methods of penetration. Access denial is also enhanced by the use of individual shipping container compartments in which the containers are closely surrounded by adjacent structures. Attempts at violent penetration of the cargo structure to gain access to the shipping container could result in the wedging of these assemblies into the adjacent structure so that their removal would be more difficult.

Figure 10-6. Conceptual Transportation Vehicle

Figure 10-7. Disassembled Shipping Container

Normal access is controlled by multiple access covers that require the use of specialized handling equipment and tools for their removal and for a second dead-bolt system that is normally locked during shipment and must be unlocked with an electronic coded switch. The access code is known only to authorized personnel.

The threaded steel cover, which is flush with the top surface of the cargo structure, provides the initial access-control barrier. Removal and installation of the cover requires the use of special handling equipment, such as a magnetic or vacuum grasping device. The cover threads may be either continuous or interrupted (as used in a breechblock) but are as resistant to a violent attack as unaltered metal. The flush design makes attempts to cut off or saw off the cover considerably more difficult. A tamper-indicating seal is used in conjunction with each cover, and the seals may be connected to the communication system.

Below the top cover is a plug of material similar to the wall material which fills the volume between the shipping container and the cover. The plug is held

Figure 10-8. Transportation Vehicle

in place by means of mounting bolts on its upper flange and the coded-switch-operated dead bolts. The mounting bolts may be designed to require a special tool for installation and removal.

The barrier technologies (Module 6) are applicable to road vehicles, ship or air transportation containers, and secure storage containers.

Before the cost and security effectiveness of any system can be assessed, testing is often necessary. Testing results in an excellent understanding of system adequacy, because it requires the gathering of detailed information regarding security effectiveness. The threat must be defined and characterized, meaningful scenarios must be developed, and the tests must be carefully planned and conducted. The test results provide positive measures of effectiveness.

Explosive attack is the primary concern of most transporter barrier systems. Figure 10-9 shows a flyer-plate explosive charge consisting of 4 kg of C-4 explosive driving a 3.6-kg plate, 25 mm thick and 150 mm in diameter. Utilizing a 3-metre

Figure 10-9. Flyer-Plate Explosive Charge

standoff, the charge was directed against a 600-mm-thick section of the steel channel matrix described earlier. As shown in Figure 10-10, the plate did not penetrate the inner liner. Figure 10-11 illustrates an identical sample panel which was initially penetrated with a conical-shaped charge containing 0.6 kg of C-4 explosive. Subsequently, a 34-mm-diameter pipe bomb, 609 mm long and containing 0.9 kg of C-4 explosive was inserted into the hole. The results after detonation are shown in Figure 10-12. In this experiment, only the inner wall prevented full penetration of the wall section.

These tests and others on this wall section revealed that the design is extremely resistant to hand and power tool attack, extremely resistant to bulk-charge explosive attack, moderately resistant to flyer-plate explosive attack, but marginally vulnerable to attacks using conical-shaped charges followed by pipe bombs. The significance of these strengths and weaknesses is a function of the application of these technologies to specific cargo and vehicle configurations.

Figure 10-10. Result of Explosive Charge Detonation Against 600-mm-Thick Steel Channel Matrix

This kind of information is necessary to properly assess the contribution of the barrier walls with respect to the enhancement of other system elements (such as additional guards).

This session has attempted to share some of Sandia Laboratories experiences and technologies associated with the development of secure transportation systems. The main considerations in this discussion are (1) problems unique to transportation, (2) the roles and attributes of major transportation system elements, and (3) transporter features and technologies and the manner in which they are evaluated. The solutions to all transportation security problems are not likely to be the same. The most cost-effective approach that also provides adequate security effectiveness requires a careful understanding of the perceived threat, the environment in which the system operates, the desirability of the cargo in comparison to other targets, and, of course, the operational requirements of the system.

Figure 10-11. Result of Detonation of a Conical-Shaped Charge

Figure 10-12. Final Result of Detonation of a Contact-Charge Charge and a Pipe Bomb

SESSION 10.2

VISUALS

NOTES

VISUALS

NOTES

TYPICAL WALL CONSTRUCTION

SNM VEHICLE CONCEPTUAL DESIGN

VISUALS

NOTES

NOTES

VISUALS

NOTES

VISUALS

NOTES

11.0 THE ROLE OF THE PROTECTIVE FORCE

Session Title: 11.0 The Role of the
Protective Force

Date: Monday, November 13

Presented By: S. D. Chester,
Sandia Laboratories

Time: 1100 to 1200

Session Objectives:

After the session, the participants will be able to

1. List the three major roles which the response subsystem of the physical protection system must perform,
2. Identify the four major physical protection subsystems which could be performed totally by large numbers of security officers,
3. List at least two skills which some but not all security officers will use, and
4. Describe the purpose of contingency plans and procedures.

Summary:

The role of the response force and some of the functions which the facility security officers can or cannot perform, depending upon whether they are armed or unarmed, are discussed. Major physical protection subsystems are discussed with respect to performance of the functions by humans rather than by equipment.

Examples of the wide range in skills required for various security officers' jobs are provided in order to illustrate the need for (1) specific job descriptions and (2) security officers trained for the job or jobs which they will perform. The need for regularly testing normal plans and procedures as well as contingency plans and procedures is discussed.

MODULE 11

THE ROLE OF THE PROTECTIVE FORCE

Quite often there is a tendency to think of three of the major subsystems of a physical protection system as being performed by equipment and the fourth major subsystem, response, as being performed by people. The protective force must track, intercept, and neutralize the adversary, and humans are particularly suited to think and to make judgments. Since a human can use judgment to determine the least amount of force necessary to neutralize an adversary, in a situation where lethal force may not be necessary it is preferable to use a human rather than to allow equipment to automatically use lethal force.

This module discusses some of the functions a protective force may perform, the interrelationship between the skills and the training required for a particular job, and the need for contingency plans and procedures. In addition, this module demonstrates that a physical protection system can be designed which is composed totally of people to detect, to delay, to communicate, and to respond to threats.

SOME BASIC FUNCTIONS OF A PROTECTIVE FORCE

Response

Although a protective force may perform many functions at a facility during normal operations, ultimately, the protective force is needed to perform the response function in a facility's physical protection system. Assuming that in response to an adversary threat, detection, delay, and communication have taken place, the response force must deploy rapidly to perform the following steps.

1. Maintain tracking of the adversary.
2. Intercept and further delay the adversary, and
3. Neutralize the adversary.

Depending upon a State's regulations, the security officers at a facility may or may not be armed. If the security officers are well armed, it is possible that they will not only be able to perform steps 1 and 2 but will also, if the number of security officers is sufficient, be able to perform step 3. If, on the other hand, a facility's security officers are not armed, they may only be able to perform step 1 and will be dependent upon an off-site armed response force for rapid interception and neutralization of the adversary. In most instances, "rapid" means within very few minutes.

Detection

At the access control points of a facility, authorized personnel, vehicles, and material often pass posted security officers. The function of these security

officers is to assure that unauthorized personnel, vehicles, or material do not enter the facility, i.e., to assure that unauthorized intrusion is detected at the entry control point(s). Consider visitor escort duty performed by security officers. Is not one of the duties of the security officers performing escort duty to detect unauthorized actions by the visitor? It logically follows that if enough security officers were posted completely around the perimeter of a facility (with overlapping visual fields of view between posts) that intrusion detection could be performed by people rather than by equipment. ~

Delay

If the same security officers who were posted completely around the perimeter of a facility to perform detection were well armed, they, rather than physical barriers, could provide the main delay for an adversary, just as armed entry control or visitor escort security officers are expected to delay an adversary.

Communications

The security officer's functions in the communication subsystem have been addressed, although briefly, in other modules. It is possible (although maybe not practicable) for security officers in sufficient numbers to perform all communications without telephones and radios.

The previous points just discussed indicate that a total physical protection system could be designed which utilizes humans for all major subsystem functions. In the United States of America, a physical protection system which is totally dependent on an adequate number of security officers to perform all functions is not cost-effective relative to other alternatives. Whereas it is difficult to measure the effectiveness of the protective force response, it may be even more difficult to measure the effectiveness of security officers in performing the functions of detection, communication, and delay.

INTERRELATIONSHIP OF SKILLS AND TRAINING

Skills and Training

A complete treatise on the skills and training that may be required for a security officer is not attempted in this training course. Instead, a few examples of the various skills required of certain security officers are discussed.

For the first example, consider a security officer at an entry control post. The security officer needs to perform procedures which allow authorized people and vehicles into a facility. He may need to accurately match a picture badge credential with the person presenting the badge. He probably needs to know what signatures and what forms are required before certain material can enter or leave a facility. He needs to be observant in order to detect unauthorized action by either an authorized or an unauthorized person. He might not be required to perform strenuous duties.

For the second example, consider a security officer at the communication center. He probably needs to process a great deal of both incoming and outgoing voice communications, to process sensor alarm information, to assess closed circuit television information, to log information, and to remain calm during an emergency or other high mental stress situation. He might not be required to perform any physically stressful duties.

For the final example, consider the response security officer. He probably needs to be physically strong, proficient in modern weapons and when and where to use them, a skilled tactician, and a good team member.

The above examples of some of the skills required for certain security officers are intended to very briefly indicate the wide range of differing skills required for different security officer positions. The point made by the examples is that security officers need to be trained for the functions which they are to perform. It is neither reasonable nor desirable to expect all security officers to be able to perform all security officers' functions. In many instances, a particular security officer's position, e.g., in the communication center, not only requires extensive training but also requires continuous performance in that position in order to maintain adequate proficiency.

Each security officer's job needs to be carefully characterized (by a job description), and people need to be trained to perform in that job. Obviously, some cross training can be done so that some security officers may be able to satisfactorily perform multiple functions.

A certain amount of testing can be performed initially in a classroom-like environment to determine an individual's basic performance in a given job. But, in addition, test exercises should be performed often enough at the facility to provide continued assurance that

1. Routine plans and procedures are followed, and
2. Contingency plans and procedures are followed.

CONTINGENCY PLANS AND PROCEDURES

Contingency plans and procedures need to be developed for situations and conditions which are not normal but which are perceived as likely to occur. Because people can quickly adapt to changing conditions, contingency plans usually affect the protective force more than they affect other subsystems in the physical protection system. Because these plans are developed before the abnormal situation or condition arises, the effectiveness of the physical protection system can be maintained during an actual contingency situation.

MODULE 11

VISUALS

NOTES

PROTECTIVE FORCE

- MAJOR SUB-SYSTEM
- FUNCTIONS
- SKILLS AND TRAINING
- CONTINGENCY PLANS AND PROCEDURES

FUNCTIONS

RESPONSE

ENTRY CONTROL

VISITOR ESCORT

RANDOM PATROL

ASSESSMENT

OTHER

VISUALS

NOTES

RESPONSE

CONFRONT ADVERSARIES

NEUTRALIZE ADVERSARIES

ENTRY CONTROL

VERIFY AUTHORIZED

PERSONNEL

VEHICLES

MATERIAL

IMPLIES

DETECT

UNAUTHORIZED

DELAY

UNAUTHORIZED

COMMUNICATE

CALL FOR HELP

VISUALS

NOTES

VISITOR ESCORT

GUIDE VISITORS WITH LIMITED AUTHORIZATION

IMPLIES

DETECT	UNAUTHORIZED
DELAY	UNAUTHORIZED
COMMUNICATE	CALL FOR HELP

RANDOM PATROL

INTRODUCES UNCERTAINTY FOR THE ADVERSARY

POSSIBLY COULD DETECT

POSSIBLY COULD DELAY

POSSIBLY COULD COMMUNICATE

VISUALS

NOTES

ASSESSMENT

ASSESS SENSOR ALARM INFORMATION RAPIDLY

ASSESS VOICE COMMUNICATION INFORMATION RAPIDLY

ASSESS RAPIDLY CHANGING SITUATIONS

PROTECTIVE FORCE

(HUMAN)

- COULD PERFORM ALL

DETECTION

DELAY

COMMUNICATION

RESPONSE

- DIFFICULT TO MEASURE THE "HOW GOOD"

- HERE—ALL HUMAN PPS ARE MUCH MORE EXPENSIVE THAN OTHER ALTERNATIVES

VISUALS

NOTES

SKILLS

FOR EXAMPLE

ENTRY CONTROL

PERFORM ROUTINE PROCEDURES

BUT OBSERVANT FOR UNAUTHORIZED

COMMUNICATION CENTER

ACCURATELY PROCESS INCOMING AND OUTGOING
ROUTINE MESSAGES

ASSESS SENSOR ALARM INFORMATION

REMAIN CALM AND PROFICIENT IN HIGH STRESS
CONDITIONS

COMMUNICATION CENTER SUPERVISOR

RAPID JUDGMENTS AND DECISIONS

TACTICIAN

RESPONSE

PERFORM AS A TACTICAL TEAM

SKILLED "SMALL FORCE" FIGHTING TEAM

PROFICIENT IN THE USE OF MODERN LIGHT ARMS

CAN ASSUME LEADER POSITION IF NECESSARY

COMMAND RESPONSE SUPERVISORS

TACTICIAN

LEADER

CALM DURING STRESS CONDITIONS

PROTECTIVE FORCE ---

TRAIN FOR SKILLS REQUIRED

- MANY DIFFERENT SKILLS REQUIRED DEPENDING ON THE PARTICULAR JOB
- DESCRIBE THE SPECIFIC JOBS
- TRAIN SPECIFIC SECURITY OFFICER FOR SPECIFIC JOBS
- SOME CROSS TRAINING MAY BE POSSIBLE
- TEST OFTEN ENOUGH
 - TO ASSURE THAT ROUTINE PLANS ARE FOLLOWED
 - TO ASSURE THAT CONTINGENCY PLANS ARE FOLLOWED

VISUALS

NOTES

CONTINGENCY PLANS AND PROCEDURES

- PURPOSE -- MAINTAIN PHYSICAL PROTECTION SYSTEM EFFECTIVENESS
- DEVELOPED FOR EXTRAORDINARY CONDITIONS
 - FOR EXAMPLE
 - FIRE -- ACCIDENT -- COMPONENT FAILURE
 - HOSTAGE -- BOMB -- DEMONSTRATION
- IMPLEMENTED QUICKLY AND EFFECTIVELY
- PROTECTIVE FORCE USUALLY MOST AFFECTED

12.0 SYSTEM CONCEPTS

Session Title: 12.1 Introduction to Physical
Protection Systems

Date: Thursday, 2 November

Presented By: P. B. Herrington, Sandia
Laboratories

Time: 0930 to 1030

Session Objectives:

After the session, the participants will be able to

1. State the objective of a nuclear facility's physical protection system,
2. List four subsystems likely to be present in a power reactor facility system,
3. List three features of an effective physical protection system, and
4. List two methods of accomplishing the objective of the physical protection system.

Summary:

The objective of a physical protection system at a nuclear facility and two methods of accomplishing this objective are discussed. The subsystems likely to be a part of a power reactor facility system and three basic features of an effective physical protection system are also discussed.

MODULE 12

SYSTEM CONCEPTS

INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS

"A system may be defined as an array of components designed to achieve an objective according to plan."¹ The objective of a physical protection system is to prevent the accomplishment of unauthorized overt or covert actions. When a physical protection system is applied to a nuclear facility, its objective is to prevent the theft and/or dispersal of certain types of nuclear materials and/or to prevent sabotage of the facility. A physical protection system is a subsystem of the total facility system, and it should be designed to interface effectively with the facility operation system, safety system, and safeguards system.

TOTAL POWER REACTOR FACILITY SYSTEM

The objectives of the total power reactor facility system are

1. To use energy from nuclear materials in the generation of electrical power,
2. To accomplish the preceding operation safely,
3. To safeguard (control and account for) the nuclear materials, and
4. To protect the nuclear materials from theft and/or dispersal and to protect the facility against sabotage.

If these four goals are the objectives of the total system, then it is possible to separate the total system into four major subsystems: (1) operations, (2) safety, (3) safeguards, and (4) physical protection.

The operations subsystem controls personnel, material, and processes in such a manner as to convert nuclear energy into electrical energy. The efficiency of this conversion is affected by the safety, safeguards, and physical protection subsystems. The effects which these subsystems have are both economic and social.

The social effects of implementation of the safety, safeguards, and physical protection subsystems should satisfy the original requirements for their implementation and should minimize social concerns.

In general, the economic effects include additional equipment installation and maintenance costs, procedures which slow the movement of personnel and material, stringent personnel requirements, and external review requirements. If it is recognized that the safety, safeguards, and physical protection subsystems are, to some extent, mutually complementary, the economic impact on the total system can be decreased.

MODULE 12

SYSTEM CONCEPTS

INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS

"A system may be defined as an array of components designed to achieve an objective according to plan."¹ The objective of a physical protection system is to prevent the accomplishment of unauthorized overt or covert actions. When a physical protection system is applied to a nuclear facility, its objective is to prevent the theft and/or dispersal of certain types of nuclear materials and/or to prevent sabotage of the facility. A physical protection system is a subsystem of the total facility system, and it should be designed to interface effectively with the facility operation system, safety system, and safeguards system.

TOTAL POWER REACTOR FACILITY SYSTEM

The objectives of the total power reactor facility system are

1. To use energy from nuclear materials in the generation of electrical power,
2. To accomplish the preceding operation safely,
3. To safeguard (control or account for) the nuclear materials, and
4. To protect the nuclear materials from theft and/or dispersal and to protect the facility against sabotage.

If these four goals are the objectives of the total system, then it is possible to separate the total system into four major subsystems: (1) operations, (2) safety, (3) safeguards, and (4) physical protection.

The operations subsystem controls personnel, material, and processes in such a manner as to convert nuclear energy into electrical energy. The efficiency of this conversion is affected by the safety, safeguards, and physical protection subsystems. The effects which these subsystems have are both economic and social.

The social effects of implementation of the safety, safeguards, and physical protection subsystems should satisfy the original requirements for their implementation and should minimize social concerns.

In general, the economic effects include additional equipment installation and maintenance costs, procedures which slow the movement of personnel and material, stringent personnel requirements, and external review requirements. If it is recognized that the safety, safeguards, and physical protection subsystems are, to some extent, mutually complementary, the economic impact on the total system can be decreased.

The measures of nuclear safety which are aimed at the prevention of accidental damage to nuclear facilities and accompanying possible radiological hazards also serve the purposes of physical protection by helping to prevent the same kind of damage which might result from a willful hostile action in the form of sabotage. Safeguards are connected with physical protection, supplying information on the type, quantity, and location of nuclear materials within the facility and detecting losses related to a theft or unauthorized diversion. Physical protection can be considered as contributing to the effectiveness of safeguards against diversion of nuclear materials by assuring the containment of the nuclear materials within designated areas. In other words, the subsystems of safety, safeguards, and physical protection are, to a great extent, mutually complementary and, therefore, the designing of each of these subsystems for a specific facility should also take into account the requirements of the other subsystems.

CHARACTERISTICS OF AN EFFECTIVE PHYSICAL PROTECTION SYSTEM

An effective physical protection system is a system which has been designed to include the following features: (1) protection-in-depth, (2) minimization of subsystem failure impact, and (3) zonal tracking.

Protection-in-Depth

Protection-in-depth means that an adversary must avoid or defeat a number of protective devices in sequence to accomplish his goal. For example, an adversary might have to penetrate three separate barriers before gaining entry to a reactor control room.

Minimization of Subsystem Failure Impact

It is unlikely that a complex system will ever be implemented which does not experience subsystem failure. Causes of subsystem failure in a physical protection system are numerous and can range from environmental factors (which may be expected) to adversary action outside of the threat spectrum used in the system design (not expected). While knowledge of the cause of a subsystem failure is important in an attempt to restore the system to normal operation, it is more important for contingency plans to be provided. These contingency plans will minimize the effects of subsystem failure so that the system continues to operate effectively. Contingency plans may be carried out automatically, e.g., when one piece of equipment fails, redundant equipment automatically begins to perform the function previously performed by the disabled equipment. However, certain subsystem failures may require aid from sources external to the facility in order to minimize the impact of the failure.

Zonal Tracking

Zonal tracking is the ability to follow the movements of an adversary until the adversary can be neutralized. The knowledge that an adversary is attempting some malevolent action against a facility may be of little value unless the protection system is able to interrupt the adversary in a known zone.

METHODS OF ACCOMPLISHING THE OBJECTIVE

The objective of a physical protection system applied to a nuclear facility is to prevent the theft of certain nuclear materials and/or to prevent radiological sabotage of the facility. There are two basic methods for accomplishing this objective: deterrence and neutralization.

Deterrence may be accomplished by the implementation of a physical protection system which is judged by all adversaries to be too difficult to defeat and therefore is an unattractive target.

Neutralization refers to the actions taken to prevent an adversary from accomplishing his goal once the adversary actually begins a malevolent action against a facility. There are several functions which the physical protection system must perform before the adversary can be neutralized. These functions must be performed in a length of time which is less than the time required for the adversary to complete his tasks. (see Figure 12-1). Normally, an adversary begins his

Figure 12-1. Required Relationships of Adversary Task Time to Physical Protection System Time Requirements

task at some time before the first alarm occurs. The total time required for the adversary to accomplish his goal has been labeled "adversary task time," and this time is dependent on the delay built into the physical protection system. The time that the first alarm occurs is labeled T_0 (Figure 12-1). After the alarm occurs, the alarm information must be communicated and assessed to determine if the alarm is valid. The need for alarm assessment is discussed in detail in Session 12.2: Functions of a Physical Protection System.

The time at which the alarm is judged to be valid is labeled T_A (Figure 12-1). The location of the alarm must be communicated to the protective force, and time is required for the protective force to respond in adequate number and with adequate equipment to interrupt and neutralize the adversary. The time at which the protective force interrupts the adversary is labeled T_I and the adversary task completion time is labeled T_C . Clearly, in order for the physical protection system to accomplish its objective, T_I must occur before T_C .

In order to accomplish its prime objective, the physical protection system is required to perform various functions. These functions are either deterrence or a combination of detection, communication, delay, response, and neutralization.

REFERENCE

1. R. A. Johnson, F. E. Kast, and J. E. Rosenzweig, The Theory and Management of Systems, McGraw-Hill Book Company, New York, 1963.

MODULE 12

SESSION 12.1

VISUALS

NOTES

TOTAL POWER REACTOR FACILITY SYSTEM OBJECTIVES

- CONVERT NUCLEAR ENERGY TO ELECTRICAL ENERGY EFFICIENTLY
- ACCOMPLISH CONVERSION SAFELY
- CONTROL AND ACCOUNT FOR NUCLEAR MATERIAL
- PREVENT THEFT OR MATERIALS AND/OR SABOTAGE OF THE FACILITY
- EFFICIENCY OF CONVERSION AFFECTED BY OTHER OBJECTIVES

- TOTAL POWER REACTOR FACILITY SYSTEM MAY HAVE FOUR SUBSYSTEMS
 1. OPERATION
 2. SAFETY
 3. SAFEGUARDS
 4. PHYSICAL PROTECTION

- EFFECTS OF EACH SUBSYSTEM ON THE OTHERS ARE EITHER SOCIAL OR ECONOMIC.

EFFECTS OF SAFETY, SAFEGUARDS, AND PHYSICAL PROTECTION

- SOCIAL
- ECONOMIC
 - ADDITIONAL EQUIPMENT
 - ADDITIONAL PROCEDURES
 - STRINGENT PERSONNEL REQUIREMENTS
 - EXTERNAL REVIEW REQUIREMENTS

VISUALS

NOTES

- EACH MAJOR SUBSYSTEM IS A SYSTEM WITHIN ITSELF, IMPACTS EACH OTHER MAJOR SUBSYSTEM, AND IS IMPACTED BY EACH OTHER MAJOR SUBSYSTEM.

EXAMPLE

CHARACTERISTICS OF EFFECTIVE PPS

- PROTECTION IN DEPTH
 - MORE THAN ONE PROTECTIVE DEVICE IN SEQUENCE
 - POSITIVE MEASURES
- MINIMIZATION OF SUBSYSTEM FAILURE IMPACT
 - PROCEDURES
 - CONTINGENCY
 - REDUNDANCY
 - EXTERNAL SOURCES
- ZONAL TRACKING
 - MULTIPLE DETECTION
 - DETECT/DELAY

VISUALS

NOTES

12.0 SYSTEM CONCEPTS

Session Title: 12.2 Functions of a Physical
Protection System

Date: Tuesday, 7 November

Presented By: P. B. Herrington, Sandia Laboratories

Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. List seven functions of a physical protection system,
2. Define these seven functions, and
3. List an important measure for each of the functions.

Summary:

Seven functions of a physical protection system are defined and the measures important to each are discussed. Subsystems which can perform the functions are introduced.

FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

An effective physical protection system may provide seven functions: detection, delay, communication, response, neutralization, access control, and deterrence. It is important to understand the definitions of the various functions and the measures of each function which are needed for total system evaluation.

DETECTION

Detection is the discovery, by the protective force, of an adversary action. In order to discover an adversary action, the following events need to occur:

1. A sensor (or set of sensors) responds to an abnormal occurrence and initiates an alarm,
2. The information from the sensor and assessment subsystems is communicated and processed for evaluation, and
3. An assessment is made of the information and the alarm is judged to be valid.

If the assessment of the information had been that the alarm was either a false or nuisance alarm, a detection would not have occurred based on this definition.

The measurements important to the evaluation of detection are probability of detection and time required for detection. The probability and time measurements may be related as shown in Figure 12-2. A sensor indicates an abnormal action at time T_0 , and, at a later time, T_1 , sensor and assessment information is received for evaluation (Figure 12-2). If the time delay between T_0 and T_1 is short, the probability of detection, P_d , rapidly approaches P_s , which is the probability that the sensor will sense the unauthorized action. Even for short time delays, the probability that a detection will be made may not equal P_s because of the possibility that a valid alarm may be assessed as false. As shown in Figure 12-2, the probability of detection decreases as the delay in beginning assessment increases.

DELAY

Delay is the impeding of adversary progress. The measures of delay are the time required by the adversary (after detection) to perform each task. Although the adversary may be delayed prior to detection, this delay may be of little value to the operation of the physical protection system.

Figure 12-2. Variation of Probability of Detection with Time Delays Between Sensing and Assessment

COMMUNICATION

Communication is the means by which sensor and assessment information is transferred to the assessment point and the response force is informed of adversary actions. The measures of communication are probability of communication and time required to communicate. The probability of communication and the time required for communication are interrelated, as shown in Figure 12-3. For some time after information is received, the probability that valid information has been communicated to the intended recipient is zero. This delay may vary considerably depending on the method of communication used. After the initial delay, the probability of valid communication begins to increase rapidly; however, this increase may be delayed several times if the communication must be repeated.

RESPONSE

Response consists of the actions taken by the protective force to prevent adversary success. The measure of response is the time between receipt of a communication on adversary action and interruption of the adversary.

NEUTRALIZATION

Neutralization is the act of stopping the adversary's progress before his goal is accomplished. The measurement of this function is the probability of neutralization and the time required to assemble a neutralization force. The time required to assemble a neutralization force depends on the size of the force and the equipment required, which, in turn, depends on the size of the adversary force and equipment used by the adversary force.

Figure 12-3. Variation of probability of a Valid Communication with Time

ACCESS CONTROL

Access control consists of allowing access to authorized personnel and detecting attempted access of unauthorized personnel and/or material. The measures of access control are throughput, impostor pass rate, and false alarm rate. Throughput is defined as the number of authorized personnel allowed access per unit time assuming that all personnel who attempt access are authorized for access. Both the impostor pass rate and the false alarm rate can be decreased by decreasing the throughput; however, a decreased throughput will probably have adverse effects on the facility operations subsystem.

DETERRENCE

Deterrence consists of decreasing the attractiveness of a facility to an adversary by increasing the resources required for the adversary to succeed in achieving a goal.

PHYSICAL PROTECTION SUBSYSTEMS

Some subsystems of a physical protection system which can be used to provide the required functions are intrusion detection systems, barriers, communication systems, the protective force, and entry control systems. Table 12-I shows the functions which may be provided by the various subsystems.

All of the functions of a physical protection system may be provided by the protective force. However, this may not be practicable in many facilities because of the large number of personnel that would be required to perform all of the functions.

TABLE 12-1
Subsystem Functions

<u>Subsystems</u>	<u>Functions</u>	
	<u>Primary</u>	<u>Secondary</u>
Intrusion Detection Systems	Detection Communication	Deterrence
Barriers	Delay	Deterrence
Communication Systems	Communication	
Protective Force	Response Neutralization Access Control Detection Communication Deterrence	
Entry Control Systems	Access Control Detection Communication	Delay Deterrence

SUMMARY

Detection, delay, communication, response, neutralization, and access control are all required functions of an effective physical protection system. In order to evaluate the performance of a physical protection system, each function must be evaluated and these evaluations combined. No physical protection system can operate effectively without each of these functions. Some potential adversaries may be deterred from taking malevolent actions against a facility because it is protected by an effective physical protection system; however, the deterrence function of a physical protection system is difficult to measure.

During this course, reference will often be made to the "four major functions" or simply "four functions" of a physical protection system. The four functions referred to are detection, delay, communication, and response. Normally, when only four functions are addressed, access control is included in the category of detection, neutralization is included in response, and deterrence is not addressed.

FUNCTIONS OF A PPS

- DETECTION
- DELAY
- COMMUNICATION
- RESPONSE
- NEUTRALIZATION
- ACCESS CONTROL
- DETERRENCE

DETECTION

DEFINITION: DISCOVERY BY THE PROTECTIVE FORCE OF AN ABNORMAL ACTION

HOW DOES IT HAPPEN?

- SENSOR(S) RESPONDS TO ABNORMAL OCCURRENCE
- DATA FROM SENSOR(S) AND ASSESSMENT SUBSYSTEM'S COMMUNICATED AND PROCESSED FOR EVALUATION
- ASSESSMENT MADE, AND ALARM JUDGED VALID

MEASURES

- PROBABILITY OF DETECTION
- TIME REQUIRED FOR DETECTION

PROBABILITY OF DETECTION

DELAY

DEFINITION: THE IMPEDING OF ADVERSARY PROGRESS

MEASURE: TIME REQUIRED BY ADVERSARY TO PERFORM TASK

NOTE: ALTHOUGH ADVERSARY DELAYED PRIOR TO DETECTION,
THIS DELAY IS OF LITTLE VALUE TO PPS.

COMMUNICATION

DEFINITION: MEANS BY WHICH PROTECTIVE FORCE IS INFORMED OF
ADVERSARY ACTIONS

● TWO TYPES

- SENSOR AND ASSESSMENT DATA TO ASSESSMENT POINT
(INCLUDED IN DETECTION)
- RESPONSE FORCE(S) INFORMED OF ADVERSARY ACTIONS

MEASURES

- PROBABILITY OF COMMUNICATION
- TIME REQUIRED FOR COMMUNICATION

**PROBABILITY OF
COMMUNICATION**

VISUALS

NOTES

RESPONSE

DEFINITION: ACTIONS TAKEN BY THE PROTECTIVE FORCE
TO PREVENT ADVERSARY SUCCESS

MEASURE: RESPONSE TIME

NEUTRALIZATION

DEFINITION: THE ACT OF STOPPING THE ADVERSARY'S PROGRESS
BEFORE HIS GOAL IS ACCOMPLISHED.

MEASURES

- PROBABILITY OF NEUTRALIZATION
- NEUTRALIZATION TIME

ACCESS CONTROL

DEFINITION: ALLOWING ACCESS TO AUTHORIZED PERSONNEL AND
MATERIAL AND DETECTING ATTEMPTED ACCESS OF
UNAUTHORIZED PERSONNEL AND/OR MATERIAL.

MEASURES

- THROUGHPUT
- FALSE ALARM RATE (TYPE I ERROR RATE)
- IMPOSTOR PASS RATE (TYPE II ERROR RATE)

DETERRENCE

DEFINITION: DECREASING ATTRACTIVENESS OF A FACILITY
TO AN ADVERSARY BY INCREASING RESOURCES
REQUIRED BY ADVERSARY.

MEASURE

- VERY DIFFICULT TO MEASURE
- NORMALLY DO NOT TAKE CREDIT FOR DETERRENCE
WHEN EVALUATING SYSTEM EFFECTIVENESS

PHYSICAL PROTECTION SUBSYSTEMS

<u>Subsystems</u>	<u>Functions</u>	
	<u>Primary</u>	<u>Secondary</u>
Intrusion Detection Systems	Detection Communication	Deterrence
Barriers	Delay	Deterrence
Communication Systems	Communication	
Protective Force	Response Neutralization Access Control Detection Communication Deterrence	
Entry Control Systems	Access Control Detection Communication	Delay Deterrence

SUMMARY

- DETECTION
 - ACCESS CONTROL
- DELAY
- COMMUNICATION
- RESPONSE
 - NEUTRALIZATION
- DETERRENCE IS NOT ADDRESSED
BECAUSE IT IS DIFFICULT TO MEASURE.

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

12.0 SYSTEM CONCEPTS

Session Title: 12.3 System Design Approach

Date: Monday, 13 November

Presented By: W. K. Paulus, Sandia Laboratories

Time: 1330 to 1400

Session Objectives:

After the session, the participants will be able to list four basic steps in the design of a physical protection system.

Summary:

The four basic steps in the design of a physical protection system (definition of objectives, facility characterization, conceptual system design, and conceptual design evaluation) are discussed.

SYSTEM DESIGN APPROACH

The design of a physical protection system for a nuclear facility involves four basic steps:

1. Define the objectives of the system,
2. Characterize the facility,
3. Develop physical protection system concepts, and
4. Evaluate the conceptual design.

This design approach in steps 3 and 4 is particularly iterative in that the conceptual design may need many modifications before it is judged capable of achieving the defined objectives. It is possible that after many design evaluations, a judgement will be made that the defined objectives must be modified.

DEFINITION OF OBJECTIVES

The detailed objectives of a physical protection system must be defined prior to any meaningful design concepts development and evaluation. The objectives should contain information and restrictions on the physical protection system which are related to

1. Performance goals,
2. Threat spectrum,
3. Costs, and
4. Impact on other facility systems.

The performance goals and costs may be specified, in part, by a group external to the facility such as a State Board of Regulation; however, the facility management may also have facility-specific performance goals and cost limitations.

In order to make an informed choice from among various physical protection concepts, the relative effectiveness of each concept needs to be evaluated against a threat spectrum.

The adversary attributes that could be considered include the following:

1. Facility access (outsiders with no authorized access, employees or visitors with access, or outsiders in collusion with employees),
2. Number of adversaries,
3. Mode of transportation (foot, all-terrain vehicles, helicopters),
4. Weapons (side arms, automatic weapons, etc.),
5. Explosives,
6. Special equipment (self-contained breathing apparatus, etc.),
7. Technical and military skills,
8. Knowledge of facility operations and layout,
9. Knowledge of the physical protection system, and
10. Motivation.

FACILITY CHARACTERIZATION

The purpose of this portion of the system design procedure is to develop a facility characterization which will include all of the technical information necessary for a physical protection system design. The information required to accomplish this facility characterization includes climatic and geological characteristics of the area and descriptions of facility buildings, processes, and systems. This information is used to perform theft and sabotage target analyses and to identify physical protection concerns for the facility. Facility characterizations which include alternative processes and facility layouts can also be developed in this design step. Facility characterization is discussed in detail in Session 12.4: Facility Characterization.

CONCEPTUAL DESIGN OF THE PHYSICAL PROTECTION SYSTEM

Based on information gained from the definition of objectives and the facility characterization and with a knowledge of the various physical protection options, the design of a conceptual physical protection system can begin; that is, the required functions of the system may be placed at chosen sites at the facility. It is important to recall, at this stage in the design procedure, that an effective physical protection system has the following characteristics: (1) protection-in-depth, (2) minimization of subsystem failure impact, and (3) zonal tracking. During this step in the design procedure, several options will be developed. The choice of which option to actually implement will be made after each option has been evaluated.

Conceptual Design Evaluation

The methods of design evaluation used in this International Training Course provide an introduction to a means of comparing the performance of various conceptual physical protection system designs. Logic trees are used to evaluate a concept based on positive measures to protect all of the adversary sequences shown on the trees. The Estimate of Adversary Sequence Interruption (EASI) model is used to evaluate the performance of the system against a few chosen adversary paths. The EASI model gives an estimate of the probability that the protective force can respond and interrupt the adversary sequence before the adversary achieves his goal. The EASI model requires the analyst to provide estimates of probability of detection, probability of communication, adversary task time (delay), and response time.

Each conceptual option can be evaluated against the performance goals and threat spectrum and the options which are considered unacceptable can be discarded. The acceptable options then need to be evaluated against the cost restrictions and impact on other facility subsystems. If, after final evaluation, none of the options satisfy the defined system objectives, either new conceptual designs are developed or the defined objectives are modified.

PHYSICAL PROTECTION SYSTEM DESIGN APPROACH

DEFINITION OF OBJECTIVES

- PERFORMANCE GOALS
- THREAT SPECTRUM
- COSTS
- IMPACTS

VISUALS

NOTES

ADVERSARY ATTRIBUTES

- FACILITY ACCESS
- NUMBER
- TRANSPORTATION
- WEAPONS
- EXPLOSIVES
- SPECIAL EQUIPMENT
- TECHNICAL AND MILITARY SKILLS
- KNOWLEDGE OF FACILITY
- KNOWLEDGE OF PPS
- MOTIVATION

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

12.0 SYSTEM CONCEPTS

Session Title: 12.4 Facility Characterization

Date: Friday, 10 November

Presented By: P. B. Herrington, Sandia Laboratories

Time: 1330 to 1400

Session Objectives:

After the session, the participants will be able to draw a state matrix for a pressurized water reactor.

Summary:

The information required for facility characterization is discussed. A hypothetical derivation of five facility states for a pressurized water reactor is made.

FACILITY CHARACTERIZATION

The objective of this portion of the system design procedure is to develop a facility characterization which will include all of the technical information necessary for a physical protection system design. The information required to accomplish this objective includes climatic and geological characteristics of the area and the descriptions of facility buildings, processes, and systems. This information is used to perform theft and sabotage target analyses, to identify physical protection concerns for the facility, and to develop physical protection system designs.

A representation of the facility should be prepared which shows all significant features of the facility site and buildings. Facility layouts should be obtained which show the site boundary, access points, building locations, and plan and elevation views of all significant buildings. All doors, gates, hatches, vents, and other openings in structural surfaces must be identified and classified according to the type of access allowed. Types of access include uncontrolled openings which allow free access, controlled openings which require identity verification for passage, and one-way emergency exits. Details of the construction of all fixed barriers and controlled openings should be provided to facilitate later estimates of barrier delay capability; however, external and internal walls and other fixed barriers which contain uncontrolled openings need to be identified since access can occur through these openings.

In this facility characterization step, a knowledge of facility operations is required in order for target analysis to be performed. The principal physical protection concern for a pressurized water reactor is sabotage; whereas, for a facility such as a fuel processing facility, where Category I* nuclear materials are present in easily handled forms, both theft and dispersal are principal concerns. In this session, a pressurized water reactor is considered as an example of a sabotage target.

For a description of a pressurized water reactor to be performed, detailed information is required on the operation of a number of systems, including

1. The primary system,
2. The shutdown system,
3. The emergency core cooling system,
4. The radioactive waste system, and
5. The fuel storage and handling system.

*See Table: Categorization of Nuclear Materials, INPCIRC 1225/Rev. 1.

Detailed information is also required on the auxiliaries to these systems, e.g., instrumentation and control, power sources, and cooling. The information required includes operating procedures, system and component capacity and redundancy, system interconnections, and locations of system components and auxiliaries. In addition, the personnel interface with these systems and the access requirements to areas containing these systems must be understood.

Information concerning the effect of various facility states on facility operation is required for target identification in physical protection system design. Facility operation during these different states may vary in areas such as personnel location and flow, facility system requirements, and location of nuclear materials. For example, during the refueling and maintenance period at a reactor, targets and access requirements would be different from those requirements in effect during normal operation. During refueling, the high pressure injection system would not be a target since the reactor would be depressurized and access to this system for maintenance could be allowed. The primary system would, however, remain a target, and access control for the containment area would be affected by the large number of workers present during refueling. Many facility states can be identified, but usually only a few of these states will have significantly different physical protection requirements.

As an example, Figure 12-4 shows a hypothetical derivation of five facility states for a pressurized water reactor. The derivation process excludes conditions that are either unlikely, impossible, or do not present a significant difference in physical protection concerns. These five facility states are combinations of reactor/reactor vessel states and facility general operation mode.

State 1. Normal Operations

- State 2. a. Limited maintenance with reactor at power. In this condition, a few outside maintenance personnel can be in the operating areas of the facility.
- b. Limited maintenance with reactor hot but not producing power. In addition to state 2a considerations, the fission product inventory may be somewhat reduced, depending on the duration of time since shutdown. For analysis and physical protection purposes, 2a and 2b are essentially the same.

State 3. Limited maintenance with reactor cold and shut down. In addition to state 2 considerations, the consequences of a sabotage event are reduced.

State 4. General maintenance outage with reactor vessel head in place on the vessel. The difference between state 4 and state 3 is that a large outside construction labor force will be in the facility.

State 5. General maintenance outage with reactor vessel head removed. In addition to state 4 considerations, the fuel is in a more vulnerable state. Whether or not refueling is actually in progress does not affect physical protection requirements.

FACILITY GENERAL OPERATION MODE	REACTOR STATUS			
	HOT, AT POWER, OR IN STARTUP OR SHUTDOWN OPERATION			
	HOT, ZERO POWER* OR PROCEEDING TO COLD			
		COLD, ZERO POWER, VESSEL HEAD ON		COLD, ZERO POWER, VESSEL HEAD OFF
NORMAL	1
LIMITED MAINTENANCE	2	2	3
MAINTENANCE OUTAGE, NO REFUELING IN PROGRESS			4	5
MAINTENANCE OUTAGE, REFUELING IN PROGRESS				5

*ZERO POWER MEANS LESS THAN THE POINT OF ADDING HEAT

= NOT POSSIBLE

1 = FACILITY STATE 1

Figure 12-4. Pressurized Water Reactor Facility State Matrix

Information about environmental conditions in various areas of the facility must also be included in the facility description. The environmental conditions in the various areas of a facility may be affected by the climatic and geographical characteristics of the area, the facility buildings, and the processes and systems employed at the facility. Environmental conditions can affect the type of physical protection components selected since weather conditions, electromagnetic interference, interior noise, heat, and humidity may degrade performance. In addition, factors such as soil type can affect installation and maintenance costs. The effect of adversary-induced conditions may also have to be considered in the target analysis and physical protection system design. For example, facility or physical protection equipment might fail if exposed to extreme conditions caused by adversary-induced steam release. The range of environmental conditions should be identified for all significant interior and exterior areas. The environmental conditions may affect the positive measures which may be employed. Operation during extreme environmental conditions such as those caused by earthquakes or hurricanes may be addressed by contingency plans.

Facility characterizations which include alternative processes and facility layouts for facilities in the conceptual stage may be developed in this design step. Alternative operational procedures for operating facilities may be developed, but these procedures need to be evaluated for impact on the facility operations subsystem.

FACILITY CHARACTERIZATION

- INCLUDES ALL FACILITY-SPECIFIC TECHNICAL INFORMATION REQUIRED FOR PPS DESIGN
 - DESCRIPTIONS OF BUILDINGS, PROCESSES, AND SYSTEMS
 - CLIMATIC AND GEOLOGICAL CHARACTERISTICS
- ONE USE IS VITAL LOCATION ANALYSIS

SIGNIFICANT FEATURES OF SITE AND BUILDINGS

- SITE BOUNDARY
- ACCESS POINTS
- BUILDING LOCATIONS
- PLAN AND ELEVATION VIEWS OF BUILDINGS
- IDENTIFY AND CLASSIFY DOORS, GATES, VENTS, AND OTHER OPENINGS BY TYPE OF ACCESS ALLOWED
 - UNCONTROLLED
 - CONTROLLED (AUTHORIZATION)
 - ONE WAY
- IDENTIFY BARRIERS WITH CONTROLLED OPENINGS
 - CONSTRUCTION
 - DELAY CAPABILITY

INFORMATION REQUIRED

- OPERATING PROCEDURES
- CAPACITY AND REDUNDANCY
- INTERCONNECTIONS
- LOCATIONS OF COMPONENTS
- PERSONNEL INTERFACE
- VARIOUS STATES FOR PPS CONSIDERATION

EXAMPLES OF PROCESSES AND SYSTEMS INFORMATION FOR PWR

- PRIMARY SYSTEM
- SHUTDOWN SYSTEM (MAINTENANCE)
- EMERGENCY CORE COOLING SYSTEM
- RADIOACTIVE WASTE STORAGE SYSTEM
- FUEL STORAGE SYSTEM
- WASTE AND FUEL INFORMATION MAY NOT
BE NEEDED FOR SABOTAGE ANALYSIS

VISUALS

NOTES

REACTOR STATUS

HEAT, AT POWER, OR IN STARTUP OR SHUTDOWN OPERATION

NOT, ZERO POWER* OR PROCEEDING TO COLD

COLD, ZERO POWER, VESSEL HEAD ON

COLD, ZERO POWER, VESSEL HEAD OFF

NORMAL	1	2	3	4
LIMITED MAINTENANCE	5	6	7	8
MAINTENANCE OUTAGE, NO REPAIRING IN PROGRESS	9	10	11	12
MAINTENANCE OUTAGE, REPAIRING IN PROGRESS	13	14	15	16

*ZERO POWER MEANS LESS THAN THE POINT OF ADDING HEAT

1 - FACILITY STATE 1

REACTOR STATUS

HEAT, AT POWER, OR IN STARTUP OR SHUTDOWN OPERATION

NOT, ZERO POWER* OR PROCEEDING TO COLD

COLD, ZERO POWER, VESSEL HEAD ON

COLD, ZERO POWER, VESSEL HEAD OFF

NORMAL	1			
LIMITED MAINTENANCE	2	2	3	
MAINTENANCE OUTAGE, NO REPAIRING IN PROGRESS			4	5
MAINTENANCE OUTAGE, REPAIRING IN PROGRESS				6

*ZERO POWER MEANS LESS THAN THE POINT OF ADDING HEAT

1 - FACILITY STATE 1

2 - FACILITY STATE 2

ENVIRONMENTAL CONDITIONS

- EXAMPLES
 - TEMPERATURE
 - HUMIDITY
 - VIBRATION
 - PRESSURE
 - ELECTROMAGNETIC
 - ACOUSTICAL
 - WIND, RAIN, SNOW, BLOWING DUST
 - AFFECTED BY
 - CLIMATIC CHARACTERISTICS
 - GEOGRAPHICAL CHARACTERISTICS
 - BUILDINGS, PROCESSES, SYSTEMS
 - PROBABLY ALL SUBSYSTEMS AFFECTED
 - MAY BE ADVERSARY INDUCED
 - CONTINGENCY PLANS FOR EXTREME CONDITIONS
-
- ALTERNATIVE LAYOUTS AND OPERATING PROCEDURES MAY BE DEVELOPED FOR FACILITIES IN THE CONCEPTUAL STAGE
 - ALTERNATIVE PROCEDURES MAY BE DEVELOPED FOR OPERATING FACILITIES
 - IN EITHER CASE, CONSIDER THE IMPACT ON THE MAJOR SUBSYSTEMS OF OPERATIONS, SAFETY AND SAFEGUARDS

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

GUEST LECTURES

Session Title: National Approaches to
Physical Protection in Iran

Date: Monday, 6 November

Presented By: M. Sarram, Atomic Energy
Organization of Iran

Time: 0830 to 0915

Session Objectives:

After the session, the participants will be able to

1. List the objectives of Iran's system of physical protection and
2. Describe the structure of Iran's system of physical protection.

Summary:

The objectives and structure of Iran's system of physical protection are discussed.

NATIONAL APPROACHES TO PHYSICAL PROTECTION IN IRAN

INTRODUCTION

The Atomic Energy Organization of Iran (AEOI) was established, by law, 4 years ago with the basic tasks of

1. Control of all nuclear activities in Iran.
2. Construction and operation of nuclear powerplants (total capacity of 23,000 MWe nuclear by the end of century), and
3. Research, development, and training.

Just recently, AEOI has been reorganized in order to separate the regulatory activities from the activities related to construction and operation of nuclear powerplants. Activities in regard to item 2 and part of 3 were transferred, by law, to the Ministry of Power which already operates all conventional plants.

GENERAL CONSIDERATIONS

Figure 1 shows a simple organizational chart of AEOI. Basically, all regulatory activities are divided into four separate divisions, namely

Figure 1. AEOI Chart

1. Nuclear Safeguards,
2. Safety of Nuclear Facilities,
3. Radiation Protection, and
4. Environmental Protection.

Figure 2 shows a chart of the Nuclear Safeguards Division (NSD). It is to be noted that Iran is a signatory to the Non-Proliferation Treaty (NPT) and right from the beginning of establishment of AEOT, a great emphasis was put on nuclear safeguards.

Figure 2. Nuclear Safeguards Division (NSD) Chart

The ambitious and fast expanding nuclear technology in Iran calls for a sound scientific approach to safeguards matters as well as a clear separation of duties of authority versus utility, taking into account that in Iran, utility is also a government organization as opposed to being "private" in some countries.

The socio-political system of Iran, its geographical location, and other local and international limitations have been taken into account in developing the national approach to nuclear safeguards programs.

SAFEGUARDS PHILOSOPHY

In general, nuclear safeguards in Iran is considered to have the following three main elements:

1. Nuclear material control,
2. Nuclear material accountancy and measurement, and
3. Physical protection of nuclear facilities and materials.

Thus, one can see that physical protection of nuclear facilities and materials is an integrated element of the overall national nuclear safeguards program. The Nuclear Safeguards Division of AEOI is responsible for regulating and controlling source and special fissionable materials (as defined by IAEA) in Iranian nuclear industry. In this respect, the rules and regulations developed are intended to protect against, deter, and detect the theft or diversion to unauthorized uses of special nuclear materials (including both source and fissionable materials) and for protecting nuclear facilities against acts of sabotage which may lead to radiological consequences.

The term radiological consequence is to be noted here. The philosophy for physical protection in Iran is that not only nuclear materials in a facility must be protected but also the nuclear facility itself must be protected against intentional acts of sabotage with radiological consequences. In some countries, the normal approach usually has been to protect nuclear material within a facility and it is only in recent years that attention has been given to acts of sabotage to facilities with radiological consequences.

As an example, let us look at an act of sabotage, where the cooling water intake pipes of a nuclear powerplant are damaged so that it may lead to partial core meltdown and release of radioactivity into the environment. (We have assumed that other safety features such as Emergency Core Cooling Systems have been made inoperative as well or that they failed to operate when needed.) Here, considering that the act of sabotage was not directed towards nuclear materials in the facility, this question comes up

"Should the approach of national authority be such as to provide rules and regulations for prevention of such incidents?"

Certainly the answer to this question is "yes" in Iran, and in developing the rules and regulations the above considerations are taken into account.

APPROACH TO PHYSICAL PROTECTION

Having discussed the philosophy, the approach to physical protection of nuclear facilities and materials in Iran consists of detailed study of the following:

1. Threat assessment,
2. Design of physical protection system, and
3. Effectiveness measurement.

For a given facility, first an assessment of threat is made taking into account the kind and amount of nuclear materials present in that facility. Then a physical protection system is designed for this facility consisting of elements such as

1. Detection,
2. Delay (physical and/or psychological deterrence), and
3. Response.

Finally, the effectiveness of the system is measured to obtain the desired level of protection. Here computer codes and modeling are most useful as well as use of event trees for determination of probability of success or failure, for example, in the case of sabotage or theft of nuclear materials.

OTHER APPROACHES

1. Confirmatory Research--It is believed that in order to have a sound scientific approach to safeguards problems, use of a "test site" for reliability analysis of electronics equipment in security fields including containment and surveillance systems is necessary.
2. Independent Measurement--A sound safeguards system must have the capability to carry out independent measurement of nuclear materials including (NDA) techniques and computer modeling.

As can be seen in Figure 2, all these ideas have been considered in setting up a nuclear safeguards program in AEOI.

OTHER ACTIVITIES

1. Training--In cooperation with IAEA and in relation to other bilateral agreements, the staff of NSD are sent to other countries for short- and long-term training in the field of safeguards.
2. Collaboration with IAEA Programs--Iran, being a signatory to NPT, has always made use of IAEA guides and standards in the area of nuclear safeguards, when applicable. Iran has also taken a great interest in the recent IAEA programs, such as "Convention on Physical Protection of Nuclear Facilities and Materials," as well as other agency programs in physical protection, such as this first international course, by being one of the three countries that collaborated with IAEA in drafting the syllabus for this training course.

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

GUEST LECTURES

Session Title: United Kingdom National Approach
to Physical Protection

Date: Monday, 6 November

Presented By: G. S. Constable, Deputy Director
of Security, UK Atomic Energy
Authority

Time: 0915 to 1000

Session Objectives:

After the session, the participants will be able to

1. List the objectives of the United Kingdom's system of physical protection and
2. Describe the structure of the United Kingdom's system of physical protection.

Summary:

The objectives and structure of the United Kingdom's system of physical protection are discussed.

UNITED KINGDOM NATIONAL APPROACH TO PHYSICAL PROTECTION

Within the United Kingdom (UK) civil nuclear industry, the prime responsibility for carrying out research and development of all aspects of nuclear power rests within a government corporation, the United Kingdom Atomic Energy Authority (UKAEA). Thus the UKAEA provides continuous research and development support for the UK nuclear industry.

Responsibility for the manufacture and supply of uranium- and plutonium-based fuels and the provision of related fuel services rests with British Nuclear Fuels Limited (BNFL), a state owned company whose shares are held on behalf of the UK Government by the UKAEA. BNFL is responsible for the conversion and enrichment of uranium, fabrication of fuel elements, and the reprocessing of nuclear fuel after use. The Central Electricity Generating Board and the South of Scotland Electricity Board are responsible for generating a reliable and economic supply of electricity in their areas of operation. This responsibility includes, subject to the approval of the relevant Secretary of State, ordering and construction of such power stations, including nuclear power stations, as they judge will enable them to carry out this function.

The UKAEA and BNFL, which together employ 25,000 people, hold almost all the UK's stocks of nuclear materials for civil purposes in accessible forms.

Responsibility for the design and construction of commercial nuclear reactors rests with the Nuclear Power Company (NPC). The NPC is a wholly owned subsidiary of the National Nuclear Corporation (NNC), which is comprised of the Government, the GEC and British Nuclear Associates Ltd. (the latter comprise a number of engineering organizations).

The transport of special nuclear materials within the UK is operated by the UKAEA and BNFL to agreed common standards. Commercial firms are not engaged in the movement of such materials.

It will be seen, therefore, that there is virtually no "private sector" in the UK nuclear industry. This is a different situation to many other countries and may be the reason for any variation in the national approach. For example, there is no need for formal detailed regulatory procedures to be issued by central government.

BACKGROUND TO CONCEPTS

It has to be recognized that sabotage or other illicit activities could be employed against nuclear plants and materials with potentially disastrous consequences, for example:

1. The risk of sabotage of nuclear installations, sites, and reprocessing plants.
2. The risk of theft of fissile and toxic materials, particularly plutonium. There are two main possibilities: the first being the construction or supposed construction of a crude nuclear bomb, and the second the threat of dispersion of toxic nuclear material by conventional explosives or other means.

It is against this background that the UK's protective security arrangements in the nuclear industry are made.

THE THREAT OF SABOTAGE

Because of the elaborate precautions taken to guard against the accidental release of the large accumulations of radioactivity in the form of highly active fission products within reactor cores and fuel reprocessing plants, which are additionally protected by massive containment structures (several metres of reinforced concrete), it would be extremely difficult to bring out a catastrophic failure and consequent release of radioactivity. It is considered, therefore, that an attack on or an occupation of such installations would probably be a political embarrassment rather than a real danger, although the economic damage that would be caused by disruption of a plant is an important aspect which cannot be overlooked.

THEFT OF NUCLEAR MATERIALS

The unauthorized removal of nuclear materials is currently the most important problem for those concerned with physical protection in the UK. It contains two aspects:

1. The theft by outsiders of nuclear materials in transit or in store.
2. The theft of nuclear materials by those with legitimate access to it.

Both these dangers present the possibility of genuine hazard, i.e., the manufacture of an improvised nuclear device (IND) or the dispersal of nuclear materials or of a threat of either where the disruptive effective could be almost as great.

PROTECTION OF NUCLEAR MATERIALS IN USE AND STORAGE

The UK has accepted the IAEA concept of physical protection of nuclear materials in use and storage which requires a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their duties), and facility design (including layout). The physical protection system has been designed specifically for each facility after taking into account the geographical location and the current assessment of the threat.

In achieving the objectives of its physical protection system, the UK has

1. Limited access to nuclear materials and facilities to a minimum number of individuals.
2. Predetermined the trustworthiness of all individuals regularly permitted access to nuclear materials or facilities.

As minimum standards, the UK has also adopted the categorization of nuclear materials recommended by the IAEA and has afforded in general to each category the protective measures the Agency has suggested. In particular it had adopted the philosophy of "defence in depth" by confining all Category I material to "inner areas" within the "protected areas" of its establishments. Close attention has been given to the application of the two-man rule and to the design and positioning of portal monitors. The difficulties in the development of these instruments has been realized, particularly to avoid being lulled into a sense of false security. The possibility cannot be discounted of an individual removing a few grammes per week without detection, thereby acquiring enough within a reasonably short period to pose a dispersion threat. In this respect, it has been realised in the UK that the control of laboratories handling nuclear materials in glove boxes presents a special problem and particular attention is being paid to it. With this point much in mind, the UK has been closely examining the possibility of upgrading its existing personnel security procedures for those persons in a position to divert Categories I and II materials.

PROTECTION OF NUCLEAR MATERIAL IN TRANSIT

In realising that the transport of nuclear material is probably the operation most vulnerable to an attempted act of unauthorized removal, the UK has also accepted the IAEA's concept of the problem that the protection provided should be "in depth" and that particular attention should also be given to the recovery system.

The UK is conscious of the need for close collaboration in the procedures necessary to safeguard international movements for nuclear materials and are taking part in current discussions on this problem.

As an additional safeguard, the concept of reducing the number of people who need to know the details of shipments has been followed. As far as possible, this has been achieved by the use of dedicated vehicles for movements and the avoidance of commercial transport companies.

CONCLUSION

Terrorism is in large measure an international phenomenon. This fact clearly makes it important for the governments concerned to cooperate fully in adequate security arrangements in all countries in which stocks of nuclear materials exist or may exist in the future and to accept standards of physical protection at least to the minimum recommended by the IAEA.

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

GUEST LECTURES

Session Title: Physical Protection of Nuclear
Facilities and Materials in
France

Date: Monday, 6 November

Time: 1030 to 1115

Presented By: Mr. A. Haroyan, Ministry of the
Interior, France

Session Objectives:

After the session, the participants will be able to

1. List the objectives of the French system of physical protection and
2. Describe the structure of the French system of physical protection.

Summary:

The objectives and structure of the French system of physical protection are discussed.

PHYSICAL PROTECTION OF NUCLEAR FACILITIES AND MATERIALS IN FRANCE

INTRODUCTION

The transition to the stage of industrial development of nuclear energy has required the implementation of physical protection at a national level, especially due to the large amounts of nuclear materials handled within the fuel cycle: re-actors, enrichment, and reprocessing plants.

The policy to establish has to ensure a maximum effectiveness.

FRENCH APPROACHES TO PHYSICAL PROTECTION

Generalities/Objectives

Nuclear facilities and laboratories as well as the associated transportation of materials involving a high degree of sensitivity must be continually protected against all adversary actions.

The concept of degree of sensitivity of the facilities, used herein, integrates diverse notions such as

1. The vulnerability to sabotage, theft of special nuclear materials, and other possible threats,
2. The economic importance of production,
3. The hazards to the health of populations, and
4. The echo in the public opinion of any adversary action.

This protection must be coherent with the regulations in force, particularly for the facilities considered to be sensitive, for the control of nuclear materials and the inspection of means taken to ensure this control, and for the transportation of nuclear materials.

By examining the set of the recorded adversary actions, two categories depending on different counteraction measures appear:

1. Direct External Actions--Included in this category are the adversary actions from the simple incident improvised by a few amateurs inexperienced to the attack by a perfectly organized and equipped commando, whose objective is the destruction of vital components of the facility or the theft of nuclear materials. In this last case, the possible existence of insider help is considered.

Taking the total strength of the guard forces into consideration, the deterrence against all of these contingencies requires the support of an external strengthening force for which is reserved the term "response and recovery force."

2. Clandestine Adversary Actions--action whose neutralization does not necessitate external support and whose implementation requires only a very limited number of individuals having legitimate access to the sensitive facilities.

The two types of malevolent actions which are described above are separately discussed in the sections which follow. A certain deterrence can be obtained by the deployment of important measures; it must not, however, be taken into consideration within the design of a concrete physical protection system.

Physical Protection of Facilities Against Direct Actions (Commando-Type)

1. Principle

Regulations ruling the physical protection of facilities are established as "protection-in-depth."

More precisely, the goal is to protect adequately the facilities and nuclear materials against overt commando-type actions (1) by early detection, (2) by interposition of delay obstacles, including the guard forces, and (3) by the action of an external response force with an intervention time and specific measures commensurate to the aggression level.

Physical protection assumes its effectiveness by good integration of three elementary functions:

- Detection
- Delay, and
- Adequate response.

One can therefore state the fundamental principle: "The delay imparted to the intervention of the response force at the place of the adversary action must be less than the time necessary for the adversaries to reach their objectives, whatever may be the detection point of the adversary action inside the facility or its periphery and whatever may be the measures implemented by the adversaries."

The quality and diversification of the measures taken in application of this principle condition the effectiveness of physical protection. These measures depend on the nature and sensitivity of the materials and facilities to be protected.

2. Elementary Functions

Detection--This function must aim at adversary action identification. One must seek to determine the place, the time, and the nature (number and means of possible adversaries) of the action that triggered the alarm.

As an essential phase of physical protection, detection must be assured by devices implementing various and complementary principles. Besides, detection involves pure reconnaissance mission carried out by the guard forces endowed with proper equipment.

Some detectors are fit to be seen in a deterrent objective, while others are carefully hidden and kept secret. They are supplied with proper and diversified electrical means; their functioning is automatically controlled and highly reliable so as to reduce the false alarm cases.

Delay--This function involves personnel and equipment. In addition to the guarding elements whose delay mission can attain the level of armed action, the personnel participate in the protection of the facilities by application of a preestablished plan for the shutting down of certain exits at the triggering of the alarm.

The delay barriers must be selective; some act in priority on the adversary equipment, i.e., walls, moats, etc. They are in general located next to the periphery of the facility. Others, on the contrary, act on the adversaries themselves (electrified high-voltage wires, barbed wires, armoured doors, etc.).

The barriers are concentrically arranged so as to accumulate their effects during the progression of the adversaries. In particular, in the center of the target areas, high effectiveness delay measures which can be expensive are to be foreseen. They limit areas of increasing sensitivity from the outside to the inside of the site (protection-in-depth). They can as well be equipped with detection devices since their surface of separation can serve as clearance zones favorable to observation (detection). The effectiveness of the delay system depends in part on the adversary ignorance of the implantation of zones and barriers; the design must be classified and the very sensitive facilities themselves must be secure from indiscretion. Personnel attention must be drawn to the necessity of high discretion with regard to information in that field.

Response and Recovery Force--Response and recovery force is characterized by

- Its numerical importance, which must allow a response adapted to the degree of adversary action,
- Its equipment, and
- Its implantation site in relation to the facility to be protected.

It can be assisted with specialized technical elements (detection of nuclear materials).

3. Combined Functions: Coupling of Elementary Functions

Physical protection must be considered as the synthesis of elementary functions that one must combine so as to reach the aimed objective with minimum means and maximum effectiveness. Two successive stages corresponding to different interactions between functions are to be noted:

- One occurs before the external response force intervention which determines the adversary action nature and intensity, and
- The other consists in the organizing of the overall response to the adversary action.

Adversary Action Evaluation--It is the result of the comparison of

- On one hand, the internal delay and protection capabilities being effective at the detection time, and
- On the other hand, the results of the detection concerning the number and means of the adversaries as well as their location in the facility.

By taking into account the two preceding analyses connected to the internal situation and the information on the external situation previously communicated by the civilian authorities, owing to permanent liaisons and urging on an increased vigilance, one deducts the degree of magnitude of the threat conditioning the further development of the physical protection actions.

Response to the Adversary Action--Two degrees which can be successive are involved:

- a. In benign estimated adversary action,
 - Strengthens the delay barriers (door closing, harrow lowering, etc.),
 - Involves internal personnel means, and
 - Puts in state of alert the external response forces.
- b. In serious estimated adversary action, one implements, in addition to the actions inherent to the benign adversary action, a pre-established plan anticipating:
 - The intervention of external response forces, in particular their cooperation with the facility as well as the organization of the direction of this set of forces,
 - The conversion of detection means to observation means informing in the best manner the authority responsible for the response to the adversary, and
 - The establishing of permanent liaisons with the civilian authorities responsible for the protection of the area on which the facility is implanted.

Protection of Special Nuclear Materials and Facilities Against Internal Clandestine Actions

1. Principle

One bases the physical protection of nuclear facilities and materials against sabotage and clandestine diversion on

- Personnel selection to authorize penetration into the sensitive areas,
- Limitation and strict control of movements of individuals and materials inside the facilities,

- Early detection of beginning of sabotage or special nuclear materials diversion, and
- Limitation of sabotage consequences and/or rapid recovery of diverted materials

2. Elementary Functions

- a. Personnel selection
- b. Limitation and control of movements by
 - An increased automation of the facility,
 - Reducing the number of entries inside the target areas keeping only those allowing a permanent control with minimum means,
 - Implantation of sensitive buildings, aside from high activity areas, and
 - Installation of posts equipped in consequence and in charge of the permanent control of movements of personnel, equipment tolerated inside the sensitive areas, and nuclear materials in transit through these areas.

- c. Detection

It is conceived in two independent manners:

- Detection by specialized equipment utilizing nuclear materials signatures to detect theft and utilizing classical physical means to detect material for sabotage (X-rays, etc.), and
- By nuclear materials accounting for detecting diversions. This function forms, owing to its importance and specificity, the subject of a separate paragraph ("Special Nuclear Materials Accounting," p. 10).

- d. Limitation of Sabotage Effects; Recovery of Special Nuclear Materials

This function consists essentially in a liaison with the facility security services (fire, health, etc.) and with the external police and recovery services (cf. "Physical Protection of Facilities Against Direct Action," p. 3).

3. Integration of the Elementary Functions in a Physical Protection System Against Clandestine Actions

To ensure effectiveness and coherence of these various functions, the detection function must be coupled to:

- The function of recovery and limitation of sabotage effects, and
- The function of limitation and control of movements for action on the guard-posts (possible shutting of accesses).

The function of recovery and limitation of the damages must be connected to the function of limitation of movements.

Special Nuclear Materials Accounting

1. Accounting at the Owner Level

Due to the possibility for detecting a diversion of nuclear materials (nature and quantities of the stolen products), a stringent accounting of these materials is one of the important elements of physical protection.

Nevertheless, it is only an element whose importance is limited by

- The precision on materials evaluation sometimes less than the protection threshold, and
- A detection time maladjusted to the recovery function.

2. Control and inspection are indispensable to maintain the continuous vigilance necessary at the different levels of responsibility but their inevitably hazardous and limited frequency cannot be considered as affecting the above-mentioned dispositions.

CONCLUSION

The policy described is applied in France in the field of protection of nuclear facilities as well as in that of transportation.

For the protection of facilities, a set of texts based on the preceding policy regulates the exploitation of plants and the handling of special nuclear materials which are carried out, in particular, by a continuous accounting of these materials.

For transportation, the implementation of the policy is carried out more particularly through an uninterrupted radio-correspondence and the implementation of liaison with the police forces situated along the route, forces in which, in the general case, equipment helpful to this mission has been previously ensured. Besides, certain special nuclear materials transportations are endowed with armed escorts.

Physical Protection of Nuclear Facilities and Materials
INTERNATIONAL TRAINING COURSE

GUEST LECTURES

Session Title: The Canadian Approach to Physical Protection of Nuclear Facilities and Materials

Date: Monday, 6 November

Time: 1115 to 1200

Presented By: D. B. Sinden, Chief, Security Section, Atomic Energy Control Board of Canada

Session Objectives:

After the session, the participants will be able to

1. List the objectives of Canada's system of physical protection and
2. Describe the structure of Canada's system of physical protection.

Summary:

The objectives and structure of Canada's system of physical protection are discussed.

THE APPROACH TO PHYSICAL PROTECTION IN CANADA

Before considering the Canadian approach to the physical protection of nuclear materials and facilities it would be useful first to comment briefly on two aspects of the Canadian nuclear program which will put the following into the proper perspective. Firstly, the Canadian nuclear power generation program does not rely on enriched uranium as a driver fuel--natural or normal uranium is used. Secondly, Canada does not and is not committed to reprocess spent fuel for its plutonium content. The economics of the CANDU cycle are such that Canada has not yet needed to make commitments to advanced reactor systems. Securable materials, (for present purposes, materials categorized in the IAEA circular INFCIRC/225 Rev. 1 will be considered securable materials) are thus not used, processed or required in Canada in great abundance. Limited quantities of highly enriched uranium are used, however, in Canada's nuclear research programs. As well, small quantities are used for reactivity augmentation in power reactors in a limited number of instances. Because the quantities of this material and the number of facilities involved are limited, all aspects of control of these materials, including their protection, are considerably simplified.

The physical protection of securable materials is but one element of the Nuclear Materials Control System. In Canada this control system is comprised of two major branches: the material accounting system and the security system. While these systems are complimentary, they seek to achieve distinctly different objectives. The security system strives to ensure that materials are not diverted, by any means, to unauthorized use. The accounting system serves as confirmation that the security system has or has not been successful. Audits of the accounting system serve as a check on those administering both the security and accounting systems.

Within the security system there are several activities performed. The first is physical protection, the activity with which this workshop is primarily concerned. The hardware, systems, and administrative measures designed to detect, delay, and apprehend persons attempting to gain unauthorized access to nuclear materials are all a part of the physical protection activity. Other security activities such as intelligence gathering and assessment and information control and protection, complement the physical measures. Arriving at a proper mix of these activities to provide effective protection for nuclear materials is a problem to be discussed presently.

* From a talk by D. B. Sinden, Chief of the Security Affairs Section, Atomic Energy Control Board of Canada, at the 1978 IAEA Physical Protection Course.

The Atomic Energy Control Board is an agency established by Canadian law to regulate and control the development and use of nuclear energy and associated materials in Canada. The Board has a clear mandate to exercise this control to ensure that the security measures adopted are adequate to protect the public security. The most effective tool at the disposal of the Board for this purpose is its power to make regulations. The Board staff has thus prepared comprehensive regulations to ensure appropriate physical protection measures are taken by all Canadian licensees. While these regulations are proceeding along the rather lengthy path to becoming law, the Board has been requiring over the past few years that all licensees upgrade security measures as a condition of their licenses to possess nuclear material. For a number of reasons it has been concluded that the promulgation of comprehensive regulations is a preferred approach, and thus the Board is following this course. These regulations will provide for protection which is at a standard higher than that recommended in INPCIRC/225.

In preparing the regulations there were a number of basic philosophical issues to be resolved. First, recognizing that physical protection is but one of the several activities which make up the security system, it was necessary to seek the proper balance between physical protection measures and those activities mentioned earlier, such as the control and protection of sensitive information and the intelligence and assessment activity. Many factors can influence this balance. The prevailing levels of violence and social unrest within the society are probably the most important factors in striking this balance. Other factors such as public and workers tolerance of the curtailment of previously held liberties, the economic and political stability of the area, and more local phenomena such as labour disputes or significant local political issues are all additional considerations. Factors such as geography and population density also have significant influence on the balancing of these activities.

Generally speaking, Canada has a very low level of violence within the society and an equally low tolerance to shows of strength by military or police authorities. For these reasons, as well as the results of intelligence and analysis activities, it has been concluded that the social cost effectiveness of the security system in Canada is maximized by providing low profile physical measures and placing emphasis on the protection of sensitive information. The limited quantities of securable material in Canada make this approach that much easier.

Saying these physical measures are low profile is not to say that these measures are not effective or do not exist. The concentric barrier concept as described in INPCIRC/225 is employed throughout the country. Emphasis is placed on controlling the movement of personnel across each barrier and on devices for detecting unauthorized entry or attempts at unauthorized entry. Facilities are required to maintain guard forces which are in continuous communication with, and indeed may be part of, the response forces. System effectiveness will be assessed by comparing the response time of these forces with the delay time offered by the several barriers which must be breached after the intruder is detected.

The matter of guard and response forces cannot be raised without making at least a short allusion to the question of arms. It is the Board's view that armed response, if necessary, must be provided by the properly constituted law enforcement agencies within the country. In Canada, this means the police and the military. Armed private guard forces are generally considered to be provocative and generally unacceptable in Canada. The Board believes that the armed guard who, without intensive and expensive training, is very likely to be poorly trained, poorly turned out, and of dubious judgment cannot have any but detrimental societal effects in the long run. Therefore, considerable time and effort have been spent to coordinate the various levels of police and military response possibilities. In cases where analysis of the response capability indicates it necessary, arms can be made available to the guard force. This is the case at a limited number of establishments. Weapons are not carried by guards at any Canadian facility at this time.

Another issue which has been examined closely is the degree to which physical protection need be provided for nuclear facilities other than those which contain securable nuclear materials. While it has been agreed that a theft of weapons grade materials could have immediate consequences for national or world security, it is less clear that the impact of malicious damage to a nuclear facility would be in the national or world context. While it is possible to imagine scenarios where sabotage activities could result in the dispersal of radioactive contaminants, such an incident is far different in significance from the theft of weapons grade materials. In sabotage incidents as opposed to theft, additional factors must be considered before any conclusions can be drawn. The design and engineering of the facility, together with its safety and containment systems, will have a major influence on the effect of a sabotage attempt. Also to be considered are the motives which might drive the saboteur. Based on these and the many social factors discussed previously, a judgment has to be made, as always, as to "how much is enough."

In examining this question it has been concluded that emphasis should be placed on the installation of devices and other hardware which would enable extremely tight access control to nuclear reactors on short notice, should this become necessary. For the time being, the levels of protection which will be required at Canadian reactors will be equivalent to those afforded Category II nuclear material. Levels would be higher, of course, if warranted by the materials involved. Furthermore, efforts are being made to keep these measures as low key as possible. Again, considerable effort is being devoted to response and other contingency plans, and particular attention is given to the intelligence and analysis activity. However, in the Canadian context, there is no perceived immediate need for Canada's nuclear generating stations to establish armed first line defences.

Insofar as material protection during transport is concerned, requirements will continue to be imposed through licensing rather than directly by regulation. There are several reasons for this approach. First, there are relatively few shipments of securable material within Canada and this enables planning to be carried

out on a case-by-case basis. Security planning in this way ensures that the plans are tailored to the specific circumstances surrounding that shipment. The second reason is that far greater flexibility of action is possible under an individual security plan which is not constrained by regulations. Through this mechanism, the licensee, the protective forces, and the Board staff are all involved together in the preparation of the security plan. As a general rule, Category I and II shipments are escorted, and in most cases the escort is comprised of professional police officers. The complete range of resources at the disposal of the police authorities is thus available.

As mentioned earlier, considerable attention is paid to the protection of information concerning storage facilities, protective systems, and shipping information. This is one area where the security system and the accounting system are not complimentary. The access to the accounting system by the IAEA under the Canadian/Agency bilateral agreement includes advance notification of some securable shipments. A completely satisfactory means of communicating this information to the agency and of being assured that the information is protected has still not been developed.

As a final observation, it is worth mentioning that experience has shown that regardless of how thorough or comprehensive regulations and guidelines might be, real security can only be achieved through the cooperation and dedication of those on the ground at the facility. Security is a complex interrelationship of procedures, hardware, and intuition which must respond quickly to unique and fast changing circumstances. It is impossible to legislate responses to all the conceivable situations. Therefore, it has been found that dealing with the people concerned on a personal basis and encouraging an understanding of the total security system is far more productive than measuring fences or generating mountains of paper.

GLOSSARY

Access Control--The equipment and procedures used to permit only authorized persons to enter and exit controlled areas.

Adversary--An individual or group attempting theft of special nuclear materials (SNM) or radiological sabotage.

Adversary Action--A specific task performed by an adversary.

Adversary-Action Sequence--A set of specific tasks performed by an adversary to achieve his objectives.

Adversary Neutralization--The termination of an adversary-action sequence by the security force. The adversary is either captured, killed, or forced to flee.

Adversary Sequence Interruption--The interrupting or halting of the progress of the adversary by the security force (guards) before his objective has been achieved.

Assessment--The determination of the cause of an alarm and the extent of the threat.

Collusion--An agreement between two or more persons to commit an illegal or malevolent act.

Common Carrier--A commercial firm engaged in the transportation of goods or people by air, land, or sea.

Communications--The system used by the security force for sending and receiving messages, e.g., radio, telephone.

Concept Formulation--The step in the design of a physical protection system which is the iterative process of selecting and locating system elements in the physical protection system zone.

Contraband--Unauthorized materials such as firearms, explosives, and special nuclear materials.

Courier--An armed person whose primary function is protection of SNM in transit.

Deceit--Adversary actions that attempt to defeat the physical protection system with the expectation that unauthorized conditions, such as false credentials, will not be detected.

Delay--The time for an adversary to defeat single or multiple physical barriers.

Detection--A determination that an unauthorized action is occurring or has occurred. Detection includes sensing this action, communicating the alarm to a control center, and assessing the alarm.

Effectiveness Evaluation--An analysis of the capability of a physical protection system to prevent sabotage or to prevent theft of SNM.

Entry Control--The equipment and procedures used to permit only authorized personnel and material to enter and exit a controlled area.

False Alarm--An alarm normally associated with malfunction of the sensing device. For some applications, nuisance alarms are included.

Force--Adversary actions that attempt to defeat the physical protection system by overt aggressive activities during which the adversary is not concerned with being detected.

Generic--Relating to or characteristic of a whole group or class.

Hoax--A trick or fraud. For example, a person may telephone a facility and say that he has placed a bomb in a vital area when in reality no bomb was placed there.

Insider--Any person authorized to enter a protected area or vital area.

Integrate--To make whole or complete by the assembly of parts.

LOCA--Loss of coolant accident which results whenever there is a break in the primary coolant boundary so that the normal coolant makeup system cannot maintain sufficient coolant in the reactor.

Logic Tree--A logic diagram which graphically represents how a combination of events can result in a specific event.

Malevolent Action--A deliberate action with intent to harm or destroy installations or people. Stealth, deceit, and force may be employed, either singly or in combination.

Material Access Area--An area inside a protected area in which SNM is processed and/or stored.

Material Accounting and Control System--The equipment and procedures used to report unauthorized movements of SNM and to monitor changes in the amount, location, and custody of it in a facility.

Modus-Operandi--A manner or way of working.

Nuisance Alarm--An alarm which is not caused by an unauthorized action and occurs when the sensing device operation is normal.

Outsider--A person who is not authorized to enter a protected area or vital area.

Path--The physical route taken by an adversary.

Physical Barrier--A fence, wall, door, distance, or similar impediment which requires some time to penetrate or traverse.

Physical Protection System--A system utilizing equipment, personnel, and procedures to prevent theft of SNM or radiological sabotage, both of which could result in a hazard to the public.

Physical Protection System Zone--A space which surrounds (but may not be occupied by) one or more targets and in which the functions of the physical protection system are to be accomplished.

Positive Feature--A component of a physical protection system that has a predictable minimum level of performance.

Positive Measure--A procedure which may include utilization of a positive feature.

Positive Personnel Identity Verification--Examination of a unique physical characteristic of a person and comparison of it to the stored personnel data. If the data match, the person's identity is verified.

Protected Area--A specifically defined controlled access area which is enclosed by one or more physical barriers.

Qualitative Analysis--An analysis in which logical implications, cause and effect sequences, or rank-order relations are used to evaluate the performance of the physical protection system.

Quantitative Analysis--Analysis in which the characteristics of the adversary, the physical protection system, and the interactions between them are represented numerically.

Radiological Sabotage--Any deliberate act which could directly or indirectly endanger the public health or safety by radiation exposure.

Reactor Transient--Any significant deviation from the normal operating value of any of the vital reactor operating parameters. Transient incidents include all those situations except breach of the primary coolant boundary (LOCA incidents) which would lead to fuel heat imbalances.

Real-Time--The term used to denote an observation made at the time the event is taking place.

Response--The action taken by the security force (guards) to prevent an adversary from achieving his objective.

Response Time--The time between receipt of the alarm and the interruption of an adversary sequence.

Scenario--A specific sequence of events leading to an adversary's accomplishing his objective.

Sensitivity Analysis--An examination of system response when one or more of its elements are changed (e.g., change in detection probability).

Sensor--A device which responds to stimuli associated with an unauthorized action such as an intrusion into a protected area or an attempt to smuggle contraband through an entry portal. The device may also respond to stimuli not associated with an unauthorized action.

SNM-Special Nuclear Materials--See Table: Categorization of Nuclear Material, The Physical Protection of Nuclear Material, INFCIRC/225/Rev. 1, page 6.

Stealth--Adversary actions that attempt to defeat the physical protection system by avoiding or inactivating its components in an attempt to prevent detection.

Subsystem--A component or group of components which constitute one unit of the physical protection system, e.g., detection.

Surreptitious--A secret, stealthy way to act.

System--A set or arrangement of components so related or connected to form a unity or whole (e.g., solar system).

Theft--The unauthorized removal of special nuclear materials from a material access area.

Threat--An individual or a group with the potential motivation and capability for theft of SNM or for sabotage that would result in a radiological hazard to the public.

Threat Strategy--The method used by the adversary(s) to accomplish his goal of radiological sabotage or of theft of SNM.

Threat Tactics--The manner or method used by an adversary to carry out the events in a scenario.

Trade-Off--A balancing of factors, all of which are not attainable at the same time.

Two-Man Rule--A procedure that requires at least two knowledgeable persons be present to verify that any actions taken are authorized.

Vault--A structure or room whose door, walls, floor, and roof are designed to make penetration difficult.

Vital Area--An area of a plant or facility containing equipment and/or material, the failure, destruction, or release of which could directly or indirectly endanger the public health or safety by exposure to radiation.

Vulnerability Analysis--A method of identifying the vulnerabilities of a facility.

PERFORMANCE EVALUATION CONCEPT OF SECURITY SYSTEM DESIGN

**Presented by
Kenneth E. Wilson, C.P.P.
Manager, Security Services
Stone & Webster Engineering Corporation**

PRESENTATION OUTLINE

INTRODUCTION

V/G #1: The advance evaluation approach to security system design:

- I - Why we take this approach
- II - What we do
- III - How we do it

PART I

V/G #2: 10CFR73.55 lead-in
V/G #3: Subsection (a)
V/G #4: Subsection (g)
V/G #5: Guard cost projection matrix
V/G #6: Factors affecting guard staffing

PART II

V/G #7: Key documents:

Threat-response study
Functional concepts agreement

V/G #8: Organization chart
V/G #9 & 9A: Program flow chart - Phases A & B
V/G #10 & 10A: Program flow chart - Phases C & D

PART III

V/G #11: Threat-response study:

Design tool - best combination of physical, procedural and human features for defensive security at least cost.

Program evaluation needed to meet performance requirements.

V/G #12: Methodology:

Probabilistic
Analytical
Reiterative

V/G #13: Major assumptions:

Random force distribution
Initial setback
Building penetration unacceptable
Interdiction definition
Insider threat
Communications systems

V/G #14: Threat-response analysis form

V/G #15: Plot plan with scenario routes

V/G #16: Generic recommendations:

Defensive envelope
Portal control
Open-area confrontation
Manpower alternatives

V/G #17: Plot plan with resolutions

V/G #18: Functional concepts agreement:

Operational criteria - what the system is to do
Mutual understanding and sign-off

V/G #19: Functional concepts contents:

I - Introduction
II - General Requirements
III - Physical Aspects
IV - System Hardware Aspects
V - System Software Aspects
VI - Maintenance Aspects

V/G #20: Deterrent portal

V/G #21: Multiple-camera CCTV tower

V/G #22: Prototypical system schematic

CONCLUSION

V/G #23: In the future:

Personnel "Maintenance"
Automated defenses

THREAT-RESPONSE STUDY

SAMPLE

CONTENTS

I. INTRODUCTION

II. ASSUMPTIONS

III. SPECIFIC CONSIDERATIONS

IV. SCENARIO SUMMARIES

V. RECOMMENDATIONS

VI. ATTACHMENTS

I. INTRODUCTION

The analyses contained herein have been conducted for two purposes:

- To be used as a design tool in determining optimum physical, procedural and human features of the defensive security program for the plant and the combination of such features that can be expected to minimize total costs - considering both initial outlay and plant-life continuing expenses.
- To provide a sound basis for demonstrating to the NRC that the program described in the Physical Security Plan will meet the "general performance criteria" of 10CFR73.55(a); i.e., that a high degree of assurance exists that the design basis threat described therein will be successfully interdicted.

Each analysis has been carried out by the probabilistic method developed by Sandia Laboratories and generally identified as the "EASI" technique and by a SWEC - proprietary addition thereto. We believe this technique to be the most useful since it can be adapted to a theoretical development of mean response time and standard deviation thereof and we think this is more realistic than either predetermined locations of individual guards - as is envisioned in the alternative approaches - or by measurements made under "drill" conditions.

Basically, the methodology used has been to select a "worst-case" scenario - normally the shortest path from a point on the perimeter boundary to a door into a building housing vital equipment - and to repeatedly perform the analytical routine while changing both defensive engineering and/or response force input parameters. When the most cost effective combination appears to have been determined, an analysis involving the shortest path from each of the other doors, into buildings containing vital equipment, to the perimeter boundary is run to ensure that a new "worst-case" scenario has not arisen as a result of the first determinations.

II. ASSUMPTIONS

In order that successive studies may generate reasonably valid comparisons, certain fundamentals must be stabilized. Exact values, under the circumstances, are of less consequence than consistency and a demonstrably conservative bias with respect to defensive effectiveness. In this vein, the following assumptions form the foundation of these analyses.

- (a) Response personnel not assigned to fixed posts will be randomly dispersed over the site on patrol or escort duty at the time of the incident.
- (b) If a significant part of response activity emanates in or from a perimeter building, neutralizing action must be anticipated.
- (c) If (b) is not operative, at least one member of the response force will be neutralized as the initial step in the action.
- (d) Travel rates of both adversary and response forces will be halved when under fire.
- (e) Successful penetration of a building containing vital equipment will reduce the probability that re-assessment and re-grouping can be done quickly enough to permit interdiction to an unacceptable level.
- (f) Interdiction will be considered as accomplished when either quantitative or qualitative superiority can be reasonably adjudged as established.
- (g) The "Insider" threat will have been minimized by a combination of physical and work-practice isolation, along with an access control and monitoring system sophisticated enough to detect abnormal location or movement of personnel - particularly at any specified point in time.
- (h) Due to the ready availability of off the shelf equipment to locate and jam the radio channels, it is presumed that the adversary will do so. It is further projected that the Gai Tronics will be captured by the insider and therefore we have arbitrarily added a secure hardwire annunciation system into the probability of communications calculations.
- (i) The effects of poor visibility and inclement weather were considered to be offsetting by aiding and/or inhibiting both sides equally. For instance, poor visibility provides cover for the intruders, but also provides cover for the defenders while they are moving to contact.

These general conditions will be supplemented by site-specific assumptions based on both physical and procedural characteristics peculiar to the particular plant and/or the client's operations practices.

III SITE SPECIFIC CONSIDERATIONS

The following parameters were factored into the scenarios which follow this section:

1. The guard force is assumed to be wearing protective clothing and armed with 12 ga. shotguns. Should they be armed solely with side arms, the results will have to be revised downwards to allow time for drawing their equipment.
2. Three channels of communication which are:
 - (a) Two channel radio transceivers.
 - (b) Gai Tronics Intercom.
 - (c) A dedicated hardwire annunciation system.
3. It is assumed that the adversaries will commit a three man force and therefore the defenders will have met the response requirements when 6 members of the security force are present to interdict in an external confrontation.
4. Travel rates for the response force are based on two members being on mobile patrol responding at 35 mph. The balance of the response force is presumed traveling on foot, with the travel rates amortized in consideration of the minimum physical requirements and the rates of a well conditioned young man with normal equipment on dry pavement.

IV. SCENARIO SUMMARIES

Scenario #1. Path of intrusion is from the North fence to door AB261-1, leading into the service water pump area via the screenwell. The target would be the pumps themselves. Response time is calculated as 2.86 minutes with a standard of deviation (sigma) of .227 minutes. The adversaries will require 1.629 minutes to make their penetration. The only barrier for which time delay credits can be taken is door #AB261-1. The penetration resistance of this door is charitably given as 1.5 minutes. Should the lock specifications remain unchanged, the delay factor of this door should be reduced to 1.0 minutes with a standard of deviation in the neighborhood of .5.

The probability of interdiction for this scenario is .00092 or .092%.

Scenario #2. A penetration of door SG261-6 by the shortest path from the North fence. Targets for this attack would be the equipment and materials in the Aux. building and the Reactor building.

The time required for the adversaries to affect a successful penetration is 1.79 minutes with a sigma of .2185. Response time to this portal for the guards is calculated as 2.637 minutes with a sigma of .179.

The probability of successful interdiction is .0044 or 0.44%.

Scenario #3. Calls for penetration of door C261-9 with the intruders approaching by the shortest path from the South fence. The time required for the adversaries to affect the penetration is 1.82 minutes. The response force will require 2.637 minutes to interdict. The target for this scenario would be the control room, and/or the Aux. building.

The probability of interdiction for this scenario is .0053 or 0.53%.

Scenario #4. Calls for penetration of door SG261-6 by the shortest path from the East fence. Time required by the adversaries to accomplish the penetration would be 1.96 minutes. Response time is calculated as 2.637 minutes with a sigma of 0.179 minutes. Target for this scenario would be the equipment and materials in the Aux. building.

The probability of interdiction in this approach is 0.013 or 1.3%.

From the standpoint of probabilistic analysis, the four chosen scenarios are ranked in order of vulnerability. From an operational or tactical standpoint, the more fruitful scenario is number three, since it offers more targets of opportunity to the adversary and a higher probability of creating a hostage situation.

V. RECOMMENDATIONS

We have conducted a variety of analyses of defensive methodologies as applied to as-built, proposed and prototype designs for nuclear power plants, using both definitive and the simpler probabilistic techniques. One of the results of these studies has been our conclusion that if an adversary team successfully penetrates the boundary of a building which contains vital equipment, the number of targets available and the diversity of paths to them that exist in most cases make threat re-assessment and response re-direction in a time frame consistent with successful interdiction impossible without an extensive, sophisticated and expensive sensor and/or deterrent installation. Because of this, we have adopted what we term the "defensive envelope" concept.

We define the "defensive envelope" as a physical boundary encompassing all buildings containing vital equipment, where such is possible. There may be cases in which more than one defensive envelope may be required - particularly in existing or pre-designed plants. In any case, the concept includes the incorporation of delay/deterrent techniques such that a primary response team of two men may, with a high degree of assurance, reach the inside of any portal in the defensive envelope prior to penetration by an adversary force. Further, that the primary response team would be appropriately equipped to successfully defend that "throttle point" on arrival.

We are convinced that open-area confrontations will work to the benefit of the adversary, who can be expected to have the advantage of surprise, coordination and motivation. Therefore, when the defensive envelope concept cannot be implemented for any reason, the use of defensive position(s) in combination with a motorized primary response team of two men (on continuous, randomized patrol/surveillance assignment), delay/deterrent techniques and foot response personnel is recommended.

Only in exceptional circumstances should reliance be placed solely on manpower as the answer to the adversary action. Not only will this prove to be the most expensive approach over the life of the plant - by several orders of magnitude - but it creates problems of personnel management, public relations ("police-state" diatribes) and humanistic concern for the individuals in the event of a confrontation. We include this as an alternative only because we recognize that certain cash-flow situations might preclude any other course.

The following three resolutions have been prepared to illustrate an application of the parameters just discussed and their effect on the threat analysis. A brief discussion follows on the approaches incorporated in each situation. For all three programs, the worst case scenario, intrusion over the North fence, has been used for comparison.

Resolution #1. Using a defensive envelope portal delay of three minutes, a mobile two man patrol, two defensive positions in the approximate locations indicated in Attachment 1 and a two man centrally dispatched response team from the centroid of the defensive envelope, a probability of interdiction of .910 or 91% is achieved.

V. RECOMMENDATIONS (CONT.)

Resolution #2. Harden all defensive envelope portals to provide a minimum delay of 3.5 minutes sigma 0.2. Guards are on foot, 8 man force with random distribution. This yields a probability of interdiction of .929 or 92.9%.

Resolution #3. Add sufficient manpower to meet the adversary with no further hardening or any other measure save continuous fully armed random patrol. With response force of 14 guards, a probability of interdiction of .930 or 93% is achieved.

FUNCTIONAL CONCEPTS

SAMPLE

FUNCTIONAL CONCEPTS

CONTENTS

- I. Introduction - Automation**
- II. General Requirements**
- III. Physical Aspects**
 - A. Primary Access Point**
 - B. Defensive Envelope**
 - C. Warehouse Perimeterization**
 - D. CAS**
 - E. Lighting**
 - F. Reaction Station**
- IV. System Hardware Aspects**
 - A. Perimeter Intrusion Detection**
 - B. CCTV**
 - C. Access Control Points**
 - 1. Perimeter**
 - 2. Internal**
 - D. Security Information Systems**
 - 1. Collection and Control**
 - a. Primary**
 - b. Secondary**
 - c. Visual Summary**
 - d. Reaction Station**

2. Annunciation and Display

- a. Alarms**
- b. Access**
- c. Visual Summary**
- d. Reaction Station**

E. Communications

- 1. Radio**
- 2. Voice**
- 3. Signal**

F. Guard Location and Movement

G. Deterrent Technology (if applicable)

V. System Software Aspects

A. Annunciation and Display

- 1. Alarms**
- 2. Access/Authorization**
- 3. Visual Summary**

B. Communications

C. Guard Tours

D. Record Keeping

VI. Maintenance Aspects