SAND80-0706
Unlimited Release
UC-15

Workshop Materials From the 2nd International Training Course on Physical Protection of Nuclear Facilities and Materials, Module 13

MASTER

Frank P. Martin, Editor

Prepared by Sandia Laboratories, Albuquerque, New Mexico 87185
and Livermore, California 94550 for the United States Department
of Energy under Contract DE-AC04-76DP00789
Printed April 1980

Sandia National Laboratories

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

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

The following pages are an exact
representation of what is in the original
document folder.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors or subcontractors.

Printed in the United States of America

Available from

National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

NTIS price codes

Printed copy: \$14.00

Microfiche copy: A01

SAND80-0706
Unlimited Release

April 1980

WORKSHOP MATERIALS FROM THE 2nd INTERNATIONAL
TRAINING COURSE ON THE PHYSICAL PROTECTION OF
NUCLEAR FACILITIES AND MATERIALS

Edited by
Frank P. Martin
Safeguards Evaluation Division 1758
Sandia National Laboratories
Albuquerque, NM 87185

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Key

INTRODUCTION

The International Training Course on the Physical Protection of Nuclear Facilities and Materials has been presented by Sandia National Laboratories in Albuquerque, New Mexico in November of 1978 and December of 1979. The course will be offered again in February of 1981. 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). The course is primarily intended for representatives from countries in which the development and use of nuclear power is underway or is planned for the near future and whose responsibilities include the preparation of regulations and the design and evaluation of physical protection systems.

Improvement and refinement of the course and the materials used therein is continuing, and the course is designed to:

1. Make the participants aware of the need for effective physical protections programs,
2. Familiarize them with the procedures and practices in the field of physical protection, and
3. Assist them in developing and implementing their own national system by providing a basic framework of knowledge in organizational aspects, technical instrumentation, and methodologies for design and evaluation.

This is the second of two volumes published by Sandia based on materials utilized in the course. The first volume, SAND79-1090 of May 1979, consisted of the texts of formal lectures and presentations made during the course by the instructional staff.

Approximately half of the course is devoted to practical problem solving exercises with the participants working in small groups (subgroups) designing a physical protection system for a hypothetical nuclear facility. This volume contains those problem solving exercises used in the subgroups.

Each problem exercise contains a section defining the problem, a section explicitly outlining any assumptions made with respect to the problem, one or more sections discussing or providing additional graphics or data necessary to solve the problem, a section entitled "Instructional Guidelines" and a section entitled "Think About Items." Participants were requested to read each exercise in preparation for the subgroup session. The Instructional Guideline section, which in some cases contained explicit answers to some of the questions asked, was distributed at the conclusion of the appropriate subgroup session. The function of the subgroup instructor was to catalyze his subgroup activities and to guide participants where necessary toward a self-generated solution to the problem. In many cases assumptions which were detailed beforehand with respect to the problem were deliberately questioned in the Think About Items section to stimulate discussion and elicit additional ideas from participants on alternative solutions. This technique was very effective.

For those readers basically familiar with the application of fault tree analysis, generic physical protection logic trees, and the Estimate of Adversary Sequence Interruption (EASI) model, the problems can be worked through with the resources provided within this volume with one exception. That exception is session 13.9, The Application of the EASI Model, which requires access to a hand-held TI-59 programmable calculator. Those not familiar with the techniques applied in these problem exercises will find relevant introductory material in SAND79-1090.

Development of the materials for the training course project has been a collective effort supervised by the course director, Christopher E. Olson of Sandia Laboratories. Frank P. Martin functioned as the lead instructor and technical material editor for the 2nd International Training Course on the Physical Protection of Nuclear Materials and Facilities in November-December 1979. Robert T. G. Lassiter served as the course administrator. The principal contributors to this volume of the course material were: Betty Biringer, Steve Chester, William Paulus, Dick Smith, Leroy Stradford, and Bruce Varnado. The first four named members of this group also functioned as sub-group instructors.

The instructional staff would especially like to thank Perry Gore and his associates at Tech Reps in Albuquerque 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, Safeguards Evaluation Division, Sandia National Laboratories, Albuquerque, New Mexico, 87185, USA.

INDEX

13.1 Hypothetical Facility Data Package

13.2 Reactor Vulnerability Applications (see Session 4.4 included in the Supplement)

13.3 Facilization Characterization Applications

13.4 Vital Area Identification Applications

Additional Graphics Include:

Figure 13.4-1 PWR Fault Tree

Figure 13.4-2 Constrained PWR Fault Tree

Figure 13.4-6 PWR Vital Area Fault Tree

13.5 Applications of Generic Logic Trees

Additional Graphics Include:

Drawing #13.18.55 Defeat Perimeter Barrier

Drawing #13.24.13 Defeat or Bypass Sensor Field

Drawing #10.49.56 Defeat Fence

Drawing #10.53.10 Defeat Building Structure

Drawing #10.58.35 Defeat Building Personnel Entrance

Drawing #10.37.30 Defeat Building Utility Openings

13.6 Barrier Technology Handbook Applications

13.7 Entry Control Systems Handbook Applications

13.8 Intrusion Detection Systems Applications

13.9 Application of Estimate of Adversary Sequence Interruption (EASI) Analysis

Additional Information Included:

Improved EASI Program Listing for TI-59--pages
13.9-29,30,31,32

13.10 Physical Protection System Applications I

13.11 Physical Protection System Applications II

13.12 Not Included (Panel Discussion)

13.13 Manpower/Technology Considerations

13.15 Total Physical Protection System Design

13.16 Cost/Impact Analysis

13.17 Not Included (Panel Discussion)

Supplement

Session 4.4--Reactor Vulnerabilities

Drawing #08.49.53--Deceit-Boundary

Drawing #08.49.53--Deceit-Boundary (Annotated)

Drawing #11.36.48--Deceit-Area

Drawing #11.23.18--Deceit-Acquire SNM

Drawing #12.27.50--Force-Boundary/Stealth-Boundary

Drawing #08.17.52--Force-Area/Stealth-Area

Drawing #13.10.10--Force-Building/Stealth-Building

Drawing #15.15.41--Force-Acquire SNM/Stealth-Acquire SNM

Drawing #11.07.11--Force-Release/Stealth-Release

Drawing #08.49.53--Deceit-Boundary (Annotated for 13.10)

Drawing #12.27.50--Force-Boundary/Stealth-Boundary (Annotated
for 13.10)

Drawing #13.10.10--Force-Building/Stealth-Building (Annotated
for 13.11)

NOTE--A valuable additional resource for the use of the Estimate of Adversary Sequence Interruption (EASI) model is SAND78-0506 of July 1978 entitled "EASI Program Improvements for HP-67 and TI-59 Calculators."

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

13.0 SUBGROUP SESSIONS

13.1 Hypothetical Facility
Data Package

MODULE 13
SUBGROUP SESSIONS

HYPOTHETICAL FACILITY DATA PACKAGE

CONTENTS

	<u>Page</u>
I. Type of Facility	13.1-5
II. General Characteristics	13.1-5
III. General Hypothetical Facility Data Summary	13.1-5
IV. Sketches	13.1-9

I. TYPE OF FACILITY

A hypothetical pressurized water reactor has been chosen for discussion in the subgroups portion of this course. This pressurized water reactor and associated facility data have been simplified so that (1) the physical protection requirements and (2) the conceptual physical protection system (PPS) design and evaluations may be accomplished during the course.

II. GENERAL CHARACTERISTICS

1. The reactor is an operating pressurized water reactor and is generating electric power,
2. The pressurized water reactor is remotely located and has one access road,
3. The facility buildings are limited to two levels, and
4. One level of the two-level buildings is underground.

III. GENERAL HYPOTHETICAL FACILITY DATA SUMMARY

Hypothetical Facility System Characteristics

1. The system is a two-loop pressurized water reactor.
2. One steam generator is sufficient for decay heat removal.
3. Transient Mitigation -- In response to transient incidents, the following functions must be provided: (a) Reactor shutdown (trip) and (b) Decay heat removal. Reactor trip is provided by the reactor safety protection system. Decay heat removal can be provided by either the power conversion system steam bypass to the condenser or by the auxiliary decay heat removal system. Auxiliary decay heat removal requires operation of the auxiliary feedwater system and the secondary steam release system.
4. LOCA Mitigation -- In response to a large LOCA, the following systems must function: (1) Emergency Core Injection System, (2) Emergency Core Recirculation System, and (3) Postaccident Heat Removal System. Emergency core recirculation is provided by the Residual Heat Removal System.
5. Auxiliary Feedwater System Description -- Two motor-driven pumps and one steam turbine-driven pump, any of which provide sufficient feedwater for decay heat removal. Coolant sources are the condensate water storage tank or the two essential service water trains.
6. Residual Heat Removal System Description -- Two motor-driven pumps with coolant drawn from the containment sump in loss of coolant incidents. Cooling for the residual heat removal system is supplied by the Essential Service Water System.
7. Electrical System -- Essential power supplied from off-site or by emergency diesel generators. Electrical power trains are separate and redundant for the redundant safety equipment.

Reactor Operating State

1. The reactor is operating and generating electrical power.
2. The two-man rule is in effect when personnel enter a vital area.

Facility Personnel

The facility employs 221 regular employees; approximately 100 employees are at the facility during the normal 5-day work week, and 30 employees are at the facility during all other shifts.

Vital Areas

The reactor and associated equipment within the containment building is one vital area. This vital area must always be protected to prevent a sabotage scenario from successfully occurring. The auxiliary feedwater pumps are vital areas; additional vital areas will be identified during subgroup working sessions.

To simplify labeling of facility areas and to assure that unique labels are assigned to each separate area of interest, a simple coding system is used. Each area is given a three-element label which includes a building or area identification code, a level (or floor number) designator, and a compartment number. Thus RB-2-1 is the label for the reactor building (RB), level 2, compartment 1. The area codes used for buildings in the hypothetical facility are given as follows:

AUX	Auxiliary Building
CB	Control Building
CWST	Condensate Water Storage Tank
DGB	Diesel Generator Building
ESWB	Essential Service Water Building
RB	Reactor Building
TB	Turbine Building
OSPW	Off-Site Power

Reactor, Auxiliary Buildings, and Control and Diesel Generator Building Construction

1. These buildings are constructed of heavily reinforced concrete (greater than 0.5 metre thick).
2. The reactor building is constructed of heavily reinforced concrete (greater than 2 metres at the base and 1 metre at the top with an inner liner of 2-cm-thick steel).
3. Two steel doors, each 4 cm thick, provide personnel access into the reactor building through an airlock. The outer airlock door is padlocked.
4. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
5. All inner doors are normally closed and unlocked.

Turbine Building Construction

1. This building is constructed of corrugated sheet metal.
2. All of the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Essential Service Water Building Construction

1. This building is constructed of reinforced concrete 0.2 metre thick.
2. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Condensate Water Tank Construction

1. This tank is constructed of welded steel plates (1 cm thick).
2. There are no access ports or hatches in this structure.

Perimeter

1. Two chain-link fences (2.5 metres high) separated by a 30-metre isolation zone surround the facility.
2. The minimum lighting in the isolation zone is 0.2 foot-candle (0.22 lumens/m²).
3. A single (combination personnel/vehicle) entrance/exit point is located in the middle of the west fenceline.
4. The perimeter fenceline is 2 km long.

Perimeter Personnel/Vehicle Entrance/Exit (and Central Alarm Facility)

1. The entrance/exit is manned 24 hours per day by at least two guards.
2. Two vehicle gates (with one gate always closed) provide an area within which guards search vehicles. The gates are heavily reinforced with pipe.
3. A personnel turnstile (2.5 metres high) controls pedestrian traffic.
4. Access is permitted to personnel with badge credentials.
5. All building and interior intrusion sensors annunciate and are displayed individually.

Secondary Alarm Facility

1. This facility is located in the reactor building control room.
2. All building and interior intrusion sensors annunciate and are displayed individually in the reactor building control room.
3. Only operational personnel are in the control room.
4. Control room personnel can authorize other personnel into facility (with a guard escort).

Reactor and Auxiliary Buildings Entrance/Exit

1. A single entrance/exit on the north side of the auxiliary building is provided for access control and is normally unlocked.
2. A guard mans the entrance/exit 24 hours per day inside the building.
3. Access is permitted to personnel with a photo badge credential and the guard issues another photo badge in exchange.

Detection System

1. Sensors
 - a) A guard is posted at the perimeter entrance.
 - b) A guard is posted at the reactor building entrance.
 - c) All other building exterior doors are locked and have magnetic door switch sensors.
 - d) One roving guard routinely patrols outside the buildings and checks building exterior doors and the inner perimeter fenceline once every 2 hours. The building checks take 1.5 hours, and walking the inner fenceline takes 0.5 hour.
 - e) The outer personnel airlock door into the reactor is locked and has a magnetic door switch sensor. Space intrusion sensors are located in the airlock.
2. Intrusion Alarm Annunciation and Display
 - a) There are audio and visual displays at the main perimeter gate station.
 - b) There are audio and visual displays in the reactor control room.
 - c) All guards can send a silent duress call with their transceivers.
3. Intrusion Alarm Assessment
 - a) The roving guard patrol is sent to assess the cause of an exterior door intrusion alarm.
 - b) Operational personnel are sent to assess intrusion door and space alarms at and within the reactor containment building.

Voice Communications

1. Each guard has a radio transceiver (two channels) with which to talk with other guards.
2. Guards at fixed stations (e.g. perimeter vehicle/personnel gate) have telephones to provide an alternative method to communicate.
3. The central alarm and secondary alarm stations both monitor the two guard radio channels and can communicate by radio or telephone to a local law enforcement agency.

Response Force

<u>On-Site</u>	<u>Average Response Time (minutes)</u>
Roving Patrol Guard (Assessment)	2
<u>If threat is assessed:</u>	
One Guard from Main Gate	2
Shift Captain	3
<u>Off-Site</u>	
Local Law Enforcement Agency	
1 Officer	5
2 Additional Officers	10
6 Additional Officers	20

IV. SKETCHES

A number of sketches have been provided which relate to this hypothetical facility. These sketches, Figures 13.1-1 through 13.1-13, will mainly be used in the following subgroup sessions:

- 13.2 Reactor Vulnerabilities Applications,
- 13.3 Facility Characterization Applications,
- 13.4 Vital Area Identification Applications,
- 13.5 Applications of Generic Logic Trees,
- 13.8 Intrusion Detection System Handbook Applications,
- 13.9 Application of Estimate of Adversary Sequence Interruption (EASI) Analysis,
- 13.10 Physical Protection Systems Applications I,
- 13.11 Physical Protection Systems Applications II,
- 13.13 Manpower/Technology Considerations,
- 13.14 System Design Application, and
- 13.15 Total Physical Protection System Design.

The following sketches are provided:

- Figure 13.1-1 Facility Perspective
- Figure 13.1-2 Facility Perspective with Perimeter Features
- Figure 13.1-3 PWR General Layout
- Figure 13.1-4 PWR Composite Plan: Ground Level
- Figure 13.1-5 PWR Composite Plan: Basement
- Figure 13.1-6 Simplified PWR System Functional Diagram
- Figure 13.1-7 Control and Diesel Generator Building Plan: Ground Level
- Figure 13.1-8 Control and Diesel Generator Building Plan: Basement
- Figure 13.1-9 Reactor and Auxiliary Building Plan: Ground Level
- Figure 13.1-10 Reactor and Auxiliary Building Plan: Basement
- Figure 13.1-11 Reactor and Auxiliary Buildings: Elevation
- Figure 13.1-12 Turbine Building Plan: Ground Level
- Figure 13.1-13 Turbine Building Elevation

Figure 13.1-1. Facility Perspective

Figure 13.1-2. Facility Perspective with Perimeter Features

Figure 13.1-3. PWR General Layout

Figure 13.1-4. PWR Composite Plan: Ground Level

Figure 13.1-5. PWR Composite Plan: Basement

Figure 13.1-6. Simplified PWR System Functional Diagram

Figure 13.1-7. Control and Diesel Generator Building Plan: Ground Level

Figure 13.1-8. Control and Diesel Generator Building Plan: Basement

Figure 13.1-9. Reactor and Auxiliary Buildings Plan: Ground Level

Figure 13.1-10. Reactor and Auxiliary Building Plan: Basement

Figure 13.1-11. Reactor and Auxiliary Buildings: Elevation

Figure 13.1-12. Turbine Building Plan: Ground Level

Figure 13.1-13. Turbine Building: Elevation

13.2 Reactor Vulnerability Applications

13.0 SUBGROUP SESSIONS

Session Title: 13.2 Reactor Vulnerability
Applications

Date: Monday, 3 December 1979

Presented By: Subgroup Instructors

Time: 1530 to 1615

Session Objectives:

After the session the participants will be able to

1. State the kinds of sabotage actions that could lead to release of radioactive material from the hypothetical facility, and
2. Identify some of the areas in the hypothetical facility from which sabotage could be initiated.

Summary:

The general concepts of light water reactor vulnerability are applied to the hypothetical facility.

REACTOR VULNERABILITY APPLICATIONS

CONTENTS

	<u>Page</u>
I. Problem Definition	13.2-5
II. Instructional Guidelines	13.2-7
III. Think-About Items	13.2-9

I. PROBLEM DEFINITION

Based on the discussion of reactor vulnerabilities in Session 4.4 and the characteristics of the hypothetical facility given in Session 13.1, identify two kinds of sabotage actions which could lead to release of radioactive material from the facility and determine the plant areas within which the actions could be accomplished. To carry out this exercise, answer the following questions:

1. What is the primary safeguards concern for the hypothetical facility?
2. What are the two general ways that a core meltdown can be caused in the hypothetical facility?
3. Where in the hypothetical facility would an adversary have to go to cause an immediate loss of coolant?
4. A loss of feedwater could lead to a delayed loss of coolant from the reactor core. What system is available to respond to a loss of feedwater in the hypothetical facility? What are the major components of this system?
5. Within what areas of the plant could an adversary disable the auxiliary feedwater system?

II. INSTRUCTIONAL GUIDELINES

1. Read and discuss the session objective and summary.
2. Read the problem definition and have participants locate the referenced material from other sessions. Ask the participants to identify the type of reactor in the hypothetical facility (light water reactor).
3. Work through the questions in the Problem Definition.
 - 3.1 Sabotage leading to core meltdown is the primary safeguards concern.
 - 3.2 Core meltdown can be initiated by (a) immediate loss of coolant through a breach in the primary coolant system or (b) delayed loss of coolant resulting from loss of heat sinks and coolant sources.
 - 3.3 Refer to simplified system diagram (Figure 13.1-6). Have someone locate the primary coolant system and indicate how an immediate loss of coolant could be caused (breach a pipe section or major component). An adversary must gain access to the reactor containment to cause the immediate loss of coolant.
 - 3.4 Refer to the simplified system diagram and trace the normal heat removal path through steam generator and secondary system. The auxiliary feedwater system is available to respond to a loss of feedwater. Major components are condensate water storage tank, auxiliary feedwater pumps, steam generator, steam release valves, and associated piping.
 - 3.5 Refer to the facility layout drawings to identify some of the areas of concern.
4. Refer to think-about items and encourage discussion as time allows.
 - 4.1 The residual heat removal system connects to the primary coolant system and goes through isolation valves to outside the containment building. If the isolation valves could be opened, primary coolant would flow outside of containment.
 - 4.2 Loss of motive power to the pumps or closure of valves could disable the auxiliary feedwater system.

III. THINK-ABOUT ITEMS

1. How could an immediate loss of coolant be initiated without gaining access to the containment building?
2. How could the auxiliary feedwater system be disabled without breaching any of the system components?

**13.3 Facility Characterization
Applications**

13.0 SUBGROUP SESSIONS

Session Title: 13.3 Facility Characterization Applications Date: Tuesday, 4 December 1979

Presented By: Subgroup Instructors Time: 1500 to 1600

Prior to Session:

Read Session 13.1.

Session Objectives:

After the session, the participants will be able to

1. Interpret general facility characterization data relative to physical protection system functions;
2. Identify the interaction of detection, delay, communication, and response in a physical protection system; and
3. Identify some potential vulnerabilities for the hypothetical facility.

Summary:

General data for the hypothetical facility are used during this session to interpret (1) features that relate to the physical protection system and (2) the interaction of these features, and to identify some of the potential vulnerabilities associated with the hypothetical facility.

Additional Resource Materials:

SAND77-0777, Barrier Technology Handbook

FACILITY CHARACTERIZATION APPLICATIONS

CONTENTS

	<u>Page</u>
I. Problem Definition	13.3-5
II. Hypothetical Facility Data--Applicable Site Features	13.3-7
III. Instructional Guidelines	13.3-15
IV. Think-About Items	13.3-17

I. PROBLEM DEFINITION

The hypothetical facility is a pressurized water reactor generating electrical power. The concern is to prevent sabotage actions leading to major radiological release from the reactor during operation.

Using the data supplied in the following section, characterize (1) the vital areas, (2) the detection system, (3) the physical barriers, (4) the communication system, and (5) the response force.

II. HYPOTHETICAL FACILITY DATA—APPLICABLE SITE FEATURES

Vital Areas

The reactor and associated equipment within the containment building is one vital area. This vital area must always be protected to prevent a sabotage scenario from successfully occurring. The auxiliary feedwater pumps are vital areas; additional vital areas will be identified during subgroup working sessions.

To simplify labeling of facility areas and to assure that unique labels are assigned to each separate area of interest, a simple coding system is used. Each area is given a three-element label which includes a building or area identification code, a level (or floor number) designator, and a compartment number. Thus RB-2-1 is the label for the reactor building (RB), level 2, compartment 1. The area codes used for buildings in the hypothetical facility are given as follows:

AUX	Auxiliary Building
CB	Control Building
CWST	Condensate Water Storage Tank
DGB	Diesel Generator Building
ESWB	Essential Service Water Building
RB	Reactor Building
TB	Turbine Building
OSPW	Off-Site Power

Reactor, Auxiliary Buildings, Control and Diesel Generator Building Construction

1. These buildings are constructed of heavily reinforced concrete (greater than 0.5 metre thick).
2. The reactor building is constructed of heavily reinforced concrete (greater than 2 metres at the base and 1 metre at the top with an inner liner of 2-cm-thick steel).
3. Two steel doors, each 4 cm thick, provide personnel access into the reactor building through an airlock. The outer airlock door is padlocked.
4. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
5. All inner doors are normally closed and unlocked.

Turbine Building Construction

1. This building is constructed of corrugated sheet metal.
2. All of the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Perimeter

1. Two chain-link fences (2.5 metres high) separated by a 30-metre isolation zone surround the facility.
2. The minimum lighting in the isolation zone is 0.2 foot-candle (0.22 lumens/m²).
3. A single (combination personnel/vehicle) entrance/exit point is located in the middle of the west fenceline.
4. The perimeter fenceline is 2 km long.

Perimeter Personnel/Vehicle Entrance/Exit (and Central Alarm Facility)

1. The entrance/exit is manned 24 hours per day by at least two guards.
2. Two vehicle gates (with one gate always closed) provide an area within which guards search vehicles. The gates are heavily reinforced with pipe.
3. A personnel turnstile (2.5 metres high) controls pedestrian traffic.
4. Access is permitted to personnel with badge credentials.
5. All building and interior intrusion sensors annunciate and are displayed individually.

Secondary Alarm Facility

1. This facility is located in the reactor building control room.
2. All building and interior intrusion sensors annunciate and are displayed individually in the reactor building control room.
3. Only operational personnel are in the control room.
4. Control room personnel can authorize other personnel into facility (with a guard escort).

Reactor and Auxiliary Buildings Entrance/Exit

1. A single entrance/exit on the north side of the auxiliary building is provided for access control and is normally unlocked.
2. A guard mans the entrance/exit 24 hours per day inside the building.
3. Access is permitted to personnel with a photo badge credential and the guard issues another photo badge in exchange.

Detection System

1. Sensors
 - a) A guard is posted at the perimeter entrance.
 - b) A guard is posted at the reactor building entrance.
 - c) All other building exterior doors are locked and have magnetic door switch sensors.
 - d) One roving guard routinely patrols outside the buildings and checks building exterior doors and the inner perimeter fenceline once every 2 hours. The building checks take 1.5 hours, and walking the inner fenceline takes 0.5 hour.
 - e) The outer personnel airlock door into the reactor is locked and has a magnetic door switch sensor. Space intrusion sensors are located in the airlock.

2. Intrusion Alarm Annunciation and Display

- a) There are audio and visual displays at the main perimeter gate station.
- b) There are audio and visual displays in the reactor control room.
- c) All guards can send a silent duress call with their transceivers.

3. Intrusion Alarm Assessment

- a) The roving guard patrol is sent to assess the cause of an exterior door intrusion alarm.
- b) Operational personnel are sent to assess intrusion door and space alarms at and within the reactor containment building.

Voice Communications

- 1. Each guard has a radio transceiver (two channels) with which to talk with other guards.
- 2. Guards at fixed stations (e.g. perimeter vehicle/personnel gate) have telephones to provide an alternative method to communicate.
- 3. The central alarm and secondary alarm stations both monitor the two guard radio channels and can communicate by radio or telephone to a local law enforcement agency.

Site Graphics

Figures 13.3-1 and 13.3-2 are the site graphics for Session 13.3.

Figure 13.3-1. Pressurized Water Reactor Composite Plan, Ground Level

Figure 13.3-2. Facility Perspective with Perimeter Features

III. INSTRUCTIONAL GUIDELINES

1. Discuss the objectives and summary of this session.
2. Review the Problem Definition and discuss why information on the five identified areas is needed.
3. Review the hypothetical facility data for the applicable site features.
Note: Have the group mark their Figure 13.3-1 to identify the vital areas.
4. When reviewing the construction details, let the group decide which of the vital areas given appears to be easier to get to, i.e., what barriers need to be penetrated to get to the reactor and what barriers need to be penetrated to get to the auxiliary pumps.
Suggestion: Have the group list the barriers to be penetrated to reach the auxiliary pumps and use the Barrier Technology Handbook (Chapter 16) to determine penetration times for a variety of tools. (Note: The only physical barriers, are the outer doors, the walls, or the roof of the turbine building.)
5. When reviewing the detection system, have the group mark up Figures 13.3-1 and 13.3-2 (simply) to identify where potential detection may occur (entry-control point), where potential sensing may occur at Building 1, and how assessment is performed.
6. Discuss the voice communication system.
7. Discuss the response force capability.
8. Choose a few paths and do very simple time comparisons, e.g., adversary (a) is on foot, crosses over the fences, crosses the area, picks lock on the outer door (open door sets off alarms), sets timed explosives on three pumps; (b) follows the same path, except for opening the outer door with a prybar.
9. Have the group summarize what the characterization indicates relative to sabotage of a vital area.
10. Discuss think-about items.

IV. THINK-ABOUT ITEMS

1. Who would gather the data needed to characterize your facility?
2. What groups might supply the data (or information) needed to characterize your facility?
3. What different operating status might need to be characterized?
4. How might you validate the data?
5. Might a written description of a feature be different from the actual feature?

13.0 SUBGROUP SESSIONS

Session Title: 13.4 Vital Area Identification Applications Date: Wednesday, 5 December 1979

Presented By: Subgroup Instructors Time: 0830 to 0930

Session Objectives:

After the session, the participants will be able to

1. State the kinds of information an analyst needs in order to identify vital areas in nuclear power reactors, and
2. Explain how a sabotage fault tree is analyzed to determine minimum sets of vital areas.

Summary:

A sabotage fault tree for the hypothetical facility is presented. Based on a number of limiting assumptions, participants simplify and then analyze the tree to determine sets of vital areas from which at least one set should be protected.

VITAL AREA IDENTIFICATION APPLICATIONS

CONTENTS

	<u>Page</u>
I. Problem Definition	13.4-5
II. Assumptions	13.4-7
III. Sabotage Fault Trees	13.4-9
IV. Vital Area Site Graphics	13.4-15
V. Vital Area Fault Tree	13.4-23
VI. Vital Area Analysis Data	13.4-27
VII. Instructional Guidelines*	13.4-29
VIII. Think-About Items	13.4-31

*To be distributed at the end of the session for reference material.

I. PROBLEM DEFINITION

This problem is associated with the hypothetical facility, a PWR as characterized in Session 13.1. Given a fault tree for radioactive material released from the hypothetical facility, (1) modify the fault tree to a tree constrained by the assumptions given in the following section, (2) associate vital areas with the constrained fault tree, and (3) determine the minimum sets of vital areas that can be utilized in the design of an effective physical protection system.

II. ASSUMPTIONS

The following assumptions are used to limit (constrain) the PWR fault tree (Figure 13.4-1).

1. Only release from the core will be considered. Events R1-10 and R1-20 are not considered.
2. Only release initiated during operation will be considered. Events R2-10 and R2-30 are not considered.
3. Only core meltdown sequences will be considered. Event R3-10 is not considered.
4. Fuel melting incidents which breach fuel cladding will lead to failure of both the primary coolant boundary and the containment. If R4-20 occurs, then R4-10 and R4-30 are assumed to also occur.
5. Only releases which result from induced transient events will be developed. Events R5-20 and R5-30 are not considered.
6. Loss of off-site power cannot be prevented. Event R7-10 is assumed to occur.
7. Loss of off-site power will result in reactor trip (shutdown). If event R7-10 occurs, then R6-10 will also occur.
8. It is not possible for a saboteur to disable the reactor trip safety system. The event R7-30 cannot occur.
9. Loss of off-site power eliminates decay heat removal through the power conversion system. The logic shows R7-10 will cause R9-40 to occur, which in turn will cause R8-20 to occur.

The following assumptions are used to constrain the vital areas associated with the constrained fault tree (Figure 13.4-2).

10. Power cables connected to a component are accessible only in the compartment or area where the component is located. For example R13-20 occurs only in area AUX-2-4.
11. Plumbing connected to components is accessible only in the compartment where the component is located. For example R11-40 occurs only in area CWST.
12. Disablement of a diesel generator requires access to the Diesel Generator Compartment, i.e., areas DGB-1-1 and DGB-1-2.
13. Initiation of secondary steam loop incidents requires access to containment area RB-2-1.

III. SABOTAGE FAULT TREES

The sabotage fault tree for the hypothetical facility PWR is given in Figure 13.4-1, and Figure 13.4-2 gives the constrained PWR sabotage fault tree. Application of Assumptions 1 through 9 should yield Figure 13.4-2 from Figure 13.4-1.

IV. VITAL AREA SITE GRAPHICS

The site graphics given in Figures 13.4-3, 13.4-4 and 13.4-5 are useful for identification of vital areas. Additional detailed site graphics are given in Session 13.1.

Note each area is given a unique label which includes up to three elements. These elements designate an item identification code, a level (or floor number) designator, and a compartment number. Thus RB-2-1 is the label for the Reactor Building (RB), Level 2, Compartment 1. The codes for the areas in the hypothetical facility are

AUX	Auxiliary Building
CB	Control Building
CWST	Condensate Water Storage Tank
DGB	Diesel Generator Building
ESWB	Essential Service Water Building
RB	Reactor Building
TB	Turbine Building
OSPW	Off-Site Power

Figure 13.4-3. Simplified PWR System

Figure 13.4-4. PWR Composite Plan, Ground-Level

**PRESSURIZED WATER REACTOR
COMPOSITE PLAN: BASEMENT**

Figure 13.4-5. PWR Composite Plan, Basement

V. VITAL AREA FAULT TREE

The vital area fault tree is given in Figure 13.4-6. Application of Assumptions 10 through 14 to the constrained PWR fault tree (Figure 13.4-2) in conjunction with the site graphics should produce Figure 13.4-6.

VI. VITAL AREA ANALYSIS DATA

Results

From the constrained vital area fault tree, sets of areas could be determined to which an adversary would have to gain access in order to sabotage the facility. The following is a complete list of the minimum sets of areas in which sabotage can be accomplished.

1. OSPW and RB-2-1
2. OSPW, AUX-2-6, DGB-1-1, and DGB-1-2
3. OSPW, AUX-2-6, DGB-1-1, and AUX-2-5
4. OSPW, AUX-2-6, AUX-2-4, and DGB-1-2
5. OSPW, AUX-2-6, AUX-2-4, and AUX-2-5
6. OSPW, CWST, ESWB-1-1, and ESWB-1-2

If access is denied to one or more of the areas in each of the six sets of areas above, then none of the sabotage sequences represented by the fault tree can be completed. Below is a complete list of the minimum sets of areas which if protected will prevent sabotage.

1. OSPW
2. RB-2-1, AUX-2-6, and CWST
3. RB-2-1, AUX-2-6, and ESWB-1-1
4. RB-2-1, AUX-2-6, and ESWB-1-2
5. RB-2-1, DGB-1-1, AUX-2-4, and CWST
6. RB-2-1, DGB-1-1, AUX-2-4, and ESWB-1-1
7. RB-2-1, DGB-1-1, AUX-2-4, and ESWB-1-2
8. RB-2-1, DGB-1-2, AUX-2-5, and CWST
9. RB-2-1, DGB-1-2, AUX-2-5, and ESWB-1-1
10. RB-2-1, DGB-1-2, AUX-2-5, and ESWB-1-2

If adversary access is precluded to all of the vital areas in any one of the above sets, sabotage cannot occur.

Logic Equations for Vital Area Analysis

The 6 minimum sets of areas in which sabotage can be accomplished may be obtained from the PWR vital area fault tree (Figure 13.4-6).

Note the following logic symbols:

- $\wedge$ logic AND
- $\vee$ logic OR

From Figure 13.4-6:

RELEASE = OSPW $\wedge$ AREA1-20
AREA1-20 = RB-2-1 $\vee$ AREA2-20
RELEASE = OSPW $\wedge$ (RB-2-1 $\vee$ AREA2-20)
AREA2-20 = AREA3-10 $\vee$ AREA3-20
RELEASE = OSPW $\wedge$ [RB-2-1 $\vee$ (AREA3-10 $\vee$ AREA3-20)]
= OSPW $\wedge$ (RB-2-1 $\vee$ AREA3-10 $\vee$ AREA3-20)

AREA3-10 = AREA4-10 $\wedge$ AUX-2-6 $\wedge$ AREA4-30
 AREA3-20 = CWST $\wedge$ ESWB-1-1 $\wedge$ ESWB-1-2
 RELEASE = OSPW $\wedge$ (RB-2-1 $\vee$ (AREA4-10 $\wedge$ AUX-2-6 $\wedge$ AREA4-30)
 $\vee$ (CWST $\wedge$ ESWB-1-1 $\wedge$ ESWB-1-2))
 = OSPW $\wedge$ (RB-2-1 $\vee$ AREA4-10 $\wedge$ AUX-2-6 $\wedge$ AREA4-30
 $\vee$ CWST $\wedge$ ESWB-1-1 $\wedge$ ESWB-1-2)
 AREA4-10 = DGB-1-1 $\vee$ AUX-2-4
 AREA4-30 = DGB-1-2 $\vee$ AUX-2-5
 RELEASE = OSPW $\wedge$ [RB-2-1 $\vee$ (DGB-1-1 $\vee$ AUX-2-4)
 $\wedge$ AUX-2-6 $\wedge$ (DGB-1-2 $\vee$ AUX-2-5)
 $\vee$ CWST $\wedge$ ESWB-1-1 $\wedge$ ESWB-1-2]
 = OSPW $\wedge$ [RB-2-1 $\vee$ AUX-2-6 $\wedge$ (DGB-1-1 $\wedge$ DGB-1-2
 $\vee$ DGB-1-1 $\wedge$ AUX-2-5 $\vee$ AUX-2-4 $\wedge$ DGB-1-2
 $\vee$ AUX-2-4 $\wedge$ AUX-2-5) $\vee$ CWST $\wedge$ ESWB-1-1
 $\wedge$ ESWB-1-2]

Final expansion results in the 6 minimum sets of areas:

RELEASE = OSPW $\wedge$ RB-2-1 $\vee$	(1)
OSPW $\wedge$ AUX-2-6 $\wedge$ DGB-1-1 $\wedge$ DGB-1-2 $\vee$	(2)
OSPW $\wedge$ AUX-2-6 $\wedge$ DGB-1-1 $\wedge$ AUX-2-5 $\vee$	(3)
OSPW $\wedge$ AUX-2-6 $\wedge$ AUX-2-4 $\wedge$ DGB-1-2 $\vee$	(4)
OSPW $\wedge$ AUX-2-6 $\wedge$ AUX-2-4 $\wedge$ AUX-2-5 $\vee$	(5)
OSPW $\wedge$ CWST $\wedge$ ESWB-1-1 $\wedge$ ESWB-1-2	(6)

Further, it can be shown that the 10 minimum sets of areas which, if protected, will prevent sabotage are obtained from the complement of RELEASE. Fortunately, computer codes are available for these calculations.

VII. INSTRUCTIONAL GUIDELINES

1. Read and discuss the session objectives and summary. Emphasize that because of the complexity of nuclear power reactors, a developed sabotage fault tree is usually very large. Only a portion of the tree will be developed for the hypothetical facility to illustrate the techniques used in the analysis.
2. Note from the list of contents that the vital area identification exercise is contained in Sections I through IV of this session. This material, along with the instructional guidelines, should allow participants to easily understand the exercise.
3. Read and discuss the problem exercise.
4. Refer to the fault tree in Figure 13.4-1 and to Assumptions 1 through 9. Using these assumptions, reduce the fault tree size. Explain the fault tree events while modifying the tree.
 - 4.1 Assumptions 1, 2, and 3 limit the scope of the analysis. Cross out the indicated events that are "not considered" or "assumed not credible," i.e., event probabilities are assumed to be 0.0.
 - 4.2 Assumption 4 is a conservative assumption. The event probabilities are assumed to be 1.0. Since these events input an AND gate they may also be crossed out.
 - 4.3 Assumption 5 limits the scope of the analysis. Cross out the events.
 - 4.4 Assumptions 6 and 9 are conservative assumptions. The event R7-10 probability is assumed to be 1.0. Modify the tree in three places for this assumption.
 - 4.5 Assumptions 7 and 8 are assumptions based upon reactor trip design reliability. Assumptions may not be conservative. Event R6-10 probability is assumed to be 1.0, and R7-10 probability is assumed to be 1.0.
5. Refer to the constrained fault tree in Figure 13.4-2. Note this tree results from application of Assumptions 1 through 9. Resolve any differences between the constrained tree and your marked-up tree. (The instructors are provided with a correct marked-up tree for reference.)
6. Associate the plant areas with the events given in the constrained fault tree.
 - 6.1 Discuss the site graphics given in Section IV, especially as they relate to the auxiliary feedwater system, which, in this exercise, is the only part of the PWR system assumed to be a possible target for attack.
 - 6.1.1 Briefly note that the feedwater system in Figure 13.4-3 consists of a water source or sources, appropriate pumping systems, water line connections to the steam generator, and steam lines which can vent to the atmosphere.

- 6.1.2 Briefly note the area symbols in Figures 13.4-4 and 13.4-5, as defined in "Vital Area Site Graphics."
- 6.2 Determine which areas are associated with which fault tree events as further constrained by Assumptions 10 through 13.
 - 6.2.1 Assumption 10: Implies area AUX-2-4 for R13-20, area AUX-2-5 for R13-40, and OSPW for R7-10.
 - 6.2.2 Assumption 11: Implies CWST for R11-40, ESWB-1-1 for R11-50, ESWB-1-2 for R11-60, AUX-2-4 for R12-20, and AUX-2-5 for R12-40.
 - 6.2.3 Assumption 12: Implies DGB-1-1 for R14-20 and DGB-1-2 for R14-40.
 - 6.2.4 Assumption 13: Implies RB-2-1 for R9-10.
7. Refer to the vital area fault tree. Note this tree results from the constrained fault tree once the vital areas are associated with events in the constrained fault tree. Note the only logic reduction for this example occurred because events R13-20 and R12-20 had the same associated area AUX-2-4 and because R13-40 and R12-40 had the same area AUX-2-5. Under what conditions would the area logic be more complicated than the fault tree logic?
8. Using the vital area fault tree, trace through a few area combinations sufficient to cause the output event. Refer to "Vital Area Analysis Data" for a complete list of minimum sets of areas requiring access for sabotage.
9. Discuss the complement concept. Remind the group that all inputs to an OR gate and any one input to an AND gate must be prevented to prevent output from the gate. Have the participants determine at least one complement location set. Refer to the complete list of minimum sets of areas requiring protection to prevent sabotage.
10. Briefly note the equations as obtained from the vital area fault tree will directly yield the sets of sabotage target areas and that the complement will yield the sets of areas which must be protected. Emphasize that a simplified version of the PWR fault tree was solved. The complete tree is usually much larger and may require extensive logic equation manipulation. In some instances logic equation reduction is only practical using sophisticated computer programs.
11. Discuss the think-about items.

VIII. THINK-ABOUT ITEMS

1. What are some of the limitations you can see in the use of fault tree analysis to identify vital areas in nuclear power reactors?
2. How can you assure that the fault tree is complete; i.e., that all sequences leading to radioactive release are represented in the tree?
3. In the simplified sabotage fault tree, only loss of power and direct mechanical breaching were considered as events leading to disablement of electrically powered components. What other events might also be considered for those components requiring cooling, ventilation, etc.?
4. In the simplified fault tree, only loss of coolant source and loss of pumping capability were considered in developing events related to disablement of cooling systems. What other elements might contribute to failure of cooling systems?
5. A sabotage fault tree is a logic model which identifies the combinations of events that could lead to radioactive release from a nuclear facility. Could such a model be used in a real-time mode to help determine guard response tactics during an attack by an adversary force?
6. Which of the assumptions do you feel were not credible and why?
7. When developing events involving disablement of a system function, the analyst must answer the following questions: (1) What systems are necessary to provide the function or what minimum systems may disable the function? (2) How and where may I initiate a system disablement? (3) What is the logic by which the disablement events must combine? What other questions may be asked?
8. When identifying vital areas, what guidelines may be used as to area size, location, etc.?
9. Could threat definition influence the definition of vital areas?
10. What aspects of vital area identification, if any, cause you some concern as to the reasonableness or usefulness of the technique?

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

13.0 SUBGROUP SESSIONS

Session Title: 13.5 Applications of Generic Logic Trees

Date: Wednesday, 5 December 1979
Friday, 7 December

Presented By: Subgroup Instructors

Time: 5 December, 1500 to 1600
7 December, 1000 to 1200

Session Objectives:

After the session, the participants will be able to

1. Name the generic logic trees (by location of use and mode of attack);
2. State why generic logic trees are used mainly for detection and delay functions;
3. Describe the three adversary tactics generic logic trees usually address;
4. State why there is no deceit logic tree for "Release;"
5. State why the deceit boundary logic tree applies to both protected boundaries and building boundaries;
6. Discuss the following three generic aspects of logic trees:
 - a) One event or subtree may apply to several identical situations,
 - b) One event or subtree may apply to several similar situations, and
 - c) One event may allow an adversary many attack options; and
7. Read generic logic trees.

Summary:

The complete set of generic logic trees is presented and discussed in this session. The participants should become familiar with the logic trees' content, applications, and limitations. Also, logic tree development is discussed for a limited set of detailed logic trees.

APPLICATIONS OF GENERIC LOGIC TREES

CONTENTS

	<u>Page</u>
I. Generic Logic Trees	13.5-5
II. Exercise 1	13.5-7
III. Exercise 2	13.5-11
IV. Detail Logic Trees	13.5-15
V. Instructional Guidelines	13-5.31
VI. Think-About Items	13.5-35

I. GENERIC LOGIC TREES

The following list gives the titles of the complete set of generic logic trees:

- FORCE-BOUNDARY and STEALTH-BOUNDARY
- DECEIT-BOUNDARY
- FORCE-AREA and STEALTH AREA
- DECEIT-AREA
- FORCE-BUILDING and STEALTH-BUILDING
- FORCE-ACQUIRE-SNM and STEALTH-ACQUIRE-SNM
- DECEIT-ACQUIRE-SNM
- FORCE-RELEASE and STEALTH-RELEASE

Due to size, these generic logic trees are contained in the pocket at the back of this notebook.

II. EXERCISE 1

Exercise 1 uses the generic site diagram given in Figure 13.5-1. The only credible threat is theft of material at the target location. Select a zone for a physical protection system (PPS) that does not go beyond the building boundary. The zone may include the building boundary and anything in the building.

Do the following:

- A1. Determine all of the generic logic trees that may potentially be applied to the problem.
- B1. Define a zone that surrounds the targets but does not actually include them within the zone volume. Determine the generic logic trees that apply to this zone.
- C1. Define the minimum-size zone that includes the targets. Determine which generic logic trees apply to this zone.
- D1. For the two selected zones, determine the initial and final boundaries for detection and delay of an outsider threat.
- E1. For the two selected zones, determine the initial and final boundaries for detection and delay of an insider threat. Recall that the threat is theft of material at the target location.
- F1. If the targets were sabotage targets, determine if the zone or zone boundaries would need to be changed (a) for an outsider threat and (b) for an insider threat.

Figure 13.5-1. Generic Site Graphic

III. EXERCISE 2

For Exercise 2, assume the control room of the hypothetical facility, as given in Figure 13.5-2, is a vital area. The control room walls, ceiling, and floor will define the zone for this vital area. The adversary threat is an outsider, and threat tactic to be considered is force only.

Do the following:

- A2. Determine which generic logic trees apply to the zone.
- B2. Identify all potentially unique penetration paths into the vital area.
- C2. Using the FORCE-BUILDING generic logic tree, determine which event or events apply to each identified penetration path. Indicate the specific penetration paths below these events.
- D2. Identify additional penetration paths into this zone boundary that are not indicated in Figure 13.5-2.
- E2. Locate these potential paths below appropriate events in the FORCE-BUILDING generic logic tree.
- F2. Identify potential penetration paths that are not implicitly given in the FORCE-BUILDING generic logic tree.

Figure 13.5-2. Pressurized Water Reactor Composite Plan, Ground Level

IV. DETAIL LOGIC TREES

Logic trees in this section provide examples of additional logic detail for selected terminal events given in the generic logic trees. These trees are not necessarily complete and may not be totally applicable to all selected sites. The intent of these trees is to provide the student with examples of the type of additional logic detail that may be associated with terminal events in the generic logic trees.

The detail logic tree titles are

- AVOID or CONFRONT GUARDS
- DEFEAT PERIMETER BARRIER
- DEFEAT or BYPASS SENSOR FIELD
- DEFEAT FENCE
- DEFEAT BUILDING STRUCTURE
- DEFEAT BUILDING PERSONNEL ENTRANCE
- DEFEAT BUILDING UTILITY OPENINGS

V. INSTRUCTIONAL GUIDELINES

It is anticipated that the first five or six items will be covered in a 1-hour session.

1. Discuss the session objectives.
2. Present the generic logic trees.
 - a) Introduce the generic site graphic (Figure 13.5-1) showing perimeter(s), area(s), building(s), target location(s), and target(s).
 - b) Referring to the sketch, indicate applicability of generic trees:
 - Boundary Trees -- any protected boundary,
 - Area Trees -- any area in and out of buildings,
 - Building Trees -- building, module, vault boundary, critical target area;
 - Acquire Special Nuclear Materials (SNM) Trees -- acquisition of material(s);
 - Release Trees -- radiological sabotage
 - c) Indicate that separate generic trees are developed for force tactics, stealth tactics, and deceit tactics, with the following exceptions:
 - There is no dispersal by deceit since authorized dispersal is never allowed, and
 - The deceit boundary tree applies to both protected boundaries and building boundaries since "logically" anything that is done at one boundary for deceit can also be done at any other boundary.

3. Discuss briefly the zone concept relative to the generic site sketch.

NOTE:

- The zone concept states detection and delay elements occur on or within the zone, and
- The zone may include one or more of the basic site features, and the zone is three-dimensional.

Give examples of zones:

- a) A site envelope zone is a three-dimensional space with a boundary extending above and below site. This zone may be associated with the limited area boundary or with the protected area boundary.
- b) A building boundary zone consists of the building boundary (again in three-dimensional space).
- c) An expanded zone consists of the site envelope, plus area up to exterior building(s), plus the building(s) boundary.

Note that the generic trees were developed so that they would be applicable regardless of the selected zone.

4. Have the participants work Exercise 1. Volunteer information only after the participants appear to be in trouble or finished with the exercise.

- A1) FORCE- and STEALTH-BUILDING, DECEIT-BOUNDARY, FORCE-, STEALTH-, and DECEIT-AREA; FORCE-, STEALTH-, and DECEIT-ACQUIRE-SNM.
 - B1) Potential zones are
 - The building boundary,
 - Vital area boundary enclosing both targets,
 - Vital areas enclosing each target, and
 - Any combinations of the above, with the intermediate areas included.
 - C1) The targets themselves would be the minimum zone. FORCE-, STEALTH-, and DECEIT-ACQUIRE-SNM are the appropriate generic logic trees.
 - D1) For an outsider threat, initial and final boundaries may both be the exterior zone boundary. Note that the final boundary could also be at some other location.
 - E1) For the insider threat, initial and final boundaries may be reversed from the outside ones. Note that opportunities for first detection may determine where the initial boundary is, and, likewise, opportunities for delay (that is, compatible with safety, criticality, etc.) may determine where the final boundary is.
 - F1) Some comments:
 - For the outsider threat, the adversary would probably not be allowed access to the targets.
 - For the insider threat, if access must be allowed, some sort of controls for the insider and/or the target may be necessary.
 - Examples may be two-man rule, authorized procedures, target designs to be inherently fail safe, restrictions on insider tools, knowledge, etc.
5. Note that the rest of the subgroup session will deal with understanding the generic logic trees. Discuss a force perimeter (FORCE-BOUNDARY or FORCE-BUILDING generic tree) as selected by the participants. Note that comments made relative to the tree apply to all generic trees.
- a) Guide the students through the force tree.
 - b) Comment on the event names:
 - All force events start with F....
 - The location or level below the end event is indicated by the first numeric. For example, F3 implies force event on level 3.
 - The remaining numerics generally imply sequential event numbering from left to right.
 - c) Comment on typical generic logic tree attributes:
 - The logic is developed from the adversary's point of view.
 - The adversary wins if the end event is accomplished.
 - Working from the tree bottom to top, the adversary wins if any one of the input events to an OR gate are accomplished and if all input events to an AND gate are accomplished.

- d) Comment on the generic aspects of the tree:
 - One event or subtree may apply to several identical situations. Examples are given for the FORCE-BOUNDARY tree.
 - Example: Defeat Personnel Entrance (F3-20) may apply to a number of identical entrances.
 - Example: Defeat Utility or Service Penetration (F3-60) may apply to sewer lines, water lines, drainage culverts, etc.
 - One event may apply to several adversary options.
 - Example: Defeat Outer Fence (F4-10) may apply to Defeat Fence by going over, under, through, etc. Further, Defeat Fence Under may apply to prying up the fence with a pole level, tunneling under the fence, etc.
 - e) Comment on use of force trees:
 - They are usually used to assess the delay elements of a PPS. Note: more will be said on this in subsequent sessions.
 - If no physical protection elements are associated with an event that is an input to an OR gate, then that event becomes an obvious adversary option.
 - Indicated elements are assessed (qualitatively) against the full threat spectrum, site operational states, etc.
6. Discuss the stealth tree that is used for the same boundary as the selected force tree. Examples given below are for the STEALTH-BOUNDARY tree.
- a) Indicate similarities between stealth and force trees.
 - Similar events have event names with the same numerical values and do not have an X in the event name. For example, S4-50 and F4-50 are similar stealth and force logic tree events.
 - The 4 numeric in S4-50 and F4-50 implies the events are located four levels below the end event in both trees.
 - b) The primary difference between stealth and force trees is that detection events such as sensors (SX5-10) and related events (SX5-20, SX5-30) are included in the stealth trees.
 - c) Stealth trees are used primarily for estimates of the likelihood of detection.
7. Discuss the DECEIT-BOUNDARY tree:
- a) Comment on generic aspects of the deceit tree. As with force and stealth trees, the deceit tree applies to any adversary.
 - b) Depending upon the adversary (such as authorized insider versus unauthorized outsider), the detection likelihood may be significantly different.
 - c) The deceit trees are used mainly for estimates of the likelihood of detection.

8. Note that the remaining generic logic trees are developed like the trees already discussed. Ask the participants if they would like to go over any of these additional trees. Do this for two or more trees at most. Note that release and acquire-SNM trees are the most unique of the remaining trees.
9. Briefly indicate that several detailed logic trees are also provided. These are intended to provide the participants with a further understanding of how terminal events (or subtrees) may be expanded. Briefly look at a couple of the detail logic trees. Suggest DEFEAT FENCE since it is simple and discuss AVOID or CONFRONT GUARDS since it is important.
10. Have the participants work Exercise 2.
 - A2) The FORCE-BUILDING tree.
 - B2) Potentially unique paths:
 - Outside walls
 - Inside walls
 - Two doors---if they have identical characteristics, treat as one
 - Electrical chase
 - Roof
 - Floor
 - C2) Mark up logic tree as indicated.
 - D2) Additional penetration paths:
 - Heating and cooling ducts
 - Ventilation openings
 - Crash-outs
 - Electrical passageways.
 - Utilities
 - E2) Mark up logic tree as indicated.
 - F2) Discuss as appropriate.

VI. THINK-ABOUT ITEMS

1. Why do we say the adversary wins if he defeats any one or more of the detection, delay, communication, and/or response PPS functions?
2. Why are the generic trees associated mainly with detection and delay functions?
3. Why does detection include sensors, communication of an alarm, and assessment?
4. Do we assess the detection and delay elements that are not included in the zone?
5. Is the likelihood of detecting an adversary using stealth tactics less than, equal to, or greater than the likelihood of detecting the same adversary using force tactics? Discuss.
6. Given previous detection, is the time after detection needed for the adversary to successfully complete a scenario using force tactics always less than or equal to the time after detection needed for the same adversary to successfully complete a scenario using stealth or deceit tactics? Discuss.
7. What are some of the reasons the force, stealth, and deceit trees are called generic?
8. Would you expect the generic logic trees to directly apply to your site? Discuss.

13.0 SUBGROUP SESSIONS

Session Title: 13.6 Barrier Technology Handbook Applications

Date: Thursday, 6 December 1979

Presented By: Subgroup Instructors

Time: 1000 to 1200
1330 to 1430

Prior to Session:

Read Chapters 1, 2, 16, and 17.

Session Objectives:

After the session, the participants will be able to determine delay times from the Barrier Technology Handbook for given paths and penetration equipment.

Summary:

A set of three exercises pertaining to a given example problem will be worked to demonstrate how to use the information contained in the Barrier Technology Handbook. This session also includes think-about items and instructional guidelines which will be distributed at the end of the session for reference material.

Resource Material:

SAND77-0777, Barrier Technology Handbook

BARRIER TECHNOLOGY HANDBOOK APPLICATIONS

CONTENTS

	<u>Page</u>
I. Example Problem	13.6-5
II. Exercise 1	13.6-7
III. Exercise 2	13.6-9
IV. Exercise 3	13.6-11
V. General Instructional Guidelines	13.6-13
V.1 Exercise 1 Guidelines	13.6-15
V.2 Exercise 2 Guidelines	13.6-17
V.3 Exercise 3 Guidelines	13.6-19
VI. Think-About Items	13.6-21

I. EXAMPLE PROBLEM

This example was chosen to illustrate usage of the data in Chapters 16 and 17, Barrier Technology Handbook.

Barrier Data

Figure 13.6-1 and its legend provide barrier numbers and barrier specifications.

Barrier Number	Type	Specification
1	Fence	2-m chain-link fence, vinyl coated, without outriggers
2	Distance	50 m (~160 ft), unpaved, smooth
3	Door	Sheetmetal, 16-gauge standard industrial door
4	Distance	12 m (~40 ft) paved
5	Wall	Reinforced, concrete 15-cm (~6-in) thick, 3000 psi reinforced with one layer No. 4 rebar spaced 20 cm (~8 in) on center

Figure 13.6-1. Example Problem Barrier Data

Specific Scenario

In the Example Problem scenario, an adversary intends to

1. Climb over fence,
2. Run to building door,
3. Penetrate building door,
4. Run to vault wall,
5. Penetrate vault wall,
6. Run to material,
7. Gather material (6-kg metal block), and
8. Escape along entry path.

Adversary, Equipment, and Objective

One highly motivated person is equipped with:

- Gloves, 0.25 kg (0.5 lb), for climbing fence
- Pipe wrench, 0.25 kg (0.5 lb), for penetrating door
- Explosives, 1.8 kg (4 lb), and hand boltcutters, 9 kg (20 lb), for penetrating vault door

The objective is to steal material.

Worksheet	Task Description	Mean Task Time (minutes)
1	Climb fence*	0.10
2	Run 50 m (~160 ft)† (~14 s = 0.23 min)	0.23
3	Penetrate building door‡	0.4
4	Run to vault: 12 m (~40 ft) (~3 s = 0.05 min)*	0.05
5	Penetrate vault wall§	2.3
6	Run to material: 6 m (~20 ft) (~1.5 s = 0.02 min)*	0.02
7	Gather material: 6 kg (estimate)	0.05
8	Run back to fence and climb over (Nos. 6, 4, 2, and 1 above) { 0.02 0.05 0.23 0.1 0.4	0.4
TOTAL TIME		= 3.55 minutes

*Barrier Technology Handbook, Chapter 16, p. 16.3-2.

†Barrier Technology Handbook, Chapter 17, p. 17.1-24.

‡Barrier Technology Handbook, Chapter 16, p. 16.3-33.

§Barrier Technology Handbook, Chapter 16, p. 16.3-13.

II. EXERCISE 1

Barrier Data

Figure 13.6-2 and its legend provide barrier numbers and barrier specifications.

<u>Barrier Number</u>	<u>Type</u>	<u>Specification</u>
1	Gate	2.4x4 m (8x13 ft) wide padlocked chain-link gate on metal pipe
2	Distance	100-m (~320-ft) paved road
3	Vehicle door	Standard industrial vehicle door, hollow steel panel, 16 gauge
4	Distance	40 m (~131 ft), paved
5	Vital area door	0.6-m (1/4-in) steel plate
6	Distance	12 m (~40 ft), paved

Figure 13.6-2. Exercise 1 Barrier Data

Specific Scenario

In the scenario for Exercise 1, the adversaries intend to

1. Crash truck through gate,
2. Drive to building vehicle door,
3. Crash truck through vehicle door,
4. Run to vital area door,
5. Penetrate vital area door with explosives,
6. Run to vital equipment, and
7. Set a 100-pound bulk explosive charge.

Adversary, Equipment, and Objective

Two highly motivated people equipped with a pickup truck and bulk explosives intend to sabotage equipment in a vital area and do not expect to survive.

<u>Worksheet</u>	<u>Task Description</u>	<u>Mean Task Time (minutes)</u>
1	Crash truck through gate	
2	Drive vehicle 100 m (~320 ft) to building vehicle door on paved road	
3	Crash through vehicle door	
4	Run 40 m (~131 ft) to Vital Area door	
5	Penetrate Vital Area door with 2.3 kg (~5 lb) bulk explosives	
6	Run 12 m (~40 ft) to vital equipment	
7	Set up a 45-kg (~100-lb) bulk explosive charge on vital equipment	
TOTAL TIME		<u>minutes</u>

III. EXERCISE 2

Barrier Data

Figure 13.6-3 and its legend provide barrier numbers and barrier specifications.

Barrier Number	Type	Specification
1	Building wall	Concrete, 10-cm (~4-in) thick, 3000 psi reinforced one layer 0.6 cm (~1/4-in) diameter, 15x15-cm (~6x6-in) mesh
2	Distance	12 m (~40 ft)
3	Vault wall	Concrete, 50-cm (~20-in) thick, 5000 psi, two layer No. 4 rebar, 15 cm (~6 in) on center

Figure 13.6-3. Exercise 2 Barrier Data

Partial Specific Scenario

In the partial scenario for Exercise 2, adversaries intend to

1. Penetrate building wall with explosives,
2. Run to vault wall, and
3. Penetrate vault wall with explosives.

Adversary, Equipment, and Objective

Two highly motivated people equipped with bulk explosives and hydraulic boltcutters intend to penetrate the building wall and then the vault wall.

Worksheet	Task Description	Task Times (minutes)		
		min.	mean	max.
1	Penetrate building wall with 1.4 kg (3 lb) of explosives	_____	_____	_____
2	Run 12 m (~40 ft) to vault wall	_____	_____	_____
3	Penetrate vault wall with 9 kg (20 lb) of explosives and tamp plate and hydraulic boltcutters	_____	_____	_____
TOTAL TIME		_____	_____	_____

Determine the safe distance that the adversaries should travel before they fire the explosives for barrier No. 1 above.

IV. EXERCISE 3

Barrier Data

Figure 13.6-4 and its legend provide barrier numbers and barrier specifications.

<u>Barrier Number</u>	<u>Type</u>	<u>Specification</u>
1	Security grille at the end of air intake duct	No. 4 rebar spaced 15 cm (~6 in) on center, horizontally and vertically, and welded to steel frame
2	Air intake duct	1-m diameter mill steel, 0.3-cm (~1/8-in) thick

Figure 13.6-4. Exercise 3 Barrier Data

Partial Specific Scenario

In the partial scenario for Exercise 3, an adversary intends to

1. Penetrate the security grille with boltcutters, and
2. Penetrate the ductwork with oxyacetylene cutting torch.

Adversary, Equipment, and Objective

One highly motivated person equipped with 1-metre (42-inch) boltcutters and a portable oxyacetylene cutting torch intends to penetrate the security grille and ductwork to enter the building.

<u>Worksheet</u>	<u>Task Description</u>	<u>Task Time (minutes)</u>
1	Cut 12 No. 4 rebars (for man-sized opening) with boltcutters to penetrate security grille	—
2	Cut a square opening in ductwork, (for man-sized opening) with oxyacetylene torch to penetrate ductwork; cut length is 120 cm (~48 in)	—

V. GENERAL INSTRUCTIONAL GUIDELINES

1. Review Section 1.1, Barrier Technology Handbook, to identify purposes of handbook and how penetration times were developed.
2. Review Section 2.1 and discuss where the PPS system can and cannot take credit for a barrier.
3. Review Section 2.3 and discuss consideration of installing barriers immediately after the sensors to aid assessment and pinpoint adversary location. Discuss balanced barrier design.
4. Review Sections 2.4, 2.5, and 2.6 and discuss as appropriate.
5. Review Section 16.1 on categories of attack tools.
6. Go through the Example Problem with your group. Explain that most units in the handbook are not metric and that the given English units in the exercise problems should be used.
7. Let the group do Exercises 1, 2, and 3. Worksheet answers are attached, and the purpose of each exercise is explained on worksheet.

V.1 EXERCISE 1 GUIDELINES

The purposes of this exercise are to

1. Let the group become familiar with extracting data from Chapters 16 and 17.
2. Point out that vehicles can quickly penetrate conventional perimeter gates and industrial doors.
4. Point out that explosives penetrate quickly.
5. Let the group interpret rate data graphs.

<u>Worksheet</u>	<u>Task Description</u>	<u>Mean Task Time (minutes)</u>
1	Crash truck through perimeter gate*	0.04
2	Drive vehicle 100 m (~320 ft) to vehicle door (~6 to 7 s)†	0.1
3	Crash through vehicle door**	0.6
4	Run 40 m (~131 ft) to Vital Area door (~10 s)‡	0.16
5	Penetrate Vital Area door with 2.3 kg (~5 lb) bulk explosives§	1.0
6	Run 12 m (~40 ft) to Vital Area equipment (~3 s)¶	0.05
7	Set up a 45-kg (100-lb) bulk explosive charge on vital equipment (~35 s)	0.58
TOTAL TIME		2.53 minutes

*Barrier Technology Handbook, Chapter 16, p. 16.3-10.

†Barrier Technology Handbook, Chapter 17, p. 17.1-26.

**Barrier Technology Handbook, Chapter 16, p. 16.3-34.

‡Barrier Technology Handbook, Chapter 17, p. 17.1-24.

§Barrier Technology Handbook, Chapter 16, p. 16.3-38.

|| Barrier Technology Handbook, Chapter 17, p. 17.1-17.

V.2 EXERCISE 2 GUIDELINES

The purposes of this exercise are to let the group

1. Discover that penetration times for reinforced concrete of differing thicknesses are quite similar, i.e., thicker concrete only requires more explosive.
2. Learn to interpolate between a number of data points to reach an educated judgement on the penetration time for barrier number 3. For example, there is no data for a 20-inch reinforced wall, but there are data points for 18- and 24-inch reinforced concrete.
3. Understand what the minimum and maximum barrier penetration times mean.

Worksheet	Task Description	Task Times (minutes)		
		min.	mean	max.
1	Penetrate building wall with 1.4 kg (3 lb) of explosives*	0.7	1.4	2.1
2	Run 12 m (40 ft) to vault wall (~3 s)†	0.05	0.05	0.05
3	Penetrate vault with 9 kg (20 lb) of explosives, tamp plate, and hydraulic bolt-cutters (estimate wall properties roughly coincide with data for ~18-in-thick wall, reinforced with two layers No. 4 rebar, 3000 psi concrete)‡	2	4	6

Determine the safe distance to retreat before firing 3 pounds of explosives.
(From page 17.1-18, Barrier Technology Handbook: Estimate 250 to 300 feet.)

*Barrier Technology Handbook, Chapter 16, p. 16.3-11

†Barrier Technology Handbook, Chapter 17, p. 17.1-24

‡Barrier Technology Handbook, Chapter 16, p. 16.3-16

V.3 EXERCISE 3 GUIDELINES

The purpose of this exercise is to have the group:

1. Become familiar with cutting rate data for various tools.
2. Become aware that slightly different tools have a significant effect on cutting rates.

<u>Worksheet</u>	<u>Type</u>	<u>Mean time (minutes)</u>
1	Cut 12 No. 4 rebars (for man-sized hole) with 1-m (42-in) hand-held boltcutters. 4 cuts (80 s) x 3 $\approx$ 320 s.* But curve is flattening: possibly one adversary would take ~8 to 12 min. (Good discussion item: uncertainty increases when data is extrapolated.)	<u>~6</u> (8 to 12)
2	Cut a square opening in duct 0.3 cm (1/8 in); cut length is 1.20 m (~98 in) with portable oxyacetylene torch (~2.5 s/in x 48 = 120 s)†	<u>~2</u>
TOTAL TIME		~8 minutes (or 10 to 12)

*Barrier Technology Handbook, Chapter 17, p. 17.1-7

†Barrier Technology Handbook, Chapter 17, p. 17.1-10

NOTE:

Have the group look at cutting rebar with oxyacetylene torch (pages 17.1-9, 12 cuts in approximately 1.5 minutes).

VI. THINK-ABOUT ITEMS

1. What terminology have we used that you would like clarified?
2. What might happen to the total scenario time for the example problem if the vault door were unlocked (e.g., during certain working hours)?
3. Why are there only one or two adversaries for most penetrations of all types of barriers?
4. Would an adversary always choose the fastest penetration method?
5. Why are a variety of hand tools shown for some barriers but only very limited penetration equipment shown for the more substantial barriers?
6. What are some of the ways that a perimeter fenceline can be upgraded to increase the delay time for vehicles?
7. What are some of the ways that a perimeter fenceline can be upgraded to increase the delay time for adversaries on foot?

13.0 SUBGROUP SESSIONS

Session Title: 13.7 Entry-Control Systems Handbook Applications

Date: Friday, 7 December 1979

Presented By: Subgroup Instructors

Time: 0830 to 0930

Prior to Session:

Read the following portions of the Entry-Control Systems Handbook:*

1. Chapter 1;
2. Section 8.1, Chapter 8; and
3. Scan the remainder of the handbook.

All page citations in this session refer to the Entry-Control Systems Handbook.

Session Objectives:

After the session, the participants will be able to

1. Select generic equipment for personnel credentials,
2. Select generic equipment for personnel verification, and
3. Select generic equipment for detecting the following contraband:
 - a) Firearms, tools
 - b) SNM
 - c) Shielded SNM
 - d) Explosives

Summary:

Exercise problems will be worked to demonstrate how to use the information contained in the Entry-Control Systems Handbook.

*Additional Resource Material:

SAND77-1033, Entry-Control Systems Handbook

ENTRY-CONTROL SYSTEMS HANDBOOK APPLICATIONS

CONTENTS

	<u>Page</u>
I. Example Problem	13.7-5
II. Exercise 1	13.7-7
III. Exercise 2	13.7-9
IV. Instructional Guidelines	13.7-11
V. Think-About Items	13.7-15

I. EXAMPLE PROBLEM

Problem Definition

Choose entry-control equipment which can be used to satisfy the requirements given below, and locate the equipment in Figure 13.7-1.

Requirements

1. Access Control -- A maximum of 50,000 authorized users are assumed to employ a maximum of 100 access points. Access points will be separated from a central control station up to a maximum distance of 3 km. Anti-passback is required. A high/medium relative resistance to counterfeiting is required. Type I error rate must be less than 5 percent.
2. Throughput -- Single booth throughput must be at least six per minute, neglecting booth doors opening and closing times.

Figure 13.7-1. Entry-Control Booth

Answers

1. Credential System (p. 2.5-1) with magnetic card technique (Card Key Systems Model 880). This system meets capacity, distance, and anti-passback requirements but does not meet high/medium resistance to counterfeiting (p. 2.4-2, top).
2. Fingerprint or hand geometry technique meets high/medium resistance to counterfeiting (p. 3.1-3,4). Hand geometry technique meets Type-I error requirement (p. 3.7-5,6) and throughput requirement (Table 3.7-I, p. 3.7-4: 6.95 seconds verification time equals a throughput of 8.5 people per minute).
3. Credential readers are located outside the booth, and hand geometry equipment is located at detector position No. 1 in Figure 13.7-1.

II. EXERCISE 1

Problem Definition

Choose additional entry-control equipment which can be used to satisfy the requirements given below, and tentatively locate this equipment in Figure 13.7-1.

Requirements

Equipment chosen must

1. Be able to detect contraband dynamite,
2. Be able to detect pistol powder (with a minimum vapor/air ratio of 1/200) carried on a person, and
3. Be compatible with the six-persons-per-minute minimum throughput requirements of the example problem.

Note:

Use information and data from p. 6.2-5 through the middle of p. 6.2-14.

III. EXERCISE 2

Problem Definition

Choose additional entry-control equipment which can be used to satisfy the requirements given below, and tentatively locate this equipment in Figure 13.7-1.

Requirements

Equipment chosen must

1. Detect 100 grams or more of contraband steel, aluminum, brass, or lead carried on a person; and
2. Be compatible with the six-persons-per-minute minimum throughput requirements of the example problem.

Note:

Use information and data from pp. 5.2-13 through 5.2-16.

IV. INSTRUCTIONAL GUIDELINES

The material in the Entry-Control Systems Handbook is difficult to use even after the book has been carefully read. The amount of review with your group is highly dependent upon the material covered in the lectures. In some instances a particular chapter need be reviewed only to point out where information and data are located. The purpose of these chapter reviews is to identify what generic equipment is available for entry-control functions and to highlight performance characteristics and limitations of currently available equipment.

1. Review Chapter 1, Section 1.1, and point out shortcomings of most entry-control systems currently in use (middle of p. 1.1-2); 1.1.1, "Objectives" (top of p. 1.1-3); 1.1.2, "Types of Entry-Control Systems" (p. 1.1-3).
2. Briefly review remainder of Chapter 1, Sections 1.1.3 through 1.1.6.
3. Briefly review the following sections in Chapter 2, "Credentials;" 2.2, "Types of Credentials;" 2.3, "Coded Credential System Features;" and 2.4.4, "Resistance to Decoding and Counterfeiting."
4. Briefly review Sections 3.1.1.1, 3.1.1.2, and 3.1.1.3 in Chapter 3, "Personnel Identity Verification System." Point out that this chapter contains information relative to machine-aided manual systems and automated systems (i.e., positive personnel identity verification).
5. Continue review of Chapter 3: Section 3.1.2, "Definitions of Characteristics" (the first three characteristics); Section 3.1.2.1, "Verification Error Rates;" Section 3.1.2.2, "Resistance to Counterfeiting;" and Section 3.1.2.3, "Throughput Rate."
6. Continue review of Chapter 3: Section 3.2.1, "Video Comparator Systems" (general); Section 3.3, "Positive Personnel Identity Verification Systems;" and generic techniques (Sections 3.3.1 through 3.3.4).
Note: Point out that there is considerable detail and data on specific equipment which can be referred to later.
7. Briefly review Section 4.1, "General" (the first and third paragraph, page 4.1-1) in Chapter 4, "Special Nuclear Material Monitors." This chapter is relevant if the concern is theft of SNM. The third paragraph shows the relative SNM monitor sensitivity for U^{235} and P^{239} , both unshielded and shielded. If the concern is theft of SNM, consider metal shielding (sensors) located with SNM monitors.
8. Briefly continue to review Chapter 4, Sections 4.1.1 through 4.1.6, to indicate generic types of SNM monitors available.

9. Briefly review Section 5.1.1, "System Description," in Chapter 5 "Metal Detectors." Point out that passive systems are unsuitable for most applications and that only active systems are addressed in this chapter.
10. Briefly review Chapter 6, "Explosive Sensors:" Section 6.1.2, "Background;" and Section 6.1.2 "Chemistry and Physics of Explosives." Point out that discrimination (specificity) and sensitivity are usually more important than the kind of explosives (selectivity). Also review the following parts of Section 6.2, "Explosive Vapor Detection:" Section 6.2.1, "Methods of Vapor Collection" (difficult); and 6.2.2, "Electron Capture" (commercially available).
11. Briefly review Section 7.1 in Chapter 7, "Package Search Systems." (Equipment for contraband carried on people has already been covered. This chapter identifies equipment for contraband packages, etc.)
12. Briefly review Section 8.1 in Chapter 8 on the criteria for selection of entry control equipment. (Point out that some of the definitions are unique to the handbook, e.g., Detection applies to contraband and Security Level applies to the detection of unauthorized persons and resistance to counterfeiting of the identity verifier.
13. Step through the Example Problem with the subgroup. The answer sheet for the example problem does not give the rationale for the equipment chosen. The rationale follows:
 - a) Magnetic credential system provides controlled personnel access into and out of facility and provides computer interface needed for anti-passback. However, counterfeiting is easy.
 - b) Hand geometry meets the high/medium counterfeiting resistance (relative) requirement and provides positive identification. It also meets the Type-I error requirement of 5 percent (or less) and the throughput requirement.
 - c) Credential readers are normally located outside the booth and allow unlocking of the booth door (by one person at a time).
 - d) Hand geometry equipment is located inside the booth near the outer door, and if access is granted, the inner booth door is unlocked. (Exiting personnel pass SNM monitors before reaching hand geometry equipment.)
14. Let the subgroup work Exercise 1. Answers:
 - a) Table 6.2-V (p. 6.2-8) indicates that all vapor detectors will detect dynamite.
 - b) Three will detect pistol powder (Elscint EXD-2, Leigh-Marsland S-201, and Xonics GC-710).
 - c) Table 6.2-VI (p. 6.2-8) indicates that only the S-201 meets the throughput requirement.

- d) Pp. 6.2-10 and 6.2-11 indicate that the Leigh-Marsland S-301 (a modified S-201) is only one of two portal models available which meets the throughput requirement.
- e) Locate the explosive detector near the personnel identifier. (Vapor collection is best when the person is not moving.)

15. Let the subgroup work Exercise 2. Answers:

- a) Table 5.2-V (p. 5.2-13) indicates that the Solco IX equipment meets the detection requirement of 100 grams.
- b) Discuss detector sensitivity variation as a function of the sample orientation (Table 5.2-IV, p. 5.2-13) e.g., Metor 112 (Weapon Detector) has a 6:1 variation for steel depending on sample rod orientation.
- c) Discuss 5.2.2.2, "False Alarms" (p. 5.2-14) and how the data was generated; discuss the "map" of the Solco IX (Figure 5.2-17, p. 5.2-16, bottom right). I.e., a 1000-gram, right circular aluminum cylinder would generate an alarm if moved outside the booth but within 130 cm (~4 ft) of the front or back of the booth or within 30 cm (~1 ft) of the sides of the booth. (Metal detectors tend to be located near the center of the booth: detector position No. 2 in Figure 13.7-1.)
- d) Discuss Figure 5.2-12, "Internal Sensitivity Map of Solco IX Shielding Detector" (p. 5.2-15, bottom left). The detector is least sensitive in the middle and most sensitive near the outer edges. All booth-type metal detectors have different "maps" or variations that need to be determined.

V. THINK-ABOUT ITEMS

1. Why, if possible, should humans be removed from the identifying process for access control?
2. Why should portal doors, roof, walls, etc. provide a delay equivalent to the perimeter or building walls in which they are installed?
3. Why should portal doors be interlocked so that only one door can be unlocked and opened at one time?
4. Where would you locate enrollment, credential, and similar equipment?

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

13.0 SUBGROUP SESSIONS

Session Title: 13.8 Intrusion Detection Systems Handbook Applications Date: Monday, 10 December 1979

Presented By: Subgroup Instructors

Time: 1030 to 1200

Prior to session:

Read Chapters 1 and 2 and review Chapter 3, Intrusion Detection Systems Handbook (Vol. I).

Session Objectives:

After the session, the participants will be able to

1. Determine number and generic types of exterior sensors from the Intrusion Detection Systems Handbook for given threat tactics and environmental conditions, and
2. Determine the need for real-time assessment for a given detection area.

Summary:

A set of exercises will be worked to demonstrate the information contained in the Intrusion Detection Systems Handbook.

Additional Resource Materials:

SAND76-0554, Intrusion Detection Systems Handbook (Vol. I & II)

INTRUSION DETECTION SYSTEMS HANDBOOK APPLICATIONS

CONTENTS

	<u>Page</u>
I. Exercise 1	13.8-5
II. Exercise 2	13.8-9
III. General Instructional Guidelines	13.8-11
III.1 Exercise 1 Guidelines	13.8-13
III.2 Exercise 2 Guidelines	13.8-15
IV. Think-About Items	13.8-17

I. EXERCISE 1

Problem Definition

An intrusion sensor system is to be installed in the isolation zone between the two chain-link fences surrounding the hypothetical facility (see Figures 13.8-1 and 13.8-2). Choose a generic sensor type (or combination of types) which provides a high probability of sensing the intruder (described below). Estimate the false alarm rate, and sketch the placement of equipment on Figure 13.8-3.

Intruder -- The intruder can be expected to bridge the outer fence with a wooden stepladder, crawl through the isolation zone, and bridge the inner fence with another stepladder.

Environmental Data

1. The site frequently has the following weather conditions:
 - Wind speed greater than 50 km/h but less than 100 km/h, and
 - Snow accumulations less than 0.3 metre.
2. The isolation zone is inhabited with small animals and large birds.
3. Overhead high-voltage power lines (30 metres high) cross the perimeter in four places.

Figure 13.8-1. Hypothetical Facility

Figure 13.8-2. Simplified Plan View of Hypothetical Facility (not to scale)

Figure 13.8-3. Cross-Sectional View of Hypothetical Facility Perimeter Isolation Zone (not to scale)

II. EXERCISE 2

Problem Definition

A combination of sensors has been chosen for a perimeter sensor field to be installed in an isolation zone. The 2-km perimeter has been subdivided in 20 sectors, each 100 metres long. Each sector will include two different sensor types colocated to reduce individual sensor vulnerability. Given the data below, determine the minimum expected false alarm rate (FAR) per day for the sensor system.

Data

<u>Sensor</u>	<u>FAR/h*</u>
Microwave	1
Taut Wire	0.1

*Alarms/h/sensor; the alarms are uncorrelated.

Requirements

The two sensors in each sector are to be combined in a "AND" output; the time window is 2 minutes.

III. GENERAL INSTRUCTIONAL GUIDELINES

Volume I of the Intrusion Detection Systems Handbook contains information relative to intrusion sensors (exterior and interior); this volume will be used extensively during this session. Volume II contains information relative to (1) assessment, (2) alarm reporting, and (3) intrusion detection system integration.

1. Review Chapter 1, "Introduction:" Section 1.1, "Purpose," and Section 1.2, "Use of Handbook."
2. Review Chapter 2, Sections 2.1 and 2.2, thoroughly. Note: Section 2.2.2, "Sensors," discusses probability of detection, i.e., probability of a sensor alarm. It does not cover probability of assessment.
3. Review Chapter 2, Section 2.3, "System Design Considerations" (p. 2.3-1), parts 2.3.1 through 2.3.6 thoroughly; briefly review the remaining sections of this chapter. Note: The last sentence of Section 2.6, "Costs," is important.
4. Review Chapter 3, Section 3.1, "General" (p. 3.1-1), through part 3.2.1.6 (ends on p. 3.2-10).
5. Thoroughly review Chapter 3, Section 3.2.2, "Detection Equipment by Technological Type" (pp. 3.2-10 through 3.2-17). Note: These are generic sensors for exterior use.
6. Review Chapter 3, Section 3.3, "Interior Detection" (p. 3.3-1). Note: This section covers basic ways of sensing, i.e., Motion, Boundary, Penetration, and Proximity.
7. Briefly review Chapter 3, Sections 3.3.1 (p. 3.3-2) through 3.3.1.7 (p. 3.3-7).
8. Thoroughly review Chapter 3, Section 3.3.2, "Detection Equipment Selection by Technological Type" (p. 3.3-8). Note: This is a section on generic interior sensors and lacks no good summary tables. Familiarity with generic sensors is the purpose of this review.
9. Briefly review the tables of contents for Chapters 4 and 5 to illustrate that more detailed data for exterior and interior sensors can be found in these chapters.
10. Briefly review the Volume II contents, specifically Chapters 6, "Alarm Assessment Systems" (p. 6.0-1) and Chapter 7, "Alarm Reporting Systems" (p. 7.0-1). Note: This volume provides guidance for the selection of equipment and designs for CCTV assessment and alarm reporting systems, but does not present this information in a summary format.
11. Let the group work Exercise 1 and then Exercise 2. Specific instructional guidelines for both problems are attached.
12. Discuss think-about items.

III.1 EXERCISE 1 GUIDELINES

Purpose: This exercise allows the group to interpret, with your help, some of the information contained in Chapter 3.

1. All of the information needed to solve Exercise 1 is contained in Table 3.2-II (p. 3.2-12), Table 3.2-III (p. 3.2-15), and Table 3.2-IV (p. 3.2-16). Note: VL = very low, L = low, M = medium, and H = high.
 - a) The microwave or E-field (Table 3.2-III) indicate M-H detection (sensing) probability for crawling intruder (taut wires not shown, but are good for sensing crawling intruders).
 - b) Relative susceptibility to False Alarms (Table 3.2-IV):

	<u>Microwave</u>	<u>E-Field</u>	<u>Taut Wire</u>
Wind	VL	L	VL
Small animals	L-H	M-H	VL
Large birds	H	M	L
Snow	L-M	L-M	L
Overhead power lines	VL	L	VL

2. The small animals would cause a high FAR for a microwave or E-field system. (The FAR given is relative.)
3. Choose microwave or E-field and taut wire. Connected for AND output, i.e., both sensors must alarm to display a signal.
4. Have the group sketch a cross section of the sensor placement between fences.
5. Discuss Figure 3.2-4 (p. 3.2-18) and discuss the correct placement of sensors. Colocation reduces individual vulnerability.
6. Discuss detection:
 - a) These sensors have a high probability of sensing a crawling intruder.
 - b) What might happen if an intruder ran through the sensor field and climbed the inner fence (without a ladder)?

Assume guard arrives in 2 minutes (from 13.1, "Hypothetical Facility Data," in this workbook). Does detection occur? Probably not. Note: This should point out the need for some method for real-time assessment: either immediate (guard looking from a fixed position) or CCTV.

III.2 EXERCISE 2 GUIDELINES

Purpose: This exercise allows the group to interpret some information in Chapter 3 relative to the False Alarm Rate (FAR).

1. All of the information to solve Exercise 2 is contained in Table 3.2-V (p. 3.2-20). Note: The point to be made is that the data contained in this table represent one sector of sensors. (The problem shows 20 sectors.)
2. The second row of the table shows the individual sensor FARs of 1 and 0.1.
3. The third column indicates the time window.
4. The fourth column indicates that the FAR for the two sensors combined for an AND output is 0.003 (with a 2-minute time window, T).
5. The 0.003 alarm/h is for one sector.
 $0.003 \text{ alarm/h} \times 24 \text{ h/day} \times 20 \text{ sectors/sensor system} = 1.44 \text{ alarms/day (FAR)}.$
6. Point out that this minimum expected alarm rate is possibly acceptable.
7. Change the data so that each sensor has an FAR of 1 alarm/h. The first row is used; for the same time window, the FAR for one sector is 0.03 alarms/h.
 $0.03 \text{ alarm/h} \times 24 \text{ h/day} \times 20 \text{ sectors/sensor system} = 14.4 \text{ alarms/day}.$
8. Discuss what might happen as the FAR increases.

IV. THINK-ABOUT ITEMS

1. What are some of the advantages for combining sensor outputs into an AND configuration?
2. What are some of the disadvantages for combining sensor outputs into an AND?
3. What are some of the advantages for using sensor outputs in an OR configuration?
4. What are some of the disadvantages?
5. Why should field testing of sensors be performed at the site where the sensors may be used in a system?
6. When are false alarms considered excessive?
7. Does a high probability of intrusion sensing always provide high assurance of detection?

13.0 SUBGROUP SESSIONS

Session Title: 13.9 Application of Estimate of Adversary Sequence Interruption (EASI) Analysis Date: Tuesday, 11 December 1979
Presented By: Subgroup Instructors Time: 1000 to 1200

Session Objectives:

After the session, the participants will be able to

1. List the data which are needed as input for an Estimate of Adversary Sequence Interruption (EASI) analysis,
2. Enter a program from a magnetic card into the TI-59 calculator memory,
3. Enter the data for EASI analyses,
4. Make sensitivity studies by changing data, and
5. Present results of analysis using two-dimensional curves.

Summary:

The EASI method of evaluation is based on the interaction of the physical protection system (PPS) elements of detection, delay, communication, and response. The result of this evaluation is an estimate of the probability of adversary sequence interruption for one scenario. This process is repeated until the analyst is confident that an evaluation of all critical paths into and out of the facility is performed.

Note: Study "Hand-Held Calculator Operation--Overview" and "EASI Analysis" in this session (with TI-59) prior to Subgroup Session.

Additional Resource Materials:

SAND78-0506, EASI Program Improvements for HP-67 and TI-59 Calculators.

APPLICATION OF ESTIMATE OF ADVERSARY SEQUENCE INTERRUPTION (EASI) ANALYSIS

CONTENTS

	<u>Page</u>
I. Hand-Held Calculator Operation--Overview	13.9-5
II. EASI Analysis	13.9-9
III. Exercise 1	13.9-11
IV. Exercise 2	13.9-19
V. Exercise 3	13.9-23
VI. Instructional Guidelines	13.9-25
VII. Think-About Items	13.9-27

I. HAND-HELD CALCULATOR OPERATION — OVERVIEW

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 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.

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 $\boxed{CLR}$ 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 $\boxed{CLR}$ key does not have to be used after the performance of calculations ending the $\boxed{=}$ key. After using the $\boxed{=}$ 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 labeled 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** **OP** **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** **OP** **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.

Data Entry

The Estimate of Adversary Sequence Interruption (EASI) program uses all of the user-defined keys. The following inputs or functions are performed by the indicated user keys.

- [2ND] [A'] Probability of communication, P_C
 [2ND] [B'] Average time required for response, T_R
 [2ND] [C'] Standard deviation of response time, σT_R
 [2ND] [D'] Number of tasks along path being analyzed
 [2ND] [E'] Program initialization, i.e., reset to begin a new problem
 [A] Probability of detection at beginning of an adversary task, P_D
 [B] Average time required for an adversary task, T_i
 [C] Standard deviation of a task time, σT_i
 [D] Number of a task to be changed or recalled
 [E] Execution of the computation command

Data is entered into the calculator in the following sequence:

1. Initialize the program by pressing [2ND] [E'] ,
2. Enter the response data by pressing keys [A'] , [B'] , and [C'] ,
3. Enter the number of tasks along the path by using key [D'] ,
4. Enter each adversary task in sequence by pressing keys [A] , [B] , and [C] , and
5. Perform the calculation of the probability of interruption after the last task is entered by pressing key [E] .

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 13.9-1).

<div style="display: flex; justify-content: space-between; align-items: center;"> <div>1 </div> <div> TEXAS INSTRUMENTS </div> <div>1</div> </div>					
EASI			9 OP 17 (239.89)		
P_C	T_R	σT_R	NO. TASKS	INITIALIZE	SECOND FUNCTION
P_D	T_i	σT_i	CHANGE NO.	EXECUTE	

Figure 13.9-1. Estimate of Adversary Sequence Interruption (EASI) Program Card

Testing the Program

After successfully reading the program card, the program and calculator can be tested for proper functioning by entering the data as shown in Table 13.9-I. If the program is functioning properly, the display should show the indicated number.

TABLE 13.9-I
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] (insert card)	0 then 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']	0.04
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 interruption	[F]	.8099375572

II. EASI ANALYSIS

Steps in EASI Analysis

It is assumed that the physical and operational characteristics of the facility are known in sufficient detail to identify potential targets. The steps for performing an EASI analysis are to

1. Postulate adversary action sequence directed toward identified targets,
2. Identify specific paths corresponding to the selected adversary action sequences,
3. Estimate the probability of communication (the capability to inform the security force that an intrusion or alarm has occurred),
4. Estimate the mean and standard deviation of the security force response time,
5. Determine the location of sensors and delay features in the paths,
6. Estimate the probability of detection for each sensor in the paths,*
7. Estimate the mean and standard deviation of the time required for the adversary to perform each task along the chosen path,
8. Enter the data for a selected path into the calculator and obtain the probability of interruption versus guard response time, and
9. Examine the sensitivity of the physical protection system to changes in response time, probability of detection, and changes in delay times, and determine the impact of these changes upon the probability of interruption.

*In the EASI program, detection occurs at the start of a task.

III. EXERCISE 1

The goal of the adversaries in this scenario is sabotage which will result in loss of coolant and core meltdown. The event selected for this scenario, which will cause loss of coolant, is the cutting of the lines feeding coolant to the reactor core.

The protection system for the facility consists of an outer fence, a 15-metre isolation area in which a sensor system is installed, personnel and vehicle access control portals in the perimeter, and intrusion sensors on all outer emergency doors and Vital Area doors. Alarms are annunciated and displayed in the personnel access control building. The normal complement of guards for the facility is seven: the shift supervisor, three guards full-time at the personnel and vehicle access portal, one guard on patrol of the area, and two guards for escort duty. During the night shifts, the guard force is reduced to four: the shift supervisor, two guards at the personnel and vehicle access portal, and the area patrol guard. Voice communication between the guards in the access control portal and the patrol and response guards is by radio. The response time of off-site forces is 7 minutes.

The adversaries are equipped with automatic weapons, grenades, explosives and hand and power tools.

The path selected for evaluation is shown on Figures 13.9-2 and 13.9-3. The sequence of events begins with penetration of the outer perimeter fence and ends with setting of the explosive devices on the targets in the vital area.

In this scenario, the adversaries' targets are the two coolant lines located in the reactor building, level 2, compartment 1 (RB-2-1). The adversaries enter the area in the southeast quadrant of the facility and run to an emergency door near the southwest corner of the auxiliary building. The emergency door is penetrated and the adversaries then move to the containment building personnel hatch. This door is penetrated and the adversaries move to their targets and set the explosive charges (primer-cord).

The input data for Exercise 1 are shown in Figure 13.9-4, and the steps for entering it into the TI-59 are shown in Table 13.9-II. A plot of the probability of adversary sequence interruption versus response force time is shown in Figure 13.9-5.

Figure 13.9-2. Reactor Facility with Path

Figure 13.9-3. Containment Building with Path

Figure 13.9-4. Adversary Time-Sequence Path

With the given input information, the estimate of adversary interruption is calculated as shown in Table 13.9-II.

TABLE 13.9-II
Program Steps for Example 1

Step	Procedure	Press (in order)	Display
1	Turn TI-59 on	(Slide-switch on)	0
2	Repartition memory	9 2ND OP 1 7	239.89
3	Clear display	CLR	0
4	Enter program card	-	1.
5	Initialize program	2ND E'	0
6	Enter P_C	0 . 9 2ND A'	0.9
7	Enter T_R	7 2ND C'	7.0
8	Enter σT_R	1 . 5 2ND C'	1.5
9	Enter number of tasks	14 2ND D'	14
10	Enter T_1	. 2 B	0.20
11	Enter σT_1	. 0 4 C	0.04 then 2
12	Enter T_2	. 0 3 B	0.03
13	Enter σT_2	. 0 1 C	0.01 then 3
14	Enter P_{D3}	. 9 A	0.9
15	Enter T_3	. 0 7 B	0.07
16	Enter σT_3	. 0 1 C	0.01 then 4
17	Enter T_4	. 2 B	0.2
18	Enter σT_4	. 0 4 C	0.04 then 5

Table 13.9-II (Continued)

Step	Procedure	Press (in order)	Display
19	Enter T_5	<input type="button" value="."/> <input type="button" value="6"/> <input type="button" value="B"/>	0.60
20	Enter σT_5	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="C"/>	0.10 then 6
21	Enter T_6	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="5"/> <input type="button" value="B"/>	0.05
22	Enter σT_6	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="1"/> <input type="button" value="C"/>	0.01 then 7
23	Enter P_{D7}	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	0.9
24	Enter T_7	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="5"/> <input type="button" value="B"/>	0.15
25	Enter σT_7	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="3"/> <input type="button" value="C"/>	0.03 then 8
26	Enter T_8	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="B"/>	0.10
27	Enter σT_8	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="2"/> <input type="button" value="C"/>	0.02 then 9
28	Enter T_9	<input type="button" value="2"/> <input type="button" value="B"/>	2
29	Enter σT_9	<input type="button" value="."/> <input type="button" value="4"/>	0.4 then 10
30	Enter P_{D10}	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	0.9
31	Enter T_{10}	<input type="button" value="."/> <input type="button" value="5"/> <input type="button" value="B"/>	0.5
32	Enter σT_{10}	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="C"/>	0.1 then 11
33	Enter P_{D11}	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	0.9
34	Enter T_{11}	<input type="button" value="1"/> <input type="button" value="."/> <input type="button" value="5"/> <input type="button" value="B"/>	1.5
35	Enter σT_{11}	<input type="button" value="."/> <input type="button" value="3"/> <input type="button" value="C"/>	0.3 then 12
36	Enter P_{D12}	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	0.9
37	Enter T_{12}	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="5"/> <input type="button" value="B"/>	0.05
38	Enter σT_{12}	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="1"/> <input type="button" value="C"/>	0.01 then 13
39	Enter P_{D13}	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	0.9
40	Enter T_{13}	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="5"/> <input type="button" value="B"/>	0.15
41	Enter σT_{13}	<input type="button" value="."/> <input type="button" value="0"/> <input type="button" value="3"/> <input type="button" value="C"/>	0.03 then 14
42	Enter T_{14}	<input type="button" value="."/> <input type="button" value="5"/> <input type="button" value="B"/>	0.5
43	Enter σT_{14}	<input type="button" value="."/> <input type="button" value="1"/> <input type="button" value="C"/>	0.1 then 14
44	Execute the computation	<input type="button" value="E"/>	0.20223

The probability of interruption of this path is approximately 0.20. The probability of interruption versus response time for Exercise I is shown in Figure 13.9-5.

Figure 13.9-5. Probability of Interruption versus Response Time

Exercise 1 Data

Table 13.9-III gives the input data for Exercise 1.

TABLE 13.9-III

Security Force Response Time 7 minutes
Standard Deviation 1.5 minutes
Probability of Communication 0.9

Task Number	Adversary Task	Probability of Detection	Adversary Task Time (minutes)	Standard Deviation
1	Defeat outer fence	0	0.20	0.04
2	Cross isolation zone to sensor 1	0	0.03	0.01
3	Cross isolation zone (20 m)	0.9	0.07	0.01
4	Defeat inner fence	0	0.20	0.04
5	Travel to auxiliary building emergency door (150 m)	0	0.60	0.10
6	Begin attack on emergency door	0	0.05	0.01
7	Defeat emergency door	0.9	0.15	0.03
8	Travel to containment building personnel hatch (20 m)	0	0.10	0.02
9	Defeat personnel hatch door No. 1	0	2.0	0.40
10	Begin attack on personnel hatch door No. 2	0.9	0.50	0.10
11	Defeat personnel hatch door No. 2	0.9	1.50	0.30
12	Start travel to targets	0.9	0.05	0.01
13	Travel to targets (20 m)	0.9	0.15	0.03
14	Set charges	0	0.50	0.10

Probability of Interruption equals ~ 0.20 .

The effect of (1) changing the task time for tasks 6 and 7 (defeat emergency door) from 0.05 and 0.15 to a combined 1.7 minutes, (2) changing the P_D for task 7 to 0, and (3) changing the P_D for task 8 from 0 to 0.9 can be examined by performing the following steps:

Step	Procedure	Key(s) Pressed (in order)	Display
1	Change to task 6	[6] [D]	6.
2	Enter T_6	[1] [.] [7] [B]	1.7
3	Enter σT_6	[.] [3] [5] [C]	0.35 then 7

<u>Step</u>	<u>Procedure</u>	<u>Key(s) Pressed (in order)</u>	<u>Display</u>
4	Enter P_D	<input type="button" value="0"/> <input type="button" value="A"/>	0
5	Enter T_7	<input type="button" value="0"/> <input type="button" value="B"/>	0
6	Enter σT_7	<input type="button" value="0"/> <input type="button" value="C"/>	0 then 8
7	Enter P_D	<input type="button" value="."/> <input type="button" value="9"/> <input type="button" value="A"/>	.9
8	Execute computation	<input type="button" value="E"/>	~0.50

The effect of changing the security force response time and standard deviation can be examined in a similar manner. Assume that the response time is changed from 7 minutes to 5 minutes and that the standard deviation is changed from 1.5 minutes to 1 minute.

<u>Step</u>	<u>Key(s) Pressed (in order)</u>	<u>Display</u>
1	<input type="button" value="5"/> <input type="button" value="2ND"/> <input type="button" value="B"/>	5.
2	<input type="button" value="1"/> <input type="button" value="2ND"/> <input type="button" value="C"/>	1.
3	<input type="button" value="E"/>	0.85

IV. EXERCISE 2

In this exercise, the group is requested to use the furnished data to construct an adversary time-sequence diagram, enter the data into the calculator, and obtain the answer in terms of probability of interruption versus security force response time.

The adversaries' target is the diesel generators located in level 1 (basement) of the control and diesel generator building. The objective of the adversaries is to cause a core meltdown by removing all sources of electrical power to the facility. The adversaries first cause loss of off-site power by blowing up a transmission line tower and then forcing their way into the diesel generator building and destroying the generators. The adversary path to accomplish this goal is shown in Figure 13.9-6. The input data for the example are shown in Table 13.9-IV. A plot of the probability of adversary sequence interruption versus response force time is shown in Figure 13.9-7.

Figure 13.9-6. Adversary Path to Control Room and Diesel Generator Room

TABLE 13.9-IV

Input Data For Example 2

Security Force Response Time 5.0 minutes
 Standard Deviation 1.0 minutes
 Probability of Communication 0.90

<u>Task Number</u>	<u>Adversary Task</u>	<u>Probability of Detection</u>	<u>Adversary Task Time (Minutes)</u>	<u>Standard Deviation</u>
1	Defeat outer protected area fence	0	0.20	0.04
2	Cross area between outer and inner protected area fences (30 metres)	0.90	0.15	0.03
3	Defeat inner protected area fence	0	0.20	0.04
4	Travel to control and diesel generator building (15 metres)	0	0.08	0.02
5	Defeat control room emergency door	0.90	0.75	0.15
6	Move to diesel generator room (60 metres)	0.90	0.35	0.07
7	Set shaped charges on turbines	0.90	0.50	0.10
8	Return to emergency door	0.90	0.35	0.07
9	Exit control and diesel generator building	0.90	0.03	0.006
10	Exit protected area	0.90	0.55	0.10

Figure 13.9-7. Probability of Adversary Sequence Interruption, Exercise 2

V. EXERCISE 3

This example will be developed by your group with the assistance of your instructor. You may wish to use a similar path to that contained in Exercise 1 or you may wish to analyze a path of your own choosing. A blank time line is included below for your convenience.

Figure 13.9-8. Blank Adversary Path Time-Line

List your assumptions regarding the facility; i.e., all factors that will influence the adversary sequence that you chose.

VI. INSTRUCTIONAL GUIDELINES

1. Materials furnished to the students will include
 - EASI Application, pp. 13.9-9 to 13.9-24.
 - TI-59 calculator with EASI Program Card
 - Diagrams of Hypothetical Facility (for Exercise 2)
2. Copies of "Things to Think About" sufficient for each student will be in the instructor packet.
3. If necessary, the initial exercise using the TI-59 calculator can be the example used during the lecture period. The student will already have a copy of this exercise in his notes.
4. A quick review or discussion of the notes contained in the "overview" section is suggested. However, this was covered during the lectures.
5. The answer to the question at the end of Exercise 1 is $P_I = .2547...$
6. One point not covered in detail in the EASI manuals is that of sensor alarm assessment. This time can sometimes be significant and is included in the response time. The time line in Figure 13.9-9 illustrates a typical response time breakdown.

Figure 13.9-9. Typical Response Time Breakdown

Response time is more than the travel time after the communication is received.

VII. THINK-ABOUT ITEMS

1. What are the advantages of using the EASI analysis method?
2. What are the disadvantages of using EASI?
3. Explain how you might determine the following:
 - 3.1 Probability of communication
 - 3.2 Probability of detection
 - 3.3 Task times and standard deviations of task times
 - 3.4 Response time and standard deviation of response time
4. What different tactics might the response force employ?
5. Explain why a facility might be judged vulnerable to a particular threat even though EASI calculations show a high probability, of interruption.
6. Which are more important in a physical protection system--detection, delay, communications, or response? Why?
7. How does EASI demonstrate the interdependence of these system parameters?
8. Can EASI demonstrate the vulnerability of a system? Explain.
9. Explain why a facility might be judged vulnerable to a particular adversary sequence even though detection is accomplished with high assurance.
10. Why is assessment of an alarm included in the response time?

APPENDIX B

Improved EASI Program Listing for TI-59

Slide the ON-OFF switch to the ON position, repartition the data memory by pressing 9 2nd Op 1 7, press LRN, and then key in the following:

<u>Key</u>	<u>Display</u>		<u>Key</u>	<u>Display</u>	
LBL	000	76	20	027	20
A	001	11	RCL	028	43
ST*	002	72	00	029	00
02	003	02	R/S	030	91
R/S	004	91	LBL	031	76
LBL	005	76	E'	032	10
B	006	12	CMS	033	47
ST*	007	72	CLR	034	25
03	008	03	R/S	035	91
R/S	009	91	LBL	036	76
LBL	010	76	B'	037	17
C	011	13	STO	038	42
ST*	012	72	05	039	05
04	013	04	R/S	040	91
PAU	014	66	LBL	041	76
RCL	015	43	C'	042	18
00	016	00	X ²	043	33
EQ	017	67	STO	044	42
00	018	00	06	045	06
30	019	30	R/S	046	91
OP	020	69	LBL	047	76
23	021	22	A'	048	16
OP	022	69	STO	049	42
23	023	23	07	050	07
OP	024	69	R/S	051	91
24	025	24	LBL	052	76
OP	026	69	D'	053	19

NOTE: Key code taken from printer listing. For actual key sequence see TI-59 Owner's Manual, Page VI-6.

<u>Key</u>	<u>Display</u>	
STO	054	42
01	055	01
X $\Rightarrow$ T	056	32
2	057	02
5	058	05
INV	059	22
GE	060	77
09	061	09
59	062	59
1	063	01
3	064	03
STO	065	42
02	066	02
+	067	85
RCL	068	43
01	069	01
=	070	95
STO	071	42
03	072	03
+	073	85
RCL	074	43
01	075	01
=	076	95
STO	077	42
04	078	04
1	079	01
STO	080	42
00	081	00
R/S	082	91
LBL	083	76
E	084	15
STF	085	86
01	086	01
RCL	087	43
01	088	01

<u>Key</u>	<u>Display</u>	
GTO	089	61
D	090	14
INV	091	22
STF	092	86
01	093	01
0	094	00
STO	095	42
08	096	08
STO	097	42
09	098	09
STO	099	42
10	100	10
RC*	101	73
03	102	03
SUM	103	44
09	104	09
RC*	105	73
04	106	04
X ²	107	33
SUM	108	44
08	109	08
RCL	110	43
07	111	07
x	112	65
RC*	113	73
02	114	02
=	115	95
STO	116	42
11	117	11
CP	118	29
EQ	119	67
01	120	01
75	121	75
RCL	122	43
08	123	08

<u>Key</u>	<u>Display</u>	
+	124	85
RCL	125	43
06	126	06
=	127	95
$\sqrt{x}$	128	34
1/X	129	35
x	130	65
(	131	53
RCL	132	43
09	133	09
-	134	75
RCL	135	43
05	136	05
)	137	54
x	138	65
1	139	01
.	140	93
7	141	07
=	142	95
INV	143	22
LNx	144	23
(	145	53
STO	146	42
12	147	12
$\div$	148	55
(	149	53
1	150	01
+	151	05
RCL	152	43
12	153	12
)	154	54
)	155	54
x	156	65
RCL	157	43
11	158	11

<u>Key</u>	<u>Display</u>	
=	159	95
+	160	85
RCL	161	43
10	162	10
x	163	65
(	164	53
1	165	01
-	166	75
RCL	167	43
11	168	11
)	169	54
=	170	95
STO	171	42
10	172	10
PAU	173	66
PAU	174	66
INV	175	22
DSZ	176	97
00	177	00
01	178	01
89	179	89
OP	180	69
32	181	32
OP	182	69
33	183	33
OP	184	69
34	185	34
GTO	186	61
01	187	01
01	188	01
RCL	189	43
10	190	10
R/S	191	91
LBL	192	76
D	193	14

Key	Display
STO	194 42
00	195 00
+	196 85
1	197 01
2	198 02
=	199 95
STO	200 42
02	201 02
+	202 85
RCL	203 43
01	204 01
=	205 95
STO	206 42
03	207 03
+	208 85
RCL	209 43
01	210 01
=	211 95
STO	212 42
04	213 04

Key	Display
IFF	214 87
01	215 01
00	216 00
91	217 91
RCL	218 43
01	219 01
X $\Rightarrow$ T	220 32
RCL	221 43
00	222 00
R/S	223 91
RC*	224 73
02	225 02
R/S	226 91
RC*	227 73
03	228 03
R/S	229 91
RC*	230 73
04	231 04
R/S	232 91

USER DEFINED KEYS			DATA REGISTERS			
A	$P(d_i)$		0	Current task no.	10	$P(I)$
B	$E(t_i)$		1	Total no. of tasks (n)	11	$P(A_i)$
C	$\sigma(t_i)$		2	Register index $P(d_i)$	12	Used
D	Task no. for data change		3	Register index $E(t_i)$	13	$P(d_i)$
E	Execute program		4	Register index $\sigma(t_i)$	13+n	$E(t_i)$
A'	$P(C)$		5	$E(t_r)$	13+2n	$\sigma(t_i)$
B'	$E(t_r)$		6	$Var(t_r)$		
C'	$\sigma(t_r)$		7	$P(C)$		
D'	Total task no. (n)		8	$\sum Var(t_i)$		
E'	Initialize		9	$\sum E(t_i)$		
FLAGS	USED	1	2	3	4	5

Physical Protection of Nuclear Facilities and Materials

INTERNATIONAL TRAINING COURSE

13.0 SUBGROUP SESSIONS

Session Title: 13.10 Physical Protection
System Applications I

Date: Tuesday, 11 December 1979

Presented By: Subgroup Instructors

Time: 1330 to 1430
1500 to 1600

Session Objectives:

After the session, the participants will be able to

1. Illustrate the design/analysis cycle for the detection function by use of the hypothetical facility given an outsider threat and a zone associated with the site outer boundary,
2. Discuss the association of site features to applicable generic logic trees,
3. Discuss evaluation of positive measures for detection,
4. Discuss the design/analysis cycle as it relates to obtaining positive measures for the detection function, and
5. Apply selected generic logic trees.

Summary:

The objectives are accomplished by the use of the hypothetical facility. An outer boundary zone is developed for the physical protection system (PPS). Only the outsider threat is considered for this example. A high degree of class participation is encouraged so that the class can become more familiar with the material presented.

PHYSICAL PROTECTION SYSTEM APPLICATIONS I

CONTENTS

	<u>Page</u>
I. Problem Definition	13.10-5
II. Perimeter Boundary Problem General Data and Guidelines	13.10-7
III. Instructional Guidelines*	13.10-17
IV. Think-About Items	13.10-19

*To be distributed at the end of the session for reference material.

I. PROBLEM DEFINITION

For this exercise, the zone starts and ends at the site perimeter boundary, as depicted in Figure 13.10-1. The adversary attack mode may utilize any of the attributes listed in Section II.1. This exercise will address only the detection function for the defined zone.

The class participants are expected to

1. Identify potential detection elements and features for the various events given in the STEALTH-BOUNDARY and DECEIT-BOUNDARY generic logic trees,
2. Qualitatively assess the features identified on the prepared STEALTH-BOUNDARY and DECEIT-BOUNDARY generic logic trees for their ability to provide positive measure for the detection function,
3. Identify events that require additional features, and provide these features, and
4. Reassess the zone features until they agree that positive measures are provided for the detection function against the defined threat structure.

II. PERIMETER BOUNDARY PROBLEM GENERAL DATA AND GUIDELINES

Contents	<u>Page</u>
II.1 Threat Structure -- Outsiders	13.10-9
II.2 Problem Guidelines	13.10-9
II.3 Site Graphic	13.10-9
II.4 Top-Level Logic Trees	13.10-9
II.5 Applicable Site Features	13.10-15

II.1 Threat Structure—Outsiders

1. Attributes

- a) Number -- Six to eight
- b) Arms -- Automatic weapons
- c) Transportation -- Foot, surface vehicles, helicopters
- d) Equipment -- Hand-held portable power tools, explosives
- e) Knowledge -- Detailed information
- f) Training -- Detailed preplanning, rehearsals, military background, technical knowledge
- g) Dedication -- High

2. Tactics

- a) Deceit -- Submit to the system
- b) Stealth -- Covert
- c) Force -- Overt

3. Intent -- Disablement of vital targets selected by the threat so that core melt and radiological release is likely.

II.2 Problem Guidelines

The goal is high assurance that an outsider (up to eight) threat which is attempting sabotage is detected at perimeter boundary zone.

The assumptions are that

- 1. Threat attributes, tactics, and intent are as given;
- 2. Detection, delay, communication, and response are the only necessary PPS functions;
- 3. This exercise is limited to the detection function only;
- 4. Outsider adversary actions prior to entry into the zone are undetected;
- 5. The adversary wins if detection does not occur when he is entering the zone;
- 6. Guards are well-trained, well-equipped, etc.; and
- 7. The PPS should be effective at all times.

II.3 Site Graphic

Figure 13.10-1 is the site graphic used in this problem.

II.4 Top-Level Logic Trees

Figures 13.10-2 and 13.10-3 are the top-level logic trees used in this problem.

Figure 13.10-1. Site Graphic with Perimeter Zone

Figure 13.10-2. Defeat PPS Zone Detection Function

NOTES:

1. THE STEALTH-BOUNDARY LOGIC TREE IS APPLICABLE TO A PERIMETER ZONE FOR DETECTION.
2. THE DECEIT BOUNDARY GENERIC LOGIC TREE IS APPLICABLE TO A PERIMETER ZONE FOR DETECTION.
3. USUALLY DETECTION OF FORCE TACTICS IS BOUNDED BY STEALTH TACTICS

Figure 13.10-3. Defeat Zone Detection Function

II.5 Applicable Site Features

The STEALTH-BOUNDARY and DECEIT-BOUNDARY generic logic trees are used mainly in this PPS Applications I Problem. These two generic trees, plus the FORCE-BOUNDARY tree, are provided. Written on these trees, beside or under primary events, are identified PPS elements and features. The circled or marked elements on the stealth and deceit trees are assumed to exist for the example problem.

Whether or not elements and features assumed to exist provide positive measures for detection against the defined outsider threat is left as a class exercise. Selection of positive measures if deficiencies are detected is also left as a class exercise.

Copies of the marked-up generic logic trees for PPS Applications I can be found in the pocket at the back of this book. The following list highlights assumed PPS elements and features that relate to detection at the perimeter boundary.

Perimeter

1. Two chain-link fences (2.5 metres high) separated by a 30-metre isolation zone surround the facility.
2. The minimum lighting in the isolation zone is 0.2 foot-candle (0.22 lumens/m²).
3. A single (combination personnel/vehicle) entrance/exit point is located in the middle of the west fenceline.
4. The perimeter fenceline is 2 km long.

Perimeter Personnel/Vehicle Entrance/Exit (and Central Alarm Facility)

1. The entrance/exit is manned 24 hours per day by at least two guards.
2. Two vehicle gates (with one gate always closed) provide an area within which guards search vehicles. The gates are heavily reinforced with pipe.
3. A personnel turnstile (2.5 metres high) controls pedestrian traffic.
4. Access is permitted to personnel with badge credentials.
5. All building and interior intrusion sensors annunciate and are displayed individually.

Secondary Alarm Facility

1. This facility is located in the reactor building control room.
2. All building and interior intrusion sensors annunciate and are displayed individually in the reactor building control room.
3. Only operational personnel are in the control room.
4. Control room personnel can authorize other personnel into facility (with a guard escort).

Detection System

1. Sensors

- a) A guard is posted at the perimeter entrance.
- b) A guard is posted at the reactor building entrance.
- c) All other building exterior doors are locked and have magnetic door switch sensors.
- d) One roving guard routinely patrols outside the buildings and checks building exterior doors and the inner perimeter fenceline once every 2 hours. The building checks take 1.5 hours, and walking the inner fenceline takes 0.5 hour.
- e) The outer personnel airlock door into the reactor is locked and has a magnetic door switch sensor. Space intrusion sensors are located in the airlock.

2. Intrusion Alarm Annunciation and Display

- a) There are audio and visual displays at the main perimeter gate station.
- b) There are audio and visual displays in the reactor control room.
- c) All guards can send a silent duress call with their transceivers.

3. Intrusion Alarm Assessment

- a) The roving guard patrol is sent to assess the cause of an exterior door intrusion alarm.
- b) Operational personnel are sent to assess intrusion door and space alarms at and within the reactor containment building.

III. INSTRUCTIONAL GUIDELINES

1. Read and discuss the "Objectives and Summary" and the "Problem Definition."
2. Discuss the general data.
 - a) The threat structure relates to a moderate outsider threat.
 - b) Problem guidelines define the design goal and the assumptions.
 - c) Using the site graphic (Figure 13.10-1), reinforce the visual understanding of what is meant by a boundary zone as a physical protection system concept. Note that the zone consists of
 - The perimeter fence region including the perimeter fences, the region between the fences, and a nominal region extending above, below, and beyond the fenced region;
 - An air-space region or canopy covering the facility site and extending down to the fenced region; and
 - A below-ground envelope under the site connecting with the fenced region.
 - d) Briefly review the top logic trees. Note the following:
 - Figure 13.10-2 -- We will study detection only in the PPS perimeter zone. Positive measures are required for an adequate design.
 - Figure 13.10-3 -- The stealth and deceit perimeter generic logic trees will mainly be used for detection.
 - e) Site features -- focus on detection associated with the site boundary.
3. Present the perimeter stealth generic logic tree without PPS elements.
 - a) Briefly review its aspects, which are that
 - The adversary can attack the homogeneous part of the boundary;
 - The adversary can attack the discontinuities such as portals, gates, shipping/receiving buildings, etc.; and
 - The adversary goal is to get through undetected.
 - b) Brainstorm parts of the tree; i.e., using the tree, solicit PPS elements that can prevent the adversary from accomplishing the selected event. Focus on detection elements for the boundary, not at the entrance (SX5-10, SX5-20, SX5-30), and detection elements at personnel entrance (input events for SX5-50 and S5-60).
 - c) Select other events as indicated by the participants.
4. After some number of elements are identified and written beside the applicable events that they influence, present the prepared stealth generic logic tree. Note the marked or circled elements are the ones it is assumed the example PPS has.
 - a) For each event, qualitatively assess the ability of the assumed PPS elements to detect the design threat. Indicate which events have positive measures.

- b) Evaluate the ability to detect all adversary options for penetration of the boundary by stealth. Indicate whether or not the PPS zone as defined has positive measures for the detection function.
 - c) Redesign the PPS by adding additional elements and features until the PPS is judged to have positive measures for the detection function.
- 5. Present the prepared deceit logic tree and discuss it. Note that the marked or circled elements are the ones it is assumed the example PPS has incorporated.
 - a) Assess the detection function against the design (outsider) threat if deceit tactics were used.
 - b) Add additional elements or features as required until the PPS is judged to have positive measures for detection of deceit tactics.
 - 6. Summarize the exercise and draw conclusions.
 - 7. Distribute the instructional guidelines and the think-about items.
 - 8. Discuss the think-about items.

IV. THINK-ABOUT ITEMS

1. Why may multiple sensors be required to assure that an alarm occurs?
2. Should multiple sensors be colocated? What does colocated mean?
3. Is "real-time" assessment required and why is assessment considered part of detection?
4. Should some minimum delay be colocated with the sensor field of view? Why?
5. Why are either entering or departing vehicles difficult to search for contraband?
6. What are the relationships, if any, between the threat attributes and the level of training, motivation, and equipment required by the guards for detection?
7. Is it legitimate to assess detection for stealth and deceit tactics and not for force tactics? Discuss.
8. How do I know the PPS elements and features are actually functioning as assessed?
9. Are hardware-intensive systems more or less desirable than people-intensive systems for the detection function?
10. What changes, if any, in the threat structure would be sufficient to defeat the assumed detection features for the PPS zone?
11. What changes in the threat structure would be sufficient to defeat the detection features for the redesigned PPS zone?
12. Is a zone as assumed in this example problem really an adequate zone? If not, how would you modify it?

13.0 SUBGROUP SESSIONS

Session Title: 13.11 Physical Protection
System Applications II

Date: Wednesday, 12 December 1979

Presented By: Subgroup Instructors

Time: 1000 to 1200
1330 to 1430

Session Objectives:

After the session, the participants will be able to

1. Illustrate the design/analysis cycle for the delay function by use of the hypothetical facility, given an outsider threat and a zone associated with the reactor and auxiliary buildings boundary;
2. Discuss the design/analysis cycle as it relates to selection of elements and features applicable to the generic logic tree and PPS functions, and then determine whether the elements and features provide positive measures; and
3. Apply selected generic logic trees.

Summary:

The objectives of this session are accomplished by the use of the hypothetical facility. A new zone is defined that begins at the reactor building exterior boundary, and the threat is an outsider threat. Modifications potentially required to analyze collusion by insiders are discussed. A high degree of class participation is encouraged so that the class can better familiarize itself with the material and concepts presented.

PHYSICAL PROTECTION SYSTEM APPLICATIONS II

CONTENTS

	<u>Page</u>
I. Problem Definition	13.11-5
II. Building Boundary Problem General Data and Guidelines	13.11-7
III. Instructional Guidelines*	13.11-19
IV. Think-About Items	13.11-21

*To be distributed at the end of this session for reference material.

I. PROBLEM DEFINITION

For this exercise, the zone starts at the auxiliary building boundaries. The adversary attack mode can encompass any of the attributes listed in Section II.1. This exercise will address only the delay function for the defined zone. Previous adversary detection is assumed. A design goal of 4 minutes delay will be used.

The class participants are expected to

1. Identify potential delay elements and features for the various events given in the FORCE-BUILDING generic logic tree,
2. Qualitatively assess the features identified in the prepared FORCE-BUILDING generic logic tree for their ability to provide positive measures for the delay function,
3. Identify events that require additional features, and provide these features, and
4. Reassess the zone features until they agree that positive measures are provided for the delay function against the defined threat structure.

II. BUILDING BOUNDARY PROBLEM GENERAL DATA AND GUIDELINES

Contents	<u>Page</u>
II.1 Threat Structure -- Outsiders	13.11-9
II.2 Problem Guidelines	13.11-9
II.3 Site Graphics	13.11-9
II.4 Top-Level Logic Trees	13.11-9
II.5 Applicable Site Features	13.11-17

II.1 Threat Structure—Outsiders

1. Attributes

- a) Number -- Six to eight
- b) Arms -- Automatic weapons
- c) Transportation -- Foot, surface vehicles, helicopters
- d) Equipment -- Hand-held portable power tools, explosives
- e) Knowledge -- Detailed information
- f) Training -- Detailed preplanning, rehearsals, military background, technical knowledge
- g) Dedication -- High

2. Tactics

- a) Deceit -- Submit to the system
- b) Stealth -- Covert
- c) Force -- Overt

3. Intent -- Disablement of vital targets selected by the threat so that core melt and radiological release is likely.

II.2 Problem Guidelines

The goal is high assurance that an outsider (up to eight) threat which is attempting sabotage is delayed from penetration of the building boundary zone.

The assumptions are that

- 1. Threat attributes, tactics, and intent are as given;
- 2. Detection, delay, communication, and response are the only necessary physical protection system (PPS) functions;
- 3. This exercise is limited to the delay function only;
- 4. Prior detection is assumed when entering the zone;
- 5. Adequate delay is a minimum of 4 minutes;
- 6. The adversary wins if delay is inadequate;
- 7. Guards are well-trained, well-equipped, etc.; and
- 8. PPS should be effective at all times.

II.3 Site Graphics

Figures 13.11-1 and 13.11-2 are the site graphics used in this problem.

II.4 Top-Level Logic Trees

Figures 13.11-3 and 13.11-4 are the top-level logic trees used in this problem.

Figure 13.11-1. Site Graphic

Figure 13.11-2. Site Graphic with Building Boundary Zone

Figure 13.11-3. Defeat PPS Delay Function Given PPS Detection

NOTES:

1. THE FORCE-BUILDING GENERIC LOGIC TREE IS APPLICABLE TO THIS ZONE.
2. USUALLY DELAYS OF STEALTH AND DECEIT TACTICS ARE BOUNDED BY EQUIVALENT ACTIONS USING FORCE TACTICS GIVEN DETECTION HAS OCCURRED. IF IN DOUBT, USE THE GENERIC TREES FOR STEALTH AND DECEIT.

Figure 13.11-4. Defeat Zone Delay Function Given PPS Detection

II.5 Applicable Site Features

The FORCE-BUILDING generic logic tree is used mainly in the PPS Applications II example problem. This tree, plus the STEALTH-BUILDING and DECEIT-BOUNDARY trees, are provided. Written on these trees, beside or under primary events, are potential PPS elements and features. The circled or marked elements are assumed to exist for the example problem. Delay elements are given primarily on the force tree.

Whether or not the elements assumed to exist provide positive measures for delay against the defined outsider threat is left as a class exercise. Selection of features for positive measures when deficiencies are detected is also left as a class exercise. A discussion is anticipated on how the PPS zone may be modified to accommodate an expanded threat including insider collusion.

Copies of the marked-up generic logic trees for PPS Applications II can be found in the pocket at the back of this notebook. The following list highlights assumed PPS elements and features that relate to delay at the building boundary.

Reactor, Auxiliary Buildings, Control and Diesel Generator Building Construction

1. These buildings are constructed of heavily reinforced concrete (greater than 0.5 metre thick).
2. The reactor building is constructed of heavily reinforced concrete (greater than 2 metres at the base and 1 metre at the top with an inner liner of 2-cm-thick steel).
3. Two steel doors, each 4 cm thick, provide personnel access into the reactor building through an airlock. The outer airlock door is padlocked.
4. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
5. All inner doors are normally closed and unlocked.

Turbine Building Construction

1. This building is constructed of corrugated sheet metal.
2. All of the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Reactor and Auxiliary Buildings Entrance/Exit

1. A single entrance/exit on the north side of the auxiliary building is provided for access control and is normally unlocked.
2. A guard mans the entrance/exit 24 hours per day inside the building.
3. Access is permitted to personnel with a photo badge credential and the guard issues another photo badge in exchange.

III. INSTRUCTIONAL GUIDELINES

1. Read and discuss the "Objectives and Overview." Note that PPS Applications I related to a perimeter boundary zone and the detection function, where PPS Applications II relates to a building boundary zone and the delay function.
2. Read and discuss the "Problem Definition."
3. Discuss the general data.
 - a) Threat structure is the same as in Applications I.
 - b) Problem guidelines change the emphasis from detection to delay for Applications II.
 - c) Using the site graphics (Figures 13.11-1 and 13.11-2), reinforce the visual understanding of what is meant by a building boundary zone. Note the zone is three-dimensional.
 - d) Briefly review the top-level logic trees. Note the following:
 - Figure 13.11-3 -- We will only study delay associated with the building boundary zone. Positive measures are required.
 - Figure 13.11-4 -- As per Note 2 on the figure, the FORCE-BUILDING logic tree will mainly be used.
 - e) Site features mainly focus on delay associated with the reactor building exterior boundary.
4. Present the prepared tree for defeating the building boundary by force (BUILDING-FORCE) and discuss it. Solicit additional PPS elements and write them down.
5. For each event, qualitatively access the ability of the assumed PPS elements to delay the design threat. Indicate which events have positive measures. Note that adequate delay was assumed to be 4 minutes and prior detection was given.
6. What about the collusion problem? Add: Any one insider may be in collusion with the outsider threat. Assume this insider will aid the outsiders in accomplishing their goal but will not directly perform the sabotage act.
 - a) If the insider is a guard, he or she can allow passage through portals where guard authorization is required, not shoot or shoot to miss, provide false instructions to the response force, divert the response force, provide false assessments of alarms, etc.
 - b) If the insider is an employee but not a guard, he or she can open emergency evacuation doors for entry, shut down equipment, disable alarms, etc.
 - c) In general, vulnerability exists where one insider alone can make a crucial decision or perform an action that defeats the PPS.
 - d) One solution is to add redundancy so that two independent people, operations, actions, authorizations, etc., are required to defeat the PPS zone functions.

- e) Some examples of implementation of this solution include
- Portal guard plus central control authorization system,
 - Overlapping fields for guards' gun fire,
 - Guard plus closed-circuit television assessment,
 - Redundant alarm enunciators, possibly located at guard towers and at the command center,
 - One-way emergency exists, and
 - Monitored communications lines and lines to indicate a failed alarm.

7. Summarize the exercise and draw conclusions.
8. Distribute the instructional guidelines and the think-about items.
9. Allow the participants some time to read the think-about items and then discuss as appropriate.

IV. THINK-ABOUT ITEMS

1. Adversary delay, given previous detection, has been considered. What may happen if the adversary is first delayed, then detected?
2. Should personnel portals provide the same minimal delay as the rest of the boundary in which they are located? Why?
3. Should all paths through the zone provide at least some defined minimal delay?
4. If the answer to item No. 3 is no, what compensating factors need to be considered?
5. What are some relationships between the threat attributes and the level of training, armament, motivation, and equipment required by the guards for delay?
6. Are explosives a good breaching aid?
7. Can a positive measure provide 100 percent capabilities?
8. Why is one insider in collusion with outsiders a potentially severe threat?
9. What would happen to the PPS if the threat included two insiders in collusion? Which ones?
10. Which insiders have more capability or opportunity to degrade or thwart the PPS?
11. Are hardware-intensive systems more or less desirable than people-intensive systems for the delay function?
12. What changes, if any, in the threat structure would be sufficient to defeat the assumed delay features for the PPS zone?
13. What changes in the threat structure would be sufficient to defeat the delay features for the redesigned PPS zone?

13.0 SUBGROUP SESSIONS

Session Title: 13.13 Manpower/Technology
Considerations

Date: Friday, 14 December 1979

Presented By: Subgroup Instructors

Time: 0830 to 1000

Session Objectives:

After the session, the participants will be able to

1. List the cost elements in the selection of a physical protection system (PPS) design,
2. Compare an equipment-intensive PPS and a personnel-intensive PPS using U.S.A. dollar cost estimates, and
3. Discuss the relative cost impact and trade-offs between equipment costs and equivalent personnel costs.

Summary:

PPS elements and estimated element costs are presented for both equipment-intensive and personnel-intensive PPS designs. A system cost comparison and trade-off studies are then made between the two designs.

MANPOWER/TECHNOLOGY CONSIDERATIONS

CONTENTS

	<u>Page</u>
I. Problem Definition	13.13-5
II. PPS Manpower/Technology Cost Examples	13.13-9
III. Instructional Guidelines*	13.13-19
IV. Think-About Items	13.13-21

*To be distributed at the end of the session for reference material.

I. PROBLEM DEFINITION

A group of people went through the iterative design/evaluation cycle to develop two different perimeter zone physical protection systems for their facility in the U.S.A. One system was equipment-intensive, and the second system was people-intensive. Cost estimates were subsequently developed for these two systems (Section II).

The given problem is to study and discuss the information contained in Section II and determine why management decided to implement the equipment-intensive PPS.

II. PPS MANPOWER/TECHNOLOGY COST EXAMPLES

Contents

	<u>Page</u>
II.1 Example Problem Outline	13.13-9
II.2 PPS Equipment-Intensive Example	13.13-11
II.3 PPS Guard-Intensive Example	13.13-13
II.4 Simplified Cost Comparison	13.13-15
II.5 System Trade-Off Summary	13.13-17

II.1 Example Problem Outline

- 1.1 Threat Objective -- sabotage of vital item(s) on facility site.
- 1.2 Threat -- up to eight adversaries, well-trained, equipped, knowledgeable, etc.
- 1.3 PPS Design -- This problem assumes PPS designs consisting of a zone on the site perimeter.
- 1.4 PPS System Guidelines -- If an adversary gets past the zone, it is assumed that adversary success is high because
 - a) It is difficult to track the adversaries once they are on-site;
 - b) Adversary sabotage targets are numerous, and it is not possible to individually protect all of them; and
 - c) There are numerous places for the adversaries to hide and ambush guards.
- 1.5 Security forces are assumed to have adequate capabilities to delay and neutralize the adversary at the perimeter.
- 1.6 Equipment and manpower PPS designs are assumed to be approximately equivalent for this exercise.

II.2 PPS Equipment-Intensive Example

2.1 Capital Equipment and Structures Cost Estimates

Useful Life (years)	Item	Cost (\$)
10	Two chain-link fences, 3.5 km at \$50/m	175,000
10	Sensor system, 1.75 km at \$165/m/sensor line, two sensor lines used (3.5 km)	577,000
10	Closed-circuit television assessment system, 1.75 km at \$170/m	300,000
10	Antipersonnel barrier, 1.75 km at \$200/m	350,000
10	Antivehicle barrier, 1.75 km at \$40/m	70,000
50	Hardened towers, three at \$100,000 each	300,000
10	Perimeter lighting, 1.75 km at \$50/m	88,000
10	Protected area lighting	250,000
50	Hardened entry control points, two at \$100,000 each	200,000
10	Helicopter barrier, 160 km ² at \$1.00/m ²	160,000
50	Hardened communication and command center, 500 m ² at \$3,000/m ²	1,500,000
50	Hardened backup communication and command center, 100 m ² at \$3,000/m ²	300,000
10	Hardened emergency power	400,000
Total Capital Costs		\$4,670,000

Amortized capital costs per year - cost/useful life = \$283,000

2.2 Security Force Deployment

	Officers per Shift
Entrances--two guards per access control structure (2 access control points)	4
Hardened towers--one guard/tower (3 towers)	3
• Detection system backup	
• Physical barriers backup	
Communication center	4
• One guard, voice communication	
• Two guards and closed-circuit television assessment console operation	
• One supervisor	
Secondary communication center	2
• One guard, voice communication	
• One supervisor	
Miscellaneous and roving patrols	3
Initial response -- eight security officers within 2 minutes at any point of the perimeter	8
Total security officers per shift	24
Supplemental response -- off-site security police personnel:	
• Five in 5 minutes	
• Eight in 10 minutes	
• Ten in 20 minutes	

II.3 PPS Guard-Intensive Example

3.1 Capital Equipment and Structure Cost Estimates

Useful Life (years)	Item	Cost (\$)
10	Chain-link fence, 1.75 km at \$50/m	87,500
50	Hardened towers, three at \$100,000 each	300,000
10	Perimeter lighting, 1.75 km at \$50/m	87,500
10	Protected area lighting	250,000
50	Two hardened communication and command centers -- 100 m ² each at \$3,000/m ²	600,000
50	Security officer perimeter posts, nine at \$10,000 each	90,000
10	Hardened emergency power	400,000
10	Hardened intraplant transporters, two at \$50,000 each	100,000
Total Capital Costs		\$1,915,000

Amortized capital costs per year - cost/useful life = \$112,300

3.2 Security Force Deployment

	Officers Per Shift
Entrances, two guards per access control structure (2 access control points)	4
Hardened towers, one guard/tower (3 towers)	3
• Backup detection of perimeter security officers	
• Backup delay of perimeter security officers	
Perimeter--security guards spaced every 200 metres	9
• Primary detection	
• Primary human barrier with suppressing firepower	
Communication center	2
• One guard, voice communications	
• One supervisor	
Redundant communication center	2
Miscellaneous and roving patrols	3
Initial Response -- eight security officers within <u>30 seconds</u> at any point of perimeter (4 teams required)	32
Total security officers per shift	55

Supplemental response -- off-site security/police personnel:

- Five in 5 minutes
- Eight in 10 minutes
- Ten in 20 minutes

II.4 Simplified Cost Comparison

	<u>Equipment Example</u>	<u>Manpower Example</u>
Amortized capital costs per year: cost divided by useful life	\$ 283,000	\$ 112,300
Equipment maintenance: at 10 percent of initial cost per year	\$ 467,000	\$ 192,000
Security personnel: \$100,000 per security officer post per year	\$2,400,000	\$5,500,000
	<hr/>	<hr/>
Total per year costs	\$3,150,000	\$5,804,300

II.5 System Trade-Off Summary

Figures 13.13-1 and 13.13-2 summarize the system trade-offs.

Figure 13.13-1. Relative Comparison of Operational Costs per Year for Equipment-Intensive and Manpower-Intensive PPS Designs

Figure 13.13-2. Security Guard Response (to any perimeter point) at \$100,000 per year per Security Guard Post Manned 24 Hours per Day

III. INSTRUCTIONAL GUIDELINES

1. Read and discuss the "Objectives and Summary" for this session.
2. Read and discuss the "Problem Definition."
3. Discuss the "Manpower/Technology Cost Examples."
 - 3.1 Examine the Example Problem outline. In particular, note assumption 1.6. These two PPS designs are not assessed or claimed to be optimum but are only assumed (or judged) to be "approximately equivalent."
 - 3.2 Have the participants set the two example problems side by side, and discuss the PPS elements and element costs for the two designs (subsections 2.1 and 3.1).
 - The equipment-intensive design has equipment detection elements for the penetration of the perimeter fenced area.
 - The equipment-intensive design has equipment delay elements for all boundary penetration options.
 - Guards in hardened towers supplement the detection and delay functions. Note that the guard towers are outside the zone but interface with it (visually and with firepower).
 - Communication and command center costs may be significantly greater for an equipment-intensive design.
 - The manpower-intensive system substitutes nine security officers in modest perimeter posts for primary detection and delay.
 - 3.3 Discuss subsections 2.2 and 3.2.
 - Each required 24-hour security officer position implies several actual officers. For example, three shifts at 8 hours per shift plus vacation and holiday time may require four to five people for one position.
 - The equipment-intensive design assures a predictable 2-minute delay, given detection, while the manpower-intensive design assures a predictable 30-second delay, given that perimeter post guards have performed detection. The key word is "predictable." Note: the predictable times are not shown but implied from the initial response force time.
 - With only a predictable 30-second delay, four times as many guards must be strategically deployed (in groups of eight), so that an equivalent number of guards as in the equipment-intensive design can respond to any point on the perimeter. The key is that only 30 seconds of travel time are available.
 - 3.4 Discuss subsection 4, "Simplified Cost Comparison." Note that inflation and interest costs are assumed to cancel each other out, so that present and future dollars are equivalent.

3.5 Discuss subsection 5, "System Trade-Off Summary Data."

- Figure 13.13-1 shows the effect of security officer costs. If security officers are free, the manpower-intensive design has a slight advantage.
- Figure 13.13-2 shows the effect of initial response force size. In the extreme, even if the initial response force is not required (i.e., the perimeter system of guard towers plus equipment or perimeter security officers is adequate for the threat), the equipment intensive system is still slightly more cost-effective if the security guard posts cost \$100,000 per year.
- Note that the manpower-intensive design assumes that four times as many security officers are required for initial response because of a 30-second versus a 2-minute predictable delay. If the delays were both the same (say 2 minutes), then the manpower-intensive system costs would parallel the equipment-intensive design costs from the zero security officer point given in Figure 13.13-2.

4. Distribute the instructional guidelines.

5. Discuss the think-about items as appropriate.

IV. THINK-ABOUT ITEMS

1. What characteristics of an equipment-intensive PPS are desirable? What characteristics are undesirable?
2. What characteristics of a manpower-intensive PPS are desirable? What characteristics are undesirable?
3. State some ways to combine the better aspects of the example manpower and equipment systems into one system design.
4. How can manpower costs be kept to a minimum?
5. How can equipment costs be optimized?

13.0 SUBGROUP SESSIONS

Session Title: 13.14 System Design
Application

Date: Friday, 14 December 1979

Presented By: Subgroup Instructors

Time: 1330 to 1430
1500 to 1600

Session Objectives:

After the session, the participants will be able to

1. Demonstrate familiarity with the complete physical protection system (PPS) design/analysis cycle using a zone design concept and generic logic trees.
2. Demonstrate familiarity with the Estimate of Adversary Sequence Interruption (EASI) program and its utility.

Summary:

The session objectives above are accomplished by the use of the hypothetical facility. Data developed in the previous subgroup sessions are combined into one complete exercise to define a new PPS zone. The class associates positive measures with the zone functions to detect, delay, communicate to the response, and respond to the defined threat. Given the PPS design which combines elements and features from the redesigned zones in PPS Applications I and II, an assessment of adversary interruption likelihood is made using EASI.

Selected adversary scenarios are provided as exercises in this session. These scenarios are modified if necessary to conform with the redesigned PPS. The class is encouraged to participate and, if possible, to further develop and improve the conceptual PPS zone design and then to assess the overall effectiveness of that design.

SYSTEM DESIGN APPLICATION

CONTENTS

	<u>Page</u>
I. Problem Definition	13.14-5
II. General Data and Problem Guidelines	13.14-7
III. Exercise Using EASI	13.14-27
IV. Instructional Guidelines	13.14-31
V. Think-About Items	13.14-33

I. PROBLEM DEFINITION

For this problem, the zone starts at the outer perimeter fence and ends at the Auxiliary and Reactor Building boundaries. The adversary attack mode can utilize the attributes listed in Section II.1.

The detection and delay positive measures developed in Sessions 13.10 and 13.11 will be used for the zone described above. Detection will be accomplished at the site perimeter, and a design goal of a minimum of 4 minutes delay will be used. Delay will be accomplished before penetration of the buildings' exterior boundaries. The threat structure is the same as that used for Sessions 13.10 and 13.11.

The class participants are expected to

1. Reassess whether the zone detection and delay functions provide positive measures when combined with the PPS communication and response functions;
2. Provide additional features, if necessary, such that all of the PPS functions provide positive measures against the defined threat structure;
3. Assess the PPS design against the given exercise scenarios using EASI; and
4. If required, provide additional features to correct function deficiencies and reassess the modified PPS against the given scenarios.

II. GENERAL DATA AND PROBLEM GUIDELINES

Contents	<u>Page</u>
II.1 Threat Structure -- Outsiders	13.14-9
II.2 Problem Guidelines	13.14-9
II.3 Site Graphics	13.14-9
II.4 Top-Level Logic Trees	13.14-9
II.5 Applicable Site Features	13.14-25

II.1 Threat Structure—Outsiders

1. Attributes

- a) Number -- Six to eight
- b) Arms -- Automatic weapons
- c) Transportation -- Foot, surface vehicles, helicopters
- d) Equipment -- Hand-held portable power tools, explosives
- e) Knowledge -- Detailed information
- f) Training -- Detailed preplanning, rehearsals, military background, technical knowledge
- g) Dedication -- High

2. Tactics

- a) Deceit -- Submit to the system
- b) Stealth -- Covert
- c) Force -- Overt

3. Intent -- Sabotage of vital targets selected by the threat so that core melt and radiological release is likely.

II.2 Problem Guidelines

The goal is high assurance that an outsider (up to eight) threat which is attempting sabotage is defeated within the PPS zone.

The assumptions are that

- 1. Threat attributes, tactics, and intent are as given;
- 2. Detection, delay, communication, and guard response are the only necessary PPS functions;
- 3. Outsider adversary actions prior to entry into the zone are undetected;
- 4. The outsider adversary "wins" if he can penetrate the inner surface of the zone before an adequate response force can intercept;
- 5. An initial guard response ratio of one guard per adversary must occur before the zone's inner boundary is penetrated;
- 6. Guards are well-trained, well-equipped, etc.; and
- 7. The PPS should be effective during all operational and environmental states of the site.

II.3 Site Graphics

Figures 13.14-1 through 13.14-4 are the site graphics for this session.

II.4 Top-Level Logic Trees

Figures 13.14-5 through 13.14-9 are the top-level logic trees for this session.

Figure 13.24-1. Facility Perspective with Perimeter Features

Figure 13.14-2. Pressurized Water Reactor Layout

Figure 13.14-3. Pressurized Water Reactor Composite Plan: Basement

Figure 13.14-4. Pressurized Water Reactor: Ground Level

Figure 13.14-5. Defeat PPS Logic

Figure 13.14-6. Defeat PPS Detection Function

Figure 13.14-7. Defeat PPS Delay Function Given PPS Detection

Figure 13.14-8. Defeat Zone Detection Function

NOTES:

1. THE FOLLOWING GENERIC FORCE LOGIC TREES ARE APPLICABLE TO THIS ZONE:

FORCE-BOUNDARY
FORCE-AREA
FORCE-BUILDING

2. USUALLY DELAYS OF STEALTH AND DECEIT TACTICS ARE BOUNDED BY EQUIVALENT ACTIONS USING FORCE TACTICS GIVEN DETECTION HAS OCCURRED. IF IN DOUBT, THE GENERIC TREES GIVEN IN NOTES 1 AND 2 OF FIG 13.14-8 ARE APPLICABLE

Figure 13.14-9. Defeat Zone Delay Function Given PPS Detection

II.5 Applicable Site Features

The analysis data for the exercise will build upon the elements and features obtained from the hypothetical facility data package (Session 13.1), the selected detection features resulting from PPS Applications I, and the selected delay features resulting from PPS Applications II. Selected features from Applications I and II are indicated on the instructor's marked-up STEALTH-BOUNDARY, DECEIT-BOUNDARY, and FORCE-BUILDING generic logic tree figures. The applicable hypothetical facility data are as follows:

Reactor, Auxiliary Buildings, Control and Diesel Generator Building Construction

1. These buildings are constructed of heavily reinforced concrete (greater than 0.5 metre thick).
2. The reactor building is constructed of heavily reinforced concrete (greater than 2 metres at the base and 1 metre at the top with an inner liner of 2-cm-thick steel).
3. Two steel doors, each 4 cm thick, provide personnel access into the reactor building through an airlock. The outer airlock door is padlocked.
4. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
5. All inner doors are normally closed and unlocked.

Turbine Building Construction

1. This building is constructed of corrugated sheet metal.
2. All of the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Perimeter

1. Two chain-link fences (2.5 metres high) separated by a 30-metre isolation zone surround the facility.
2. The minimum lighting in the isolation zone is 0.2 foot-candle (0.22 lumens/m²).
3. A single (combination personnel/vehicle) entrance/exit point is located in the middle of the west fenceline.
4. The perimeter fenceline is 2 km long.

Perimeter Personnel/Vehicle Entrance/Exit (and Central Alarm Facility)

1. The entrance/exit is manned 24 hours per day by at least two guards.
2. Two vehicle gates (with one gate always closed) provide an area within which guards search vehicles. The gates are heavily reinforced with pipe.
3. A personnel turnstile (2.5 metres high) controls pedestrian traffic.
4. Access is permitted to personnel with badge credentials.
5. All building and interior intrusion sensors annunciate and are displayed individually.

Secondary Alarm Facility

1. This facility is located in the reactor building control room.
2. All building and interior intrusion sensors annunciate and are displayed individually in the reactor building control room.
3. Only operational personnel are in the control room.
4. Control room personnel can authorize other personnel into facility (with a guard escort).

Reactor and Auxiliary Buildings Entrance/Exit

1. A single entrance/exit on the north side of the auxiliary building is provided for access control and is normally unlocked.
2. A guard mans the entrance/exit 24 hours per day inside the building.
3. Access is permitted to personnel with a photo badge credential and the guard issues another photo badge in exchange.

Detection System

1. Sensors
 - a) A guard is posted at the perimeter entrance.
 - b) A guard is posted at the reactor building entrance.
 - c) All other building exterior doors are locked and have magnetic door switch sensors.
 - d) One roving guard routinely patrols outside the buildings and checks building exterior doors and the inner perimeter fence line once every 2 hours. The building checks take 1.5 hours, and walking the inner fence line takes 0.5 hour.
 - e) The outer personnel airlock door into the reactor is locked and has a magnetic door switch sensor. Space intrusion sensors are located in the airlock.
2. Intrusion Alarm Annunciation and Display
 - a) There are audio and visual displays at the main perimeter gate station.
 - b) There are audio and visual displays in the reactor control room.
 - c) All guards can send a silent duress call with their transceivers.
3. Intrusion Alarm Assessment
 - a) The roving guard patrol is sent to assess the cause of an exterior door intrusion alarm.
 - b) Operational personnel are sent to assess intrusion door and space alarms at and within the reactor containment building.

Voice Communications

1. Each guard has a radio transceiver (two channels) with which to talk with other guards.
2. Guards at fixed stations (e.g. perimeter vehicle/personnel gate) have telephones to provide an alternative method to communicate.
3. The central alarm and secondary alarm stations both monitor the two guard radio channels and can communicate by radio or telephone to a local law enforcement agency.

III. EXERCISE USING EASI

The following scenario is provided to reinforce the use of the EASI program in the design/analysis cycle. Modify specific task times and detection probabilities to reflect the effect of additional class-developed PPS elements and features. Consider developing new scenarios to evaluate potentially weak paths and additional aspects of the threat spectrum such as helicopter attack, insiders, insider collusion, etc.

Exercise Problem Statement and Scenario

The scenario selected for analysis involves penetration of either the Auxiliary or the Reactor Building. From the facility characterization, the dimensions of interest are (1) the length and width of the facility--700 and 300 metres respectively; (2) the distance between the outer and inner perimeter fences--30 metres; and (3) an arbitrary distance of 50 metres between the inner fence and the Auxiliary and Reactor Buildings. Again from the facility characterization data, there are no perimeter detection system and no positive measures to impede an adversary's progress. An adversary would not be detected unless he were seen by the roving guard or until he had penetrated the building through a door. A typical sequence for the existing facility would be as follows.

<u>Task.</u>	<u>Task Time (minutes)</u>
1. Penetrate outer fence	0.02
2. Cross isolation area (rate = 4.3 m/s)	0.12
3. Penetrate inner fence	0.02
4. Cross to auxiliary building (rate = 4.3 m/s)	0.20
5. Penetrate auxiliary building emergency door (prybar)	0.20
TOTAL TIME	0.56 minutes

The above sequence is shown graphically on Figure 13.14-10.

The participants, using the data generated in this session, are requested to fill in the protective force response time and standard deviation, the probability of communication, the adversary task times and standard deviations, and the probability of detection for the sensors located within the zone. The capability of the revised PPS is to be calculated using the EASI program.

Figure 13.14-10. Facility Sketch with Adversary Path

Protective Force Response Time: ____ (minutes)

Standard Deviation: ____

Probability of Communication: ____

<u>Adversary Task</u>	<u>Probability of Detection</u>	<u>Task Time (minutes)</u>	<u>Standard Deviation</u>
1.			
2.			
3.			
4.			
5.			

Probability of Interruption: ____

IV. INSTRUCTIONAL GUIDELINES

1. Read and discuss the "Objectives and Overview."
 - a) This subgroup session is designed to allow the class to combine the data from previous subgroup sessions into one complete exercise.
 - b) Emphasis is placed on having the class participate in the design/analysis cycle.
2. Read and discuss the "Problem Definition."
3. Discuss the general data package.
 - a) Threat Structure -- Review.
 - b) Problem Guidelines -- Review.
 - c) Site Graphics -- To be used as an aid in visualization of the new PPS zone. Let the group sketch the new zone to be used in this exercise. Note that the zone is three-dimensional and includes the two other zones used in Applications I and II as well as the region between these zones.
 - d) Top-Level Logic Trees -- Review quickly for determination of applicable generic logic trees.
 - Figure 13.14-5 -- All four functions will be addressed for this problem.
 - Figure 13.14-6 -- For detection, we will assume the PPS has the detection features obtained during the redesign for PPS Application I.
 - Additional features the hypothetical facility may have in the zone will only be considered in EASI scenario evaluations.
 - Figure 13.14-7 -- For delay, we will assume the PPS has the delay features obtained during the redesign for PPS Application II. Additional features the hypothetical facility may have in the zone will only be considered in EASI scenario evaluations.
 - Figure 13.14-8 -- Assumptions are the same as with PPS Applications I, i.e., only the STEALTH-BOUNDARY and DECEIT-BOUNDARY generic trees will be used for detection function.
 - Figure 13.14-9 -- Assumptions are the same as with PPS Applications II, i.e., only the FORCE-BUILDING tree will be used for delay.
 - e) Site features relate to detection and delay within the zone and communication and response.
4. Review the generic logic trees with the selected PPS elements and features applicable to the PPS zone. Note these features are the features agreed upon in PPS Applications I and II.
 - a) Let the class determine any additional features they wish to use for detection and delay. Write the features beside or under the applicable events on the generic logic trees.
 - b) Address communication and response. Note the assumed PPS features from the site-features list. Write the assumed design features on the trees. These features may be associated with the reinforcements event on the generic trees. Add any additional desired features.

5. Qualitatively assess whether there are adequate positive measures associated with all PPS functions for the zone.
6. Review the previously developed adversary scenarios.
 - a) Modify these scenarios as necessary to apply to the PPS conceptual design.
 - b) Estimate detection likelihoods, delay times, etc. as required for the scenarios.
 - c) Assess adversary interruption likelihood using EASI program.
7. Summarize the exercise and let the class draw conclusions. Where are the weak points in the design (if any)?
8. Distribute the instructional guidelines.
9. Discuss the think-about items as appropriate. Note that the participants will be allowed to address any or all of these think-about items in the next subgroup session.

V. THINK-ABOUT ITEMS

1. What part of the PPS design do you feel the most confident about?
2. What part of the PPS design worries or concerns you the most? What part has the least predictability?
3. Does the PPS design need more conceptualization effort before you are willing to start design details?
4. What happens if the threat changes with regard to
 - Fire power?
 - Number of outsiders?
 - Number of insiders?
 - Site knowledge?
 - PPS knowledge?
 - Threat objectives?
5. What other ways, if any, would you use to assess PPS capability?
6. What may happen if there are several adversary targets within the zone? How might the design be modified to cover this condition?
7. What problems does your site PPS have that were not directly addressed in this workshop? Discuss.

13.0 SUBGROUP SESSIONS

Session Title: 13.15 Total Physical
Protection System
Design

Date: Monday, 17 December 1979

Presented By: Subgroup Instructors

Time: 0900 to 1000
1030 to 1200
1330 to 1430
1500 to 1600

Session Objectives:

After the session, the participants will be able to

1. Demonstrate familiarity with the complete physical protection system (PPS) design/analysis cycle using a zone design concept and generic logic trees, and
2. Demonstrate familiarity with the Estimate of Adversary Sequence Interruption (EASI) program and its utility.

Summary:

The objectives are accomplished by the use of the hypothetical facility. Both the threat(s) and the PPS zone(s) are selected by the class. The class associates positive measures with the zone functions to detect, delay, communicate to the response, and respond to the defined threat. Given the selected PPS design, an assessment of adversary interruption likelihood is made using EASI analysis. Selected adversary scenarios are provided for this exercise as an alternate to class-developed scenarios. These scenarios are modified to conform with the class-designed PPS. The function of the class instructor is minimized. The class is expected to define the problem, develop a conceptual PPS design, and then assess the effectiveness of that design.

TOTAL PHYSICAL PROTECTION SYSTEM DESIGN

CONTENTS

	<u>Page</u>
I. Problem Definition	13.15-5
II. Facility, Threat, and Problem General Data	13.15-7
III. Generic Logic Trees	13.15-33
IV. Representative Exercises for EASI	13.15-35
V. Instructional Guidelines*	13.15-43
VI. Think-About Items	13.15-45

*To be distributed at the end of the session for reference material.

I. PROBLEM DEFINITION

For this exercise, the class participants are expected to apply the techniques learned in this training course to their own physical protection system (PPS) design for the hypothetical facility. The students are first expected to apply the design and analysis techniques using generic logic trees, as demonstrated in Sessions 13.10, 13.11 and 13.14. The students are then expected to apply the EASI scenario analysis techniques, as demonstrated in Sessions 13.9 and 13.14. Facility and related basic problem data are given in Section II of this session. The participants are expected to utilize these data and the data given in III and IV as reference material which can be modified for their specific problem.

The class participants are expected to

1. Define a threat, threat attributes, tactics and intent;
2. Define a system performance goal;
3. Establish problem guidelines, assumptions, and limitations;
4. Define a PPS zone or zones;
5. Provide features relative to the detection, delay, communication and response functions that can potentially provide positive measures;
6. Assess qualitatively whether the PPS functions have positive measures, and redesign as required until positive measures are obtained; and
7. Assess the PPS design against selected scenarios using EASI to obtain a quantitative estimate of adversary interruption probability.

II. PROBLEM GENERAL DATA

Contents

	<u>Page</u>
II.1 Threat Spectrum and Threat Structure	13.15-9
II.2 Problem Guidelines	13.15-10
II.3 Site Graphics	13.15-10
II.4 Top-Level Logic Trees	13.15-10
II.5 Applicable Site Features	13.15-29

II.1 Threat Spectrum and Threat Structure

A class-developed threat spectrum is required. Table 13.15-I gives potential threat spectrums, and the data following it give potential threat structures for outsider and insider threats. The participants may use these data directly, modify these data, or develop their own data.

TABLE 13.15-I
Potential Threat Spectrums

	CONVENTIONAL	OUTSIDER AND/OR INSIDER		
	Very Low (Outsider)	Low (Outsider)	Moderate (Outsider/Insider)	High (Outsider/Insider)
<u>Attributes</u>				
Number	1 to 2	2 to 4	6 to 8 (O/I), 1 (I)	16 to 25 (O/I), 2 to 3 (I)
Arms	Small arms	Shoulder-fired auto- matic weapons	Shoulder-fired auto- matic weapons	Crew-served weapons
Transportation	Foot	Foot or surface vehicles	Foot, surface vehi- cles, helicopters	Foot, surface vehi- cles, any type aircraft
Equipment	Hand tools	Hand-held portable power tools, explosives	Hand-held portable power tools, explosives	Heavy equipment explosives
Knowledge	Remote visual observation of operational/logistic information	Public domain infor- mation	Detailed information and help	Detailed information and help
Training	Preplanning	Detailed preplanning	Detailed preplanning, rehearsals, military background, technical knowledge	Detailed preplanning, rehearsals, guerrilla training
Dedication	Low	Moderate to high	High	Very high

Potential Structure

Outsiders

1. Attributes

- a) Number -- Six to eight
- b) Arms -- Automatic weapons
- c) Transportation -- Foot, surface vehicles, helicopters
- d) Equipment -- Hand-held portable power tools, explosives
- e) Knowledge -- Detailed information
- f) Training -- Detailed preplanning, rehearsals, military background, technical knowledge
- g) Dedication -- High

2. Tactics

- a) Deceit -- Submit to the system
- b) Stealth -- Covert
- c) Force -- Overt

3. Intent -- Sabotage of vital targets selected by the threat so that core melt and radiological release is likely.

Insider

1. Attributes

- a) Number -- one
- b) Arms -- Automatic weapons
- c) Transportation -- Foot, surface vehicles
- d) Equipment -- Hand-held portable power tools, explosives
- e) Knowledge -- Detailed information
- f) Training -- Detailed preplanning, technical knowledge
- g) Dedication -- High

2. Tactics

- a) Deceit -- Submit to the system
- b) Stealth -- Covert
- c) Force -- Overt

3. Intent -- Sabotage of vital targets selected by the threat so that core melt and radiological release is likely.

II.2 Problem Guidelines

The participants are requested to develop problem guidelines. An example follows.

The PPS performance goal is high assurance that an outsider (up to eight) threat which is attempting sabotage is intercepted before vital targets are disabled.

The assumptions are that

- 1. Threat spectrum and intent are chosen by the class participants;
- 2. Detection, delay, communication, and guard response are the only necessary PPS functions;
- 3. Outsider adversary actions prior to entering the zone are undetected;
- 4. The adversary wins if he/she is not intercepted and neutralized when in the PPS zone;
- 5. An initial response of one guard per adversary must intercept while the adversary is in the zone;
- 6. Guards are well-trained, well-equipped, etc.; and
- 7. The PPS should be effective during all operational and environmental states of the site.

II.3 Site Graphics

Figures 13.15-1 through 13.15-6 are the site graphics for this session's exercises. More detailed site graphics are given in Session 13.1.

II.4 Top-Level Logic Trees

Figures 13.15-7 through 13.15-11 are the applicable top-level logic trees for this session.

Figure 13.15-1. Hypothetical Facility Perspective

Figure 13.15-2. Hypothetical Facility Perspective with Perimeter Features

Figure 13.15-3. Pressurized Water Reactor Layout

Figure 13.15-4. Pressurized Water Reactor Composite Plan: Ground Level

Figure 13.15-5. Pressurized Water Reactor Composite Plan: Basement

Figure 13.15-6. Simplified PWR System Functional Diagram

Figure 13.15-7. Defeat Physical Protection System

Figure 13.15-8. Defeat PPS Detection Function

Figure 13.15-9. Defeat PPS Delay Function Given PPS Detection

NOTES:

1. THE STEALTH-BOUNDARY, STEALTH-AREA, STEALTH-BUILDING, STEALTH-ACQUIRE SNM, AND STEALTH-RELEASE GENERIC LOGIC TREES MAY BE APPLICABLE.
2. THE DECEIT-BOUNDARY, DECEIT-AREA, AND DECEIT-ACQUIRE SNM GENERIC LOGIC TREES MAY BE APPLICABLE.
3. USUALLY DETECTION OF FORCE TACTICS IS BOUNDED BY STEALTH TACTICS.

Figure 13.15-10. Defeat Zone Detection Function

NOTES:

1. THE FOLLOWING GENERIC FORCE LOGIC TREES MAY BE APPLICABLE:

FORCE-BOUNDARY
FORCE-AREA
FORCE-BUILDING
FORCE-ACQUIRE SNM
FORCE-RELEASE

2. USUALLY DELAYS OF STEALTH AND DECEIT TACTICS ARE BOUNDED BY EQUIVALENT ACTIONS USING FORCE TACTICS GIVEN DETECTION HAS OCCURRED. IF IN DOUBT, THE GENERIC TREES GIVEN IN NOTES 1 AND 2 OF FIG. 13.14-10 ARE APPLICABLE.

Figure 13.15-11. Defeat Zone Delay Function Given PPS Detection

II.5 Applicable Site Features

The analysis data for the exercise will build upon the elements and features obtained from the general hypothetical facility data (Session 13.1). The selected detection features resulting from PPS Applications I and the selected delay features resulting from PPS Applications II should be useful reference material for this exercise. The hypothetical facility data are summarized as follows:

Vital Area Sets

Given the assumptions and limitations from Session 13.4, the following is a complete list of the minimum sets of areas which, if protected, will prevent sabotage:

1. OSPW
2. RB-2-1, AUX-2-6, and CWST
3. RB-2-1, AUX-2-6, and ESWB-1-1
4. RB-2-1, AUX-2-6, and ESWB-1-2
5. RB-2-1, DGB-1-1, AUX-2-4, and CWST
6. RB-2-1, DGB-1-1, AUX-2-4, and ESWB-1-1
7. RB-2-1, DGB-1-1, AUX-2-4, and ESWB-1-2
8. RB-2-1, DGB-1-2, AUX-2-5, and CWST
9. RB-2-1, DGB-1-2, AUX-2-5, and ESWB-1-1
10. RB-2-1, DGB-1-2, AUX-2-5, and ESWB-1-2

Reactor, Auxiliary Buildings, Control and Diesel Generator Building Construction

1. These buildings are constructed of heavily reinforced concrete (greater than 0.5 metre thick).
2. The reactor building is constructed of heavily reinforced concrete (greater than 2 metres at the base and 1 metre at the top with an inner liner of 2-cm-thick steel).
3. Two steel doors, each 4 cm thick, provide personnel access into the reactor building through an airlock. The outer airlock door is padlocked.
4. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
5. All inner doors are normally closed and unlocked.

Turbine Building Construction

1. This building is constructed of corrugated sheet metal.
2. All of the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Essential Service Water Building Construction

1. This building is constructed of reinforced concrete 0.2 metre thick.
2. All the outside doors are standard industrial hollow-core steel construction. Doors are locked to prevent entry from the outside but have panic lock-release hardware inside.
3. All inner doors are normally closed and unlocked.

Condensate Water Tank Construction

1. This tank is constructed of welded steel plates (1 cm thick).
2. There are no access ports or hatches in this structure.

Perimeter

1. Two chain-link fences (2.5 metres high) separated by a 30-metre isolation zone surround the facility.
2. The minimum lighting in the isolation zone is 0.2 foot-candle (0.22 lumens/m²).
3. A single (combination personnel/vehicle) entrance/exit point is located in the middle of the west fenceline.
4. The perimeter fenceline is 2 km long.

Perimeter Personnel/Vehicle Entrance/Exit (and Central Alarm Facility)

1. The entrance/exit is manned 24 hours per day by at least two guards.
2. Two vehicle gates (with one gate always closed) provide an area within which guards search vehicles. The gates are heavily reinforced with pipe.
3. A personnel turnstile (2.5 metres high) controls pedestrian traffic.
4. Access is permitted to personnel with badge credentials.
5. All building and interior intrusion sensors annunciate and are displayed individually.
6. Control room personnel can authorize other personnel into facility (with a guard escort).

Secondary Alarm Facility - Summary Features

1. This facility is located in the reactor building control room.
2. All building and interior intrusion sensors annunciate and are displayed individually in the reactor building control room.
3. Only operational personnel are in the control room.

Reactor and Auxiliary Buildings Entrance/Exit

1. A single entrance/exit on the south side of the auxiliary building is provided for access control and is normally unlocked.
2. A guard mans the entrance/exit 24 hours per day inside the building.
3. Access is permitted to personnel with a photo badge credential and the guard issues another photo badge in exchange.

Detection System

1. Sensors
 - a) A guard is posted at the perimeter entrance.
 - b) A guard is posted at the reactor building entrance.
 - c) All other building exterior doors are locked and have magnetic door switch sensors.
 - d) One roving guard routinely patrols outside the buildings and checks building exterior doors and the inner perimeter fenceline once every 2 hours. The building checks take 1.5 hours, and walking the inner fenceline takes 0.5 hour.

- e) The outer personnel airlock door into the reactor is locked and has a magnetic door switch sensor. Space intrusion sensors are located in the airlock.

2. Intrusion Alarm Annunciation and Display

- a) There are audio and visual displays at the main perimeter gate station.
- b) There are audio and visual displays in the reactor control room.
- c) All guards can send a silent duress call with their transceivers.

3. Intrusion Alarm Assessment

- a) The roving guard patrol is sent to assess the cause of an exterior door intrusion alarm.
- b) Operational personnel are sent to assess intrusion door and space alarms at and within the reactor containment building.

Voice Communication

- 1. Each guard has a radio transceiver (two channels) with which to talk with other guards.
- 2. Guards at fixed stations (e.g., perimeter vehicle/personnel gate) have telephones to provide an alternative method to communicate.
- 3. The central alarm and secondary alarm stations both monitor the two guard radio channels and can communicate by radio or telephone to a local law enforcement agency.

Response Force

<u>On-Site</u>	<u>Average Response Time (minutes)</u>
Roving Patrol Guard (Assessment)	2
<u>If threat is assessed:</u>	
One Guard from Main Gate	2
Shift Captain	3
<u>Off-Site</u>	
Local Law Enforcement Agency	
1 Officer	5
2 Additional Officers	10
6 Additional Officers	20

III. GENERIC LOGIC TREES

The following trees, given in the generic logic trees subgroup session (13.5), may be applicable to this section.

The generic logic trees are

- FORCE-BOUNDARY and STEALTH-BOUNDARY
- DECEIT-BOUNDARY
- FORCE-AREA and STEALTH-AREA
- DECEIT-AREA
- FORCE-BUILDING and STEALTH-BUILDING
- FORCE-ACQUIRE-SNM and STEALTH-ACQUIRE-SNM
- DECEIT-ACQUIRE-SNM
- FORCE-RELEASE and STEALTH-RELEASE

The following trees, given in Session 13.5, may be applicable to this session since they provide examples of additional logic detail for selected terminal events in the generic logic trees:

- AVOID or CONFRONT GUARDS
- DEFEAT PERIMETER BARRIER
- DEFEAT or BYPASS SENSOR FIELD
- DEFEAT FENCE
- DEFEAT BUILDING STRUCTURE
- DEFEAT BUILDING PERSONNEL ENTRANCE
- DEFEAT BUILDING UTILITY OPENINGS

IV. REPRESENTATIVE EXERCISES USING EASI

The attached exercises are provided as an aid to the class in development of their own scenarios. Specific task times, detection probabilities, communication probabilities, and response times will have to reflect the effectiveness estimate.

Note that the use of the EASI program in this subgroup session is optional, depending upon time available and class interests.

EXERCISE 1— SABOTAGE BY OUTSIDERS USING MAINLY DECEIT AND STEALTH TACTICS

General

Three outsiders will attempt the sabotage. They have previously acquired necessary site information from facility tours, the Final Safety Analysis Report, informants, and site surveillance. Deceit will be used as the primary tactic to gain access on-site, into buildings, and into vital component locations. Stealth will be attempted if deceit fails or if the adversaries think they have a better chance of success using stealth. Only deceit and stealth tactics will be used up to the point of the actual disablement of selected targets. Target disablement will be a simultaneous explosive disablement of all selected targets. At this point, the adversaries have succeeded. While not necessary for sabotage success, adversary escape will still be attempted.

Equipment

Equipment consists of a government (or company) vehicle, employee false credentials, employee clothes, automatic weapons, explosives, explosive timer systems, and a communication system.

Scenario

The three outsiders drive to the vehicle gate in their pseudo government (or company) vehicle. At this gate, the adversaries present their fake credentials to gain access. The vehicle contains hidden automatic weapons, explosives, shaped charges, timers, etc. These are not detected by either the guard or vehicle entrance detection systems.

After entry to the facility site, the adversaries conceal their explosives and weapons on their persons. They then separate and proceed to a number of preselected targets outside of the main building. Explosives with timer systems are placed on these targets.

The adversaries now approach the main building; one adversary, who does not at this time possess any explosives or metallic weapons or tools, enters first. This adversary again uses false credentials to gain access. Given that the first adversary gains access, the remaining two adversaries attempt access using their false credentials; these two adversaries have hidden explosives, weapons, etc. The first adversary positions himself where he can aid his partners if they are detected. Guard disablement without detection by the PPS security operations center is a potential stealth backup option.

Given that the three adversaries gain access to the main building, they then separate and go to preselected targets that do not have additional barriers. After placing the appropriate explosives and timer systems to disable these targets, the adversaries then attempt penetration of the remaining target, which has additional barriers. Penetration is systematically attempted in a manner similar to that for penetration of the building entrance. Given penetration, the necessary explosives and timer systems are then placed on the preselected targets and the adversaries

exit the site using their false credentials. Simultaneous target disablement then occurs.

Exercise 1 Data Summary

Guard Response Time (minutes)	Class to provide
Guard Response Time Standard Deviation	Class to provide
Probability of Communication	Class to provide

Adversary Task	Mean Task Time ^a (minutes)	Standard Deviation ^a	Probability of Detection
1. Enter vehicle gate	0.1	0.02	--
2. Pass gate security with false cre- dentials	0.2	0.05	b
3. Pass vehicle inspection	0.2	0.05	b
4. Drive vehicle to final location	0.2	0.05	--
5. Gather and conceal explosives, weap- ons, etc.	1.0	0.2	b
6. Separate and travel to targets outside main building	2.0	0.5	--
7. Place explosives and timers, etc., on targets	3.0	1.0	b
8. Travel to main build- ing personnel entrance	2.0	0.5	--
9. First adversary enters main building	0.3	0.1	b
10. Two remaining adver- saries enter main building	0.3	0.1	b
11. Separate and travel to targets without additional barriers	0.3	0.1	b
12. Place explosives and timers, etc., on targets	3.0	1.0	b
13. Travel to vital target location	1.5	0.5	--
14. First adversary (two if two-man rule) enters target location	0.5	0.1	b
15. Remaining adver- sary(s) enters target location	0.4	0.1	b
16. Travel to target(s)	0.5	0.1	--
17. Place explosives and timers on target(s)	2.0	0.3	b

^aThe time estimates are examples of what might be expected if the site has a vehicle gate guard, a building guard, and vital location guards but does not have metal or explosives detectors, etc., except potentially at the vital location entrance. Students are to provide actual time estimates based upon their PPS features.

^bStudents are to provide likelihood estimates based upon their PPS features.

<u>Adversary Task</u>	<u>Mean Task Time^a (minutes)</u>	<u>Standard Deviation^a</u>	<u>Probability of Detection</u>
<u>Scenario Objective Accomplished</u>			
18. Exit vital location	0.3	0.1	--
19. Exit main building	0.3	0.1	--
20. Enter vehicle	0.15	0.03	--
21. Exit facility site through vehicle gate	0.3	0.05	--

^aThe time estimates are examples of what might be expected if the site has a vehicle gate guard, a building guard, and vital location guards but does not have metal or explosives detectors, etc., except potentially at the vital location entrance. Students are to provide actual time estimates based upon their PPS features.

^bStudents are to provide likelihood estimates based upon their PPS features.

EXERCISE 2— SABOTAGE BY OUTSIDERS USING DECEIT AND STEALTH, THEN FORCE

General

Exercise 2 is the same as Exercise 1 except that force will be used to gain access to the vital locations.

Equipment

Equipment is the same as in Exercise 1.

Scenario

This scenario is the same as Scenario 1 up to the vital target location. Note this location contains the final target(s). The adversaries assemble and then approach the vital location entrance as if they are employees. At an opportune time, the adversaries either shoot or capture the entrance guard(s). The adversaries then penetrate the entrance, place explosives with a fuse or timer system, and exit the vital location. The explosives detonate and the adversaries then evacuate the building through an emergency exit. The adversaries then enter their vehicle and crash the vehicle gate to exit the site.

Exercise 2 Data Summary

Guard Response Time (minutes)	Class to provide
Guard Response Time Standard Deviation	Class to provide
Probability of Communication	Class to provide

Adversary Task	Mean Task Time ^a (minutes)	Standard Deviation ^a	Probability of Detection
1. Enter vehicle gate	0.1	0.02	--
2. Pass gate security with false creden- tials	0.2	0.05	b
3. Pass vehicle inspection	0.2	0.05	b
4. Drive vehicle to final location	0.2	0.05	--
5. Gather and conceal explosives, weap- ons, etc.	1.0	0.2	b
6. Separate and travel to targets outside main building	2.0	0.5	--
7. Place explosives and timers, etc., on targets	3.0	1.0	b
8. Travel to main build- ing personnel entrance	2.0	0.5	--
9. First adversary enters main building	0.3	0.1	b

^aThe time estimates are examples of what might be expected if the site has a vehicle gate guard, a building guard, and vital location guards but does not have metal or explosives detectors, etc., except potentially at the vital location entrance. Students are to provide actual time estimates based upon their PPS features.

^bStudents are to provide likelihood estimates based upon their PPS features.

<u>Adversary Task</u>	<u>Mean Task Time^a</u> <u>(minutes)</u>	<u>Standard</u> <u>Deviation^a</u>	<u>Probability</u> <u>of Detection</u>
10. Two remaining adversaries enter main building	0.3	0.1	b
11. Separate and travel to targets without additional barriers	0.3	0.1	b
12. Place explosives and timers, etc., on targets	3.0	1.0	b
13. Travel to vital target location	1.5	0.5	--
14. Adversaries approach entrance	0.3	0.1	b
15. Adversaries disable entrance guard	0.2	0.05	b
16. Travel to target(s)	0.5	0.1	7-
17. Place explosives and timers on target(s)	1.0	0.1	b
18. Exit vital location and detonate explosives	1.0	0.2	b
<u>Scenario Objective Accomplished</u>			
19. Exit building through emergency exit	0.1	0.05	--
20. Enter vehicle	0.1	0.03	--
21. Exit facility site by crashing through vehicle entrance	0.2	0.05	b

^aThe time estimates are examples of what might be expected if the site has a vehicle gate guard, a building guard, and vital location guards but does not have metal or explosives detectors, etc., except potentially at the vital location entrance. Students are to provide actual time estimates based upon their PPS features.

^bStudents are to provide likelihood estimates based upon their PPS features.

INSTRUCTIONAL GUIDELINES

1. Discuss the "Objectives and Overview."

NOTE:

- This subgroup session is designed to allow the class to combine their knowledge from previous subgroup sessions into one complete exercise.
 - Emphasis is placed on having the class formulate the design.
2. Discuss the facility and threat data package and review the contents, which include
 - a) Potential Threat Spectrum and Potential Threat Structure -- Review and have the class select the threat(s).
 - b) Example Problem Guidelines -- Review and revise as directed by the class.
 - c) Site Graphics -- Use as an aid in selection of the PPS zone or zones. Note that vital areas obtained in Session 13.4 are shaded in Figures 13.15-4 and 13.15-5. Sets of vital areas are given in II.5.
 - d) Top-Level Logic Trees -- Review for determination of applicable generic logic trees.
 3. Select the generic logic trees applicable to the PPS zone(s) and develop the conceptual design. The instructors are provided an extra set of clean and marked-up trees for class use.
 - a) Let the class determine which features they wish to use for detection and delay. Write the features beside or under the applicable events on the generic logic trees.
 - b) Address communication and response. Write the selected design features on the trees. These features may be associated with the reinforcements event on the generic trees.
 4. Qualitatively assess whether there are adequate positive measures associated with all PPS functions. Redesign as required until positive measures are obtained.
 5. Develop adversary scenarios against the site with its selected PPS conceptual design.
 - a) If requested, use the provided scenarios as an aid in the development of the class scenarios or as an alternate to class-developed scenarios.
 - b) Assess adversary interruption likelihood using the EASI program.
 6. Summarize the exercise and let the class draw conclusions. Where are the weak points in the design (if any)? etc.
 7. Distribute the instructional guidelines.
 8. Discuss the think-about items as appropriate.

9. Note that the marked-up generic trees used in this work session are available in the resources room for those who wish to review or make notes from them.

VI. THINK-ABOUT ITEMS

1. What part of the PPS design do you feel the most confident about?
2. What part of the PPS design worries or concerns you the most? What part has the least predictability?
3. Does the PPS design need more conceptualization effort before you are willing to start design details?
4. What happens if the threat changes with regard to
 - Fire power?
 - Number of outsiders?
 - Number of insiders?
 - Site knowledge?
 - PPS knowledge?
 - Threat objectives?
5. What other ways, if any, would you use to assess PPS capability?
6. What problems does your site PPS have that were not directly addressed in this workshop? Discuss.

13.0 SUBGROUP SESSIONS

Session Title: 13.16 Cost/Impact Analysis Applications

Date: Tuesday, 18 December 1979

Presented By: Subgroup Instructors

Time: 0830 to 1000
1030 to 1200

Session Objectives:

After the session, the participants will be able to

1. State the type of information an analyst needs to perform a cost/impact analysis for an entry-control system,
2. Explain how a cost/impact analysis is performed, and
3. Perform a cost/impact analysis.

Summary:

Operational data for the hypothetical facility are presented. From these data, participants perform an analysis of the operational impact due to the given entry-control system for both the normal plant operational state and for refueling. The results show the impact in the time required to perform plant operations.

These results represent one element in a cost/impact analysis. The think-about items are used to discuss other cost impacts.

COST/IMPACT ANALYSIS OF TOTAL SYSTEM DESIGN

CONTENTS

	<u>Page</u>
I. Problem Definition	13.16-5
II. Problem Data	13.16-7
III. Instructional Guidelines	13.16-45
IV. Think-About Items	13.16-47

I. PROBLEM DEFINITION

This sample problem examines the potential increases in operational task times which might be encountered due to the implementation of an entry-control system at the hypothetical PWR.

In this sample problem, two modes of operation are examined: normal power operation for a period of 1 month and the entire refueling mode.

The class participants are expected to

1. Read and understand the analysis for the normal power operational mode.
2. Perform an equivalent analysis for the refueling mode. Section II.5 states specific requirements.
3. Identify all types of cost/impacts associated with the given entry-control system.

II. PROBLEM DATA

Contents

	Page
II.1 Personnel Data and Assumptions	13.16-9
II.2 Entry-Control Data and Assumptions	13.16-10
II.3 Power Operational Mode Analysis	13.16-19
II.4 Refueling Mode Analysis Data	13.16-31
II.5 Analysis Results Summary	13.16-43

II.1 Personnel Data and Assumptions

Based upon experience with actual operating PWRs, a staff of 221 is assumed to be employed at the hypothetical PWR. Of these, 30 employees are assigned to management/administrative functions, 60 to operations, 90 to maintenance, 36 to technical support, and 5 to training functions. In addition, during refueling operations, a number of contractor personnel are assumed to work at the hypothetical facility.

Using staff function as an identifier, the total available hours and estimated hours spent on jobs in the plant operational areas are shown in Table 13.16-I. Management/administrative and training personnel are assumed to spend all of their time outside of the plant operational areas.

The assumed availability for all personnel is 155 hours per month. Vacation, sick leave, etc. have been accounted for in choosing this number.

TABLE 13.16-I

Job Hours Spent in Plant Operational Areas

<u>Total Staff</u>	<u>Total Available Hours</u>	<u>Job Hours, Power Mode^a</u>	<u>Job Hours, Refuel Mode^b</u>
Mgmt/Admin. 30	4,700	0	0
Operations 60	9,300	7,800	7,700
Maintenance 90	14,000	5,540	9,900
Technical Support 36	5,600	2,100	3,700
Training Personnel 5	780	0	0
Contractor 200	31,000	NA	23,000

^aOne month of power operation.

^bRefueling is assumed to require 30 days.

For the power operating mode, residence times and the required number of entries to an area per job are as follows:

(a) Operations Personnel	2 hours per job 1 entry per job
(b) Maintenance Personnel	6 hours per job 3 entries per job
(c) Technical Support Personnel	4 hours per job 2 entries per job

It is assumed that during refueling, an additional 200 contractor employees will be on-site to assist in the refueling effort. Of these, 175 are maintenance contractors and 25 are consultants, vendor representatives, etc. Assumptions made

regarding residence times and required entries to an area per job during refueling are based upon the following:

(a) Operations Personnel	4 hours per job 2 entries per job
(b) Maintenance Personnel	8 hours per job 4 entries per job
(c) Technical Support	6 hours per job 3 entries per job
(d) Contractor Personnel	8 hours per job 3 entries per job

Additional access to the reactor building is available during the refueling mode. This access is from the on-site area through the containment equipment hatch.

II.2 Entry-Control Data and Assumptions

The methods used to control access to vital areas within the reactor buildings are (1) magnetic strip badges which are read by badge readers and (2) badge exchange portals, some of which also have metal detectors.

Entry-control locations and the designated features at each location are shown in the composite plans in Figures 13.16-1 and 13.16-2. Control features consist of a card reader or a badge exchange system for normal access. Note that some entrances (Turbine Building--Figure 13.16-2) preclude access during normal operational modes. One location, the Control Building CB2-1 in Figure 13.16-1, also has a metal detector system. Details of the assumed access control features are given in Table 13.16-II. This table also gives the ΔT delay time associated with each feature. Metal detectors at access points increase access time. It should be noted that the ΔT due to personnel passing through a metal detector is negligible. However, a false alarm rate has been assumed. The access delay resulting from guard response and subsequent detainment of an employee due to a false alarm is estimated to increase each Δt transit time an average of 5 percent. It has been assumed that for the purposes of this sample problem, personnel movement through the metal detectors is in one direction only.

Table 13.16-III lists an area designator number for each operational area. Operational area names and numbers are also shown in the composite plans (Figures 13.16-1, 13.16-2) for convenience.

The estimated total job hours from Table 13.16-I have been allocated to the designated operational areas (given in Table 13.16-III) based upon typical experience with actual operating PWRs. Tables 13.16-IV and 13.16-V give these data for the operational mode and refueling mode, respectively. Given the job hours in each area, the hours per job, and the required entries into an area per job, the required entries into each area can be calculated. These data are also given in Tables 13.16-IV and 13.16-V.

Figure 13.16-1. PWR Ground Level with Access Control

Figure 13.16-2. PWR Basement with Access Control

TABLE 13.16-II

Entry-Control Features and Associated ΔT

<u>Entry-Control Features</u>	<u>Description</u>	<u>ΔT (hours)</u>
Card Reader	An individual who wishes to enter an area, the access to which is controlled by a card reader, must insert his card into the reader which then verifies his identity and authorization to enter the area.	0.008
Badge Exchange	A badge exchange system reduces the possibility of a badge being falsified. Under this system, duplicate photo-ID badges are held at each access control point. A guard matches the individual requesting entry to the photo on the corresponding badge. When identity is verified, the guard exchanges badges and the individual is granted access. The badges are again exchanged upon exiting the area.	0.017
Metal Detector	Metal detectors are installed the control room access points and are used to detect weapons and tools which may be used in an act of sabotage.	5%*

*The actual ΔT due to the use of metal detectors is assumed to be 5 percent of Δ transit time. This is due to false alarms.

TABLE 13.16-III

Operational Area Numbers

<u>Area Designator Code</u>	<u>Operational Area</u>
1	AUX 1-1
2	AUX 2-1
3	CB 2-1
4	CWST*
5	DGB 1-1
6	DGB 1-2
7	ESWB
8	RB 1-1
9	RB 2-1
10	TB 2-1
11	OSPW
12	On-site

*Includes demineralized water tank, auxiliary feedwater tanks, etc.

TABLE 13.16-IV

Power Operation Mode Data (1 month)

Operational Area	Residence Times (job)				Required Entries for Jobs			
	Ops.	Maint.	Tech.	Total	Ops.	Maint.	Tech.	Total
1 AUX-1-1	1160	920	380	2460	580	460	190	1230
2 AUX-2-1	1160	920	380	2460	580	460	190	1230
3 CB-2-1	780	54	580	1414	390	27	290	707
4 CWST	1560	260	42	1862	780	130	21	931
5 DGB-1-1	76	108	22	206	38	54	11	103
6 DGB-1-2	76	108	22	206	38	54	11	103
7 ESWB	380	880	42	1302	190	440	21	651
8 RB-1-1	76	108	106	290	38	54	53	145
9 RB-2-1	76	108	106	290	38	54	53	145
10 TB-2-1	2400	1860	420	4680	1200	930	210	2340
11 OSPW	78	108	0	186	39	54	0	93
Total	7822	5434	2100	15,356	3911	2717	1050	7678

TABLE 13.16-V

Refueling Mode Data (1 month)

Operational Area	Ops.	Maint.	Tech.	Cont.	Total
	Residence Times (job)				
1 AUX-1-1	780	1100	740	3467	6087
2 AUX-2-1	780	1100	740	3467	6087
3 CB-2-1	780	198	38	235	1251
4 CWST	780	900	36	235	1951
5 DGB-1-1	240	300	36	0	576
6 DGB-1-2	240	300	36	0	576
7 ESWB	78	400	186	933	1597
8 RB-1-1	1900	1980	740	5867	10,487
9 RB-2-1	1900	1980	740	5867	10,487
10 TB-2-1	150	1580	380	3200	5310
11 OSPW	78	100	36	0	214
Total	7706	9938	3708	23,271	44,623

Required Entries					
1 AUX-1-1	390	550	370	1300	2610
2 AUX-2-1	390	550	370	1300	2610
3 CB-2-1	390	99	19	88	596
4 CWST	390	450	18	88	946
5 DGB-1-1	120	150	18	0	288
6 DGB-1-2	120	150	18	0	288
7 ESWB	39	200	93	350	682
8 RB-1-1	950	990	370	2200	4510
9 RB-2-1	950	990	370	2200	4510
10 TB-2-1	75	790	190	1200	2255
11 OSPW	39	50	18	0	107
Total	3853	4969	1854	8726	19,402

II.3 Power Operational Mode Analysis

Required access times without entry-control are given in Figure 13.16-3, and access time with entry-control is given in Figure 13.16-4. Table 13.16-III provides the code key between the 12 indicated area numbers and the actual site locations. The per-person access times are based upon typical PWR site considerations with the additional impact of entry-control times (Table 13.16-II) added for the "with entry-control" case. These data are summarized in Table 13.16-VI. Figure 13.16-5 gives the diagram for total number of entries to each designated location. Note that this figure is assumed valid for access with and without entry-control. Detailed entry data are given in Table 13.16-VII. The route is indicated for each required location entry. Note several assumptions were used in generating these tables. Route data for the hypothetical PWR were essentially assumed. These route data give the number of entries to each location, as summarized on Figure 13.16-5.

Table 13.16-VIII gives the total ΔT impact due to the entry-control system. Time with entry-control system (ECS) is obtained by multiplying times from Figure 13.16-4 with number of entries for each location as given in Figure 13.16-5. Time without ECS is obtained in a similar manner from Figure 13.16-3 and Figure 13.16-5. The ΔT is the difference in these two times.

Figure 13.16-3. Power Operation Mode: Access Times (minutes) without Entry Control.

Figure 13.16-4. Power Operation Mode: Access Times (minutes) with Entry Control

TABLE 13.16-VI

Transit Time Summary, Power Operation Mode^a

<u>Path</u>	<u>Entry-Controls Used</u>	<u>Transit Time without Entry-Control</u>	<u>Transit Time with Entry-Control</u>	<u>ΔTransit Time</u>
2-1	None	1.02	1.02	0
6-1	Card Reader	0.48	0.96	0.48
1-2	None	1.02	1.02	0
3-2	Badge Exchange	0.48	1.5	1.02
9-2	Badge Exchange	10.2	11.22	1.02
10-2	Card Reader	1.02	1.5	0.48
12-2	Card Reader	0.9	1.38	0.48
2-3	Badge Exchange	0.48	1.56 ^b	1.08 ^b
5-3	Card Reader	1.5	1.98	0.48
10-3	Badge Exchange	1.2	2.28 ^b	1.08 ^b
12-4	None	0.9	0.9	0
3-5	Card Reader	1.5	1.98	0.48
1-6	Card Reader	0.48	0.96	0.48
12-7	None	3.9	3.9	0
9-8	None	1.02	1.02	0
2-9	Badge Exchange	10.2	11.22	1.02
8-9	None	1.02	1.02	0
12-9	Badge Exchange	0.48	1.50	1.02
2-10	Card Reader	1.02	1.5	0.48
3-10	Badge Exchange	1.2	2.22	1.02
12-10	None	2.1	2.1	0
12-11	None	3.9	3.9	0
2-12	Card Reader	0.9	1.38	0.48
4-12	None	0.9	0.9	0
7-12	None	3.9	3.9	0
9-12	Badge Exchange	0.48	1.5	1.02
10-12	None	2.1	2.1	0
11-12	None	3.9	3.9	0

^a All times in minutes^b Includes metal detector false alarm rate

Figure 13.16-5. Power Operation Mode: Number of Entries

TABLE 13.16-VII

Power Operation Routing Data

<u>Operational Area</u>	<u>Required Entries</u>	<u>Route</u>	<u>Notes</u>
1 AUX-1-1	1200	12-2-1	1
2 AUX-2-1	1200	12-2	1,4
3 CB-2-1	700	12-2-3	1
4 CWST	600	12-4	1
	300	12-2-12-4	2
5 DGB-1-1	50	12-10-3-5	1
	50	12-2-3-5	1
6 DGB-1-2	100	12-2-1-6	1
7 ESWB	400	12-7	1
	300	12-2-12-7	2
8 RB-1-1	100	12-2-9-8	1
9 RB-2-1	100	12-2-9	1
10 TB-2-1	1300	12-10	1
	500	12-2-10	2
	500	2-10	3
11 OSPW	50	12-11	1
	50	12-2-12-11	2

- Notes: 1. Assumed route is from off-site to area and then reversed.
2. Assumed route is from off-site to area via extra area (for job orders, tools, etc.), and then route is assumed to be reversed.
3. Assumed starting area is not from off-site, and route is reversed.
4. Some routes are extended to other operational areas as per note 3; however, this does not require changes for initial route.

TABLE 13.16-VIII

Entry-Control Impact Evaluation Summary for Power Operation Mode^a

<u>Operational Area</u>	<u>Residence Time</u>	<u>Required Entries^b</u>	<u>Total Entries^c</u>	<u>Total Time with ECS</u>	<u>Total Time without ECS</u>	<u>ΔT</u>
<u>Power Operation</u>						
1 AUX-1-1	2500	1200	1400	24	23	1
2 AUX-2-1	2500	1200	8500	224	158	66
3 CB-2-1	1400	700	900	25	10	15
4 CWST	1900	900	900	14	14	0
5 DGB-1-1	200	100	100	3	3	0
6 DGB-1-2	200	100	100	2	1	1
7 ESWB	1300	700	700	46	46	0
8 RB-1-1	300	100	100	2	2	0
9 RB-2-1	300	100	300	39	36	3
10 TB-2-1	4700	2300	2400	74	65	9
11 OSPW	200	100	100	7	7	0
12 On-site	0	0	8300	234	192	42
TOTAL	15,500	7500	23,800	694	557	137

^aAll times in hours

^bThe number of entries required for jobs to be performed in the indicated area

^cThe total number of entries into the indicated area

II.4 Refueling Mode Analysis Data

Required access times without entry-control are mostly summarized in Figure 13.16-6, and access times with entry-control are summarized in Figure 13.16-7. These figures are incomplete, as indicated by the asterisk (*). The class participants are requested to provide the required data. Table 13.16-IX provides appropriate transit times.

Figure 13.16-8 mostly summarizes the total number of entries to each operational area. Data for required entries for areas 1 through 7 are summarized. The class participants are requested to provide the additional data due to required entries into locations 8 through 11. Table 13.16-X provides applicable route data.

Table 13.16-XI mostly summarizes the total ΔT impact due to the entry-control system for the refueling mode. The participants are requested to complete this table as a class exercise.

Figure 13.16-6. Refueling Mode: Access Times (minutes) without Entry Control

Figure 13.16-7. Refueling Mode: Access Times (minutes) with Entry Control

TABLE 13.16-IX

Transit Time Summary, Refueling Mode^a

<u>Path</u>	<u>Access Controls Used</u>	<u>Transit Time without Entry-Control</u>	<u>Transit Time with Entry-Control</u>	<u>Δ Transit Time</u>
2-1	None	1.02	1.02	0
6-1	Card Reader	0.48	0.96	0.48
1-2	None	1.02	1.02	0
3-2	Badge Exchange	0.48	1.5	1.02
9-2	Badge Exchange	1.8	2.82	1.02
10-2	Card Reader	1.02	1.5	0.48
12-2	Card Reader	0.9	1.38	0.48
2-3	Badge Exchange	0.48	1.56 ^b	1.08 ^b
5-3	Card Reader	1.5	1.98	0.48
10-3	Badge Exchange	1.2	2.28 ^b	1.08 ^b
12-4	None	0.9	0.9	0
3-5	Card Reader	1.5	1.98	0.48
1-6	Card Reader	0.48	0.96	0.48
12-7	None	3.9	3.9	0
9-8	None	1.02	1.02	0
2-9	Badge Exchange	1.8	2.82	1.02
8-9	None	1.02	1.02	0
12-9	Badge Exchange	0.48	1.5	1.02
2-10	Card Reader	1.02	1.5	0.48
3-10	Badge Exchange	1.2	2.22	1.02
12-10	None	2.1	2.1	0
12-11	None	3.9	3.9	0
2-12	Card Reader	0.9	1.38	0.48
4-12	None	0.9	0.9	0
7-12	None	3.9	3.9	0
9-12	Badge Exchange	0.48	1.5	1.02
10-12	None	3.9	3.9	0
11-12	None	2.1	2.1	0

^aAll times in hours^bIncludes metal detector false alarm rate

*INDICATES ADDITIONAL ENTRIES REQUIRED DUE TO LOCATIONS 8 THROUGH 11

Figure 13.16-8. Refueling Mode: Number of Entries

TABLE 13.16-X
Refueling Mode Routing Data

<u>Operational Area</u>	<u>Required Entries</u>	<u>Route</u>	<u>Notes</u>
1 AUX-1-1	1600	12-2-1	1,4
	500	2-1	3,4
	500	9-2-1	3,4
2 AUX-2-1	1600	12-2	1,4
	500	2-1	3,4
	500	9-2	3,4
3 CB-2-1	600	12-2-3	1
4 CWST	500	12-4	1
	400	12-2-12-4	2
5 DGB-1-1	100	12-10-3-5	1
	100	12-2-3-5	1
	100	1-2-3-5	3
6 DGB-1-2	200	12-2-1-6	1
	100	1-6	3
7 ESWB	400	12-7	1
	300	12-2-12-7	2
8 RB-1-1	1500	12-9-8	1,4
	1500	12-2-9-8	1,4
	1500	9-8	3,4
9 RB-2-1	1500	12-9	1,4
	1500	12-2-9	1,4
	1500	8-9	3,4
10 TB-2-10	1300	12-10	1
	500	12-2-10	2
	500	2-10	3
11 OSPW1	50	12-11	1
	50	12-2-12-11	2

- Notes:
1. Assumed route is from off-site to area and then reversed.
 2. Assumed route is from off-site to area via one or more extra areas (for job orders, tools, etc.), and then assumed route is reversed.
 3. Assumed starting area is not from off-site, and route is reversed.
 4. Some routes are extended to other areas as per note 3; however, this does not require changes for initial route.

Table 13.16-XI
Entry-Control Impact Evaluation Summary for Refueling Mode^a

		<u>Residence Time</u>	<u>Required Entries^b</u>	<u>Total Entries^c</u>	<u>Total Time with ECS</u>	<u>Total Time without ECS</u>	<u>ΔT</u>
Operational Area		Power Operation					
1	AUX-1-1	6100	2600	3700	63	60	3
2	AUX-2-1	6100	2600	18,300	500	338	162
3	CB-2-1	1300	600	1200	35	16	19
4	CWST	2000	900	900	14	14	0
5	DGB-1-1	600	300	300	10	8	2
6	DGB-1-2	600	300	300	5	2	3
7	ESWB	1600	700	700	46	46	0
8	RB-1-1	10,500	4500	6000	d	d	d
9	RB-2-1	10,500	4500	13,000	d	d	d
10	TB-2-1	5300	2300	2500	78	68	10
11	OSPW	200	100	100	7	7	0
12	On-site	<u>0</u>	<u>0</u>	<u>15,200</u>	<u>399</u>	<u>275</u>	<u>124</u>
Total		44,800	19,400	47,000	1624	1182	442

^aAll times in hours

^bNumber of entries required for jobs to be performed in the indicated area

^cTotal number of entries into the indicated area

^dParticipants to provide values

II.5 Analysis Results Summary

Table 13.16-III shows the impact of the implementation of entry-control measures on the time required to access the various operational areas.

The column labelled "Residence Time" represents the total time spent at that particular area. The column labelled "Total Entries" gives the total number of entries into each area. The column labelled "With ECS" gives the total access times into an area after the implementation of the proposed entry-control system (ECS). The column labelled "Without ECS" gives the total access times without implementation of the ECS. The column labelled " ΔT " shows the difference between the "With ECS" and "Without ECS" column. This difference represents the increase in time required to access the various areas.

The major item of interest which can be seen on this table is the comparison of the various ΔT 's with their associated residence times. For example, in the power operation case, it can be seen that 2500 hours is the residence time in the AUX-1-1 area. The ΔT for access to this area is 1 hour, which represents only 0.04 percent of the total residence time. When this comparison is made, it can be seen that the implementation of entry-control measures clearly has little impact compared to the total residence time in this case. However, by comparing the access times without entry-control to the access times with entry-control, yields a different result. For example, in the case of the CB-2-1 area during the refueling mode, the access time is doubled by the implementation of entry-controls. The conclusion about the impact of entry-control on plant operation for this sample problem depends upon the analyst's perspective. When compared to total access time requirements, the impact is significant (26 percent for power operation and 35 percent for refueling). However, when compared to the total time spent in the operational areas (residence time) the change with entry-control is negligible.

III. INSTRUCTIONAL GUIDELINES

1. Discuss the session objectives. Note that while the overall objective is to develop an analysis capability for entry-control cost/impact studies, the subgroup session exercises actually assess entry-control system user-time impact.
2. Discuss the problem description. Note that we will review an impact analysis for the normal operational mode, and then the students will perform an equivalent analysis for the refueling mode. Specific student requirements are given in Section II.4.
3. Review the personnel data section. Note that (1) the number of people at the site, (2) time spent in entry-controlled locations, and (3) plant transit paths are all required for an effective analysis. Data given in this section are assumed for this problem. These data are believed to be reasonable.

Note:

- People are not in entry-controlled locations at all times. Table 13.16-I implies 38 to 84 percent depending upon the type of employee.
 - Residence times to perform a job function are approximately 2 hours per entry in all cases except for contractor personnel during refueling which have slightly larger residence times.
4. Review the entry-control data. In particular, Note the following:
 - Figures 13.16-1 and 13.16-2 show entry-control locations and also give area numbers and area identification names.
 - Table 13.16-II details the entry-control features. In particular, note the ΔT values and the footnote. This information is later used in the analysis.
 - Tables 13.16-III and 13.16-IV give the total entries to each operational area. Ask how these were obtained. The answer is that residence times (Table 13.16-I) for each type of staff were allocated to areas the staff would be expected to access. These times with operations mode and refueling mode assumptions yield number of entries.
 - Table 13.16-V -- Note all tables list the areas from area number 1 to 11 or 12. Note area 12 is "On-Site." This area provides the transition between the Reactor and Auxiliary Buildings and other areas such as OSPW and ESWB.
 5. Review the operational mode analysis in Section II.4.
 - Figures 13.16-3, 13.16-4, and 13.16-5 contain all of the necessary analysis data. These figures are developed directly from the data provided in Tables 13.16-VI and 13.16-VII.
 - In Table 13.16-VI, data for transit time without entry-control are obtained by estimates based upon actual entry location specifics. For

transit time with entry-control, add the additional ΔT due to the specified control features, shown in Figures 13.16-1 and 13.16-2. Show how these times are recorded on the diagrams. Pick paths 2-9, 9-2 and 2-3, 3-2 for examples.

- Table 13.16-VII gives the routes for numbers of entries. Entry numbers were obtained from Table 13.16-III. Routes are assumed. Discuss the footnotes in Table 13.16-VII. Show how the entry data are logged in Figure 13.16-5 for the first two areas.
 - Regarding Table 13.16-VIII, review how Figures 13.16-3 or 13.16-4 and 13.16-5 are used to obtain the analysis results. For area 1, total entries are multiplied by time per entry with and time per entry without ECS to get total times. ΔT is then the difference in times. Note that for completeness, Table 13.16-VIII also gives operational residence times.
6. Have the participants perform the required analyses, as specified in Section II.4. Assist when required. Note that completed Figures 13.16-6, 13.16-7, and 13.16-8 are provided for the instructors.
 7. Discuss the analyses results. Ask the participants if they feel the ΔT impact is significant.
 8. Hand out the instructional guidelines.
 9. Read and discuss the think-about items.

IV. THINK-ABOUT ITEMS

1. Assumptions were made in Table 13.16-VII for the selected routes. Do you think that these assumptions would be valid for a real plant situation?
2. How would you obtain entry data for an existing site?
3. How might a malfunctioning entry-control system impact operations?
Consider
 - Locked out (Type I error).
 - Malfunctioning metal detector
4. What impact might entry-control system have on the security guards?
Consider
 - Type I and II errors require more guards
 - Enrollment time and costs, deletion costs
5. How might an entry-control system impact the safety of operations?
Consider
 - Delayed response to fire, criticality accidents, etc.
 - Evacuation restrictions (turnstiles)
6. How might false alarms impact your design for Type I errors? Consider that
 - High Type I error rate may cause bypass of features
 - Type I competes with Type II
7. Based on past subgroup discussions, do the entry-control features identified in this exercise appear to have logical bases for their locations?
8. The difference(s) in access times for this analysis were very short compared to the residence times for performing various jobs, and a cost figure could be associated with the total difference in access times. What other costs might be considered if you were performing a cost/impact analysis? Consider
 - Personnel queuing at entries
 - System debugging
 - Maintenance
 - Response to Type I errors
 - Performance verification and testing
 - Enrollment/deletion costs
 - Central control system operations
 - Software
 - Protection of entry-control systems--i.e., hardware, software, feature thresholds, etc.--from adversary compromise
 - Guard and operations personnel training

9. How might you change the arc and node diagram to include entry from off-site? (Example: Make node 13 off-site, and connect 13 to 12 and to 11). Are other changes desirable or necessary?
10. Why are the entry-control features located within the buildings between areas?

4.0 REACTORS

Session Title: 4.4 Reactor Vulnerabilities

Date: Monday, 3 December 1979

Presented By: G. B. Varnado
Sandia Laboratories

Time: 1330 to 1430

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 two 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 4.4-I. 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 4.4-I
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 (Criticality incident	Sabotage or Theft 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 4.4-1.

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 4.4-1. 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 4.4-2.

Figure 4.4-2. 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 4.4-3 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 4.4-3. 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, that is, 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

piping 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 3 fuel assemblies; a rail cask can weigh as much as 100,000 kilograms and carry 10 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,

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 4.4-II. The events which

TABLE 4.4-II

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 4.4-4 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 4.4-4. 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 4.4-5 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 4 4-5 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 4.4-6 shows a fuel storage well for a high-temperature, gas-cooled reactor.

Figure 4.4-6. 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 4.4-III. 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 4.4-III

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

Distribution:

G. Weisz, Director
Office of Safeguards & Security
Department of Energy
Mail Stop A2-1016
Washington, DC 20545

L. M. Brenner
Office of Safeguards & Security
Department of Energy
Mail Stop A2-1016
Washington, DC 20545

W. Haggis
Office of Safeguards & Security
Department of Energy
Mail Stop A2-1016
Washington, DC 20545

Katherine Larson
International Atomic Energy Agency
Wagramerstrasse 5
P. O. Box 100, A-1400
Vienna, Austria

R. Erickson, Chief
Physical Security Development Branch
Division of Safeguards
Office of NMSS
Nuclear Regulatory Commission
Washington, DC 20555

G. R. Keepin
Los Alamos National Scientific Laboratory
Mail Stop 550
Los Alamos, NM 87544

P. Ebel
Allied General Nuclear Service
P. O. Box 847
Barnwell, SC 29812

B. M. Jenkins
The Rand Corporation
1700 Main Street
Santa Monica, CA 90406

R. A. Knief
Department of Chemical &
Nuclear Engineering
University of New Mexico
Albuquerque, NM 87131