SAND2013-5693P

Contingency Plan Development and Tabletop Exercise

Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities – INFCIRC/225/Revision 5

Course Outline

- Introductions
- Background on INFCIRC/225/Revision 5
- Physical Protection Systems
- Development of Draft Contingency Plan
- Scenario Development
- Tabletop Exercise
- Contingency Plan Evaluation and Path Forward
- Summary

Introductions

- Moderators
- Participants
  - Name
  - Organization
  - Experience with INFCIRC/225/Revision 5
  - Experience with Response Contingency Plans
  - Experience with Table Top Exercises

Format of the Workshop

- Presentations on Subject
- Group Discussion and Exercise: work on team(s) to complete Contingency Plan Draft
- Tabletop Exercise(s)

INFCIRC/225/Revision 5 Requirements for Contingency Planning

Course Objectives

After completing this course, you should be able to:

- Describe the INFCIRC/225 recommendations for contingency plans
- Distinguish between security plans, contingency plans, and emergency plans
- Identify the recommended requirements for contingency planning
- List the elements and considerations for contingency planning
- Create a draft contingency plan
- Conduct a tabletop exercise

Student Learning Objectives

After completing this module, students should be able to:

- Describe the INFCIRC/225 recommendations for contingency plans
- Distinguish between security plans, contingency plans, and emergency plans
- Identify the recommended requirements for contingency planning

Physical Protection Regime

Physical Protection Regime Entities

- State
- Competent Authority
- Licence Holders
  - Operator of nuclear facilities
  - Shipper for transport of nuclear materials

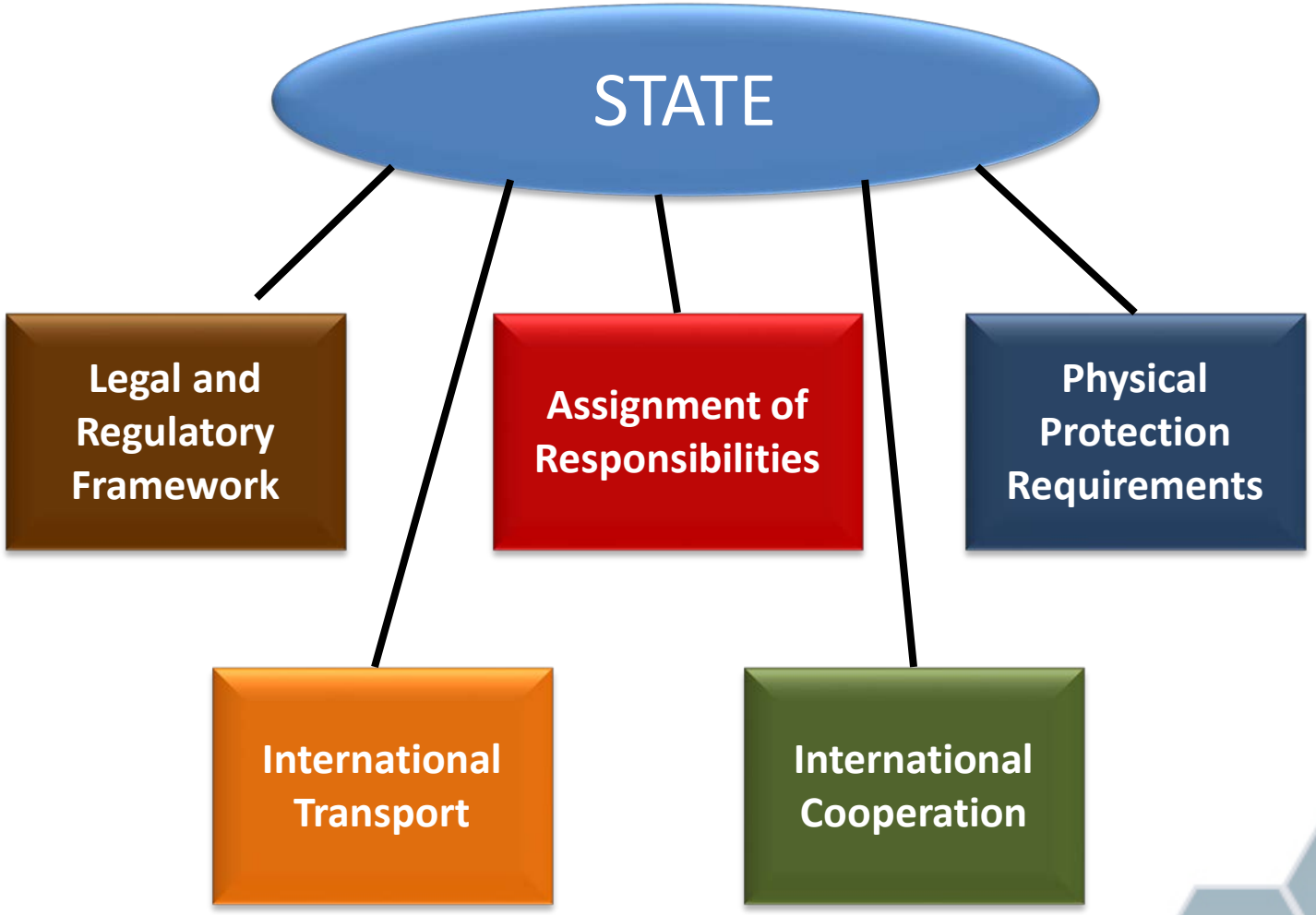
Nuclear Security Culture crosses all three levels

State

Fundamental Principle A

The responsibility for the establishment, implementation, and maintenance of a physical protection regime within a State rests entirely with that State.

State Responsibility



Objectives of State's Physical Protection Regime

- **To protect against unauthorized removal:** protecting against theft and other unlawful taking of nuclear material.
- **To locate and recover missing nuclear material:** ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material.
- **To protect against sabotage:** protecting nuclear material and nuclear facilities against sabotage.
- **To mitigate or minimize effects of sabotage:** mitigating or minimizing the radiological consequences of sabotage.

State Responsibility

- Establishment, implementation, and maintenance of a physical protection regime
  - All nuclear material in use and storage
  - During transport
  - For all nuclear facilities

Competent Authority

Fundamental Principle D

The State should establish or designate a competent authority that is responsible for the implementation of the legislative and regulatory framework and is provided with adequate authority, competence, and financial and human resources to fulfill the assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.

Competent Authority

- Designated by the State with clearly defined legal status and independent from
  - Applicants
  - Operators
  - Shippers
  - Carriers
- Provided adequate
  - Legal authority
  - Competence
  - Financial resources
  - Human resources

Competent Authority Responsibility

- Responsible for review and approval for Licence Holder Security and Contingency Plans
- Have access to State's system for nuclear material accountancy and control
- Responsible for verifying continued compliance
- Conducting evaluation based on performance testing
- Ensure corrective actions are taken when needed
- Provide timely reports for nuclear security events

Licence Holders

Fundamental Principle E

The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licences or of other authorizing documents (e.g., operators or shippers).

Licence Holders Responsibility

Defined as operators or shipper/carriers

- Compliance with regulations
- Cooperation & coordination with State entities having physical protection responsibilities
- Material accountancy and control
- Development of security plan and contingency plan
- Optimum site selection and design
- Development and implementation of means and procedures for evaluation and maintenance of the PPS
- Compensatory measures

Definitions

- **Security Plans** – Based on design basis threat/threat assessment and include design, evaluation, implementation and maintenance of physical protection system and contingency plans

- **Contingency Plans** – Predefined sets of actions for response to security events such as unauthorized acts indicative of attempted unauthorized removal or sabotage designed to effectively counter such acts

- **Emergency Plans** - Predefined sets of actions for response to safety events or other emergency events

Examples

Contingency Plan Response to Security Events	Emergency Plan Response to Safety/ Emergency Event
Protestors at the facility	Fire on site
Criminal activity at the facility	Flooding
Hostage situation	Extreme weather with impacts to the site
Unauthorized Removal of Nuclear Material	Loss of Power
Sabotage of vital equipment	Loss of Communications
Possible Insider Threat	Medical Emergency

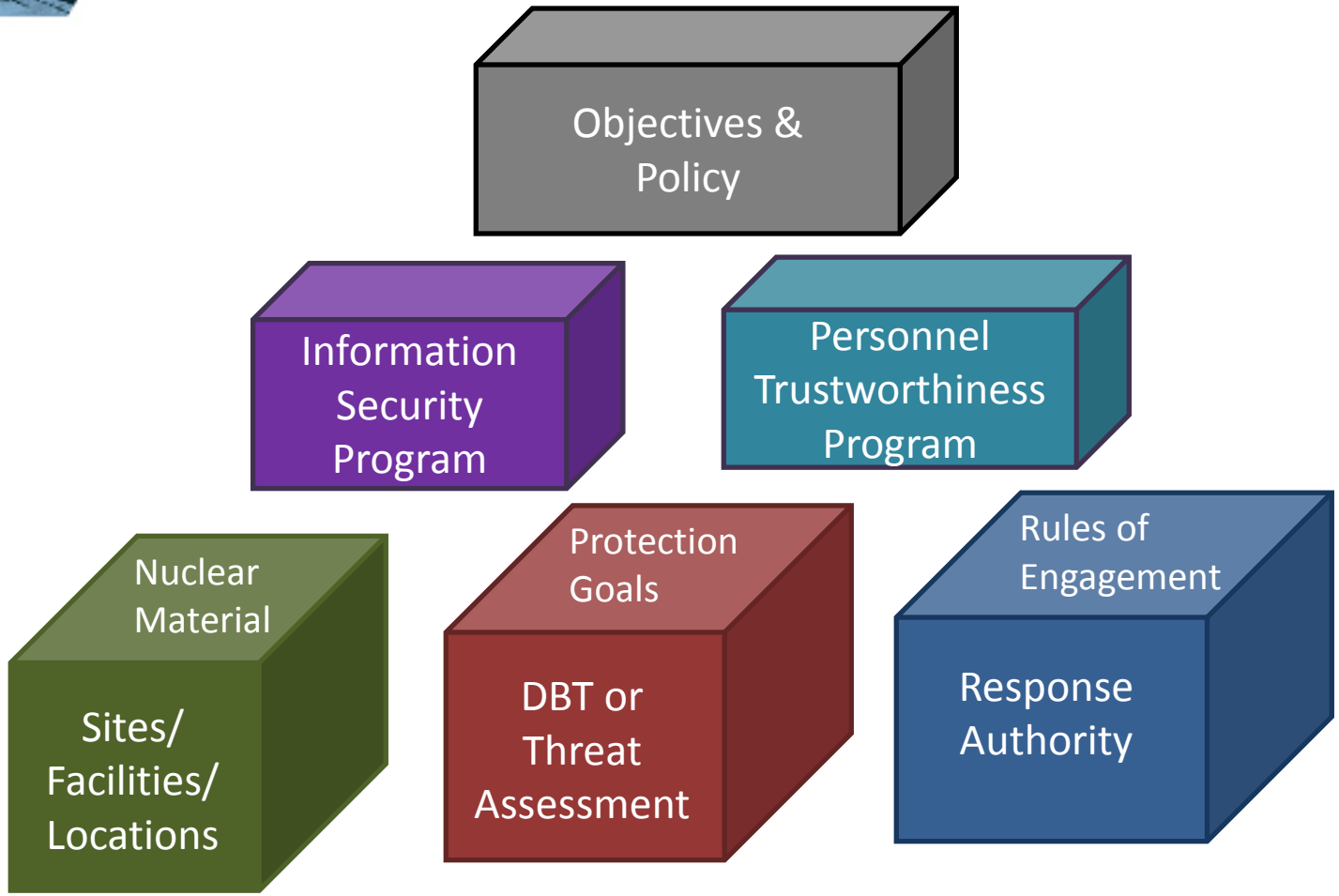
Safety/Security Interface

- While nuclear safety and security share a common objective, there are points of potential conflict between the measures taken in each area to accomplish that objective
  - Safety requirements for emergency egress versus security requirements to minimize access points
  - Safety requirements for transparency versus security requirements to maintain confidentiality of security information
- Designers and operators must take care to ensure that security measures do not compromise safety and that safety measures do not compromise security

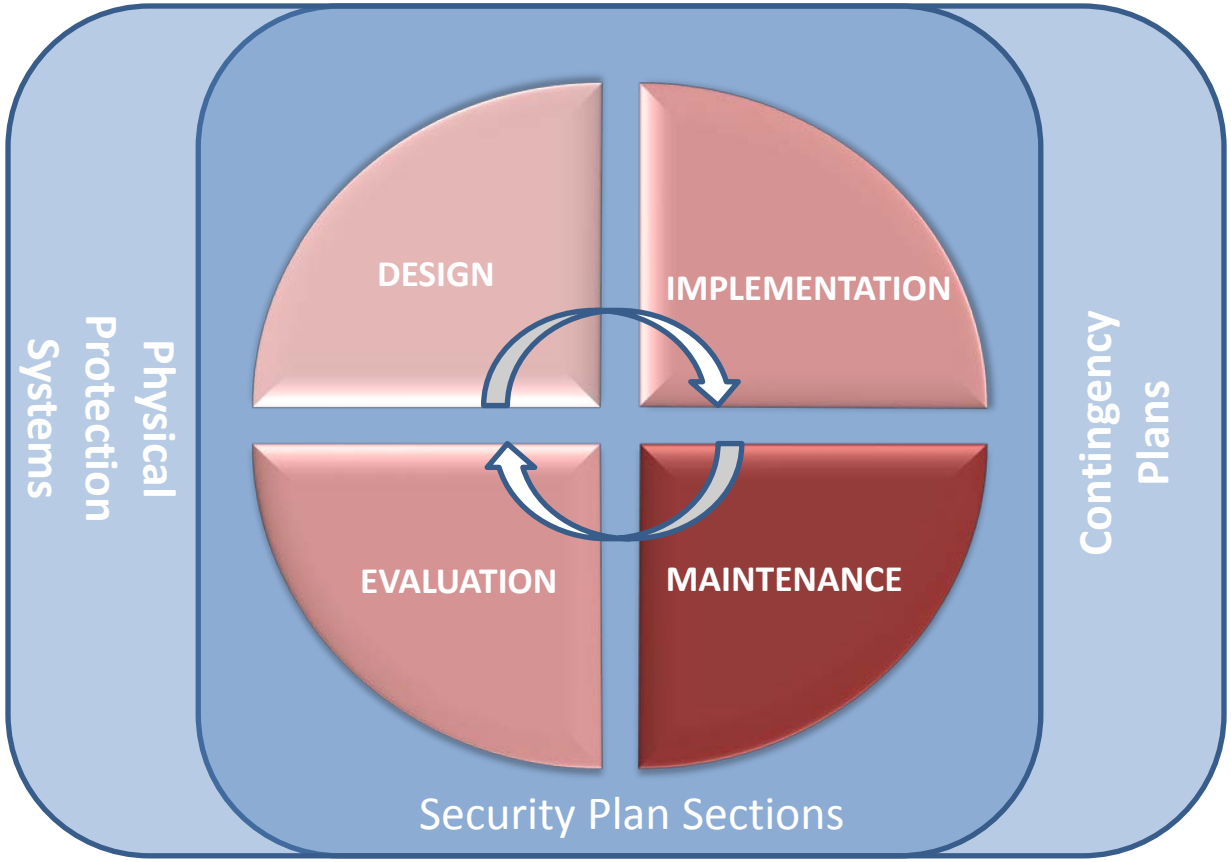
Planning and Preparedness for and Response to Nuclear Security Events

- Established by the State
- Competent authority ensures operator contingency plans are consistent with and complementary to the State's contingency plan
- Operator contingency plans (approved by the competent authority) should effectively counter the threat taking the actions of response forces into consideration
- Coordination between guards and response forces during a nuclear security event should be regularly exercised
- Effectiveness of physical protection systems should be maintained during emergency conditions
- Initiated after detection and assessment of any malicious act.

State Security Plans



License Holder Security Plans



- Part of an application to obtain a license
- Approved and verified by the competent authority
- Regularly reviewed and updated for changes approved by the competent authority

Contingency Plans

- Fundamental Principle K: Contingency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned
- Recommended Requirements: 3.58-3.62

Contingency Plans

- Roles, Responsibilities, and Associated Structure
- Description of Objectives
- Policy and concept of operations for a systematic, coordinated, and effective response
- Arrangement and protocols for appropriate State agencies, operators/shippers/carriers, and other response organizations or relevant entities
- Plans to counter the threat assessment or design basis threat
- Actions of the response force both on-site and off-site
- Maintenance of physical protection effectiveness

State Contingency Plan

Fixed Sites and Transportation

Minimization/Mitigation of Sabotage Radiological Consequences

- Includes objectives, policy and concept of operation for all the response agencies
- Structure authorities, and responsibilities for a systematic, coordinated, and effective response
- Based on arrangements and protocols for coordinated implementation of measures for
  - Preventing further damage
  - Protecting emergency equipment and personnel
  - Onsite radiation protection for response personnel

State Contingency Plan

Fixed Sites and Transportation

Locate and Recovery

- Defines the roles and responsibilities of appropriate State response organizations and operators
  - National Police
  - Hazmat Teams
  - Border Control
- Goal of rapid recovery and appropriate re-securing of material

State Contingency Plan

Fixed Sites and Transportation

Exercised to:

- Assess and Validate contingency plan
- Train site personnel and responders on actions to be taken
- Joint exercises held with appropriate organizations
- Ensure response forces
  - Are familiar with
    - Sites
    - Nuclear material locations
    - Sabotage targets
  - Have adequate knowledge of radiation protection
- Review and update
- Incorporate lessons learned

License Holder Contingency Plan

- Approved by Competent Authority
- Initiated after detection and assessment of a malicious act
- Should include the objectives, policy and concept of operation for response to a security incident
- Interfaces with the state plans for rapid recovery of material
- Interfaces with the Security and Safety plans

License Holder Contingency Plan

- Implemented:
  - To protect against unauthorized removal
  - To locate and recover missing nuclear material
  - To protect against sabotage
  - To mitigate or minimize effect of sabotage
- Focus on preventing further damage, securing the site and protection of equipment and personnel
- Regularly tested and evaluated
  - Exercises to train and validate plan
- Other requirements similar to those listed for State

Locate & Recover Requirements In Use & Storage (4.50-4.63)

State	Licence Holder
Ensure rapid response to locate and recover	Timely detection of missing material
Define roles and responsibilities	Confirmation of missing material through rapid inventory using NMACS
Ensure State and operator contingency plans exist	Notification of competent authority
Assure exercise and review of State contingency plans	Contingency plans, including • Off-site pursuit, if needed • Measures to locate and recover material
	Ability to secure and return material to appropriate nuclear facility
	Provide assistance to the State

Mitigation/Minimization Requirements In Use & Storage (5.44-5.58)

State	Licence Holder
Define roles and responsibilities	Prepare facility personnel to act in full coordination with response
Ensure State and operator contingency plans exist, are complementary, and regularly reviewed and updated	Establish contingency plans
Coordinate response to prevent further damage, security of the nuclear facility, and protect emergency equipment and personnel	Take measures to prevent further damage, security of the nuclear facility, and protect emergency equipment and personnel
Response force familiarization with site and sabotage targets	Notify competent authority of sabotage or sabotage attempt

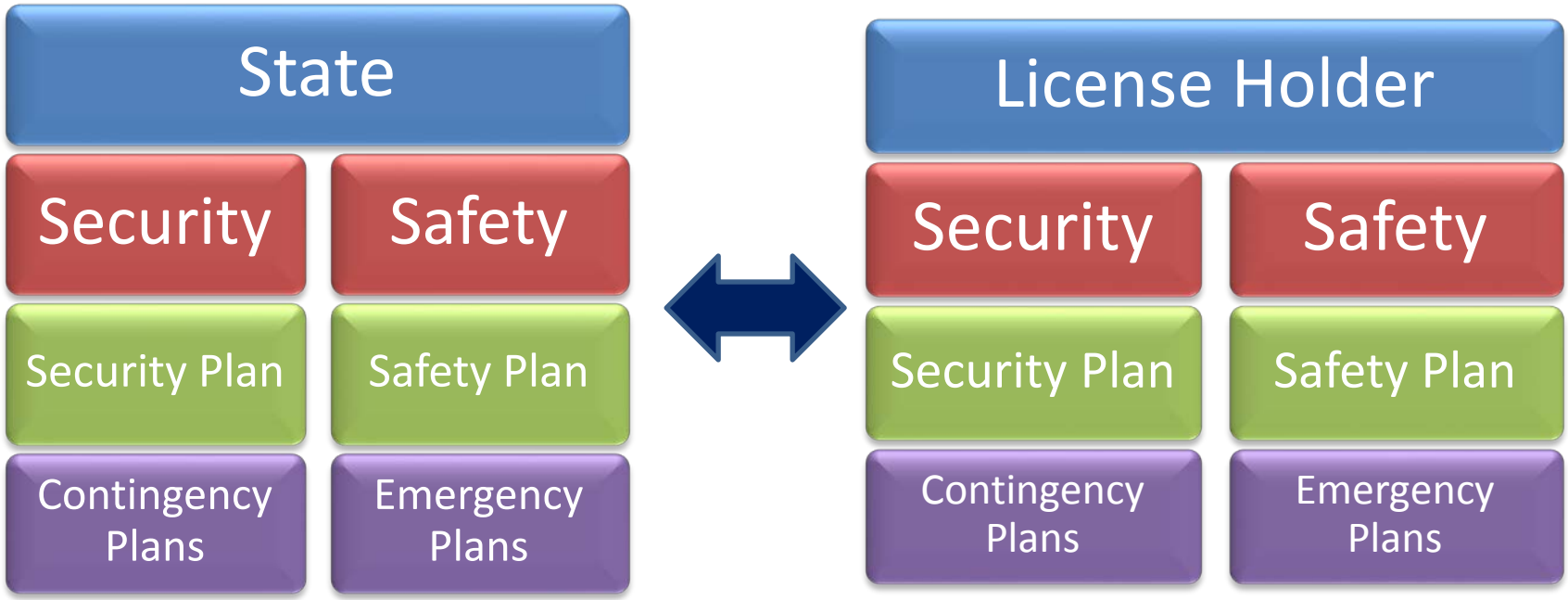
Locate & Recover Requirements Transport (6.44-6.55)

State	Carrier
Ensure rapid response to locate and recover	Alert for indication of theft or tampering
Define roles and responsibilities	Determination of missing material or misplaced, but still under control
Ensure State and operator contingency plans exist	Notification of competent authority and shipper
Assure exercise and review of State contingency plans	Provide assistance to the State

Mitigation/Minimization Requirements - Transport (6.60-6.73)

State	Carrier
Define roles and responsibilities	Prepare transport personnel to act in full coordination with response
Ensure State and operator contingency plans exist, are complementary, and regularly reviewed and updated	Establish contingency plans that interface with safety as appropriate
Coordinate response to prevent further damage, security of the nuclear transport, and protect emergency personnel	Take measures to secure the transport and minimize the consequences of the act.
Response force familiarization with typical transport operations and sabotage targets	Notify shipper, competent authority, response forces, and other relevant State organizations of sabotage or sabotage attempt

State and Licence Holder Plans Should Be Consistent



Summary

- The Nuclear Security Regime includes contingency planning as part of a State's and Licence Holders Security Plan
- The Security Plan contains elements that pertain to the design, implementation, evaluation, and maintenance of contingency plans
- The Contingency Plan includes predefined sets of actions for response to malicious acts during a security incident

Physical Protection System Concepts

Student Learning Objectives

After completing this module, you should be able to:

- Discuss basic physical protection concepts
- Explain the physical protection design process
- Identify transportation, insider, and cyber security issues

Physical Protection System

Definition:

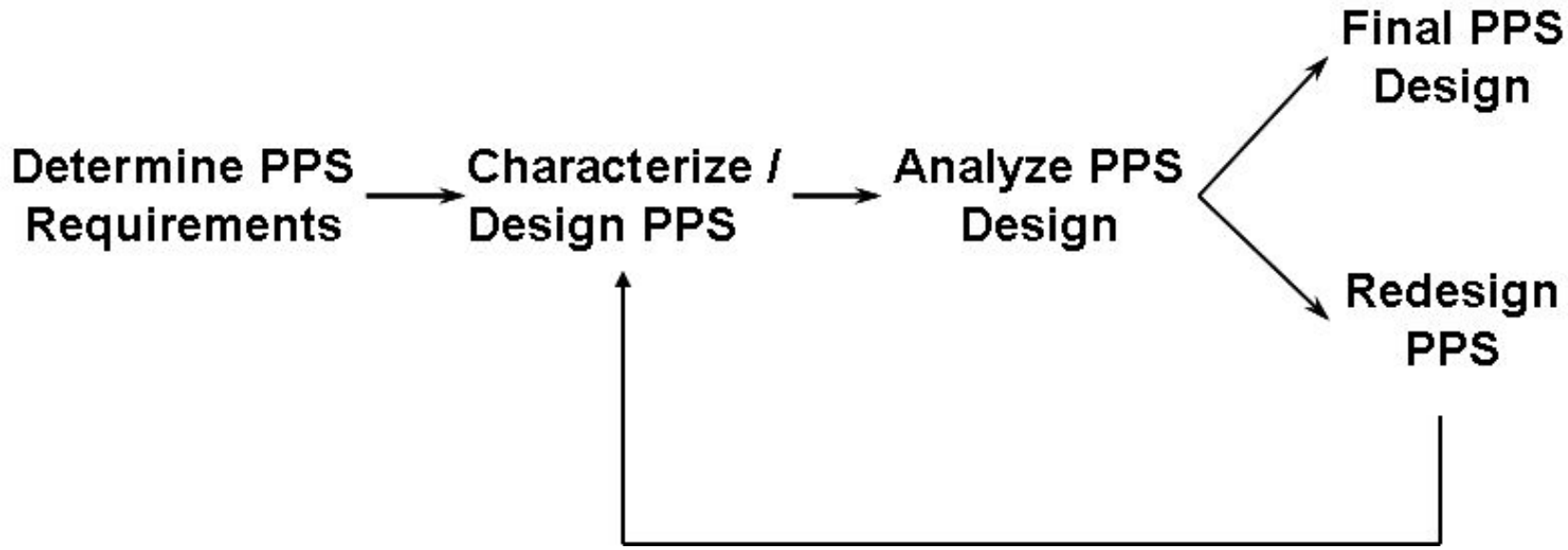
A physical protection system is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks

Objectives of a PPS

- Protect against unauthorized removal of nuclear materials during use, storage, and transport (theft)

- Protect against sabotage of nuclear facilities and sabotage of nuclear material during use, storage, and transport (radiological sabotage)

Physical Protection System Design and Evaluation Cycle



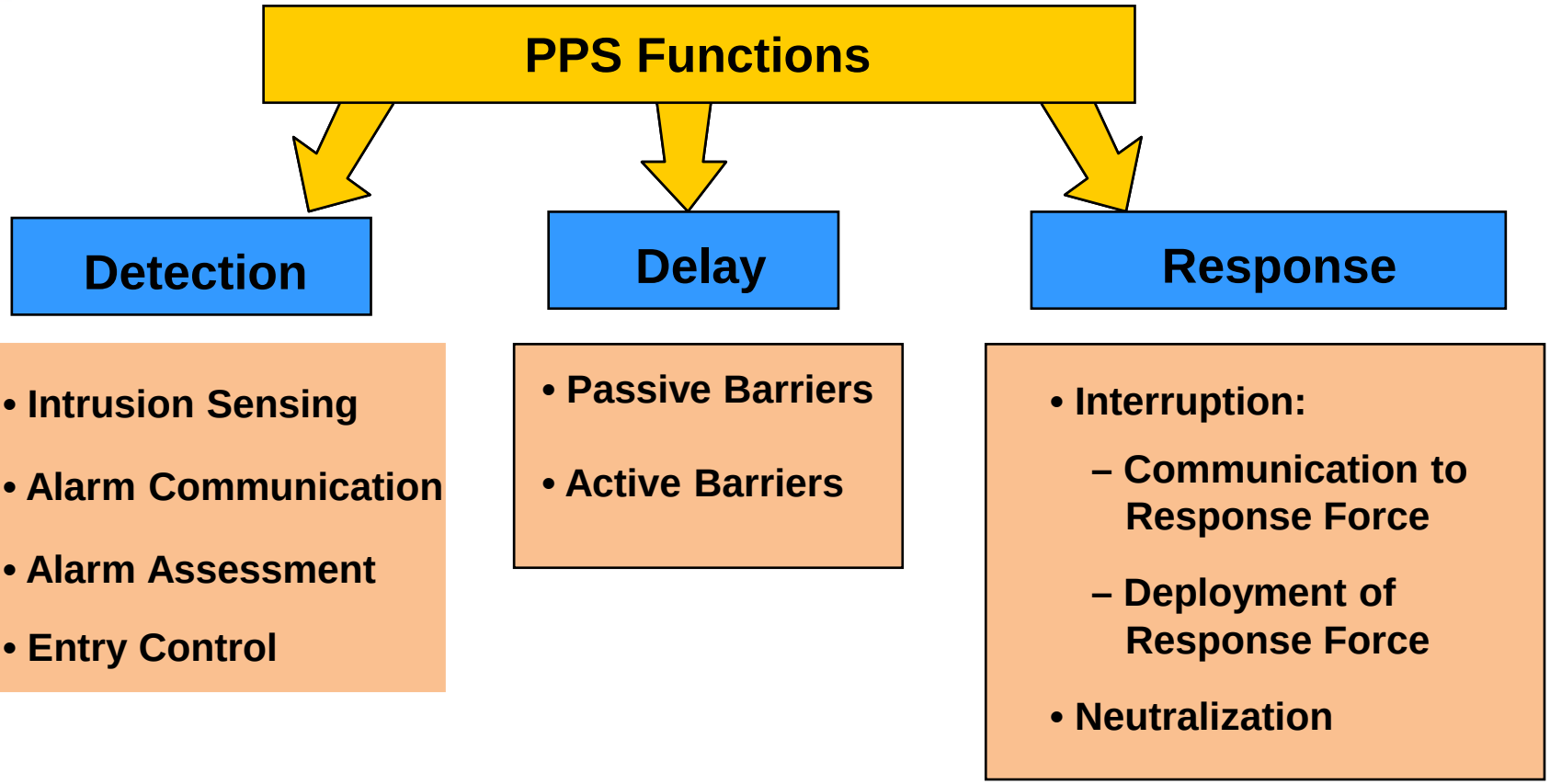
Three Questions that define the requirements for a PPS

1. What must I protect? (What are the assets to be protected?)

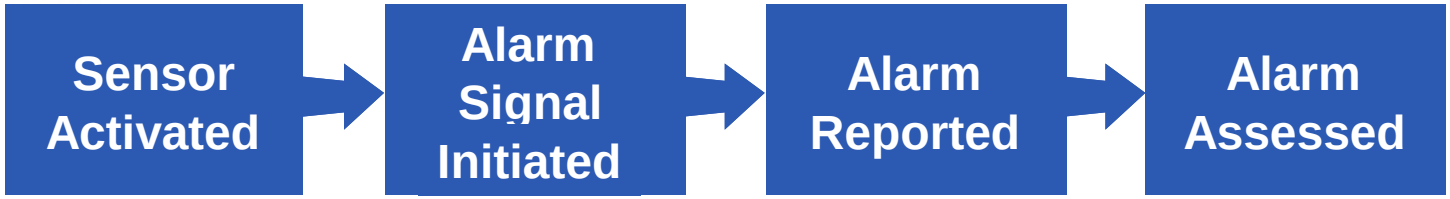
2. What must I protect against? (What is the threat against which the PPS must be designed?)

3. What level of protection is adequate? (What is the acceptance criteria for the PPS?)

PPS Functions



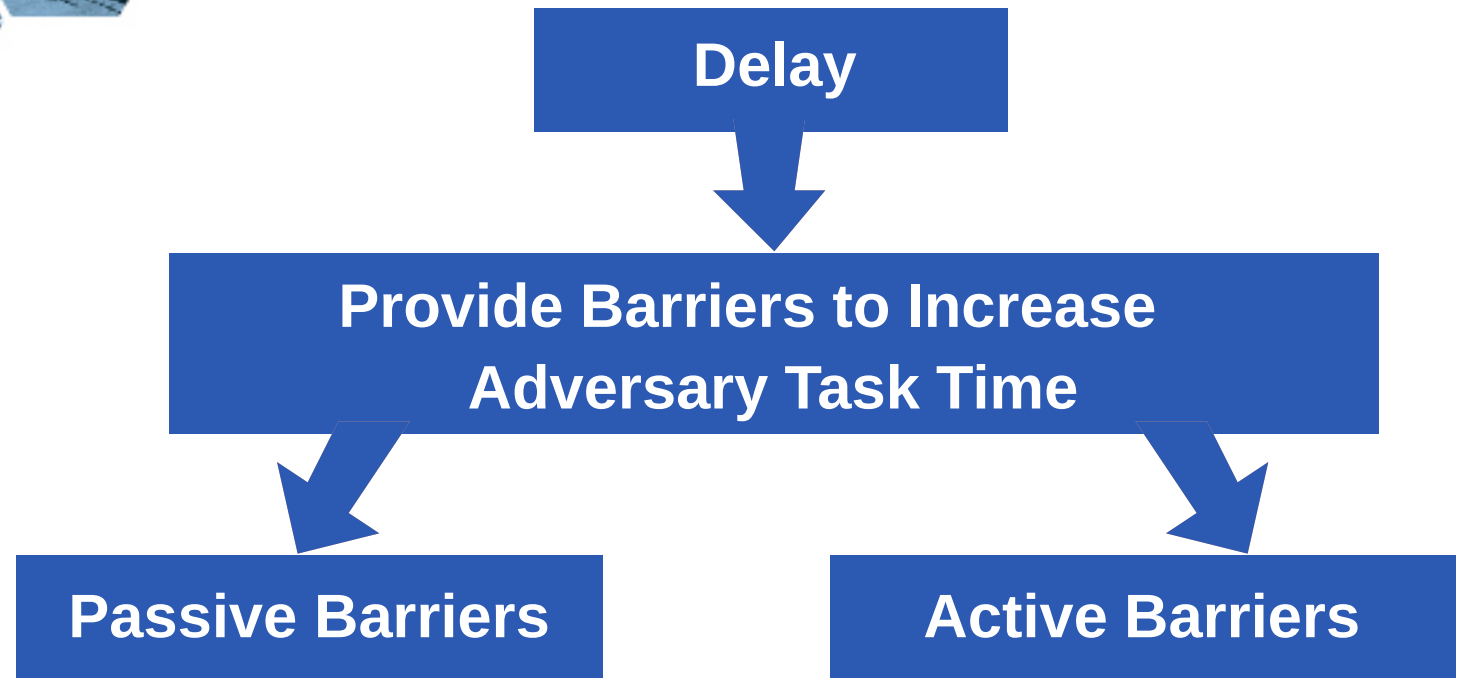
Detection Process



Technologies → **Guards**

- Performance measures:
  - Probability of sensor alarm
  - Communication and Assessment Time
  - Probability of Assessment
  - Nuisance Alarm Rate
  - Assessed detection

Delay Process



- Performance measures
  - Time to penetrate or bypass barriers
  - Time to travel across areas

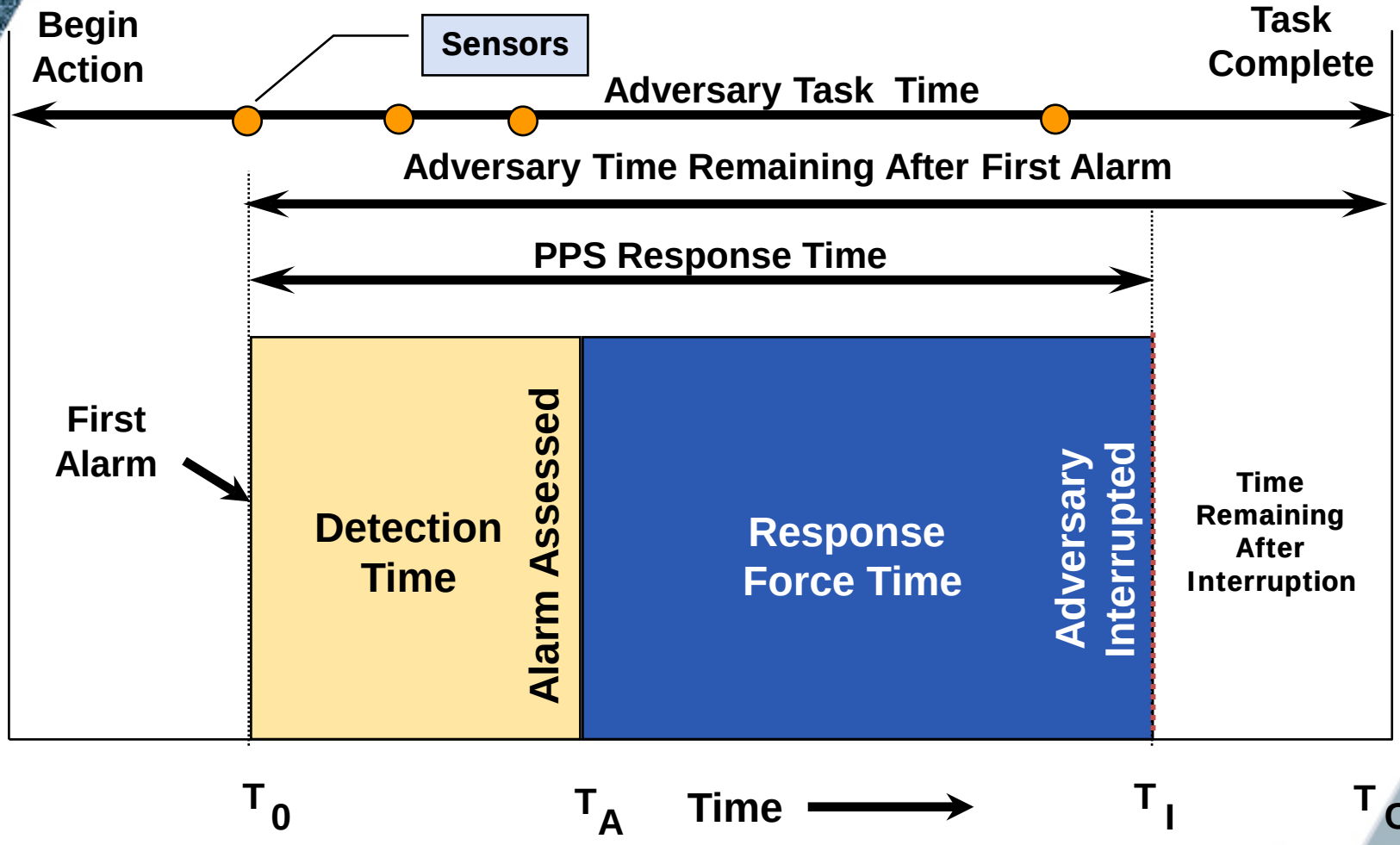
Response Process

- Performance measures
  - Probability of communication to response force
  - Communication time
  - Probability of deployment to adversary location
  - Deployment time
  - Response force effectiveness

Two Competing Timelines

- Adversary Timeline
  - Cross areas
  - Penetrate or bypass barriers
  - Remove or sabotage target
- PPS Timeline
  - Detection process
  - Delay process
  - Response process
- Overlay of two timelines illustrates requirement for PPS effectiveness

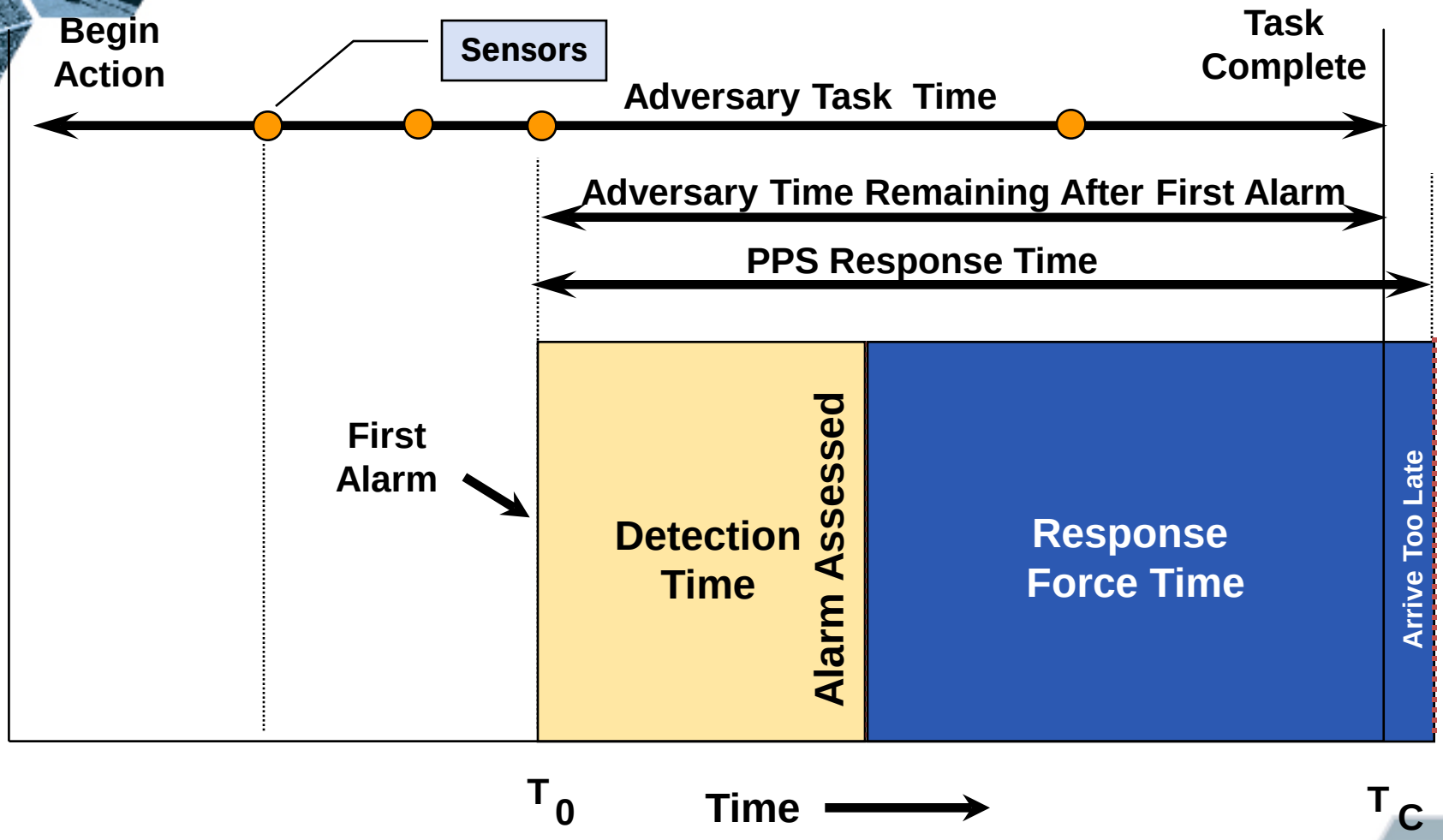
Adversary and PPS Timelines



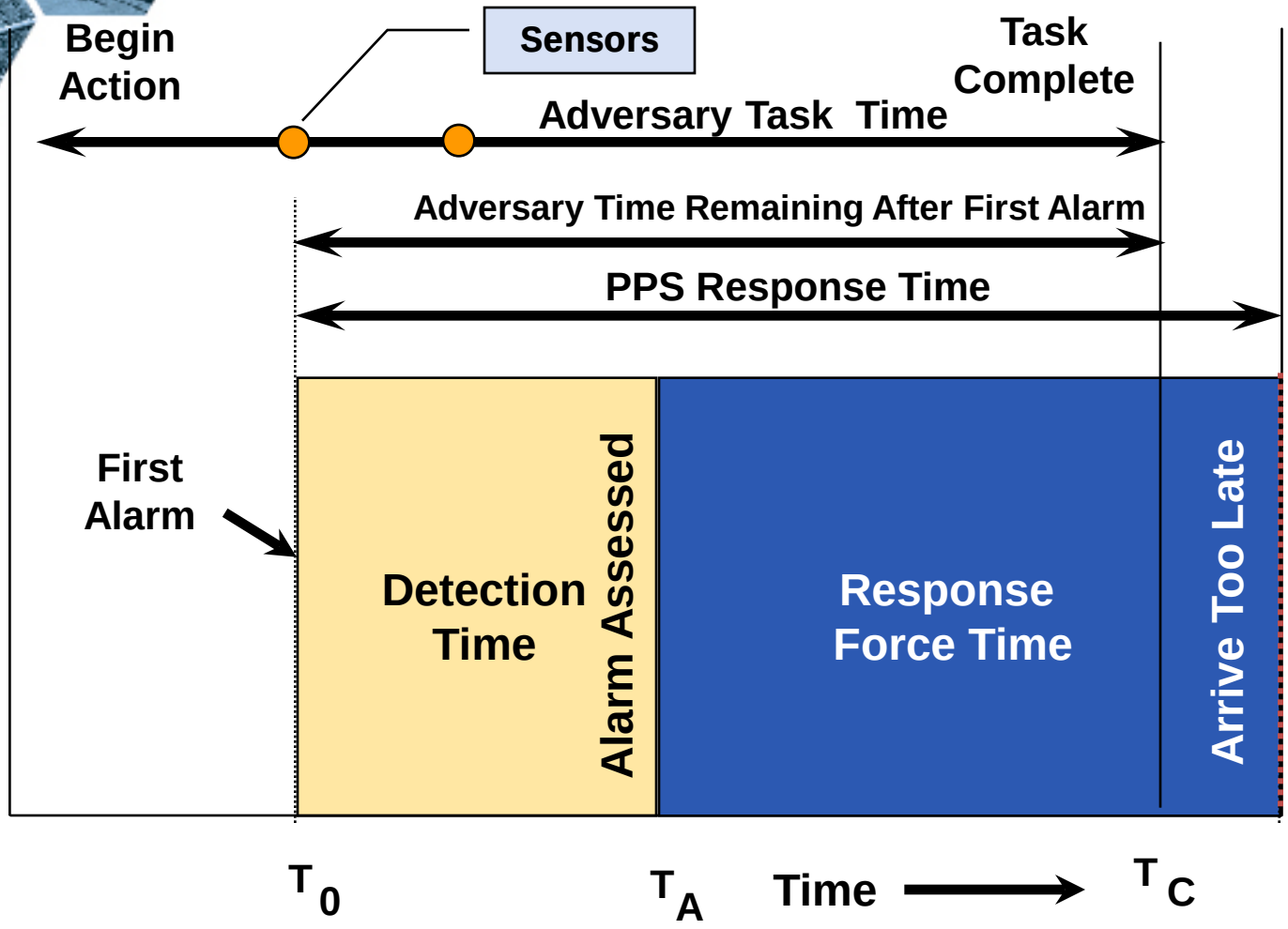
Principle of Timely Detection

- To interrupt the adversary before the theft or sabotage task is complete, the PPS response time must be less than the adversary task time remaining after first detection
- The critical detection point (CDP) is the last detection point along an adversary path for which the PPS response time is less than the adversary task time remaining after first detection
- To be an effective PPS, timely detection must be achieved against the DBT along all adversary paths

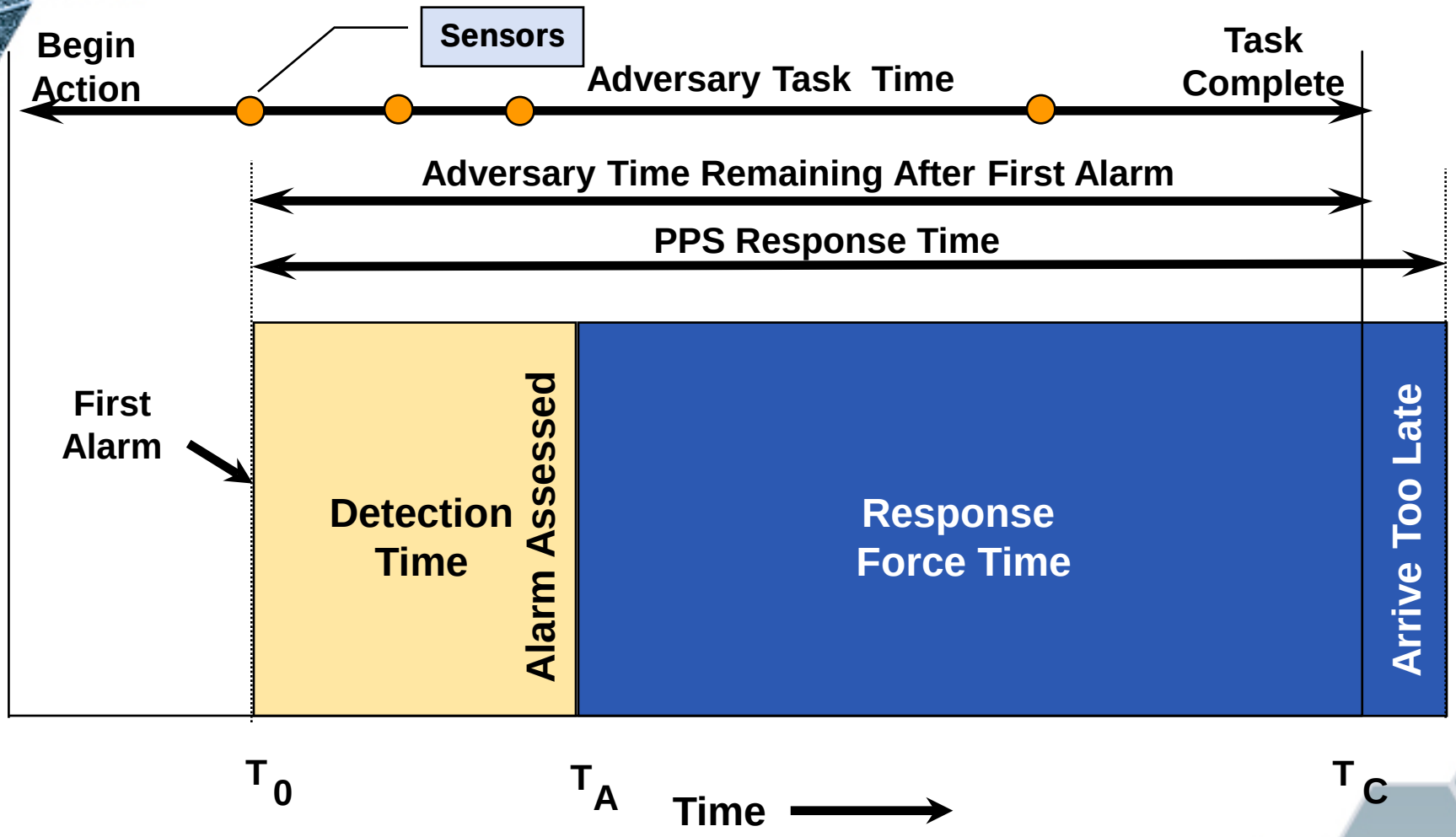
Late Detection



Insufficient Delay



Slow Response



Neutralization

- Very difficult to measure
- Subject matter experts
- Tabletop exercises
- Computer simulation models
- Force-on-force exercises
- The winning combination
  - Right people
  - Right equipment
  - Right training

PPS for Material Transportation

- Physical protection of nuclear material in transport presents challenges not present for fixed sites
- Requires similar physical protection system elements as a fixed site
  - Detection
  - Delay
  - Response
- Follows the same design process
  - Determine system requirements
  - Characterize existing system
    - Detection / Delay / Response
  - Analyze PPS
- Requires scenario analysis to determine system effectiveness

Additional Security Considerations

- Insider Threat
  - Access, Knowledge, Authority
  - Time, Tools, Test, Teaming
  - Group by various factors
  - Develop and test scenarios to calculate probability of detection
  - Various levels of Human Reliability Program
- Information and Cyber Security
  - Consider publicly available information
  - Protection of all PPS related information
  - Protection of Vulnerability Analysis and performance test information
  - Use graded approach to protect information
  - Use of media on-site and limit internet/wireless based networks

PPS Effectiveness

In order to be effective in preventing malicious acts, the three PPS functions must be balanced in order to:

- Provide timely detection
- Provide adequate delay
- Provide effective response (prior to task completion)

Characteristics of Effective PPS Design

- Balanced protection
  - Provide adequate protection against all threats along all adversary paths
- Defense-in-depth
  - Adversary must defeat or avoid a number of varied protective devices in sequence
- High System Reliability
  - Redundant equipment
    - Multiple complementary sensors
    - Multiple complementary barriers
    - Multiple response force groups
  - Contingency plans
    - Compensatory measures
    - Spare parts

Summary

- The purpose of a physical protection system is to prevent successful malicious attacks (theft or sabotage)
- Fundamental design strategy
  - Defeat adversary and use the Design Evaluation Cycle process
- Basic PPS functions
  - Detection
  - Delay
  - Response
- Performances measures
  - Probability of Detection
  - Delay Time
  - Response Time, Probability of Interruption, and Probability of Neutralization

Summary (continued)

- Principle of timely detection
  - To interrupt an adversary before completion of the theft or sabotage task, the PPS response time must be less than the adversary task time remaining after the first sensing
- Additional principles for designing effective PPS
  - Defense-in-depth
  - Balanced protection
  - High system reliability

Contingency Plans

Overview

Student Learning Objectives

After completing this module, you should be able to:

- List the different types of attacks covered in a contingency plan (CP)
- Discuss what areas should be covered by an effective CP
- Indicate considerations to be addressed when developing a CP

Overview - Definitions

- **Security Plans** – Based on design basis threat/threat assessment and include design, evaluation, implementation and maintenance of physical protection system and contingency plans

- **Contingency Plans** – Predefined sets of actions for response to security events such as unauthorized acts indicative of attempted unauthorized removal or sabotage designed to effectively counter such acts

- **Emergency Plans** - Predefined sets of actions for response to safety events or other emergency events

Overview - Attacks and other considerations covered in CP

- Unauthorized removal from the facility, the limited area, the protected area or from an inner area
- Sabotage of a vital area
- Locate and recover missing nuclear material (NM)
- Insider attacks
- Cyber attacks
- Other attacks – airborne, stand-off, hostage/shooter
- Other events – natural disaster, medical, fire, evacuation, civil disturbance
- Bomb threat/bomb found

The different types of attacks may be given code names and have checklists which outline responses, roles/responsibilities, people.

Overview - An effective CP should

- Address the areas of prevent, respond, restore and improve
- Document guidance to personnel to accomplish specific defined objectives related to threats such as theft and/or sabotage to nuclear material or facilities.
- Ensure a timely, effective response and coordinated response at all levels in the event of a malicious (security) event.
- Should be approved by the Competent Authority. Both the State and the facility Operators should have CPs, each covering different types of events.
- Identify the participants in the CP, their specific responsibilities, and be complementary to any emergency plans and/or business continuity plans.

Overview - The CP should include

- Predetermined set of decisions/actions to meet objectives
- Identification of the data, criteria, policies, plans and procedures, concept of operations to implement the CP
- Identification of different individuals/groups and their roles and responsibilities
- Interfaces/coordination with different organizations
- Description of the facility, operations, assets to protect and possible threats
- Details on the response plan for different security events
- Information on training and how performance is measured
- How the CP is reviewed/tested (metrics) and updated

Overview - Contingency Plans

- Based on event type and prepared to counter or mitigate the event consequences.
- Includes – **what, who, when, and where**
- Should be well understood by all response forces
- Should include interfaces with safety (emergency plan)
- Should be periodically drilled/exercised such as
  - Security exercises
  - Fire drills
  - Evacuation drills
  - Shelter in place

Overview - Contingency Plans - What

- Facility characterization
- Target consequence based response strategy (containment or denial)
- For each type response personnel involved:
  - On-site or Off-site
  - Procedures for what they must do including response area location, response time requirement, deployment tactics, rules of engagement
  - Communication protocols
  - Required Equipment (weapons, ammunition, support equipment, vehicles, radios)
  - Facility recapture procedures

Overview - Contingency Plans - Who

- Response Personnel Duties
  - Central Alarm Station personnel or other recipient of alarm
  - Guards
  - On-site Response Force
  - Off-site Response Forces
- Incident Response Personnel – Safety, Emergency, and Operations personnel
- Site Personnel

Overview - Contingency Plans - When

- When to respond
- When to change tactics
- When to escalate use of force
- When to notify other agencies
- When to communicate to the public

Overview - Contingency Plans - Where

- Where are mustering/coordination points
  - Onsite?
  - Off-site coming onsite?
- Where are normal operations patrol areas?
- Where are primary response locations for security incident?
- Where should response move to as the situation progresses?

Overview - Other Decisions

- Can this malicious act lead to radiological consequences?
- What equipment or emergency personnel must be protected to minimize consequences?
- What are the overlaps between safety, security and operations and which has priority?
- When does the incident start and when is it over?

Summary

- Both the State and Operator have CPs
- CPs are based on a event/incident type
- CPs cover various attack scenarios
- What should an effective CP enable the response force to do and areas it should address

Contingency Plans

1.0 Introduction

Student Learning Objectives

After completing this module, you should be able to:

- Identify information to be part of the introduction section of contingency plans (CP)
- Identify references for CP
- Explain the importance of threat in developing a CP

Example Content of CP Introduction

The following are areas to be included in the Introduction Section:

- Scope
- Assumptions
- Threat

CP Introduction - Scope

- What possible scenarios or security events are addressed in the CP
- What conditions are addressed in the CP (normal operations, security/safety abnormal events, severe natural events, other man-caused events)
- What other groups/individuals are part of this CP
- Does the CP address conduct of training or exercises
- List of the pertinent regulations, other requirements, guidance which provide a basis for the CP

CP Introduction - Assumptions

- Support from State, Competent Authority and other key decision-makers
- Defined Risk (threat, consequences, protection)
- Level of any interactions/coordination done
- Any agreements with other organizations
- Any regulatory, policy or legal constraints that would affect response to security incidents/events (use of deadly force, employee property, off-duty personnel, jurisdictional boundaries)
- Any administrative/logistical/training considerations
- Availability of resources to support the CP (financial, personnel, communications)

CP Introduction - Threat

- Reference to existing State threat assessment or design basis threat (DBT)
- Statement of the possible threats which exist for the specific facility (terrorist, criminal, insider, special interest)
- Discussion of possible high-level malevolent threat scenarios
- Any threats external to the facility which could cause harm (natural, infrastructure)
- Any historical information which would be useful for the implementation of the CP

CP Introduction - Threat

Actions taken by the facility should include:

- Potential threats should be identified, prioritized and responses should be pre-planned and tested
- Response plans should be coordinated with other relevant responders including emergency services
- Protocols for different threat scenarios identified
- Location of primary and alternate incident command center should be identified

Summary

- Example of content for CP introduction section
  - Scope
  - Assumptions
  - Threat

Contingency Plans

2.0 Facility Description

Student Learning Objectives

After completing this module, you should be able to:

- Discuss general information that is part of a facility description
- Provide an overview of the facility operations
- Identify critical areas and nuclear materials
- Describe the physical protection system
- Identify security locations and security levels

CP Facility Description - General

- Contains a brief profile of the facility and key personnel
- Provides a list of administrative information
  - Facility name, owner, address, other information
  - Key contacts, phone numbers, other

CP Facility Description - Overview

- Brief overview of facility operations
  - Identify critical operations, activities
  - Determine potential consequence if damaged
- Description of physical layout of facility
  - Showing critical locations
  - Showing security layers and entry control points between layers
  - Locations of some guard/response forces, selected physical security system components

CP Facility Description – Critical Areas and Nuclear Materials

- Provide a brief overview and location of critical areas (e.g. vital, inner areas)
- Identify vital areas
  - Critical equipment, locations
  - Specific actions necessary to cause undesired event
- Identify nuclear materials at the facility
  - Facility name, facility location
  - Description and form of the nuclear material
  - Amount of nuclear material (category, type)
  - Level of radiation

CP Facility Description – Physical Protection System Description

- Provide an overview of the facility physical protection system
  - Detection, assessment
  - Delay
  - Entry control, contraband detection
  - Alarm communications, monitoring
- Protection goals/objectives
- Some protection activities
- Security locations and levels (buildings, areas and type of security level)

Summary

- Facility description overview
- Facility critical areas and nuclear material
- Facility physical protection system

Contingency Plans

3.0 Guard/Response Force (GF/RF) Operations

Student Learning Objectives

After completing this module, you should be able to:

- Describe the facility Guard Force (GF) / Response Force (RF) mission
- Describe the facility GF/RF organization, responsibilities, and duties
- Identify what people may be part of the GF/RF
- Develop some rules of conduct for GF/RF
- Develop a GF/RF command and control
- Describe the communication systems for alarm reporting, assessment and GF/RFs
- Describe GF/RF weapons, equipment, and training

GF/RF Operations – Mission

- Brief description of the GF/RF mission
- Security/protection objectives
  - theft, sabotage, trespass, compromise sensitive information
  - Containment, denial

GF/RF Operations – Organization, Responsibilities and Duties

- Brief overview of the security organization with emphasis on the GF/RF
- Specific GF/RF duties and responsibilities to support security or protection objectives
- Listing of on-site GF/RF personnel, their locations/posts and areas of responsibility

GF/RF Operations – GF/RF Protection Activities

- Examples of possible protection activities include:
  - Activities at fixed posts and roving patrols
  - Detection by GF/RF
  - Assessment and reporting by GF/RF
  - Response and back-up
  - Interdiction by GF/RF
  - Delay by GF/RF
  - Use of prepared defensive positions

GF/RF Operations – Personnel and Locations

- Listing of GF/RF personnel and their initial deployment locations
- Number of personnel at each post/location during normal work periods and non-work periods
- Identification and description of off-site RF personnel and capabilities/number of responders

GF/RF Operations – Rules of Conduct

- Listing of some rules concerning conduct of the GF/RF
  - Use of facility property
  - Perform in a professional manner
  - Pay attention to their duties
  - Be able to operate assigned equipment and use assigned weapons
  - Understand the facility policies and procedures
  - Understand facility constraints

GF/RF Operations – Command and Control

- Section should identify members of the GF/RF and the chain of command and succession
- For each response action the responsible organization should be identified

GF/RF Communications

- Communications would include voice, data and video
- How the alarms are received, assessed and information transmitted to on-site and off-site responders
  - Central Alarm Station (CAS) location, staffing and responsibilities
  - Secondary Alarm Station (SAS) location, staffing and responsibilities
- Communications equipment and procedures for GF/RF
- Specific procedures in the event of lost communications due to jamming or other causes
- Communications with off-site organizations and responders

GF/RF Operations – Weapons and Equipment

- Section should include a description of the weapons and equipment that will be available to the GF/RF.
  - GF weapons and equipment
  - RF and tactical responder weapons and equipment
  - Special equipment available
- Locations where the equipment is stored
- Procedures to obtain necessary equipment

GF/RF Operations – Training

- Section would include a detailed description of the type of training required for the GF/RF
  - Knowledge of facility policies, procedures
  - Physical training
  - Weapons training
  - Records documentation training
  - Frequency of training
- General security training for personnel authorized access to the facility

Summary

- Reviewed information that is part of GF/RF mission, organization, duties and responsibilities
- GF/RF rules of conduct
- GF/RF personnel and locations
- GF/RG command and control, communications
- GF/RF weapons, equipment and training

Contingency Plans

4.0 Incident Response Procedures

Student Learning Objectives

After completing this module, you should be able to:

- Describe rules of engagement
- Discuss use of force authority
- Identify possible response force strategies and procedures
  - Response/defensive strategy
  - Phased alert responses
- Indicate times for physical protection functions and response
- GF/RF actions for specific scenarios
  - Theft, recapture and recovery
  - Sabotage, minimize and mitigate

Incident Response Procedures – Pre-Incident Deployment Planning

- Procedures for notifying responders
- Location of GF/RF, post number, number of personnel for different shifts
- Times for different on-site response functions
  - Alarm communications/assessment times
  - Time to communicate to responders
  - Preparation time for responders
  - Travel time by responders
  - Deployment time by responders
- Off-site RF description, equipment, weapons, transport, number of personnel and time to respond

Incident Response Procedures – Rules of Engagement

- Section addresses the rules of engagement and the force continuum
  - Presence
  - Verbal commands
  - Use of hands
  - Less than lethal options
  - Deadly force
- Use of force authority for given situations

Incident Response Procedures – Force Continuum and Rules of Engagement

- A **Force Continuum** may be established that directs response forces to use the minimum amount of force necessary to:
  - Control the situation
  - Apprehend and perhaps arrest
  - Perform other actions to stop/prevent a malevolent act
  - May include: presence, verbal use of hands, less lethal, or deadly force
- **Rules of Engagement** define when a response force can use weapons against adversaries

Incident Response Procedures – Use of Force Authority

- Response force personnel should have the ability to apply sufficient force to stop an adversary's actions.
  - Should have a legal basis
  - Should be clearly documented
  - Should be used to develop rules of engagement
- The CP should specify procedures for use of force
  - May vary based on the type of responders (GF, RF)
  - May vary on the location of the adversaries
  - May vary if hostilities (shots fired, explosives) occur

Incident Response Procedures – Response Procedures

- Section defines GR/RF actions to incidents
- Identify the beginning/end of events
- Define the specific objectives to accomplish each event – predetermined actions, procedures, number of responders, times for deployment
- GF/RF procedures when notified of an alarm
- Protection strategies and approaches
- Application of a phased alert/response

Incident Response Procedures – Protection Planning Concepts

Thorough protection planning is critical in ensuring an organized and effective response to a security incident and includes:

- Identifying and prioritizing potential targets
- Determining if targets are theft or sabotage targets and the protection strategy
- Identifying optimal response force configuration
- Determining probable adversary actions
- Establishing pre-determined response plans
- Developing realistic scenario-based training programs

Incident Response Procedures – Response Force Strategies

- **Containment** – prevent adversaries from leaving the site with an asset
- **Denial** – preventing adversaries from getting an asset
- **Recapture** – taking over by force a critical location on site occupied by adversaries
- **Pursuit and Recovery** – attempting to recover an asset removed from the site by adversaries
- **Protest Strategy** – preventing significant impact to the facility's mission caused by demonstrators

Incident Response Procedures – On-site Alarm Response Procedures

- Procedures for the receipt, assessment and processing of alarms should be presented. This will include procedures for personnel within the CAS/SAS and the response force.
- Upon notification of an alarm the response force:
  - Collects their firearms
  - Assembles any equipment include personal protective items
  - Prepares to respond by foot or vehicle
  - Follow prescribed contingency plan based on direction from the RF Commander

Incident Response Procedures – Phased Alert/Response Procedures

- The CP may address a number of different phases – response, resumption, recovery and restoration
- For the Response Phase some of the general actions to be done include:
  - Establish immediate and controlled presence
  - Conduct preliminary assessment of incident
  - Communicate information to appropriate people, groups
- For the LIMP facility there are three alert/response phases (1-3)
  - GF/RF do not have Use of Force Authorization (possible site intrusion)
  - GF/RF do not have Use of Force Authorization (confirmed site intrusion)
  - RF do have Use of Force Authorization (hostilities have occurred)

Incident Response Procedures – GF/RF Actions for Specific Scenarios

Different scenarios may be part of one CP or in separate CPs. Some possible scenarios are:

- **Theft** and discussion of the specific actions by the GF/RF for the different targets. It may include actions if the asset remains on-site or is removed from the site.
- **Sabotage** and discussion of the specific actions by the GF/RF for the different targets. It may include actions related to security response as well as actions related to minimizing or mitigating the effects.
- **Other** scenarios may be discussed. These could include actions for an unannounced landing of an aircraft on the site.

Incident Response Procedures – Recapture and Recovery

- Section defines how the GF/RF will respond in the event of a theft scenario and actions and other information related to recapture and recovery
  - Actions by specific GF/RF personnel
  - Coordination with off-site organizations
  - Securing nuclear material

Incident Response Procedures – Minimize and Mitigate

- Section defines how the GF/RF will respond in the event of a sabotage scenario and actions and other information related to minimizing and mitigating the consequences
  - Actions to deny access
  - Prevent sabotage event from occurring
  - Minimize effects of a potential radiological release
  - Coordination with other organizations, emergency response, radiation safety

Summary

- Discussed force continuum and rules of engagement
- Discussed use of force, response force strategies
- Discussed concepts important to protection planning
- Discussed on-site response and phased alert and response procedures
- Discussed actions for specific scenarios such as theft or sabotage

Contingency Plans

5.0 Coordination and
6.0 Protection of
Information

Student Learning Objectives

After completing this module, you should be able to:

- Identify areas to be considered in coordination with other individuals, groups, and agencies
- Discuss the need to protect sensitive CP information

Coordination and Protection of Information – Coordination Activities

- Section should discuss arrangements as documented in memorandums of understanding (MOU) with external organizations. If possible the MOUs should be included as an attachment to the CP.
- Implementation of the CP and associated actions and procedures must be coordinated with other on-site plans to preclude conflict during normal, security events and emergency conditions.
- Security CPs and emergency plans should be comprehensive and complementary. Detailed instructions should be included regarding coordinating emergency services. The focus should be on preventing further damage, securing the facility, protecting emergency equipment and personnel.

Coordination and Protection of Information – Coordination Activities (cont.)

- The safety/security interface is an important area that requires considerable coordination.
- Coordination with facility operations is also very important. It will help in avoiding conflicts and potentially causing damage to the facility and will also facilitate the transition of the facility to a safe operating state if that is necessary.
- Off-site responders must be familiar with the sensitive areas and hazards within the site.
- Training exercises involving all parties is necessary.

Coordination and Protection of Information - Interaction with Outside Agencies

If the facility is utilizing outside or off-site agencies, protection requirements need to be carefully documented and rehearsed.

- Written agreements or understandings are needed
- If more than one law enforcement or response agency is involved then agreements should be made to designate the lead authority.
- Joint training exercises and validations conducted. Response forces should be familiar with the facility.
- Key issues to consider:
  - Role of support agencies
  - Specific information needed in the agreements
  - Integrated communications

Coordination and Protection of Information - Outside Agency/Local Law Enforcement

- Benefits of utilizing outside agencies/local law enforcement
  - Reduces cost for contingencies
  - Resolves many jurisdictional issues
  - Allows increased pursuit capabilities
- Challenges
  - Difficulty in ensuring performance
  - Difficulty attaining dedicated response forces, times
  - Requires training with external personnel
  - Requires integrated communications

Coordination and Protection of Information - Protection of Sensitive Information

- Section discusses how the information contained within the CP is protected. It should address the marking or classification of sensitive information and how the information is controlled and released.
- The information within the CP along with other parts of the facility security plans contain sensitive information which must be protected.
- The State should establish requirements for protecting the confidentiality of this information (fundamental principle L).
- The facility operator shall protect sensitive information from unauthorized disclosure and access will be provided to only those whose trustworthiness has been established and who have a need to know.
- A challenge for the facility is ensure protection of sensitive information and at the same time providing the necessary information to the people, groups that need it.

Summary

- Areas to consider in coordination with on-site and off-site individuals and groups.
- The importance or having coordinated, integrated CPs and emergency plans.
- The importance of protecting sensitive information contained in the CP and other plans.

Contingency Plans

Figures, Tables and Appendices

Student Learning Objectives

After completing this module, you should be able to:

- Identify areas that may be included in the CP as:
  - Figures
  - Tables
  - Appendices

Figures, Tables and Appendices – Figures

- The following information may be part of the CP:
  - Country/region/city map showing location of facility and other key areas
  - Drawings and layouts of the facility, specific buildings and entry control points
    - Location of buildings, roads, physical barriers
    - Location of critical assets, equipment
    - Location of nuclear material
    - Location of GF/RF locations
    - Paths and distances into and within the facility for responders
  - Physical protection security layers and elements shown on a facility map/layout. Detection, assessment zones may also be shown.
  - Paths at personnel and vehicle entry/exit points.
  - Representation of alarm and security force communications system

Figures, Tables and Appendices – Tables

- The following information may be part of the CP:
  - Facility administrative information (location, contacts, contact info)
  - Listing of critical assets (vital areas)
  - Listing of nuclear material (location, material form, amount, radiation level)
  - Listing of security locations and security levels (LAA, PA, VA, IA)
  - Listing of GF/RF locations, description and number of personnel for on-site and off-site responders
  - Times for physical protection system functions including those related to RF (preparation, travel, deployment)
  - Responsibilities table/matrix for security, GF/RF personnel

Figures, Tables and Appendices – Appendices

- The following information may be part of the CP:
  - List of acronyms and definitions
  - Procedures for specific events, incidents and/or activities (bomb threat, hostage, active shooter, insider attack, airborne attack, stand-off attack, cyber, natural disaster, medical, fire, evacuation, civil disturbance, compromise of sensitive information)
  - Rules of conduct, use of force and other guidelines for GF/RF
  - Descriptions of the GF/RF training, weapons qualification requirements
  - Security training for facility personnel
  - Copies of the MOUs and other agreements with external organizations
  - Decision flow diagrams for specific scenarios

Summary

- Supplemental information in figures, tables and appendices including:
  - Facility drawings
  - Pictures
  - List of critical assets
  - Maps showing RF primary positions
  - MOU’s

Scenario Analysis

Student Learning Objectives

After completing this module, you should be able to:

- Describe the scenario analysis process
- Identify the parameters of scenario development
- Explain the process for selection of scenarios for testing

Scenario Analysis

Scenario analysis: A method of analyzing various adversary attack scenarios on a site's existing or proposed Physical Protection System (PPS)

- Analyzes PPS elements and Contingency Plans
- Provides insight into a PPS that can be used for:
  - Tabletop analysis
  - Combat computer simulation tools
  - Force-on-Force exercises

Scenario Analysis Process

- Identify stakeholders
- Create a scoping agreement
- Scenario development parameters
- Determine attack scenario characteristics
- Develop attack scenarios
- Review and select attack scenarios

Identify Stakeholders

- Identify people who are responsible for the design, implementation, evaluation, and risk-acceptance of the PPS
  - Competent authority
  - Response force management
  - Vulnerability analysis team
  - Adversary planning subject-matter experts (SMEs)
  - Security management
  - Facility operations
  - Other required people. . .

Scoping Agreement

Scoping Agreement: A contract among appropriate stakeholders that identifies the parameters of the scenario analysis

- Define requirements
- Design basis threat (DBT) statement
- Characterize facility
- Identify targets (type of targets)
- Identify credible SMEs for attack planning
- Determine types of attacks and numbers of scenarios (sabotage/theft)
- Identify and agree on assumptions
- Determine type of insider (passive/active, etc.)
- Sign Memorandum of Understanding with government
- Review security posture
- Determine picture-in-time
- Agree on simulation tools and the process for using them

Scenario Development Parameters

- Stakeholder(s) familiar with the design and evaluation of the PPS should be included in scenario development
- All participants should:
  - Agree to confidentiality of all site/adversary information
  - Remain unbiased toward site or adversaries
  - Ensure the adversary scenarios are within the parameters of the scoping agreement
  - Ensure accuracy of the PPS and target information
    - Thickness of vault walls
    - Assessment capability
    - Response capability

Adversary Attack Plan

- Scenario: A time-ordered, detailed description of an adversary attack used in analyzing system effectiveness
  - For scenario analysis to be of maximum value, scenarios should be:
    - Detailed
    - Credible
    - Limited to threats within the DBT
    - Internally consistent
    - Intellectually honest
    - Well documented

Adversary Scenario Definitions

- ***Adversary Strategy***: Short description of the scenario used to achieve the adversary's objective
- ***Defeat Strategy***: General method used to defeat a path element or a PPS function
- ***Defeat Method***: Way to prevent a component within a path element from accomplishing its purpose or function

Adversary Strategy

- Two classes of adversary scenarios
  - ***Direct***: Adversary follows a direct path to target
    - ***Adversary goal*****:** Minimize probability of interruption by defeating system detection or delay elements
  - ***Indirect****:* Adversary attacks PPS infrastructure before attacking target
    - ***Adversary goal:*** Minimize probability of interruption and neutralization to:
      - Increase response time
      - Decrease response numbers
      - Disable critical systems

Defeat Strategies and Methods

- Three basic adversary defeat strategies and methods can be used
  - Avoid, degrade, or disable detection systems
    - Include entry control and contraband detection systems
  - Degrade, disable, or circumvent delay systems
  - Degrade or eliminate response
    - Identify weak links and single points of failure

Structured Approach to Create Scenarios

- Create a range of scenarios
  - Identify site vulnerabilities
  - Exploit the identified site vulnerabilities
    - Build scenarios
  - Review and select final scenarios based on criteria

Identify Site Vulnerabilities

- Collect site-specific PPS data
  - Outside sources (internet, libraries, etc.)
  - Passive insider information
  - Site surveillance
- Identify site vulnerabilities across various operational conditions and states
  - Operational conditions (operational versus non-operational)
  - Target material configurations (reactor load-out versus operations)
  - Response force alert levels
- Identify sources of vulnerabilities
  - Experts (site personnel, police)
  - Path analysis
  - Previous vulnerability studies and performance tests

Exploit Identified Site Vulnerabilities

- Determine how an adversary could exploit identified site vulnerabilities
- Create a list of essential tasks that have to be accomplished for the attack to succeed
- Create task plans describing how an adversary team can perform each task within resource constraints
  - Who is involved?
  - What are they doing as a function of time?
  - How are they performing each step?
  - What equipment are they using?
  - How are they transporting the equipment?

Scenario Development Planning and Complexity Factors

- The best scenario for the adversary does not always use *all* equipment allowed within the DBT
  - Not all equipment will provide an advantage to the adversary
  - Adding equipment may increase the complexity of the scenario
- Coordinating actions and synchronizing time between groups increases difficulty

Review and Select Final Scenarios (1 of 3)

- Include stakeholders in the review and selection process
- Review and select final scenarios based on scoping agreement criteria
- Are all analysis objectives covered?
  - Are conditions and states covered adequately?
  - Do the scenarios address several means of adversary approach (on foot, in land vehicles, on water, or by air) that apply, based on the DBT?
- Are scenarios credible, limited by threats within the DBT, etc.?

Review and Select Final Scenarios (2 of 3)

- Consider impact of colluding insider
  - Modify appropriate detection, delay, response force time, or response force numbers to reflect what insider can accomplish
  - Examples of collusion scenarios
    - Detection: Insider tampers with alarm communication lines
    - Delay: Insider opens vault door at time of attack
    - Response:
      - Insider activates an emergency alarm in a different location to divert response force
      - Insider detonates explosive at armory

Review and Select Final Scenarios (3 of 3)

- Performance test scenario input data
  - Probability of detection for intrusion detection system
  - Delay barrier breach times
  - Response force times

Analysis of Attack Scenarios

- Attack scenarios are now ready for use in analysis process
  - Tabletop exercises
  - Combat computer simulations
  - Force-on-Force exercises

Summary

- Scenario analysis is a method of analyzing various adversary attack scenarios on a site's existing or proposed Physical Protection System (PPS)
- It is used to analyze the system effectiveness of a PPS or specific contingency plan
- Is used to support further analysis and testing (tabletop exercise, combat computer simulations, and FoF exercises)

Table Top Exercise

Student Learning Objectives

After completing this module, you should be able to:

- Describe a tabletop exercise
- Recognize roles and responsibilities and how to implement a tabletop exercise
- Recognize how to evaluate results of exercise

What is a Tabletop Exercise?

Tabletop exercise: A method of simulating an adversary attack on a site's existing or proposed Physical Protection System (PPS)

- Analyzes PPS elements and Contingency Plans
- Provides insight into a PPS that can stand alone or be used in further analysis
- Evaluate Contingency Plans to determine action of events
- Helps determine the most appropriate actions needed

When to Conduct a Tabletop Exercise

- **To Evaluate:**
  - Current and proposed PPSs
  - Tactics, techniques, procedures, policies
  - Current and changing (postulated) threats
  - Interagency contingency plans
  - Scenario selection for use in other analysis tools

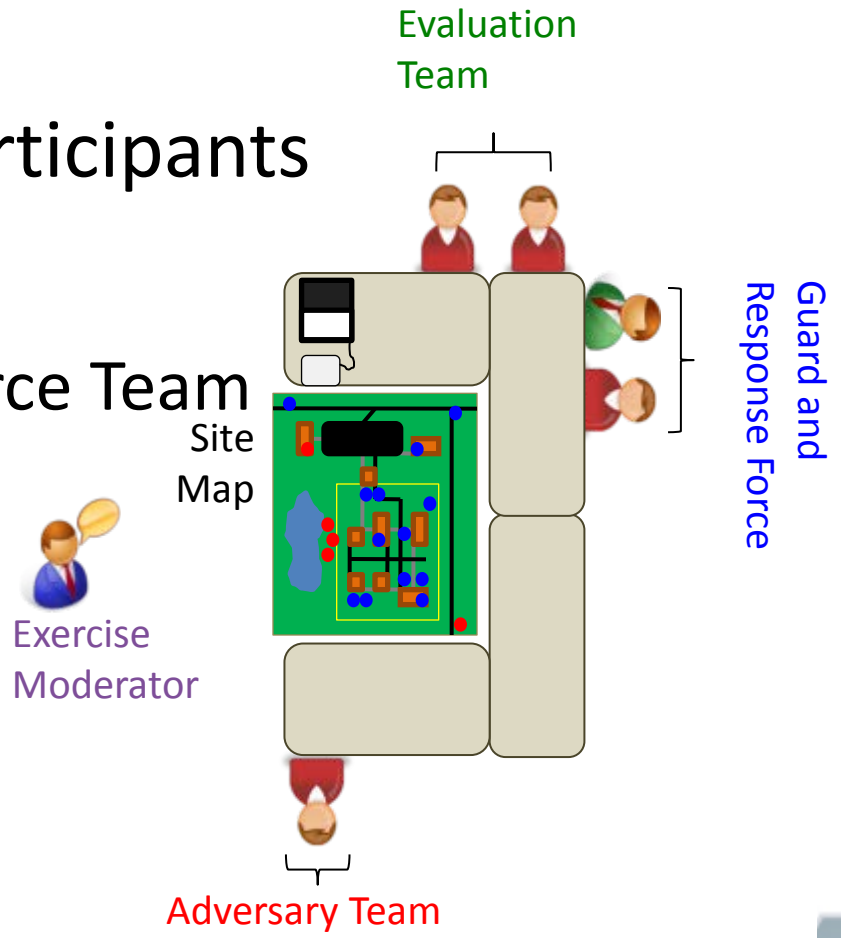
- **As a Training Tool:**
  - Rehearses local and interagency contingency plans
  - Maintains guard and response force proficiency

Tabletop Exercise Process

- Determine team
- Prepare for simulations
- Simulate the attack
- Record events
- Conduct evaluation meeting
- Determine vulnerabilities
- Recommend changes and upgrades

Organize Tabletop

- Gather all necessary participants
- Determine teams
  - Guard and Response Force Team
  - Adversary Team
  - Evaluation Team
  - Exercise Moderator



Organize Tabletop (Cont'd)

- Gather Appropriate Resources
  - Contingency Plan
  - Maps/Models
    - Types
    - Scales
  - Whiteboards/Flip Charts
    - Track critical events and engagements
  - Player Tracking
    - Dry-erase markers
    - Game pieces
  - Tool to Determine Chance-based Outcome
    - Random number generator
    - Dice
    - Data tables

Roles and Responsibilities (1 of 3)

- Guard and Response Force Team
  - Lay out initial response positions on game table (map, three-dimensional model, aerial photograph)
  - Manage response actions and reactions
  - Apply appropriate tactics based on contingency plan
- Adversary Team
  - Lay out initial adversary positions on game table (map, three-dimensional model, aerial photograph)
  - Manage adversary actions and reactions
  - Apply appropriate tactics based on adversary plan

Roles and Responsibilities (2 of 3)

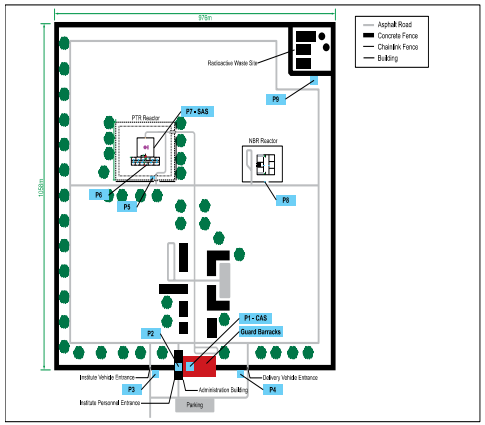
- Evaluation Team
  - Serves as referee or honest broker
  - Provides input to the moderator to determine results of critical events and engagements
  - Defines practical detection points
    - Communication protocols
    - Effectiveness of detection and assessment component capabilities
    - Effectiveness of delay components
  - Resolves conflicts between guard/response force and adversary teams

Roles and Responsibilities (3 of 3)

- Exercise Moderator
  - Serves as referee or honest broker
  - Facilitates the exercise
  - Determines (with input from the evaluation team) results of critical events and engagements
  - Ensures all player movements are properly annotated on the game table
  - Keeps the exercise on pace to reach final exercise objectives

Guard and Response Force Picture-in-Time

- ***Picture-in-Time:*** A current snapshot of the exact locations and configurations of the existing security force.
- Picture-in-Time provides the stakeholders with:
  - Post and Patrol
    - Locations
    - Activities
    - Equipment status
    - Numbers
- How to collect Pictures-in-Time
- Evaluation Team should be familiar with or briefed on general contingency plans



Tabletop Preparation (1 of 3)

- Gather Data and Generate Assumptions
  - Facility and PPS (Tour, Briefings)
  - Performance Test Data of PPS
    - Detection probabilities
    - Barrier delay times
    - Alarm assessment and communication times
    - Guard and response force times

Tabletop Preparation (2 of 3)

- Review Necessary Information
  - Facility and PPS
  - Picture-in-Time
  - Types and number of scenarios
  - Adversary scenario steps and timeline
  - Contingency plan implementation
  - Type of equipment, vehicles, weapons, and tactics that the adversary and the security force will use

Tabletop Preparation (3 of 3)

- Gather Required Documentation
  - Design basis threat
  - Adversary scenarios
  - Contingency plans

Note: Have documentation readily available for the evaluation team to clarify adversary or response force assumptions made during the exercise

Definitions Used in Tabletop

Critical Event: Any event that requires attention and resources to overcome (detection, delay, engagement)

Engagement: An interaction that occurs between the guard and/or response force and the adversary along the adversary attack path

Simulate the Attack

- Adversary Timeline, Guard and Response Force, and Picture-in-Time are overlaid on the game table
- Each adversary event is played out during each time interval
- Tabletop timeline (Time 00:00) typically begins at initial point of detection or engagement
- Guard and Response Force will respond to adversary events within each time interval

Simulate the Attack (Cont'd)

- Critical events and engagements are discussed, determined, and recorded (who, what, when, where)
- Timeline and participant status are adjusted and moved forward to the next event in time
  - Update timeline to the next time interval
  - Update the players on both sides to the next time interval
  - Perform previously scheduled events (bomb detonation, detection, etc.)
- Critical events and engagements continue to be evaluated until the exercise objective is achieved

Analyze Engagements

1. Verify
   - Engagement feasibility
   - Line of sight between shooter and target
   - Target within range of weapon system
2. Identify characteristics of the persons involved
   - Standing still, walking, running, prone, kneeling, in vehicle
   - Type of weapon and round, number of rounds, mounted, bipod, supported
3. Identify characteristics of target
   - In/out of vehicle, level of armor on vehicle, speed of vehicle
   - Body armor level, behind cover, in prepared fighting position
   - Prone, kneeling, standing, walking, running, low crawling

Note: Determine probability of casualty calculations and declare the results of the engagement

Documenting Results

- Documentation provides
  - Outcome of the overall exercise
  - Explanation for each vulnerability identified in the exercise
  - Justification and rationale for each potential upgrade
- Document each engagement, vulnerability, outcome, and performance test issue

Note: Ensure all documentation is accurate, clear, and concise to mitigate misinterpretation

Evaluation Meeting

- Evaluation meetings are held with appropriate stakeholders and participants after the exercise has been completed.
- Evaluation criteria:
  - Win or loss
  - Response force casualties
  - Access to target
  - Duration of engagement
  - Compensatory measures
  - Performance testing concerns
  - Response discrepancies
  - Vulnerabilities exploited

Note: Use the evaluation criteria to determine consistency with results from different analysis tools

Evaluation Meeting (Cont'd)

- Why do adversary attacks fail?
  - Early detection (adversaries detected earlier than expected)
    - Detection by intelligence organizations directly or by populace
    - Discovery during lead-up to the attack
  - Non-combat failures (typically due to failure to plan and stock for contingencies)
    - Logistic failures (inability to get weapons, etc.)
    - Breakdowns of vehicles, communications equipment
    - Exhaustion of team members during the attack
    - Tool/explosive failure to breach
    - Timing and synchronization failures
    - Wrong plan due to bad information
  - Inadequate training and rehearsal

Evaluation Meeting (Cont'd)

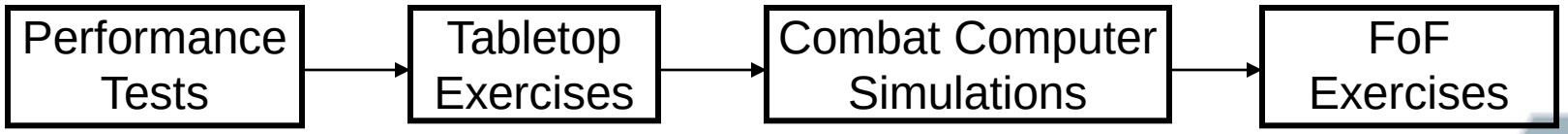
- Why do Response Forces fail?
  - Inadequate detection, assessment or communication of attack
  - Lack of delay
  - Inadequate contingency plan
  - Inadequate training
  - Inadequate number of responders or equipment

Evaluation Meeting (Cont'd)

- Discussion among experts
- Capture lessons learned
  - PPS strengths
  - Opportunities for improvement
  - Sensitivity cases
- Provide recommendations for improving the overall effectiveness of the PPS
- Identify and discuss potential upgrades that should be modeled in subsequent analyses
- Identify adversary scenario variations for additional analysis
- Determine the qualitative effectiveness of the PPS

Further Analysis of Attack Scenarios

- Tabletop exercises can often predict logistic issues that will arise in computer simulations and FoF exercises
  - In some cases, issues are identified in tabletop's that have to be addressed before other simulations can be performed
- Address any issues identified and move on to computer simulations and FoF exercises



Summary

- A tabletop exercise is a method of simulating an adversary attack on a site's existing or proposed PPS
- Critical events and engagements must be documented and analyzed for a productive result
- Tabletops provide valuable insight, are simple, cost effective and require minimal resources

Table Top exercise

- Using your Contingency Plan
- Assign group members to play the different roles
  - Adversary
  - Guard and Response team
  - Exercise Moderator
- Simulate the attack
  - Using DBT data
  - Contingency Plan
- Collect lessons learned

Emergency Operations Center

In Support of the Contingency Plan

Student Learning Objectives

After completing this module, you should be able to:

- Define the role of the emergency operations center
- Describe when incidents transition to emergency response
- Describe the role of the CAS during an incident response

Incident Commander Role

- Incident Commander operates in the field and is responsible for the site response (not including Guard/Response Force response)
- Knows when to activate the EOC
  - Under what conditions
  - Based on resource requirements
  - Based on staffing requirements
  - Based on reporting, categorization requirements
- Knows how to activate the EOC
  - Triggering factors
  - Request procedures
  - Alerting considerations

EOC Definition

- Emergency Operations Center (EOC)
  - A central location that supports Incident Command by making executive/policy decisions, coordinating interagency relations, dispatching and tracking requested resources, and collecting, analyzing, and disseminating information.

EOC Role

- Provides resources, planning and support to the Incident Commander and Response Force Commander
- Assists the Incident Commander with
  - additional information
  - support as the strategic objectives and goals are defined for the incident
- Networks through the EOCs of other organizations for support and notification requirements

EOC Communications Role

- Key to providing accurate information between the EOC and to the Incident Commander in the field who is supporting the Response Force Commander
- Tasked to make notifications, transmit emergency information and gather information
- Communication Coordinators must keep the flow of information available so that decision makers can properly do their jobs

EOC Coordination Activities

- Gathering facility information
- Communication of hazardous material locations
- Safety considerations
- Coordination with off-site agencies as needed
- Locating resources to assist in the incident
- Notifications to on-site and off-site
- Classification guidance

Central Alarm Station (CAS)

- The CAS serves as a operations center for guard and response force during a security incident and ensures that information is gathered, communicated, and documented for records
- Initiate Security Response
- CAS communicates with EOC when activated during a security incident

Summary

- The EOC provides information, planning and support to the incident commander
- The EOC plays a vital role when it comes to communicating during the incident
- The CAS serves as a operations center for guard and response force during a security incident

Incident Response

Multi-Agency Coordination for Implementing Contingency Plans

Student Learning Objectives

After completing this module, you should be able to:

- Describe the utility of an organized multi-agency response
- Identify organizations involved in incident response
- Match responsibilities to roles associated with incident management

Incident Response

- Incident response operations are not “business as usual”
- Anyone may be called to respond in an incident
- Incident response may require participation by multiple agencies and organizations

Potential Response Agencies

- Site guard and response force
- Local Law Enforcement
- State Law Enforcement
- Military
- Fire Department
- Ambulance
- Emergency Management
- Specialty Teams (hazardous response)

Purpose of Integrated Response

- Provide structure and coordination for incident stability
  - Standardized for all organizations involved
  - Common terminology, less jargon
- Provide for security and safety
  - Secure nuclear material
  - Life safety
  - Mitigate and minimize sabotage consequences
  - Environment protection

Goals of Integrated Response

- General
  - Establishing command for onsite and offsite response
  - Ensuring responder safety
  - Assessing incident priorities
- Developing an appropriate organizational structure for contingency plan implementation
- Maintaining an effective span of control by coordinating activities of all responding agencies

Multi-agency Response Structure

- Structure
  - Roles and Responsibilities under one incident commander or unified command
  - Implementation
  - Interagency Coordination
  - Command Structure
  - Training for multi-agency response

Major Components

- Common terminology
- Modular organization
- Integrated communications
- Unity of command
- A unified command structure
- Site contingency plan as primary

Communication

- Common language and terminology
- Common communications plan
- Common frequencies
- Use of cellular phones is not recommended
- Ensure sensitive or secure information is not broadcast over radios or cell phones

Modular Organization

- Organization of onsite forces
- Organization of offsite forces
- Special units can be added to address special needs
- Units no longer needed can be systematically released during different phases of the operations

Position Titles

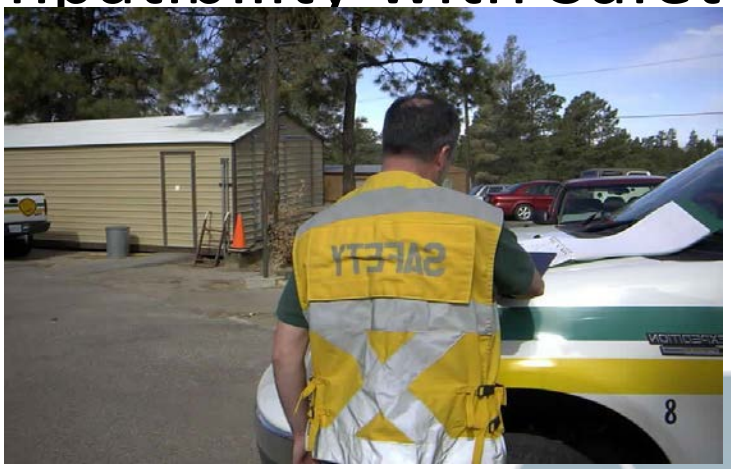
- Guard Force Commander
- Response Force Commander
- Incident Commander
- Command Staff – support the incident commander
  - Safety Officer
  - Liaison Officer
  - Information Officer
- General Staff
  - Operations Section
  - Planning Section
  - Logistics Section
- EOC supports the Incident Commander

Incident Commander

- Operates outside of security incident area providing support for security response
- Develops an appropriate organizational structure for other responding elements
- Maintains an effective span of control
- Manages Incident Resource

Safety Officer

- Has overall responsibility for Incident Safety
- Minimizes risks to site personnel and off-site response elements
- Reviews the Security and Contingency Plans to ensure some level of compatibility with Safety Plans
- Writes the Safety Plan



Liaison Officer

- Point of contact for assisting agencies
- This may include, local fire and police departments, and other organizations
- Usually not required for on site emergencies

General Support Staff

- Support the Incident Commander
  - Operations Section
    - Responsible for all site operations; the primary mission of the Incident Command System
    - May have Fire, EMS, and Facility Branches
  - Planning Section - Collects and analyzes information used in developing the current, probable and alternative plans for the incident
  - Logistics Section - Provides materials, resources, and facilities to support the incident

Other Positions

- Staging Area Manager
  - Reports to the Operations Section Chief
  - Stages equipment, personnel and other resources at an suitable area

- Facility Manager
  - Known as the Facility Command Leader
  - Responsible for providing information on incident, actions, and site specific hazards

Summary

- Important to provide structure and coordination in order to maintain stability during the security incident response
- Requires various staff members with different responsibilities to ensure structure is present
- Response agencies should also be included as part of the organizational model.

Contingency Plans

Evaluation and Action Plan

Student Learning Objectives

After completing this section, you should be able to:

- Identify the strengths and weaknesses of their draft contingency plan
- Identify gaps in their contingency plan
- Create list of information missing from their contingency plan
  - Identify action plan to obtain information
  - Identify actions to finalize contingency plan

Evaluation of Contingency Plan

- Summarize the results of table top exercise
  - What worked and what didn't
  - Were the response force scenarios successful
  - What information was missing
  - What information was extraneous

Action Plan to Update CP

- Who will collect any missing information
- Who will obtain necessary memorandum of understanding with responding organizations
- Who will update the contingency plan
- What is the completion date for finalization of the contingency plan
- Who will review and approve contingency plan
- Develop schedule to exercise contingency plan

Contingency Plans

Course Summary

Course Summary - Overview

After completing this course, you should be able to:

- Describe basic PPS concepts and design process
- Discuss the INFCIRC/225 recommendations for CPs
- Identify what should be in a CP and be able to create a draft CP
- Describe the scenario analysis process and tabletop exercise
- Explain the role of the emergency operations center and incident response in contingency planning

Course Summary - PPS

- PPS concepts and objectives
  - People, procedures and equipment
  - Protect against unauthorized removal and sabotage
- PPS design process, PPS functions
  - What to protect
  - Who to protect against
  - How well is it protected
  - Detection, delay and response
- Adversary and PPS timelines – timely detection, interruption, and neutralization
- Characteristics of an effective PPS
  - Balanced protection
  - Defense in depth
  - High system reliability

Course Summary – INFCIRC 225 Recommendations

- Definitions for a CP (security), emergency plans (safety) and security plans
- State, Competent Authority and Licence Holder responsibilities concerning CPs
- Recommended requirements for CPs

Course Summary – Scenario Analysis and Tabletop Exercise

- Scenario analysis process – design, develop, implement and evaluate
- Specific roles and responsibilities for the scenario analysis steps
- Conduct of a tabletop exercise

Course Summary – EOC and Incident Response

- Role of an emergency operations center (EOC) in support of a CP
  - Communications
  - Coordination
  - Resources
- Incident response
  - Multi-agencies
  - Integrated response
  - Organization, roles and responsibilities

Course Summary - Conclusion

- Contingency plans (CPs) identify the actions necessary to respond to security events such as unauthorized removal or sabotage.
- CPs exist at the State or Licence Holder level and include:
  - Roles and responsibilities
  - Organization and structure
  - Concept of operations for effective response
  - Plans, policies and procedures to counter the identified threat and various adversary scenarios

Revised Hypothetical Facility Data

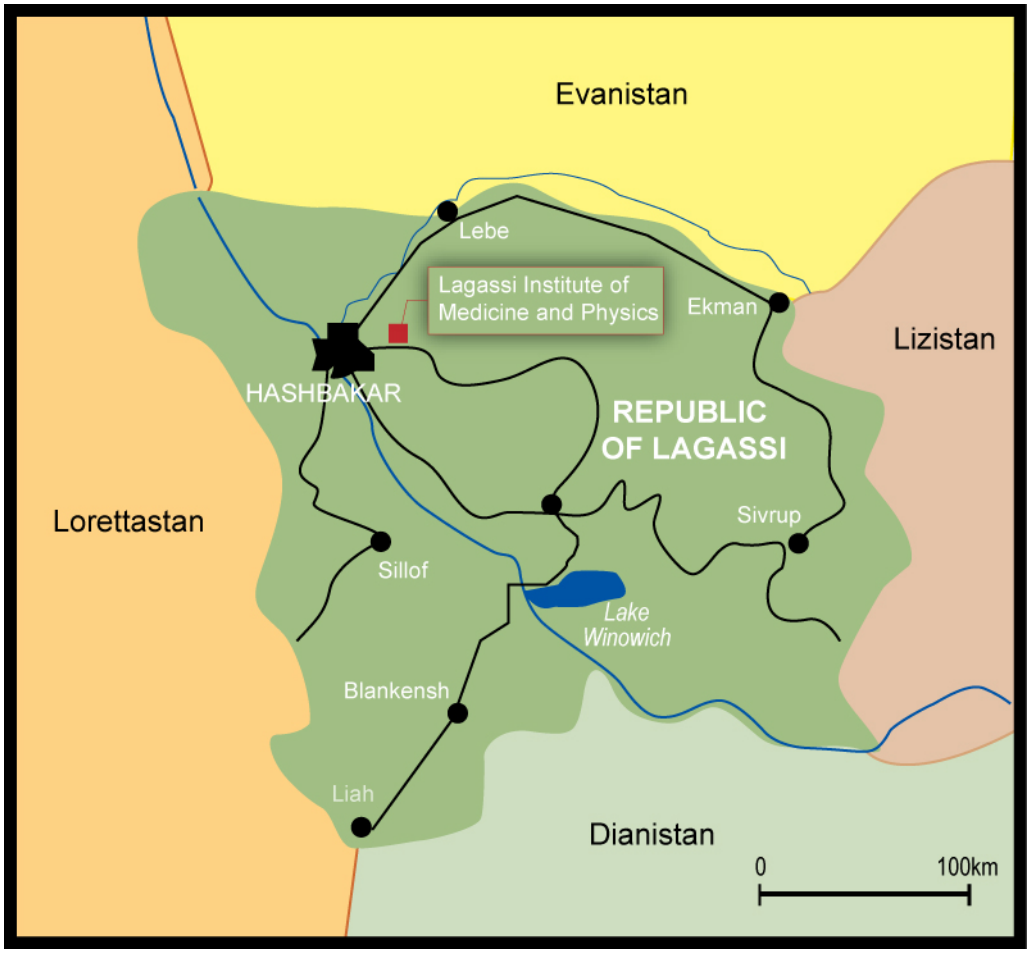
The Lagassi Institute of Medicine and Physics (LIMP)

Table of Contents

Section 1. Country of Lagassi Description and Map

Lagassi, the smallest of the regional republics, possesses large fossil fuel reserves and plentiful supplies of other minerals and metals. It also has a large agricultural sector featuring livestock and grain. Lagassi's industrial sector rests on extracting and processing these natural resources and also on a growing machine-building sector that specializes in construction equipment, tractors, agricultural machinery, and some defense items. The country's solid 3.5% economic growth is largely due to its booming energy sector, but also to economic reform, good harvests, and foreign investment. In order to prevent overdependence on the oil sector, the country has embarked on an industrial policy designed to diversify the economy by developing light industry and a nuclear energy infrastructure.

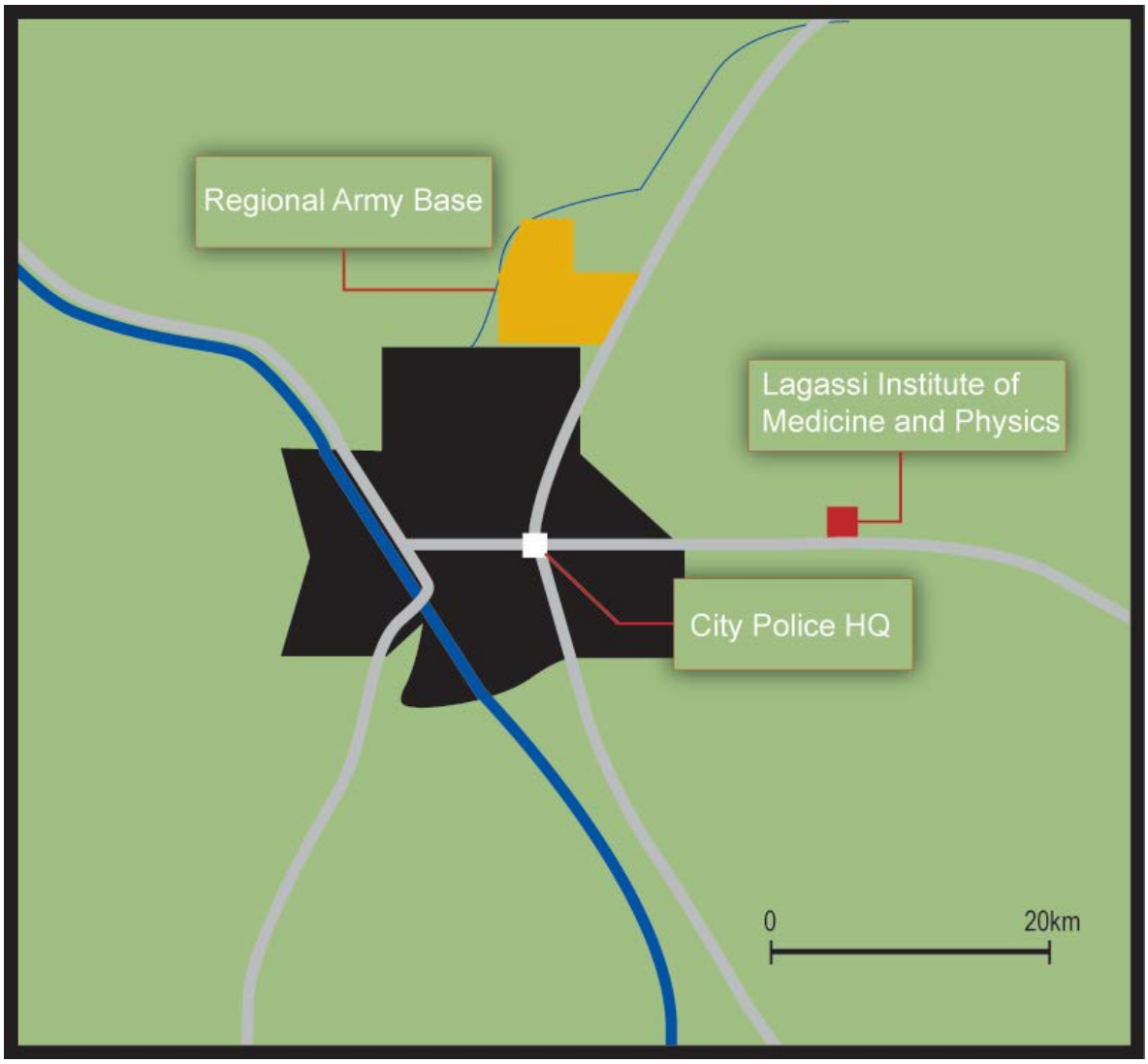
Current issues include expanding the development of the country's emerging nuclear energy resources, achieving an export capacity of electrical energy to border countries, and strengthening relations with neighboring states and other foreign powers.



Country Map of Lagassi

Section 2. City of Hashbakar Description and Map

The capital of Lagassi, Hashbakar, is an ancient city that arose from the crossroads of early trading lanes. Today, the city is a modern metropolis of two million inhabitants. It contains a major roadway, a rail system, a private and military airport, and a limited waterway.



Hashbakar City Map

Section 3. LIMP Introduction with Environmental and Physical Conditions

The Lagassi Institute of Medicine and Physics

The hypothetical nuclear research center, Lagassi Institute of Medicine and Physics (LIMP), was started in 1950 to serve as the nation's premier nuclear energy research facility. The Institute houses various research, administrative, and plant support facilities. The LIMP is located in the Republic of Lagassi, approximately 29 km (18 mi) east of Hashbakar.

Topography

LIMP is located in the semi-arid steppes of Central Asia.

Vegetation

Small shrubs, cacti, hardy desert trees, and grass are the only vegetation.

Wildlife

Small animals inhabit the area, such as rabbits, squirrels, prairie dogs and coyotes. Birds of all sizes are also present.

Background Noise

Regional earthquakes cause seismic disturbances occasionally. Some noise may also occur because of heavy passenger vehicle traffic and low-flying aircraft.

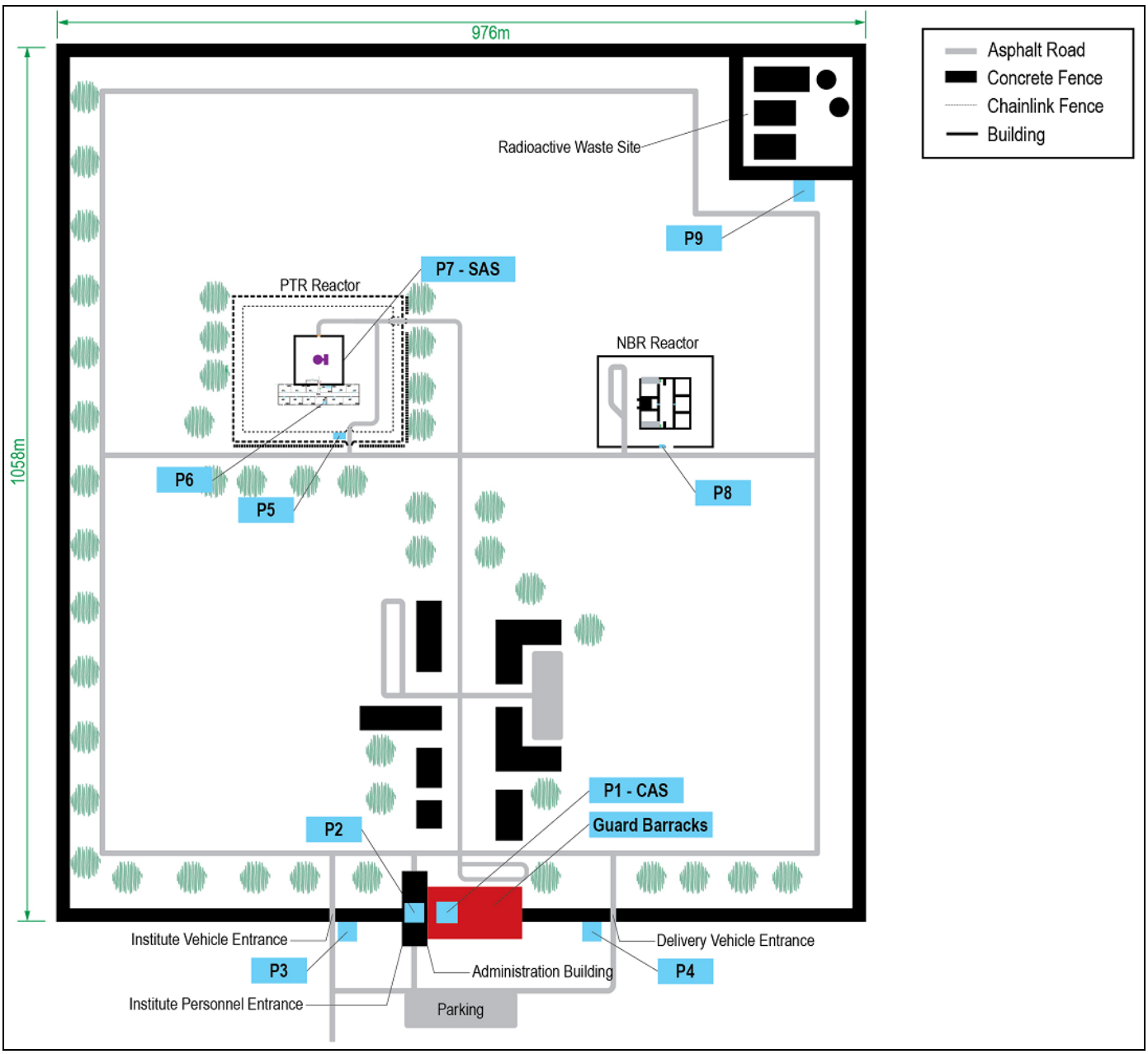
Climate/Weather

The climate is a typical high-desert environment with approximately 300 clear days of bright sunshine per year. On cloudy days, there are areas with a high light-to-dark ratio because of moving cloud shadows. Rainfall is about 15 cm per year, with the majority occurring during thunderstorms in the late July-August rainy season. The spring is very windy for 2 to 3 months, with continuous winds of 2 to 5 km/hr and gusts up to 50 km/hr. Dry debris, dust, and dead vegetation are blown about during the windy season.

Table 1. Nuclear Materials and Their Enrichment at the LIMP

Facility	Location	Form of Material	Amount of Material on Site (wt% enrichment)	Total Isotope Amounts	Level of Radiation
PTR Research Reactor	Reactor	$BeO\text{-}UO_2$ Fuel Rods (236 in reactor)	67.5 kg U (36% ^{235}U)	24.3 kg ^{235}U	High >1 Gy/hr at 1m
	R090 Fresh Fuel Vault	$BeO\text{-}UO_2$ Fresh Fuel Rods (50 in storage)	14.3 kg U (36% ^{235}U)	5.2 kg ^{235}U	Low
	Irradiated Fuel Pool	$BeO\text{-}UO_2$ irradiated fuel Rods (100 in pool)	28.6 kg U (35% ^{235}U	10.0 kg ^{235}U	High 0.02-0.03 Gy/hr at 1m
	R091 Product Vault	Pu Experiments HEU metal Other Sources	9.3 kg $^{239}PuO_2$ (100% ^{239}Pu) 23 Kg U (95% ^{235}U) Cs, Am, Sr	8kg ^{239}Pu 22 Kg ^{235}U 3 kg total	Low Low High
NBR Reactor Facility	R100	Fuel in Reactor Core (10 discs)	14 kg U (93% ^{235}U)	13 kg ^{235}U	Low
	R102	HEU-metal Fresh Fuel (9 discs)	12.6 kg U (93% ^{235}U)	11.7 kg ^{235}U	Low
	R102	Used Fuel (1 discs)	1.4 kg U (93% ^{235}U)	1.3 kg ^{235}U	Low <0.003 Gy/hr contact
Waste Storage Facility	Vats	Liquid Mixture (2 vats, 2,000 liters ea)	Trace Amounts of Pu (75% ^{239}Pu) and U (18% ^{235}U)	trace	High 0.5-1.0 Gy/hr at 1m
	Sheds	Solidified Waste (50 containers)	Trace Amounts of Pu(31% ^{239}Pu) and U(12% ^{235}U)	trace	High <0.5 Gy/hr at 1m

Section 4. LIMP Site Layout and Response Force Location



Section 5. Threat Assessment

The following Threat Assessment is prepared to assist the Development of the State Design Basis Threat (DBT). The Threat Assessment is organized into threats from: ideological terrorist groups, geo-political terrorist groups, subversives, criminal groups, and activist groups. As you review the Threat Assessment, consider the following policy issues for the State of Lagassi when developing the DBT:

- Lagassi is a developing state with limited economic resources. Significant increase in protection costs could strain the fragile economy.
- Lagassi has evolved from a somewhat unknown state on the world stage to an emerging economic state. This emergence has quickly increased the crime rate and a recently growing interest from terrorist groups.
- The people of Lagassi are proud of the historical accomplishments and their intellectual contribution to science. This includes the many accomplishments of the research reactor, including the recently awarded Nobel Prize for Physics.
- The state is politically democratic but has several political factions. The current government struggles to maintain its power base.
- A DBT review is scheduled for every 3 years.
- The people of Lagassi trust their government to make the appropriate decisions to protect them, any breach of that trust will greatly undermine the government's ability to maintain power.

International Ideological Terrorist Groups:

There are two ideological terrorist groups assessed in this report: The Antarctics and Peoples Liberation Movement.

The Antarctics

The Antarctics are founded, and continue to be a lead by Adrian Baker, a former professor of global economics. His deputy is Jose Digger, a former nuclear scientist and committed revolutionary. Baker embraced anarchist politics as a graduate student and developed a distinctive academic stance. He was dismissed from his academic post for his revolutionary views. He spent time working with various rebel groups before he put his thoughts into print. His most famous book, "The Antarctic Economy," was published in 1985. In it he argued that global trade is responsible for all environmental degradation and that the major economic blocks deny the opportunity for the rest of the world to develop environmentally sustainable local economies. In the book he develops his arguments by theorizing how an anarchist terrorist group might return the world to a pre-trade era. He chose the name the Antarctics because, he said, it had symbolic value. It was white, pure, and pristine.

Baker disappeared until 1998 when a small explosion occurred on a pipe-line north east of the Republic of Varnado. The explosion was commonly thought to be the work of a local terrorist group, but they denied it. Noticed only by one or two of the world's intelligence agencies – and dismissed as a hoax – was a claim on a website in the name of the Antarctics.

Less is known about Jose Digger. After national service in a nuclear submarine, he trained as an engineer and has worked at nuclear power plants. He is believed to have spent some time on a research project designing novel small nuclear reactors. He was a committed

revolutionary. It has been suggested that he blames western capitalism for the world's poverty and for this purpose he has allied himself with Baker.

Digger came to official notice after a second explosion at an oil refinery in Northern Stoyia. The explosive was placed on sensitive processing equipment within the controlled area of the refinery. It was again attributed to, but denied by, a local political terrorist group. Again, the Antarctics, claimed responsibility and included a description of the device, confirmed months later by forensic analysis, on their website.

The whereabouts of Baker and the Digger are typically unknown but recent highly sensitive intelligence reports them being in the mountains just north of Lagassi. They are thought to move easily among a number of separatist groups (Uplanders), and because of their intelligence and competence as well as their anti-everybody stance, are trusted by serious criminals. The latter are believed to offer them protection, and in exchange for small favors, operational support such as false documentation and small arms. These criminals, however, will not risk prejudicing their lucrative lifestyles by becoming too closely identified with the Antarctics.

The Antarctics originally believed that they should only have two members. However, the numbers of plausible Antarctic claims have risen substantially in the last 18 months and it is clear that they have recruited some dedicated support. It is estimated that there are up to five capable operatives involved. Forensic evidence suggests that there is now more than one bomb maker, although it is likely that they are all trained by the Digger. Analysis of the metals used suggests that he has created a sophisticated workshop or small factory. The metal case of one device contained minute quantities of CO_{60} but it was not possible to say whether this was from contaminated scrap metal or had been picked up in the factory.

It is believed that Baker is feeling older, he may even be terminally ill. If so, the fear is, he will want to do as much damage as he can before he dies. He cannot be confident that his beliefs and passion will outlive him. Based on this belief, his greatest desire would be to cause a nuclear winter and Digger's explosive expertise may be designed to support this effort. The intelligence consensus is that he now has no constraints other than to avoid capture. That too may end as he nears death and he may be prepared to risk arrest to achieve one final victory.

The most common means of attack used by the Antarctics is the improvised explosive device (IED). Improvised is something of a misnomer. These are sophisticated, highly reproducible devices built to precision. There is a preference for plastic explosives but black powder as well as a variety of non-commercial explosive mixtures have been used.

To supplement their income, the Antarctics have been accused of several bank robberies in a series of central continental states. This is unproven, but the professional planning and use of sophisticated, light equipment and weapons tends to point to the group. The method of operation for the robberies was three Individuals enter the bank, take control of the employees, customers, and guards and complete the robbery, while one of two others provided cover and escape. In each case, the alarm communications systems of the bank had been disabled just before the robbery and the video cameras diverted.

It is unlikely that the Antarctics will turn to suicide attacks. There is no evidence that they are even willing to risk their life, but their ultimate motivation, and Baker's health may change that.

The People's Liberation Movement

The People's Liberation Movement (PLM) was founded in 1994 by their religious messiah, know publically as Reverend X. The group's goal is to lead the world to the pious way prior to the end of the earth through dialogue, proselytism, and, if necessary, intimidation. They view governments as the barrier to the path to piety and are therefore, staunchly anti-government. They are also competitively anti-other religious beliefs, believing their theology, which is a mixture of the world's major religions, is the only true approach. The group's objective was announced publically on Dec 31, 1999 when they claimed responsibility for a truck bomb made of fertilizer and diesel fuel, which leveled the Evanistan parliament building. There were no casualties, but the announcement came with a warning to head the way or else.

A break up in 2002 greatly weakened the group's organization, and many leaders—not including Reverend X—were arrested. Since this time, PLM members have dispersed, gone underground, and infiltrated many other organizations. They await instruction from Reverend X. As a result, they are viewed as very resourceful, highly educated, very dangerous, and potentially suicidal.

A recent PLM member was captured during a foiled attempt to disable a military airport traffic control station using a home-concocted lethal gas in Dianistan. Interrogation of the member by a military officer at the air traffic center provided great insight into the mindset of the membership at large. From what was learned, it appears that members work alone and have little communication with each other. The PLM received instruction and the recipe for the lethal gas from an unknown (to him) source.

Indigenous Threats

The indigenous threat is complex and falls roughly into two types: criminal and ethnic.

Geo-political background of indigenous threats

Indigenous threats are largely an issue of the north and west. Its roots pre-date independence. The populations in some of the mountains and high pastures have always been robustly independent and self-sufficient. They have never really wished to be part of any state to which they would have to pay taxes, provide national service, etc. When independence was being established, the cartographers drew the lines roughly along the watersheds except where it made more sense, for example, in wide valleys to draw the line half way along from what was going to be Lagassi to whichever country was at the far end of the valley. The effect was that families that had shared the same mountain for centuries suddenly found themselves in different countries. Valleys that had been thoroughfares for traders and nomadic farmers suddenly achieved international boundary status. Those borders, of course, needed to be guarded and the local residents were formed into a militia. The governments of the day alienated the populations of the uplands and then armed them. It continued to do so until about 1950 when a dedicated Border Unit was created within the regular army.

It wasn't then, and certainly isn't now, as simple as that. Some of the people in the valleys and family groups believe that belonging to state Lagassi is the lesser of the two evils. Originally, Lagassi was largely pastoral and these groups could carry on in their traditional fashion. Other family groups, especially some large groups that ended up in different

countries, have been protesting violently ever since. Some groups want border changes (some would increase Lagassi's area, others would diminish it), some want to have greater autonomy but remain part of Lagassi, yet others want outright independence. The situation is made more complex by the provocation of Evanistan. Evanistan wants to annex the entire northern mountains and makes this claim on the basis that the groups living there are Evanese. Evanistan, therefore, covertly supports the groups in those mountains on the Lagassi side of the border. Not everyone supports this especially those on the Evanistan side of the border who want the mountains to be independent. Intelligence suggests that Evanistan wants the whole of the Northern Range for the minerals and rainfall, which falls largely on the southern slopes (Note: The Lagassi uranium mine is in this area).

Upland Criminal Organization (UCO)

Before describing the UCO, it is worth commenting briefly on policing in the area. As I am sure you will appreciate, policing is difficult and the population despises central authority. The population is armed and willing to defend itself. The weaponry is chiefly hand-guns and rifles and are mostly from the first half of the Twentieth Century. From time to time regional governors have tried to bring the area into line. This has almost always been counter-productive. Not only has there been open confrontation between the armed civilians and the police but the Uplanders have also resorted to terrorist attacks in towns, including the capital. The most effective governors (effective in terms of minimizing terrorist attacks) have been those willing to turn a blind eye to comparatively low level criminal activity. In return, the Uplanders do, from time to time, turn over their more extreme young men responsible for atrocities to the authorities. Time in prison, coupled with growing older and wiser, seems to have the desired calming effect. However, at least two individuals have developed a strong resentment and are leading the call for a unified mountain state.

For most of the last decade UCO activity has taken the form of a protection service, prostitution, and drug trade with violence to retain a market edge. The UCO would on occasion kidnap government officials, especially those involved with taxation. These officials were always released before the police and army could respond. On two occasions, militia units guarding the border were "arrested" by the UCO and their weapons confiscated. It is not known what happened to those weapons but we understand that at least one of these UCO groups now has at least 6 modern pistols and 2 modern sub-machine guns.

There are intelligence reports that document the group as transitioning to larger scale crime and away from its traditional business. This is partly due to the limited economic resources of the region. The addition of weaponry will enable larger scale "attacks" to achieve economic objectives.

The UCO has focused attacks in recent months that seemingly undermine authority, law and order, and the national infrastructure in the region. Since 2006 there have been over 700 civilian casualties and 11 army and police deaths. Army and police deaths have been mostly in or near the western mountains. A handful of deaths have been the result of rifle sniper fire but the majority is the result of a roadside ambush including IEDs detonated by cable. Improvised mortars have been used on barracks and one military hostel was set on fire (it is believed by an incendiary device hidden in a video). Civilian deaths (5 in total) have mostly been away from the Mountains, chiefly in or near the capital or railway stations. One device was a vehicle born IED triggered by a movement detector, there were about 10 improvised incendiary devices, and the rest were hand portable IEDs of about 5kg each carried in sports bags, shopping bags etc. Nearly all were triggered by cheap mechanical timers. Circuitry in a couple of more recent devices has been sent for further forensic

analysis. We believe they may have been triggered by mobile telephone. The explosives in the IEDs tend to be constructed from chemicals and fuel readily available to the farming community.

Most recently, the group committed an armed assault of a branch of the Bank of Lagassi. Their approach was overt, violent, and effective. The assault was initiated by detonating an IED at the local government headquarters. The bank robbery then proceeded quickly with use of weapons and physical intimidation of the bank employees and customers. Both bank guards were killed at the onset of the robbery.

Our sources provide limited pre-emptive intelligence. Parts of that area of the country are barely governable. The sources are generally reliable.

Ethnic Terrorist Group

Within the mountain areas are three valley complexes each virtually cut off from the outside world. One of these is in the area that Evanistan wishes to annex; the other two are in the western mountains. Most of the surface transport routes to developed countries run through these western mountain passes but travelers will be totally unaware that only a few miles away there are two counties that are virtually untouched by modern life. These three valley complexes have something in common, they are each home to an ethnic group brought in or left behind by ancient waves of population movement.

These groups share the vigorous independent mindedness of the other mountain peoples. However, by and large, they wish to be left alone. Intelligence sources consistently report that the county elders wish to do nothing that might cause the authorities to try to take control. They recognize that in the end they would lose, because the UCO would not protect them. The UCO despises these enclaves and have been known to attack individuals from the group.

There are increasingly vocal ethnic views being expressed in both the valleys. These views are expressed by only a few and they tend to be ostracized by the rest of their communities. However, intelligence suggests that this isolation is causing them to become radicalized. We believe there may be up to four small and completely independent groups of radicals each no more than 6 strong. There is no intelligence to support this but we believe it is only a matter of time before we see suicide attacks of the same sort seen elsewhere in the world.

Their weaponry is primarily primitive hunting rifles with which they are very effective. There is no evidence of use of explosives, although future use cannot be ruled out.

Indigenous terrorism from the western mountains constitutes a serious potential challenge. It represents something more than superficial sparring between the state and ethnic groups that wish to distance themselves to a greater or lesser degree from the state. Although there is no specific intelligence, past experience suggests it is only a matter of time before a leader emerges who will unite the groups.

Our sources provide limited pre-emptive intelligence. Parts of that area of the country are barely governable.

Domestic Threats

Yellow-Green League

Although vehemently denied by its official spokesman, the Yellow-Green League is the political front for the **Environmental Defenders (ED),** one of the oldest environmental activist groups. The Yellow-Green League stands in elections and currently holds about 15% of the seats in the Regional Assembly. It came in a close second in four of the National Parliamentary seats at the last election.

The ED has historically pursued aggressive and even violent means to achieve its ends, which are to protect the environment from damage for future generations. The approach has included protests, sabotage of facilities and transport, and physical violence against workers and government officials related to the research reactor. There is reported to be vigorous debate within the League and ED about future strategy. A younger leadership is emerging that believes that any hint of violence may be counter-productive to the desire to pursue a national anti-nuclear stance, whereas older members are more inclined to pursue methods that have worked in the past.

The last large activity of the group was a demonstration two years ago that turned violent. A group of 300 protesters advanced on the reactor at dawn on a Sunday morning and climbed the fences in unison. The guards were called out but were quickly overwhelmed by the mob who came to paint a slogan on the reactor building. A few guards tried to use force to repel the protestors, and the confrontation turned violent. One guard was killed, and two were hospitalized. It is thought that a few violent instigators were responsible for inciting the violence. There is some evidence that the group may have been infiltrated by local terrorist groups.

Miscellaneous intelligence thought to be relevant

1) **Yellow-Green League**

Intelligence

A source has reported that the YGL leadership plans to buy land adjacent to the site of the research reactor. The land includes the road over which fuel shipments are transported. The intention is to resell the land in lots of 1 sq. m.

Assessment

The source volunteered this information to us. The source is new and unproven but is known to have direct access to the ED leadership. We believe the source to have been motivated by personal vengeance and assess the intelligence to be credible.

Section 6. Response Forces at the Lagassi Institute of Medicine and Physics

Types of Response Force Personnel

The response force consists of two types of security personnel:

- unarmed guards
- the tactical response force

Responsibilities of Response Force

These security personnel are responsible for:

- assessment of alarms
- administrative duties such as access control and key service
- routine patrol and staffing of fixed posts
- armed response to all intrusion alarms

All posts and patrols have defined policies and procedures with which the security personnel must comply.

Supervisors

For each shift, two supervisors are present:

- Supervisor 1 supervises the guards that conduct administrative duties and access control
- Supervisor 2 is the commander of the tactical response teams

Tactical Response Team Members

Tactical response teams have five members each. A two person response team is on random patrol. All members are trained in close-quarters combat and have the authority to enter target locations to ensure the safety of critical assets and target material.

The tactical response force commander for each shift is responsible for the oversight and supervision of all daily activities as well as emergency response to intrusion alarms.

During **operational hours**, three teams are present at the institute, with the following responsibilities:

- Team 1 responds to the research reactor
- Team 2 responds to the NBR facility
- Team 3 is in a training mode, but can be available to respond as directed by the response force commander

During **non-operational hours, weekends, nights, and holidays**, there are two tactical response teams on site. They are dedicated to intrusion alarm response at either the research reactor or the NBR facility.

Equipment: Guards

All **guards** are equipped with:

- a straight baton
- one set of handcuffs
- a small flashlight
- a handheld radio

Equipment: Tactical Response Team

The **tactical response** team members are equipped with

- a Markov pistol with a fully loaded magazine but without a round in the chamber and

- a Kalishnikov assault rifle with a fully loaded magazine but without a round in the chamber
- two spare magazines of ammunition for each weapon. Both weapons are carried with a fully loaded magazine but without a round in the chamber.
- a straight baton
- handcuffs
- flashlight
- handheld radio
- body armor is readily available in the response force building

Training

Classroom training (all security staff):

- access control procedures
- use of force continuum
- target locations
- response procedures
- chain of command
- other administrative responsibilities

Tactical response team personnel receive additional training on:

- close quarters combat
- recapture and recovery of nuclear material/facilities
- advanced firearms training for both the pistol and the assault rifle

Firearms training:

- Tactical response team personnel are required to qualify with their firearms four times a year
- Tactical response teams are provided with firearms training each month to ensure proficiency

All personnel receive routine physical fitness training when in the training mode.

Alarm Stations and Communication

The **Central Alarm Station** (CAS) is located in P1 and is staffed by two guards during the day and one guard at night. All alarms are received at the CAS. Alarms from the PTR facility are assessed by P1 using video. Alarms from the NBR are assessed by the guard at P8.

The **Secondary Alarm Station** (SAS) is located in P-7 and is staffed by two guards during the day and one guard at night. The SAS monitors the activities of the CAS to ensure appropriate actions are taken. The CAS only relinquishes monitoring and control during maintenance and other temporary facility outages.

Both the CAS and the SAS are equipped with:

- 100-watt radios that can communicate to all posts and patrols within the boundaries of the Institute.
- 2 telephone lines. One is linked to each fixed post via a buried telephone cable and the second telephone is a direct link to the Ministry of Interior headquarters located in the city.

Extensive testing of the communication system has shown that the radio communications are good throughout the Institute with the exception of the lower level interior of the NBR facility. Testing concluded that security personnel inside the NBR facility are able to monitor transmissions from both the CAS and the SAS but are unable to transmit to the CAS and the SAS with their handheld radios.

All handheld radios and fixed posts are equipped with a duress switch to allow a covert signal to the CAS and SAS of unauthorized activity. When the CAS or SAS receive a duress alarm, the response team is notified and the response force commander initiates a tactical response.

Deployment of Response Force

The response force is deployed as described in the following table.

Table 2. Response Force Deployment Data

Post No.	Description	Security Personnel	No. of Personnel	
			Workdays	Non-workdays
S-1	Response Force Commander	Captain	1	1
S-2	Guard Commander	Lieutenant	1	1
P-1	Response Force Headquarters	Response Force	15	10
P-1	Central Alarm Station	Guard	2	1
P-2	Institute Personnel Entrance	Guard	3	1
P-3	Institute Vehicle Gate	Guard	2	1
P-4	Institute Delivery Vehicle Gate	Guard	1	0
P-5	PTR Personnel/Vehicle Portal	Guard	1	1
P-6	PTR Building Personnel Portal	Guard	1	0
P-7	Secondary Alarm Station	Guard	2	1
P-8	NBR Personnel Portal	Guard	1	1
P-9	Waste Storage Facility	Guard	1	1
P-10	Random two-man patrol of Institute	Response Force	2	2
		Totals	**33**	**21**

Response Procedure for Response Force

All alarms are received and assessed at the Central Alarm Station. The Secondary Alarm Station verifies the CAS operator's assessment to ensure all alarms are properly assessed. The CAS operator immediately notifies the Commander of the Response Force so preparations for deployment can begin by the appropriate tactical team. In addition, institute procedures require that the nearest guard also be dispatched to the point of the alarm to provide additional assessment and to observe and report any unauthorized activity. The appropriate response force:

- collects their firearms from the armory,
- puts on their body armor, and
- prepares to respond either by foot or vehicle as directed by the commander.

Once the tactical team arrives at the appropriate facility, they deploy as a team and proceed with operations to enter the facility and ensure the protection of material and assets.

Response Force Performance Data

The Institute has conducted extensive performance testing of the response force in the areas of alarm assessment, alarm communication, preparation, travel and deployment times to alarms at the research reactor and the NBR facility. The average times are listed in Table 3. Institute procedures require that all tactical responders be available to respond to an alarm from P-1. All tactical responders are fully equipped with their duty gear with the exception of their rifles, which are kept in storage in the armory until needed.

Table 3. Average Times for Physical Protection Systems Functions

Description	Research Reactor	NBR Facility
Alarm communication time	1 second	1 second
Alarm assessment time	45 seconds	45 seconds
Response force communication time	18 seconds	18 second
P-1 Response force preparation time	90 seconds	90 seconds
P-1 Travel time by vehicle	75 seconds	65 seconds
P-1 Travel time by foot	250 seconds	200 seconds
P-1 On-site deployment time (after arrival)	90 seconds	90 seconds
P-10 Preparation time	0 seconds	10 seconds
P-10 On-site deployment time (after arrival)	20 seconds	30 seconds
P-10 Travel time by vehicle	45 seconds	45 seconds

Section 7. Operations at Gates and Portals at LIMP

Institute Vehicle Gate (P3)

The gate is unlocked and open during normal working hours and locked during off-shifts.

Guard Force Staffing: During operational hours, 2 guards are present; one at the gate and one available for other duties. At night, 1 guard is present.

1. **On entry**, vehicles drive slowly and all passengers show the guard their badges.
2. The guard looks inside the vehicle and allows it to pass.

1. **On exit**, the vehicles must stop and wait for the guard to wave them out.
2. A guard observes exiting vehicle for proper actions.

Institute Personnel Entrance (P2)

Guard Force Staffing: 3 guards are present, including one inside the front door all the time; however, only 1 guard is present at night.

1. **On entry**, personnel form a single line and show the guard their badge as they enter. If an individual does not have a badge, the guard directs him or her to the badging station in Administration Building.
2. Personnel enter through the front door of the Administration Building and continue out the back of the building to go to other areas in the facility.
3. A guard observes personnel for unusual behavior.

1. **On exit**, personnel wait in a line inside the Administration Building.
2. The guard waves personnel to pass one at a time out the front door.
3. The guard observes personnel for unusual behavior.

Institute Delivery Vehicle Gate (P4)

This gate is normally closed and locked with a high security padlock.

Guard Force Staffing: 1 guard is present during the workday, none at off-shift.

1. **On entry**, when a delivery truck arrives, the guard at P4 notices it.
2. The guard inspects the vehicle and the authorization papers.
3. The guard inspects the badges of the driver and passengers in the vehicle. If an individual does not have a badge, the guard directs him or her to the badging station in Administration Building.
4. If all is acceptable, the guard unlocks and opens the gate.

1. **On exit**, the guard at P4 notices the vehicle approaching.
2. The guard unlocks the gate, inspects the vehicle, and then opens the gate and allows the vehicle to proceed.

PTR Personnel/Vehicle Portal (P5)

Guard Force Staffing: 1 guard is present at P5 at all times. If a vehicle requires entry into the PTR, the guard at P5 calls another guard to assist with the vehicle entry.

Personnel Entry:

1. **On entry**, personnel approach the portal door, run the badge through the reader, and, if necessary, press the electric buzzer button on the door to alert the guard.
2. If authorized from the badge code or by the guard inside P5, the gate will unlock and a single person enters the portal.
3. Under observation of the guard in P5, the person presents a picture badge at the window.
4. If the badge picture matches the employee's face, the guard in P5 electronically unlocks the inner door.

1. **On exit**, the personnel form a line at the portal door.
2. Personnel run the badge through the reader, and, if necessary, press the electric buzzer button on the door to alert the guard.
3. If authorized from the badge code or by the guard inside P5, the door will unlock and a single person enters the portal.
4. The person presents the picture badge to the guard at window.
5. The guard at P5 electrically opens the outer door and lets the person exit.
6. If there is any question, the person is held in the portal.

Vehicle Entry:

1. **On entry**, the vehicle's driver drives the vehicle up to the outer gate. (Vehicles larger than 30 feet are not permitted in the PTR.)
2. The driver may push an electric buzzer button at the gate to alert the guard.
3. The P5 assist-guard radios the CAS to pre-announce expected alarms from the BMSs and IR sensors in the vehicle portal. Then the assist-guard at P5 unlocks and opens the outer gate.
4. The vehicle enters the portal and the assist guard inspects the paperwork authorizing the vehicle in the area, then the driver and any passengers leave the vehicle and go to the personnel portal to enter.
5. The assist-guard shuts and locks the outer vehicle gate.
6. The driver, and any passengers, enter the pedestrian portal, and is subjected to the same checks as all personnel entering the PTR area. They proceed to the inner vehicle portal gate.
7. While the driver/passengers are in the personnel portal, the assist-guard inspects the vehicle for contraband while it is still in the vehicle portal.
8. When the inspection is complete, the guard unlocks and opens the inner vehicle gate and waits for the driver/passengers.
9. The driver/passengers reenter the vehicle, and drive into the area.
10. The inner gate is closed and locked by the assist-guard.

1. **On exit**, the process is slightly different than the reverse. The vehicle's driver drives the vehicle up to the inner gate.
2. The driver may push an electric buzzer at the gate to alert the guard.
3. The guard at P5 calls for assistance at the P5 vehicle portal.
4. The assist-guard inspects driver/passenger badge and paperwork. The assist-guard inspects the vehicle for stolen material.

5. Once cleared, the P5 assist-guard radios the CAS to pre-announce expected alarms from the BMSs and IR sensors in the vehicle portal.
6. The assist-guard at P5 unlocks and opens the inner gate.
7. The vehicle enters the portal and the assist-guard closes the inner gate.
8. Then the assist-guard the guard unlocks and opens the outer vehicle gate.
9. The vehicle exits the vehicle portal.
10. The assist-guard shuts and locks the outer gate.

PTR Emergency Vehicle Portal

Guard Force Staffing: Manned only in times of emergency or special use.

1. **For entry**, a guard must be present to unlock and open the outer gate manually,
2. The guard manually checks the vehicle and the driver.
3. The guard unlocks and opens the inner gate and allows the vehicle to proceed quickly.
4. The guard shuts and locks both gates.

1. **On exit**, the process is reversed.
2. A guard must be present to unlock and open the inner gate manually.
3. The guard manually checks the vehicle and the driver.
4. The guard unlocks and opens the outer gate and allows the vehicle to proceed.
5. The guard shuts and locks both gates.

PTR Building Personnel Portal (P6)

Guard Force Staffing: 1 guard is present whenever there is any person inside the inner area. At other times, the doors are locked and the guards are not present.

1. **On entry**, the employees, one at a time, enter through the unlocked outer door.
2. Each person presents his picture badge to the guard for badge exchange.
3. If the picture on both badges and the person's face match, the person can continue.
4. Under the observation of the guard, the person walks through the metal detector.
5. If there is an alarm or if a package is suspicious, the guard manually inspects the package.
6. Once past the metal detector, the employee scans the exchanged badge and enters his personal identification number (PIN.)
7. The turnstile will turn and allow entry into the building.
8. The guard will allow the next employee to enter the portal and repeat the process.

On exit, the process is reversed. The employees exit through the door next to the turnstile.

1. If the portal is empty, the first person scans the exchanged badge and enters a PIN.
2. If the PIN is correct, the door will open to let them enter the portal.
3. The person walks through the metal detector under the observation of the guard.
4. If there is an alarm or if a package is suspicious, the guard manually inspects the package.
5. The person re-exchanges his badge with the guard and exits the portal.

NBR Personnel/Vehicle Portal (P-8)

Guard Force Staffing: 1 guard is present at P8 at all times. Using an alarm system workstation, the guard places all alarms for the NBR facility, except D103, in "access" at the beginning of the shift and places the alarms in "secure" at the end of the shift. The guard and a second authorized individual unlock the high security padlocks on the main entrance at the beginning of the shift and lock the padlocks at the end of the shift.

Pedestrian Portal:

1. **On entry**, personnel show the guard their badge at the P8 entry window.
2. The guard waves personnel to the gate and "buzzes" them through, unlocking the magnetic lock.
3. Personnel scan their badge at Door D40/1 and enter a PIN.
4. If the PIN is correct, the door will open allowing them to enter the building.
5. The personnel walk through the metal detectors and if there is an alarm, the person ensures he/she does not have contraband.

1. **On exit**, personnel scan their badge at Door D40/1 and enter PIN.
2. If the badge is valid, the door will open allowing the person to exit.
3. Personnel then approach P8 and show the guard their badge at the exit window.
4. The guard waves personnel to the gate and "buzzes" them through, unlocking the magnetic lock.

Vehicle Portal:

1. **On entry**, driver, and any passengers, approach the entry window at the P8 pedestrian portal and shows the guard their badge and authorization to drive into the facility.
2. The guard leaves P8 and unlocks and opens the vehicle entrance.
3. The guard allows the vehicle to enter and relocks the gate.

1. **On exit**, driver and any passengers approach the guard shows their badge at the P8 exit window.
2. The guard leaves P8 and unlocks and opens the vehicle entrance.
3. The guard allows the vehicle to exit and relocks the gate.

Section 8. Waste Storage Site—Description

General Description

The Waste Storage Site is located at the northeast corner of the Lagassi Institute of Medicine and Physics, a hypothetical nuclear research center. The Waste Storage Site is an IAEA Category III site that is used for the storage of radioactive wastes from the PTR, NBR, and other reactor facilities. The site contains an unloading structure, a storage area for low-level liquid wastes, a burial area for wastes mixed with concrete, and three storage buildings for medium-level and high-level wastes, isotopes, and metals. Because of recent theft attempts by local civilians and a group of students, all of whom were contaminated during the theft attempts, the site is now under 24-hour guard. The medium-level and high-level metals and isotopes are the main concern of LIMP safety and health physics personnel.

Liquid Wastes

Liquid wastes are placed in one of two buried tanks until the tanks are full. The tanks have two-metric-ton lids that can only be lifted by crane. When the tanks are full, the liquid is mixed with concrete and then buried.

Low-level and Medium-level Solid Wastes

Low-level and medium–level wastes are stored in sealed containers in two of the three storage buildings. The majority of these wastes consist of contaminated clothing, irradiated components, and maintenance equipment.

High-level Wastes, Isotopes, and Metals

High-level waste consists of severely irradiated components, isotopes, and isotope-contaminated materials, and some highly irradiated metals. This material is stored in sealed containers in one of the three storage buildings. The material in this building has been the target of two theft attempts that resulted in contamination and radiation exposure of some of the thieves.

Section 9. PTR Research Reactor

Note: The description of this reactor is purely hypothetical.

General Description

The PTR is a light water moderated, highly enriched uranium (HEU) fueled research reactor located within the Lagassi Institute of Medicine and Physics, a hypothetical nuclear research center. The Institute is located in the Republic of Lagassi, approximately 29 km (18 mi) east of the capital city of Hashbakar, the major population center.

The reactor is used for research on advanced reactor components, special fuel assemblies, and production of radionuclides for the medical industry. Other experiments are performed to investigate power reactor fuel when heated to the point of melting. A neutron radiography facility is also available as well as extensive irradiation tubes and hot cell facilities.

A total of 32 people work at the PTR Research Reactor and usually the reactor is not operated during the evening and off-shifts. During the off-shift periods, only response force guards are at the facility and doors to the reactor building itself are locked and alarmed.

Reactor Data

1. The pool-type research reactor is used in a steady-state operation of 2 MW.
2. The central irradiation cavity is dry and 23 cm in diameter.
3. The annular core is formed by 236 cylindrical fuel elements arranged in a hexagonal grid around the central irradiation cavity.
4. The reactor is controlled by 7 fuel-followed control rods with rod drive motors accessible.
5. At least 5 control rods must be removed for the reactor to go critical.
6. Fuel material is BeO-UO_2, 22 wt% UO_2, 78 wt% BeO with uranium enriched to 36 percent ^{235}U.
7. Each fuel element is approximately 1 meter long, 2 cm in diameter and weighs a total of 2 kg.
8. Each fuel element contains 103 grams of ^{235}U and is clad in stainless steel.
9. Fuel rods are placed in a grid and may be removed with a rigid fuel-handling tool.
10. Centerline fuel temperatures range up to 1,500 °C.
11. The core is located in an open pool 3.1 meters in diameter and 8.5 meters deep.

Cooling System

1. The pool contains 62.5 cubic meters of deionized water at a maximum temperature of 60 °C.
2. The core is cooled by natural convection in the water pool.
3. The pool is constructed of stainless steel.
4. A forced air/water heat exchanger is used to discharge the waste heat to the atmosphere.
5. The heat exchanger is inside the reactor building with air ducts (and grids) through the building walls.
6. Air ducts are mild steel, 0.3 cm thick and the grill is #4 (13 mm) rebar on 15 cm centers.
7. The reactor core is designed so that if a complete loss of water occurs after sustained 2-MW operation, air is sufficient for cooling. (However, natural circulation of air is essential.)
8. Pumps are located below the reactor coolant level to ensure adequate Net Positive Suction Head.

9. The cleanup loop flow rate of 1 to 2 liters/sec is used to:
    - remove impurities,
    - maintain pH,
    - maintain resistivity within specifications, and
    - provide deionized makeup water.

Irradiated Fuel Storage and Handling

1. Irradiated fuel elements are transferred underwater to the spent fuel storage pools.
2. The elements are transferred in storage racks using rigid handling tools.
3. The dose rate of freshly discharged spent fuel is approximately 20-30 rad/hr. (0.2 to 0.3 Gy/hr) at 1 meter.

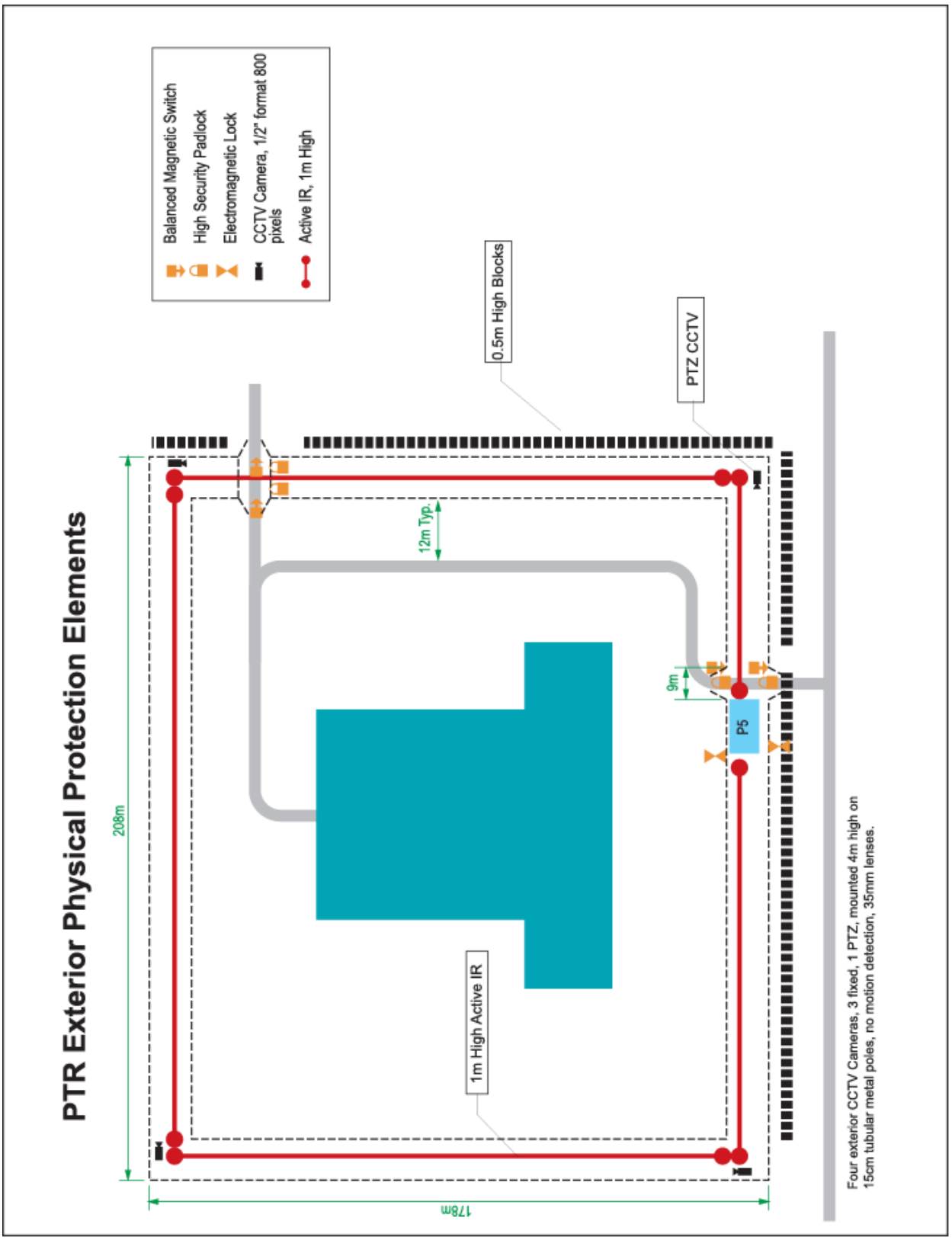
Nonirradiated Fuel Storage and Handling

1. Fuel rods arrive in shipping containers.
2. Fuel rods are stored in a reinforced concrete storage vault, R090, in the reactor building.
3. Fuel storage racks capable of holding 10 fuel rods are used to transfer new fuel rods into the reactor pool.
4. The storage vault can hold 5 storage racks.
5. Cotton gloves are worn when directly handling the fuel elements.
6. A rigid fuel-handling tool is used to transfer the fuel element to its intended position once in the reactor pool.

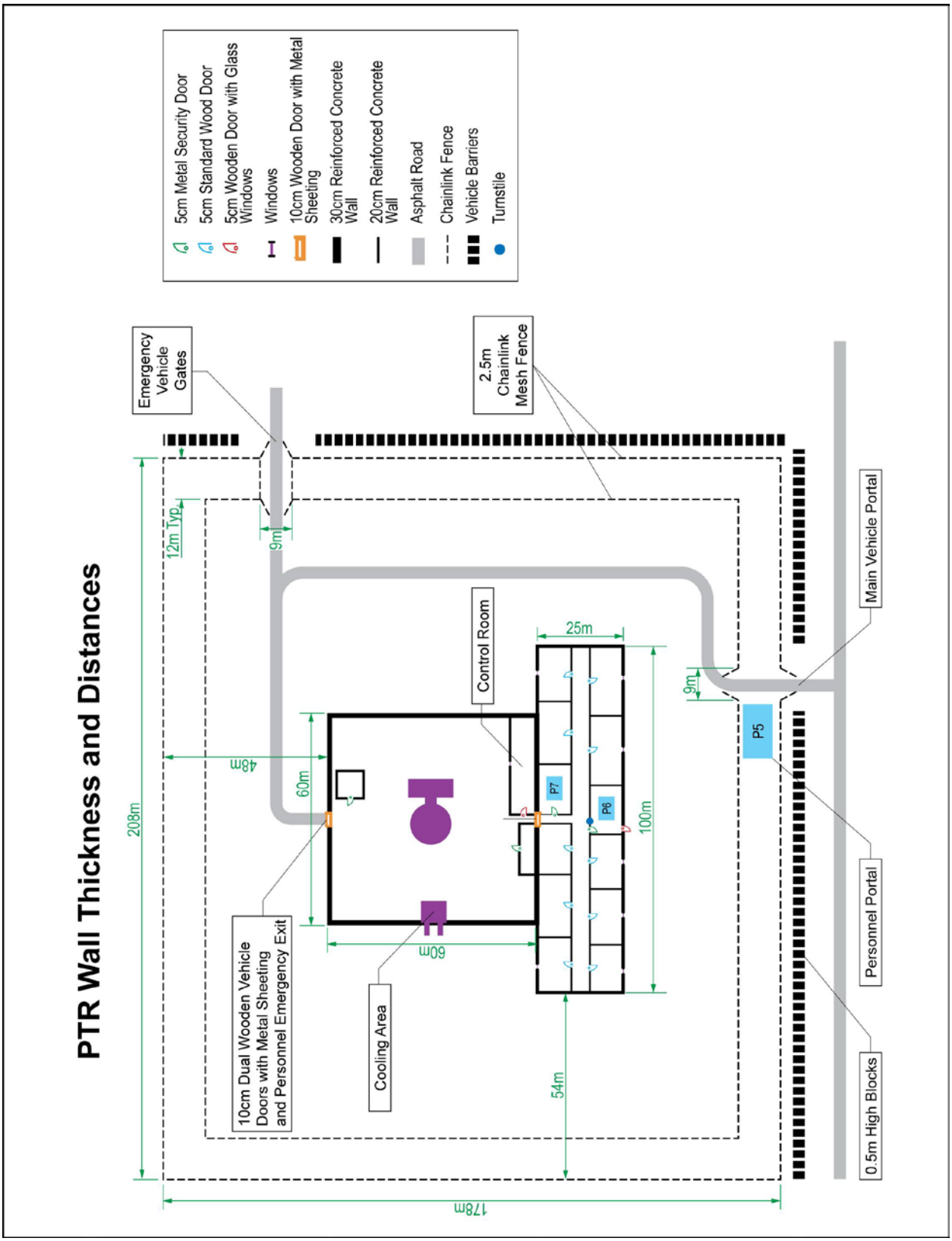
Experiment Materials

1. Three kilograms total of highly radioactive medical radionuclides, including Cs, Am, and Sr^{90}.
2. Mixed oxide fuel rods. A maximum of one assembly is in the reactor core at one time and no more than 4 are located on site at one time. Each MOX assembly weighs a total of 30 kg and each contains 2 kg of plutonium^{239}.
3. Targets are used in other irradiation and activation experiments.

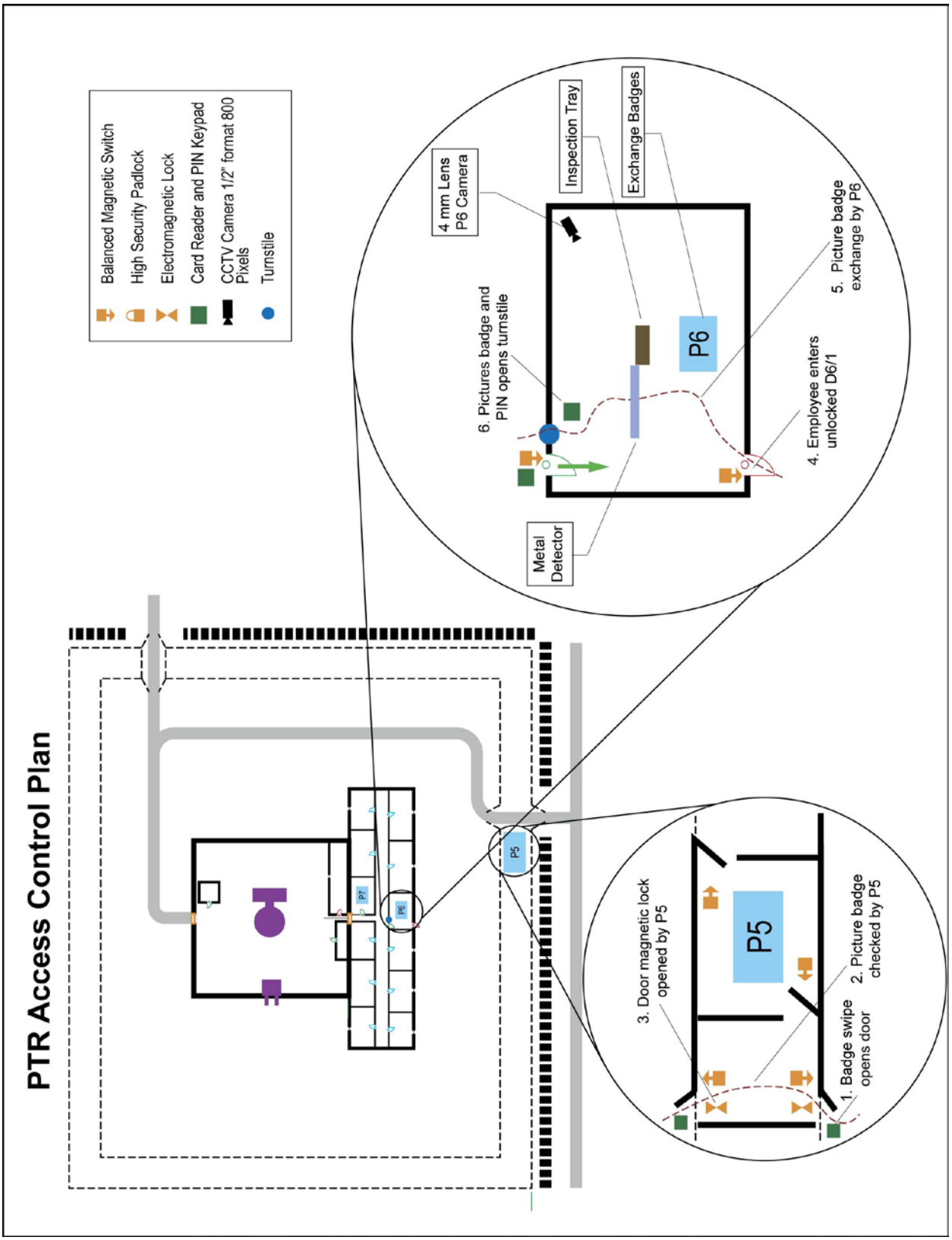
Section 10. PTR Exterior Physical Protection Elements



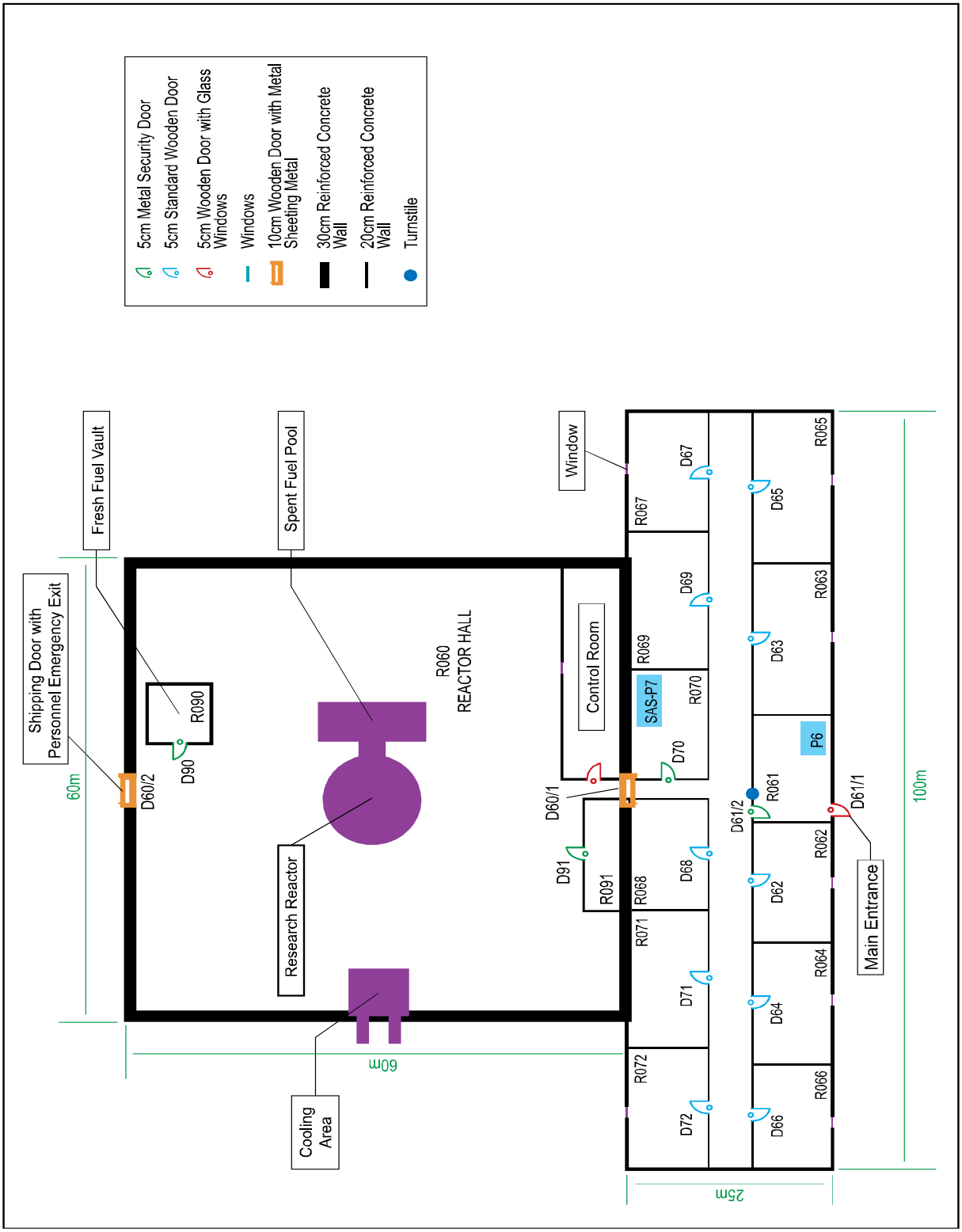
Section 11. PTR Wall Thicknesses and Distances



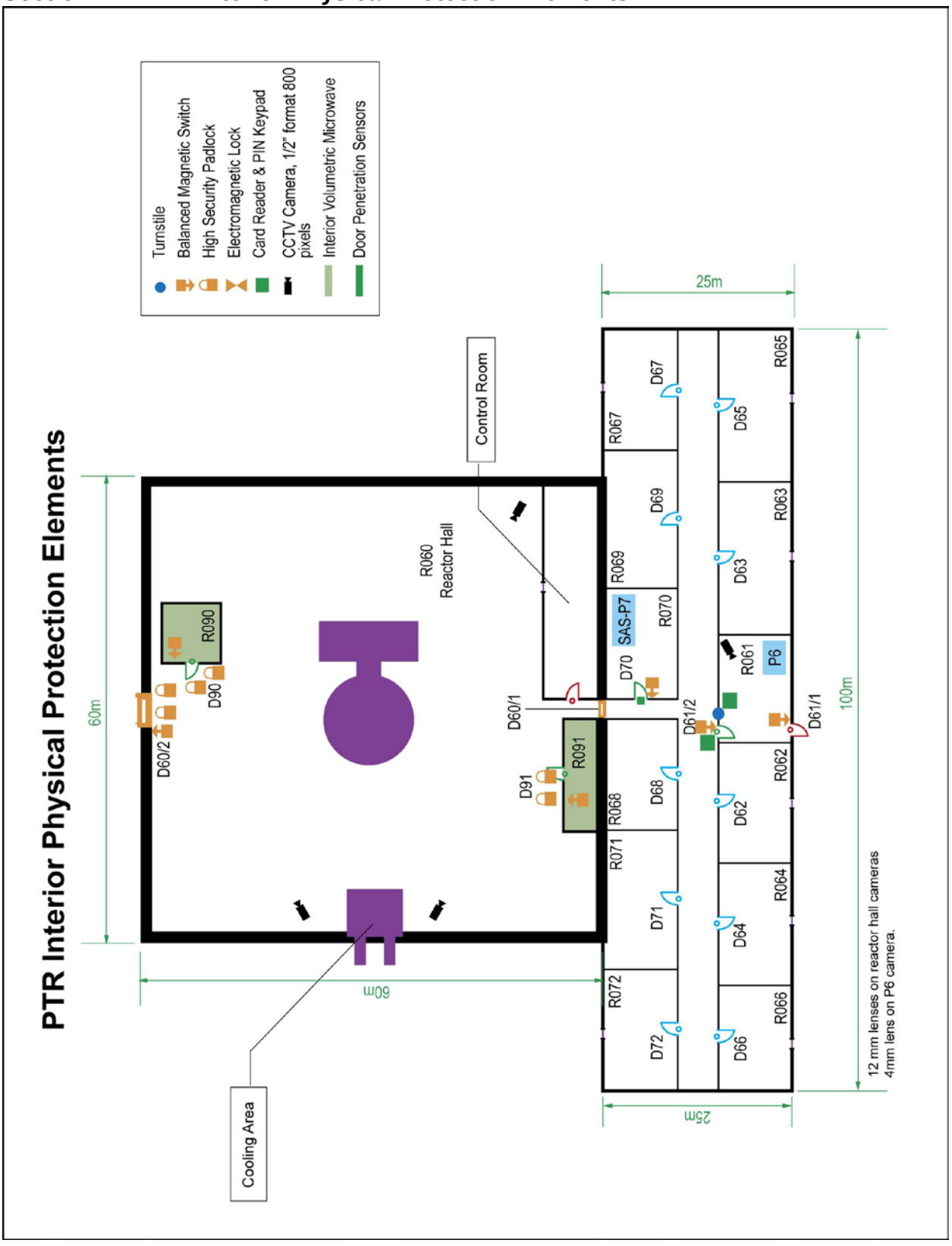
Section 12. PTR Access Control Plan



Section 13. PTR Building Floor Plan



Section 14. PTR Interior Physical Protection Elements



Section 18. NBR Pulse Reactor—Description

Note: The description of this reactor is purely hypothetical.

General Description

The LIMP Neutron Burst Reactor (NBR) is a reflected GODIVA-type research reactor designed for conducting experiments related to the collection of basic nuclear physics data for code validation purposes. The reactor fuel assembly is a metallic oralloy (93.71 wt% U-235, 5.24 wt% U-238, 1.05 wt% U-234) sphere of 14-kg weight surrounded by a 10-cm thick beryllium reflector. This design allows material quantities—and thus theft consequences — at a minimum level, in contrast to bare-core designs. The core assembly (fuel and reflector) is actually segmented into ten equal-weight plates of constant mass (1.4 kg uranium), but varying in thickness and overall diameter. The plates are normally separated by very small air gaps such that the assembly is normally subcritical. In a test "firing", a compressed air cylinder momentarily shoves the plates together into what becomes a critical configuration, resulting in the production of a burst of energy (e.g., neutron radiation) for experimental purposes (it is also interesting to note that this energy release also serves to drive the plates apart, returning the core to a subcritical configuration).

Reactor Data

1. The NBR pulse reactor is capable of very short duration pulsed operation for neutron burst experiments.
2. The reactor core is formed by 10 disc fuel elements of varying dimension (constant weight of 1.4 kg) that, when stacked together with a reflector, exactly form a critical sphere.
3. The reactor is controlled by momentarily decreasing the gaps between the fuel element discs.
4. The fuel is HEU metal (93.71 wt% U-235, 5.24 wt% U-238, 1.05 wt% U-234).

Cooling System

Between test firings the reactor has a procedural and safety-interlock controlled down time to allow the core time to cool. (No forced cooling system provided.)

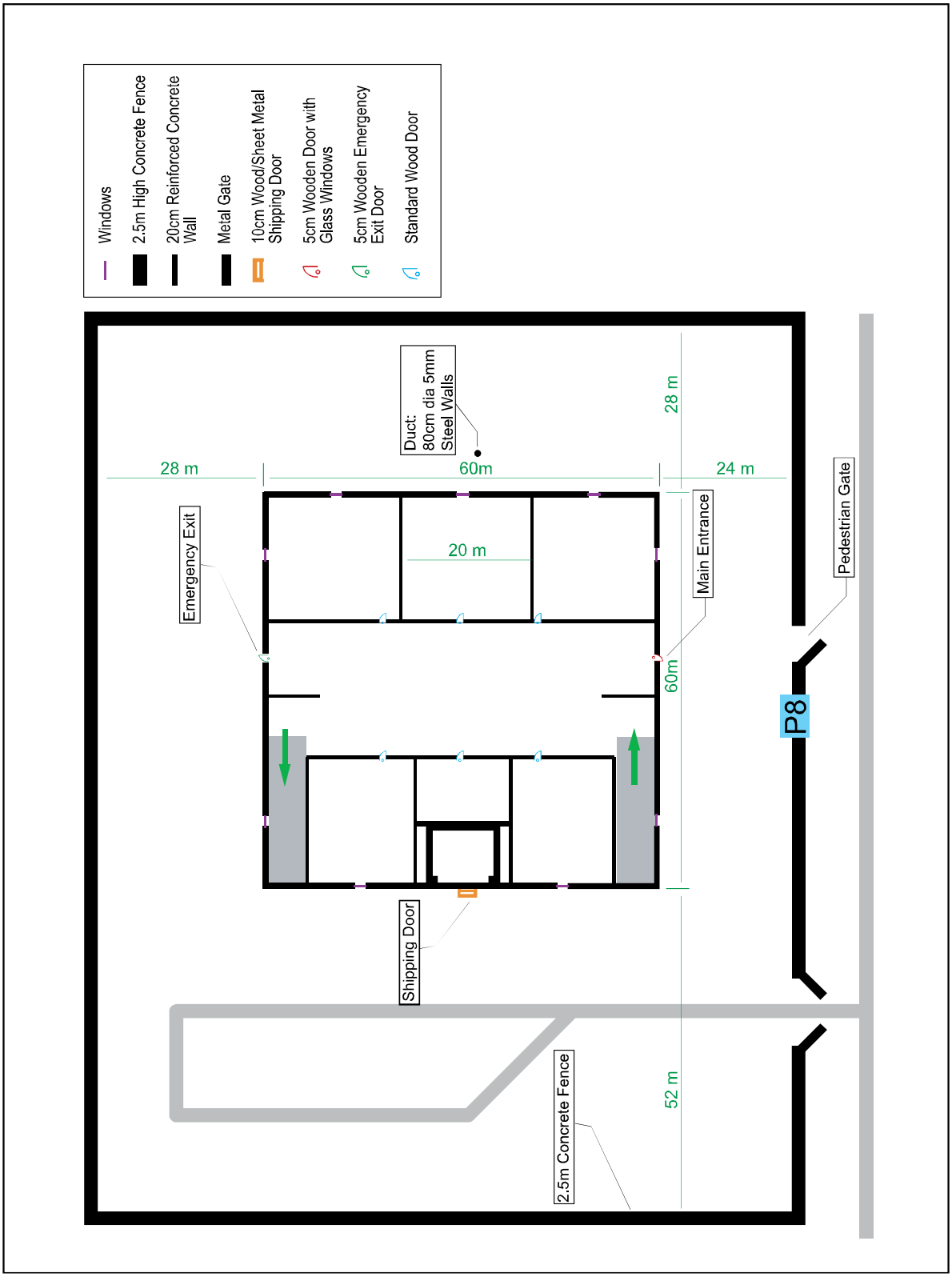
Irradiated Fuel Storage and Handling

1. Because of its designed use, the NBR fuel is never subjected to any significant burn up, and thus it will never be "spent". However, on rare occasions the shock and thermal stresses in the fuel elements cause cracks to form. In such cases the damaged fuel plate is replaced with a spare and stored as "used fuel" for later reforging.
2. Damaged fuel elements are transferred manually to the "used fuel" storage container.
3. Damaged fuel elements are transferred in locked storage boxes.
4. The "used fuel" locker is located in the fuel vault, R102, in the NBR reactor building lower level.
5. The surface dose rate of used (damaged) NBR fuel is approximately 2 mSv/hr, while the dose at one meter is hard to distinguish from background (100 nSv/h).

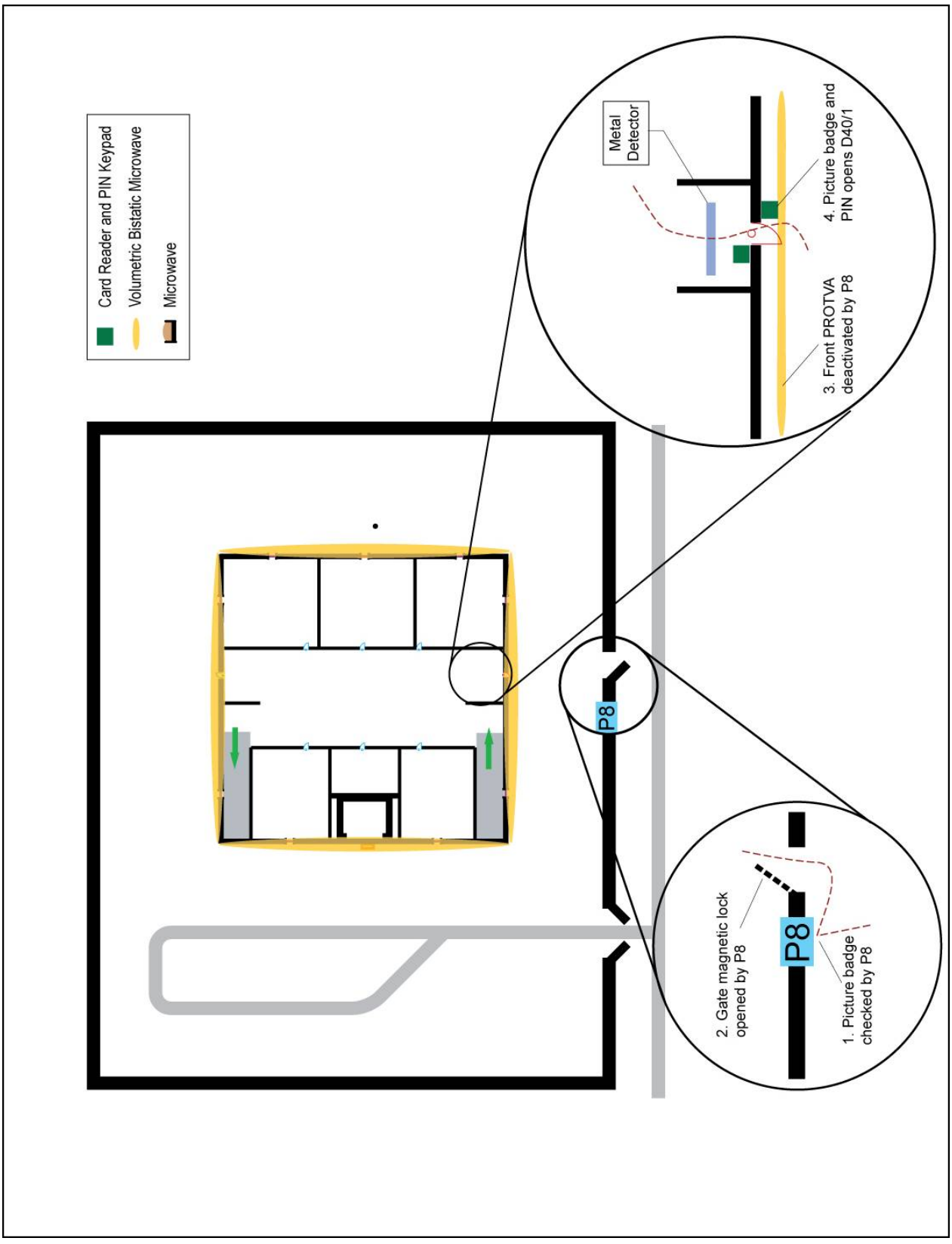
Nonirradiated Fuel Storage and Handling

1. Fresh fuel discs are forged on-site.
2. Fuel discs are stored in storage lockers in the fuel vault, R102, in the NBR building lower level.
3. The storage vault can hold up to 50 discs.
4. Cotton gloves are worn when directly handling the fuel discs.

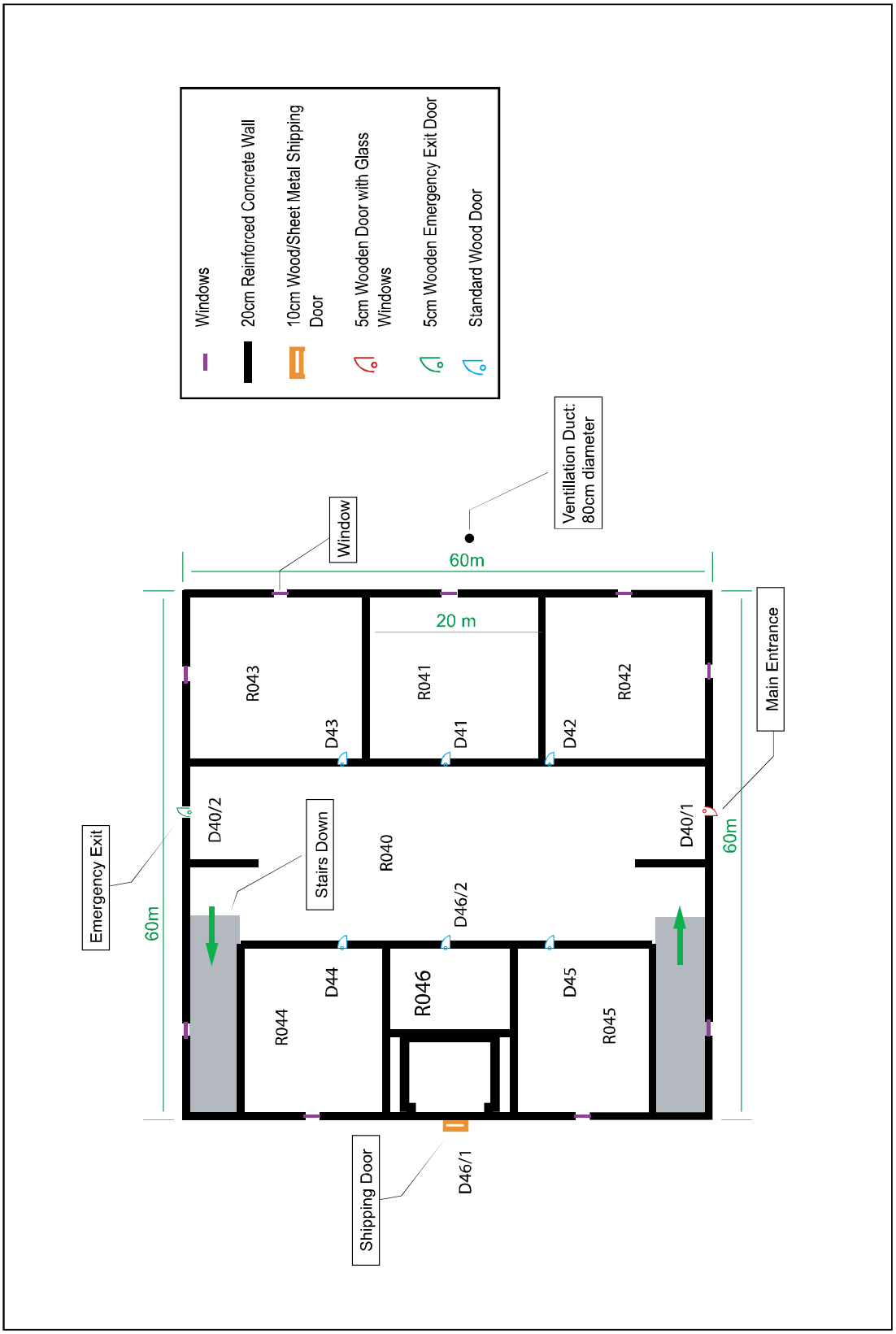
Section 19. NBR Above-ground Wall Thicknesses and Distances



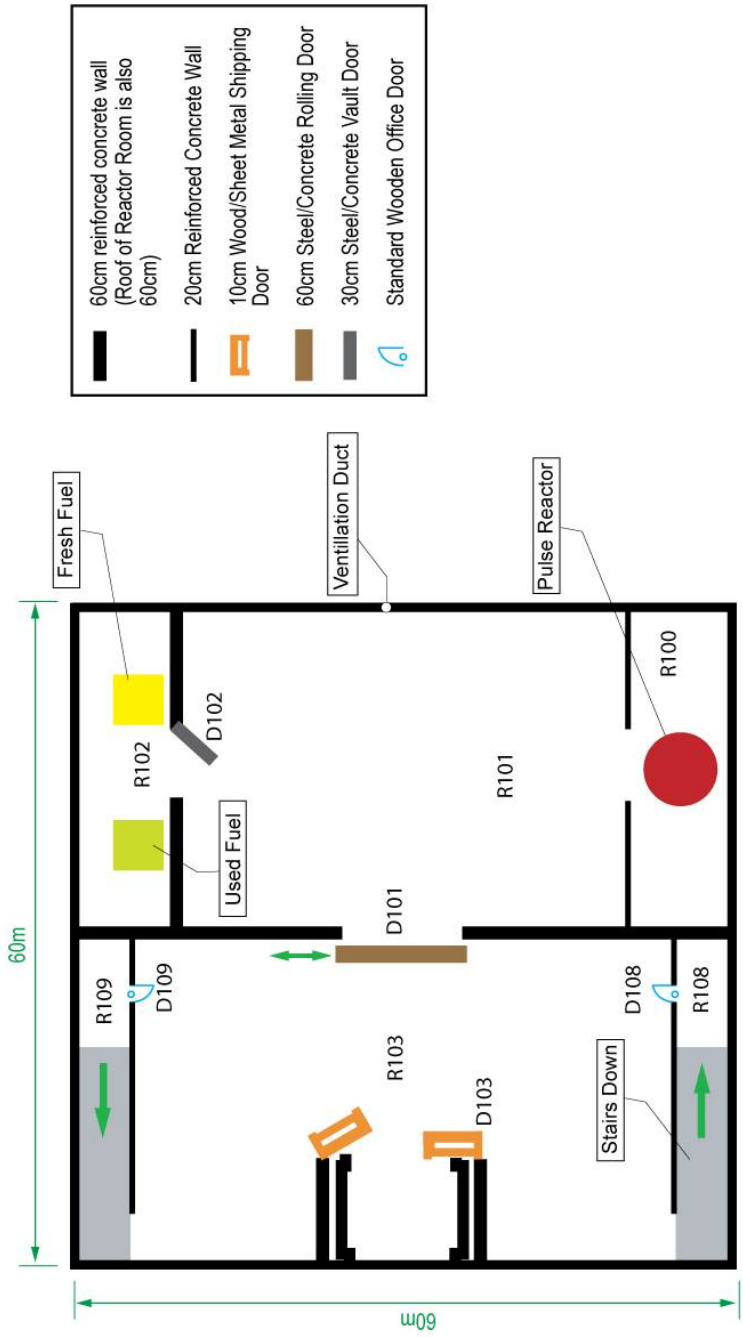
Section 20. NBR Above Ground Access Control



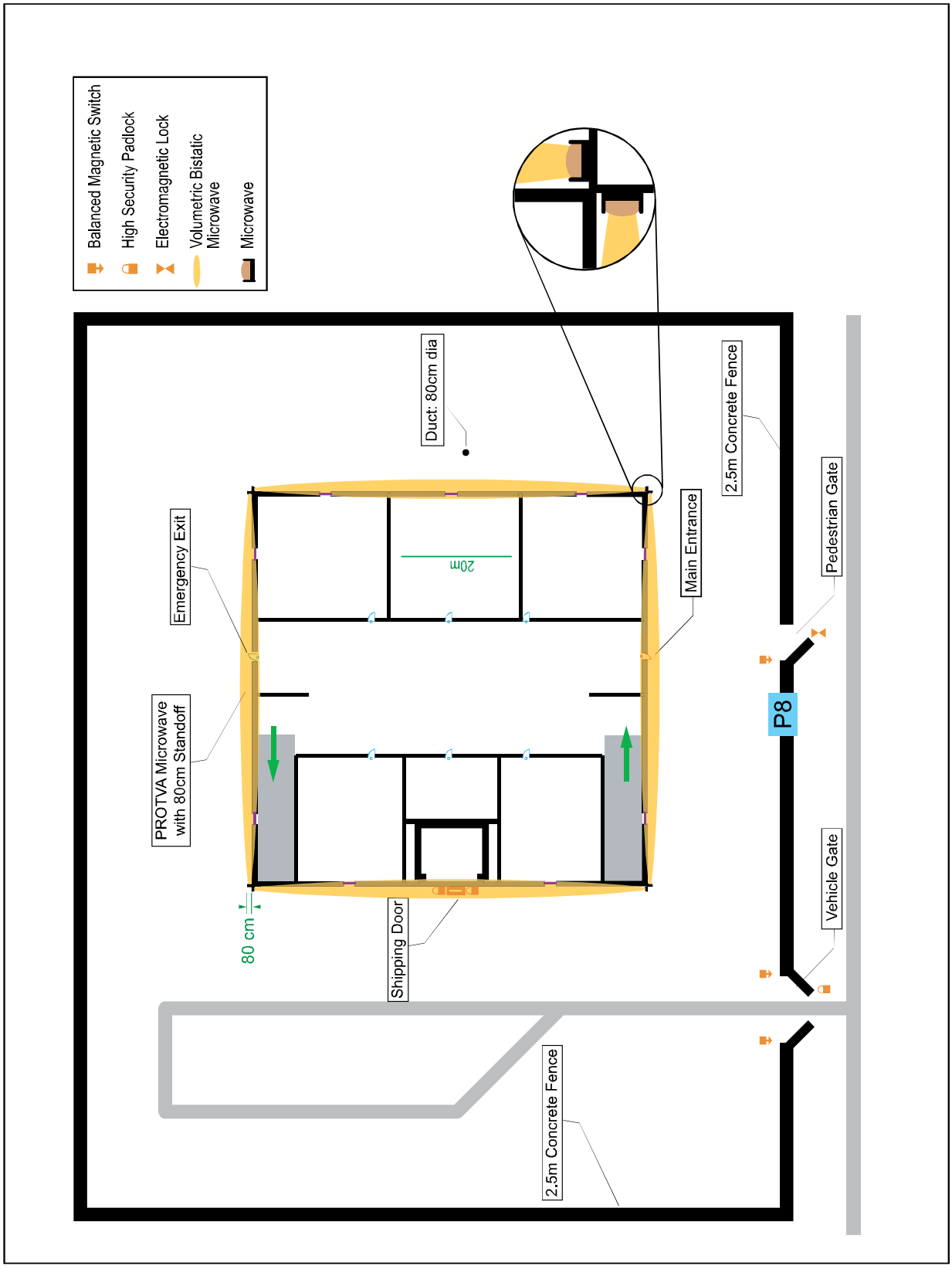
Section 21. NBR Above Ground Building Floor Plan



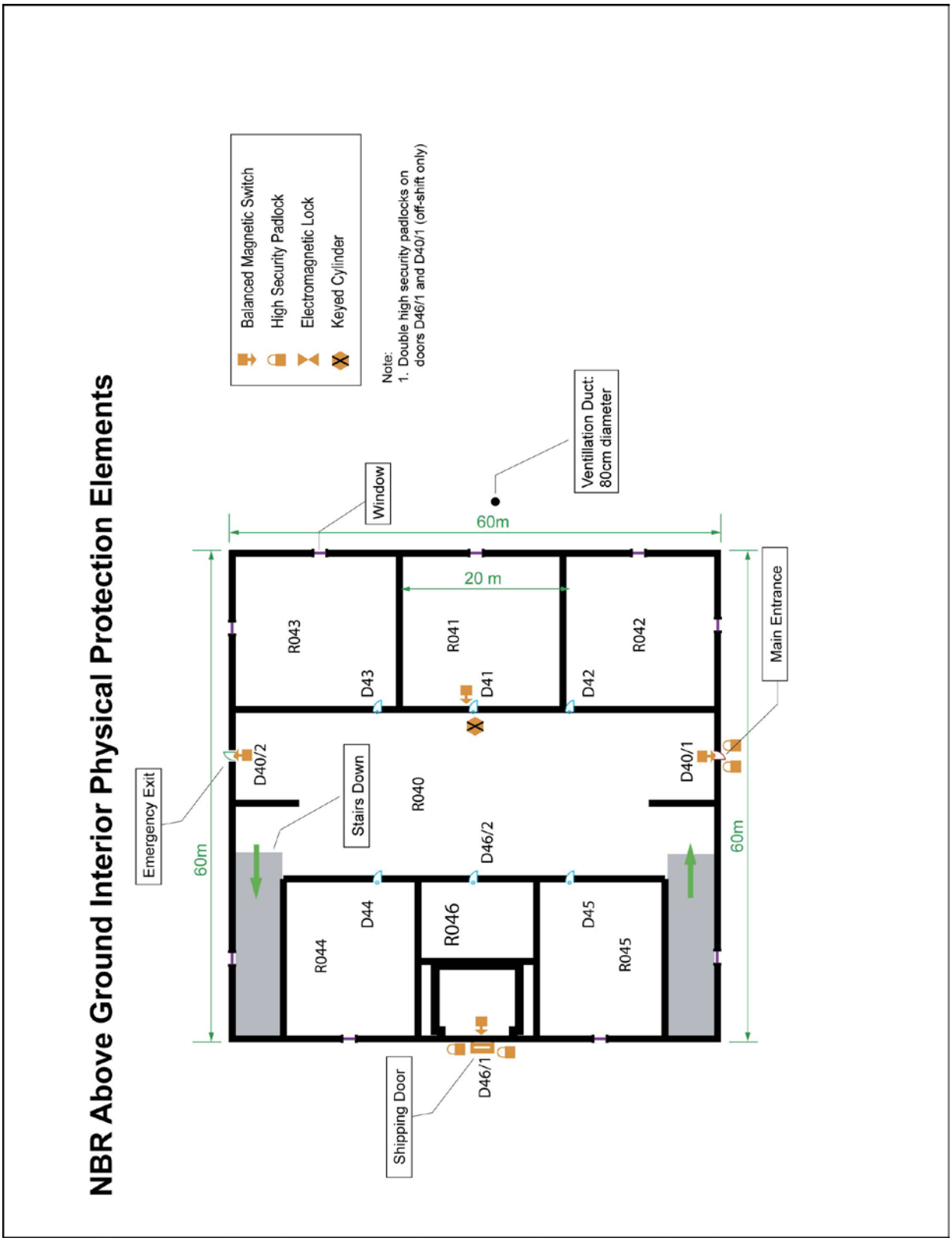
Section 22. NBR Below Ground Building Floor Plan



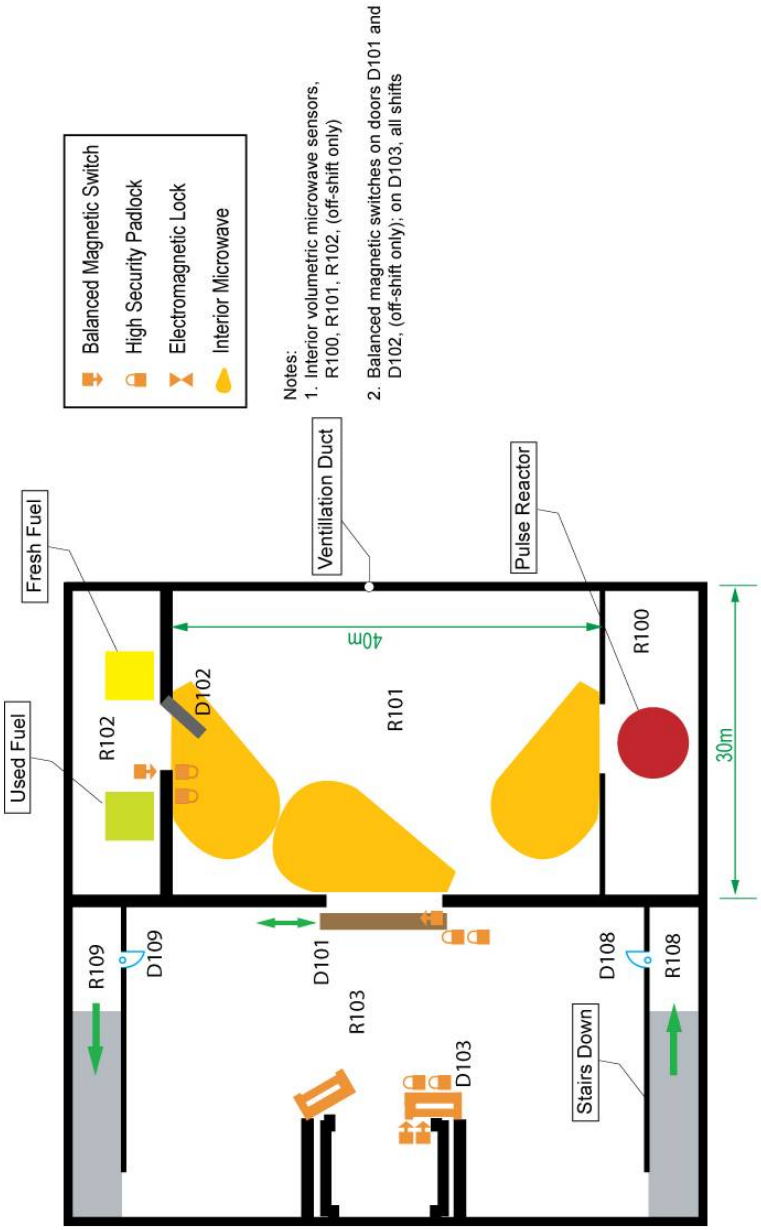
Section 23. NBR Exterior Physical Protection Elements



Section 24. NBR Above Ground Interior Physical Protection Elements



Section 25. NBR Below Ground Interior Physical Protection Elements



Contingency Plan
Content by Section

Table of Contents

1. Introduction

This section introduces the contingency plan and its purpose. The contingency plan is a documented plan that describes how personnel implement the physical protection program to defend against threats to the facility. The goals of the plan are to:

- *Organize the response effort*
- *Provide predetermined, structured response*
- *Ensure integration of the response by all responding entities*

1.1 Scope

This section will help users quickly assess the security events to which the plan is applicable. This section should also include a list of which regulation(s) are being addressed in the contingency plan. This is important if the plan is designed to fulfill the requirements of more than one regulatory program.

1.2 Assumptions

This section documents the assumptions that have been made in the development and execution of this contingency plan. This should include assumptions for information/decisions that have been made and/or are present as well as information/decisions that have NOT been made.

1.3 Threat

This section documents the threats considered in contingency plan based on the threat assessment and/or design basis threat (DBT).

2.0 Facility Description

This section contains a brief description of the facility, operations and layout. It may

2.1 General Facility Information

This section should contain a brief profile of the facility and its key personnel to facilitate rapid identification of vital administrative information. It should include the follow elements:

a. *Facility name*
b. *Facility Owner and/or operator (include physical address, office and phone numbers)*
c. *Physical address of the facility (include county, latitude/longitude, GPS, and directions if necessary)*
d. *Mailing address of the facility*
e. *Other identifying information*
f. *Key contact(s) for plan development and maintenance*
g. *Phone number(s) for key contact(s)*
h. *Facility phone number*
i. *Facility fax number*

2.2 Overview of Facility Operations

This section should provide a brief overview of facility operations and describe, in general, the physical layout of the facility, the types and quantities of material located at the facility, and all associated the processes. This summary should include site-specific information that will be critical to the response, along with information on potential vulnerable receptors. A site plan of the facility would be useful as part of this description. More detailed facility information could be provided in an Appendix.

2.3 Critical Areas and Nuclear Materials

This section should provide a brief overview in table format of the critical areas and nuclear material to be protected.

2.4 Physical Protection System Description

This section should provide an overview of the facility physical protection program. Also, the general goals, objectives and operational concepts underlying the implementation of this plan should be described.

3.0 Guard/Response Force (GF/RF) Operations

This section should provide a brief overview of the organizational structure for the guard and response forces on site as well as specifying what external organizations are responsible for providing services at the facility.

3.1 GF/RF Mission

This section should provide a brief description of the mission of guard and response forces.

3.2 GF/RF Organization, Responsibilities and Duties

This section should provide a brief overview of the organizational structure with special emphasis on the organization of the facility response team. This should include the response team leaders, team members, and other supervisors or staff that may be called upon to respond to a security event. This description should include the duties and responsibilities of each and any changes in the duties and responsibilities in the absence of other team members. This section should also include a statement giving authority to the designated coordinators to commit the necessary resources to implement the plan.

This section should also include any additional duties the response team may be assigned and how/if these additional duties interfere with the duties assigned as part of this contingency plan.

3.3 GF/RF Personnel and Locations

This section should provide a listing of the response force locations and details about the personnel stationed at that location.

3.4 GF/RF Rules of Conduct

This section should cover the State laws, local ordinances and facility policies that will govern the response. These could include:

- *Use of employee property*
- *Use of off-duty employees*
- *Site jurisdictional boundaries*

3.5 GF/RF Command and Control

This section should identify the RF commander and the GF commander and the succession of command. One person must be named as primary team leader with others identified as alternates.

This section should also contain detailed information for the organizational entities responsible for each decision and action associated with specific responses. This information should provide an overall picture if the response actions and their interrelationships and could be represented in a tabular form.

3.6 GF/RF Communications

This section should contain detailed information for the response team and team leader to follow for the notification of the different response groups and external entities. This plan should also contain information about how and when to communicate with employees and other individuals located on the site.

3.7 GF/RF Weapons and Equipment

This section should include a description of the weapons and equipment that will be provided to the responders, where the weapons and equipment are stored and what procedures should be followed by the response force to obtain the necessary equipment.

3.8 GF/RF Training

This section should include a description of the type of response training provided to and required of the responders. Training should include familiarization with the facility contingency plan and response procedures. Records documenting that required training has been conducted can be included in an Appendix.

4.0 Incident Response Procedures

4.1 Rules of Engagement

This section should include the rules of engagement, to define when and where force is authorized.

4.2 Response Procedures

This section defines how the response is organized and coordinated. Identify those events that will be used to signal the beginning of the event. Define the specific objectives to be accomplished relative to each event. The objective of the event may be to prepare for further response or successfully reduce the adversary consequences.

This section should include

- *All predetermined actions, areas of responsibility and timelines for the deployment of the response personnel*
    - *Theft scenarios*
    - *Sabotage*
- *Contain procedures that limit the exposure of the response personnel to possible attack*
- *Define the timelines to be used for notifying the offsite support response forces*
- *Define the minimum number of responders*

4.3 Recapture and Recovery

This section defines how the response is organized when the adversary has left the site in a theft scenario. Include the protocols that will be used to coordinate the different response teams, the chain of command and any shift in the responsibilities.

This section should include

- *All predetermined actions, areas of responsibility and timelines for the deployment of the response personnel*
- *Contain procedures that limit the exposure of the response personnel to possible attack*
- *Define the timelines to be used for notifying the offsite support response forces*
- *Define the minimum number of responders*

4.4 Minimize and Mitigate

This section defines how the response is organized to help minimize and mitigate the consequences of a radiological sabotage attack.

5.0 Coordination

It should describe arrangements as documented in the Memorandums of Understandings (MOU) agreed to by these external organizations, local police, military, etc. These MOUs should be obtained whenever possible and included in an Appendix. Where State or local authorities decline to enter into such arrangements, the facility must document the refusal in their operating record and in an Appendix. Detailed instructions should be included regarding how coordinated emergency services should be obtained, what will be provided, and how they will be managed. Where more than one law enforcement agency might respond to emergency, agreements should be made designating the primary authority.

The facility should attempt to make arrangement with these external agencies, local law enforcement, State and Military response teams to familiarize them with the layout of the facility, entrances to roads inside the facility, and possible evacuation routes. Detailed information on the layout of the facility and the surrounding environment should be maintained in an Appendix.

A copy of this contingency plan and all revisions should be sent to those agencies that are expected to respond to a situation. A distribution log of where each copy is sent should be maintained in an Appendix.

6.0 Protection of Information

This section discusses how the information contained within the contingency plan is protected. It would address the marking or classification of sensitive information and how the information is released.

Appendices

The appendices are as needed to provide supplemental information.

LAGASSI INSTITUTE OF MEDICINE AND PHYSICS (LIMP)*

(A HYPOTHETICAL FACILITY)

CONTINGENCY PLAN

Note: This is a living document to be updated by the Program Representative as necessary

Rev 1

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PAGE LEFT BLANK

1.0 INTRODUCTION

This Contingency Plan describes the normal security operations as well as the security incident response actions for the Lagassi Institute of Medicine and Physics (LIMP). This plan outlines the roles and responsibilities of the LIMP guard force (GF) and response force (RF) as well as the roles and responsibilities of off-site responders. The Contingency Plan may be implemented in a phased approach to security incidents of concern. It will be fully implemented during a confirmed adversary attack.

This document provides a comprehensive security approach that enhances the overall physical protection system effectiveness. The Contingency Plan is a part of the LIMP Security Plan approved by the Competent Authority.

This Contingency Plan has been developed in conjunction with the State and the Competent Authority and establishes procedures to be followed in the event of a security-related incident/disruption to the operations of the LIMP. This may include: external or internal malevolent threats, hostage situations, riot or major civil disturbance, and security officer requires assistance. This Contingency Plan must be able to be executed in a range of conditions including: normal operations, natural disasters, evacuation, and internal/external hazardous threats.

1.1 SCOPE

This Contingency Plan establishes policies and procedures to protect the LIMP during security incidents. The plan provides a smooth, rapid transition from normal operations to emergency security operations by implementing one or more phases of enhanced security conditions designed to prevent unauthorized removal or sabotage of nuclear material. This plan focuses on a theft and sabotage scenarios. Other contingency plans may be developed to address specific security incidents (e.g., locate and recover missing nuclear material, addressing insider threat, stand-off attacks, airborne attacks, cyber-attacks or compromise of sensitive information).

The GF and RF assigned to the site are responsible for protecting personnel and onsite resources. The plan makes efficient use of this force by placing personnel in a state of readiness and in position to prevent disruption of the site's capability to continue operations or to provide timely response during an adversary attack. The plan realizes that to accomplish the protection of the nuclear materials and the facility, the site GF and RF may require additional support, this support will be provided by offsite local law enforcement agencies as well as military tactical response (MTR) teams. The necessary agreements with these external agencies have been developed.

The information contained in this plan represents management's demonstrated commitment and the Competent Authority's approval to the safety and security of the facility and materials used at the site. The measures and procedures documented in this plan are designed to protect the facility and its resources, by deterring, detecting and delaying adversaries and by having response tactics that will interrupt the adversary and prevent an act of sabotage or theft of nuclear material.

Maintaining a state of readiness to prevent an act of sabotage or theft requires both response plans and adequate training to those plans. The plans are contained in this Contingency Plan and training will be conducted on a regular basis to maintain the state of readiness. Training will occur on at least an annual basis. As a result of the training exercises, this plan will be reviewed and updated.

The development of the Contingency Plan is required to meet executive decisions and regulatory requirements. This Contingency Plan is being developed in accordance with the following regulatory directives:

- IAEA Nuclear Security Series No. 13, INFCIRC/225/Rev 5, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*
- IAEA Nuclear Security Series No. 14, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*
- Any State requirements
- Any CA requirements

1.2 ASSUMPTIONS

1. The Memorandum of Agreement between the local law enforcement agencies have been negotiated and signed by all parties.
2. The Memorandum of Agreement between the military agencies have been negotiated and signed by all parties.
3. Coordination has been accomplished between the LIMP and other emergency response forces (e.g., medical, fire, radiation).

1.3 THREAT

A threat assessment has been done for LIMP and possible threats exists which involve the theft of nuclear materials and possible sabotage.

2.0 FACILITY DESCRIPTION

This section describes the facility, operations and layout. It includes the locations of initial locations of the on-site guard and response forces as well as the locations of critical areas and nuclear material. More details can be found in the LIMP facility description.

2.1 GENERAL FACILITY INFORMATION

The hypothetical nuclear research center, Lagassi Institute of Medicine and Physics (LIMP), was started in 1950 to serve as the nation's premier nuclear energy research facility. The Institute houses various research, administrative, and plant support facilities. The LIMP is located in the Republic of Lagassi, approximately 29 km (18 mi) east of Hashbakar.

The key to protection of the facility is for all personnel to be conscious of activities in and around the facility, especially the critical areas of the facility. Any individual who observes an act, event, unusual conduct of others or any suspicious activity should consider such activity a potential threat and report this to the CAS, the RF/GF commander or any individual in a position of authority. All responses due to a perceived or actual security event will be directed by the RF/GF Commander.

The following administrative information for LIMP should be included in the CP:

a. Facility name
b. Facility Owner and/or operator (include physical address, office and emergency phone numbers)
c. Physical address of the facility (include county, latitude/longitude, GPS, and directions if necessary)
d. Mailing address of the facility
e. Other identifying information
f. Key contact(s) for plan development and maintenance
g. Phone number(s) for key contact(s)
h. Facility phone number
i. Facility fax number

2.2 OVERVIEW OF FACILITY OPERATIONS

The LIMP is comprised of a number of high value assets that the GF/RF is responsible for protecting. This section details those critical nuclear material and facilities as well as the locations of some Physical Protection System (PPS) elements and security forces.

The site layout and response force locations are shown below for LIMP and Pool Type Reactor (PTR).

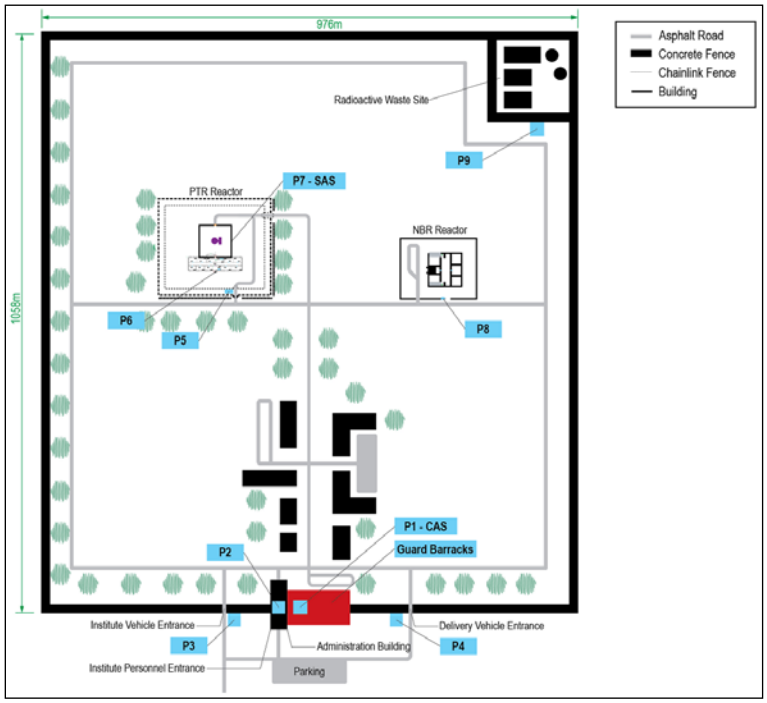


Figure 1 - LIMP Site Layout and Security Force Locations

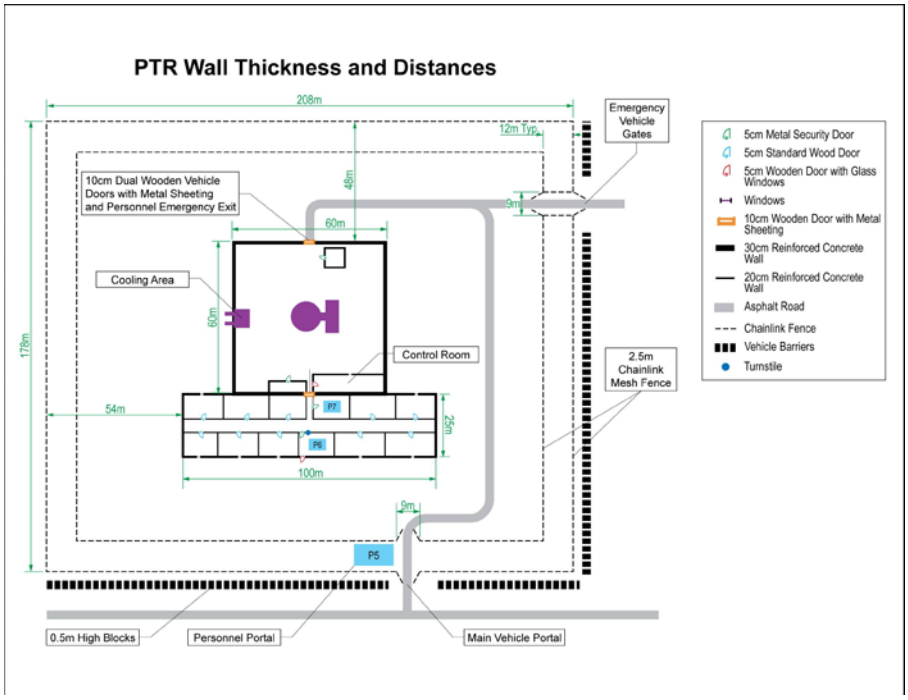


Figure 2 PTR Protected Area

The PTR is a light water moderated, highly enriched uranium (HEU) fueled research reactor located within the LIMP, a hypothetical nuclear research center. The reactor is used for research on advanced reactor components, special fuel assemblies, and production of radionuclides for the medical industry. Other experiments are performed to investigate power reactor fuel when heated to the point of melting. A neutron radiography facility is also available as well as extensive irradiation tubes and hot cell facilities.

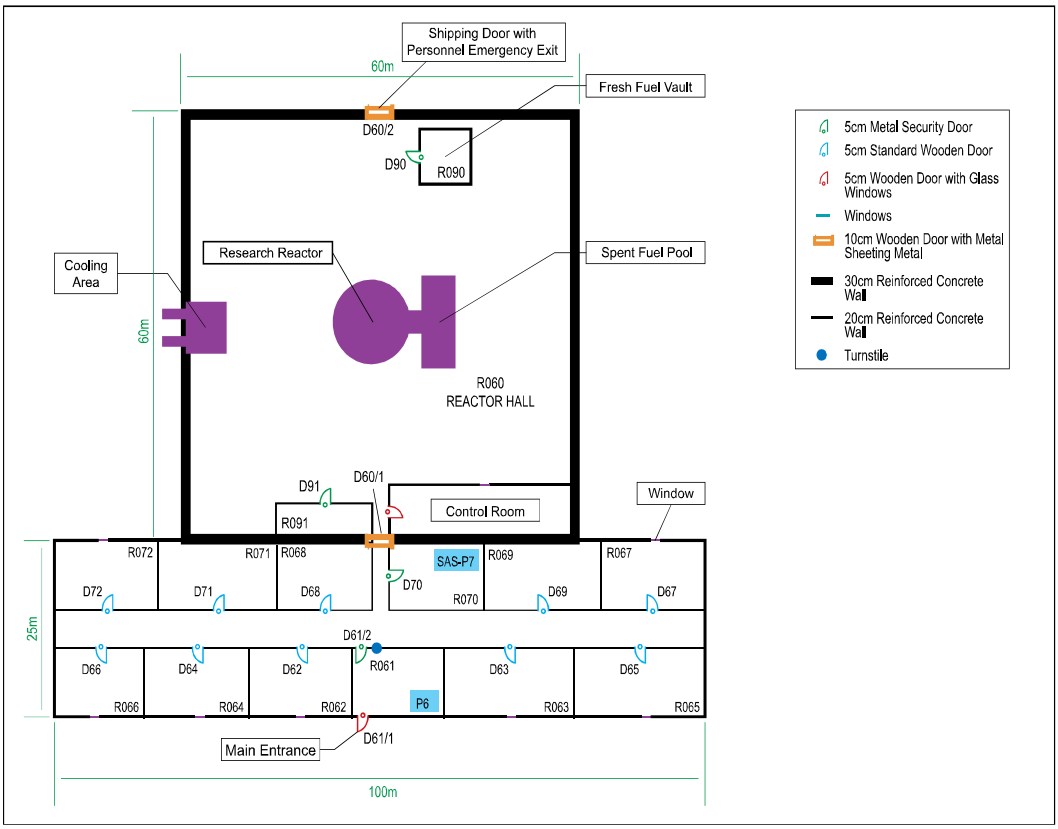


Figure 3 PTR Building Floor Plan and Security Force Locations

The LIMP Neutron Burst Reactor (NBR) is a reflected GODIVA-type research reactor designed for conducting experiments related to the collection of basic nuclear physics data for code validation purposes.

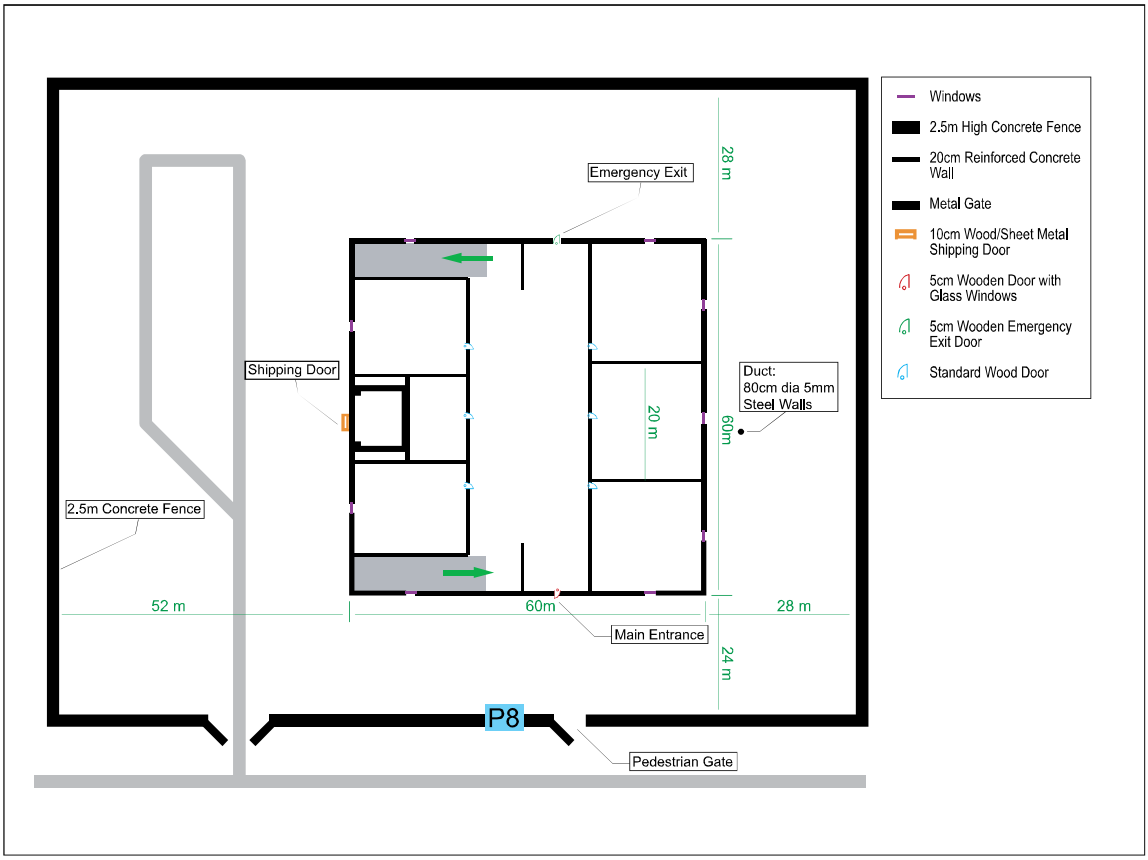


Figure 4 NBR Above Ground Floor Plan and Security Force Location

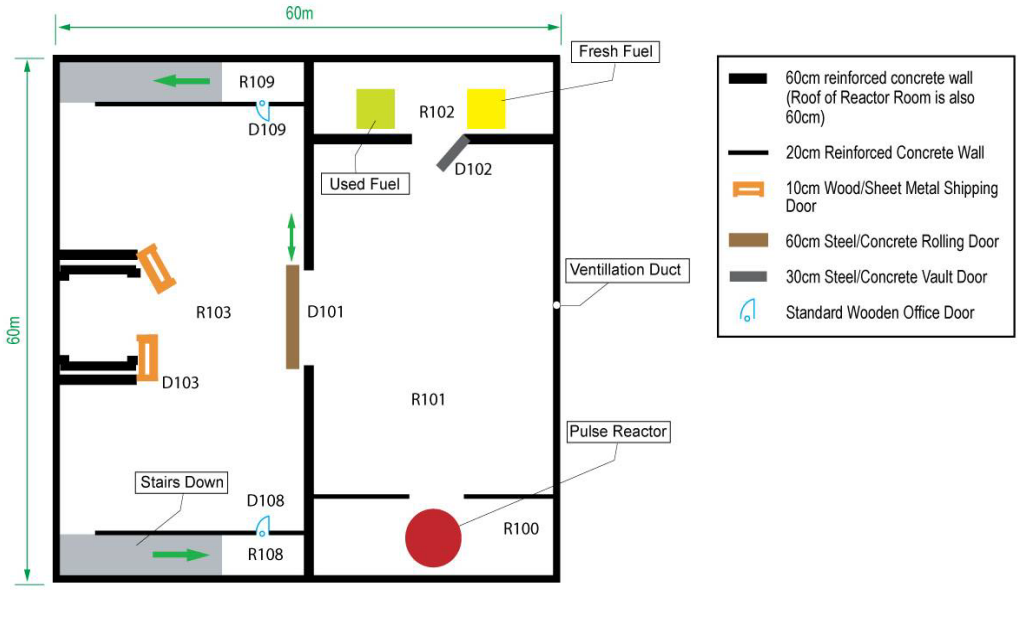


Figure 5 NBR Below Ground Floor Plan

2.3 CRITICAL AREAS AND NUCLEAR MATERIALS

The following table identifies the nuclear materials and related facilities located at the LIMP.

Table 1 Nuclear Materials at the LIMP

Facility	Location	Form of Material	Security Category	Radiological Sabotage	Level of Radiation
PTR Research Reactor	Reactor	$BeO\text{-}UO_2$ Fuel Rods (236 in reactor)	Category II	URC	High
	R090 Fresh Fuel Vault	$BeO\text{-}UO_2$ Fresh Fuel Rods (50 in storage)	Category I	<URC	Low
	Irradiated Fuel Pool	$BeO\text{-}UO_2$ irradiated fuel Rods (100 in pool)	Category II	URC	High
	R091 Product Vault	Pu Experiments HEU metal	Category I	<URC	Low Low
NBR Reactor Facility	R100	Fuel in Reactor Core (10 discs)	Category I	URC	Low
	R102	HEU-metal Fresh Fuel (9 discs)	Category I	<URC	Low
	R102	Used Fuel (1 discs)	Category II	<URC	Low
Waste Storage Facility	Vats	Liquid Mixture (2 vats, 2,000 liters ea)	N/A	URC	High
	Sheds	Solidified Waste (50 containers)	N/A	URC	High

N/A: Not Applicable

2.4 PHYSICAL PROTECTION SYSTEM DESCRIPTION

The LIMP Facility contains detection, assessment, entry control and delay protective elements and detailed information can be found in the LIMP hypothetical facility description along with other PPS measures.

Listed below are some protection activities:

- **Utilization of Internal Roving Patrols**: Roving Patrols will be deployed within the LIMP perimeter to detect, assess, report, respond, delay, and contain persons engaging in criminal activities on site. Roving Patrols will utilize vehicles during patrol, and can be used on foot as appropriate.
- **Detection**: Detection as it relates to analysis will be dependent upon technology. Detection as it relates to guard location will be more a function of immediate assessment capabilities.

In the event of a security incident, the roving patrols will be deployed in or dispatched to areas of particular concern or along most probable avenues of approach to provide detection and assessment. The objective is to detect and assess the adversary as soon as possible, report the observation, and provide defense in depth.

- **Assessments and Reporting**: A roving patrol or stationary responder notified of, or observing activities in his sector, should respond by moving to an observation point to gain as much visual information as possible that can be reported to the Central Alarm Station (CAS). This information should be transmitted via the communication system to notify the entire site security force. The responder should observe the actions of the adversary at this time, and the RF will engage the adversary using deadly weapons in accordance with the Rules of Engagement (ROE), if it becomes necessary.

  This early in the adversary timeline, intelligence of adversary location is just as important as interdiction.

- **Response and Back-up**: Initial contact, as a minimum, maintains visual control of the intruders. The tactical leader and mobile responders from other sectors will deploy in a preplanned sector response plan. The tactical leader will deploy forces from initial response positions and other sectors dependent on the tactical situation.

- **Interdiction**: The RF leader will deploy RF to an appropriate blocking position to limit the movement or forward progress of the adversary and achieve interdiction. Early interdiction of the adversary force mitigates the damage it can accomplish and ultimately limits or prevents its mission success.

- **Delay**: Delay as it relates to analysis will be dependent upon technology/barriers. Delay as it relates to guard location will be more a function of impeding adversary progress.

- **Prepared Defensive Positions**: The defensive plans utilize hardened fighting positions along the most likely avenues of approach to achieve interdiction at the target. Fighting positions are not continually manned, but are available for immediate use by RF personnel as the facility is threatened.

Provided in the following table is a listing of selected security locations.

Table 2 LIMP Security Locations and Security Levels

Security Location	Security Level
LIMP Site Boundary	Limited Access Area
PTR Site	Protected Area
PTR Administration building area	Protected Area
PTR reactor hall, R060	Protected Area, research reactor and spent fuel pool inside the hall (vital areas)
PTR Fresh Fuel Storage Vault, R090	Inner Area
PTR Product Storage Vault, R091	Inner Area
PTR Reactor Control Room	Vital Area
NBR reactor, R100	Inner Area
NBR vault, R102	Inner Area

3.0 GUARD/RESPONSE FORCE (GF/RF) OPERATIONS

3.1 GF/RF MISSION

LIMP will conduct enhanced security operations to preserve the integrity of facilities, protection of critical operating components and response to assaults on personnel and property. All of these actions are supportive of the LIMP security mission which is to provide reasonable assurance that the protection of nuclear material and facilities is effectively and efficiently applied from malevolent acts during heightened security periods.

Therefore, the security objective is to defend LIMP personnel, property, and resources against theft, sabotage, vandalism, assault, trespass, and compromise of sensitive information. This is accomplished using the GF/RF to:

- Control general site access and entry into known security areas.
- Oversee the Entry Control Point (ECP) locations and access control technology.
- Patrol designated areas and other points of security or property protection interests.
- Detain unauthorized persons or violators of law.
- Maintain an armed response capability to react to contingency requirements and adversary actions with assigned equipment and in accordance with established plans and orders.
- Protect personnel through safe havens and site evacuation.

3.2 GF/RF ORGANIZATION, RESPONSIBILITIES AND DUTIES

The site response force consists of two types of security personnel:

- Unarmed guard force (GF)
- The tactical response force (RF)

These security personnel are responsible for:

- Assessment of alarms
- Administrative duties such as access control and key service
- Routine patrol and staffing of fixed posts
- Armed response to adversary intrusions

All posts and patrols have defined policies and procedures with which the security personnel must comply. For each shift, two supervisors are present:

- GF Commander supervises the guards that conduct administrative duties and access control
- RF Commander is the commander of the tactical response teams

3.2.1 GUARD FORCE

INFCIRC 225 defines a guard as a person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.

3.2.2 RESPONSE FORCE

INFCIRC 225 defines the response force as persons, onsite or offsite, who are armed and appropriately equipped and trained to counter an attempted unauthorized removal or an act of sabotage.

Site tactical RF teams have five members each. A two person response team is on random patrol. All members are trained in close-quarters combat and have the authority to enter target locations to ensure the security of critical assets and target material.

The tactical RF commander for each shift is responsible for the oversight and supervision of all daily activities as well as emergency response to intrusion alarms.

During **operational hours**, three teams are present at the institute, with the following responsibilities:

- RF Team 1 responds to the research reactor
- RF Team 2 responds to the NBR facility
- RF Team 3 is in a training mode, but can be available to respond as directed by the response force commander

During non-operational hours, weekends, nights, and holidays, there are two tactical response teams on site. They are dedicated to intrusion alarm response at either the research reactor or the NBR facility.

3.3 GF/RF PERSONNEL AND LOCATIONS

The response force is deployed as described in the following table.

Table 3 Response Force Deployment Data

Post No.	Description	Security Personnel	No. of Personnel	
			Workdays	Non-workdays
S-1	Response Force Commander	Captain	1	1
S-2	Guard Force Commander	Lieutenant	1	1
P-1	Response Force Headquarters	Site RF	15	10
P-1	Central Alarm Station	Site GF	2	1
P-2	Institute Personnel Entrance	Site GF	3	1
P-3	Institute Vehicle Gate	Site GF	2	1
P-4	Institute Delivery Vehicle Gate	Site GF	1	0
P-5	PTR Personnel/ Vehicle Portal	Site GF	1	1
P-6	PTR Building Personnel Portal	Site GF	1	0
P-7	Secondary Alarm Station	Site GF	2	1
P-8	NBR Personnel Portal	Site GF	1	1
P-9	Waste Storage Facility	Site GF	1	1
P-10	Random two-man patrol of Institute	Site RF	2	2
		Totals	**33**	**21**

Table 4 Local Police Patrol Deployment Data

Local Police Patrol Deployment Data					
Location	Description	Post	Personnel Type	Number Of Personnel	
				Day Shift	Night Shift
Offsite	Patrols in local area - outside LIMP (two patrols with two personnel each	N/A	Police Patrol Units	2 per vehicle	2 per vehicle
			Totals	**4**	**4**

Table 5 Military Tactical Response Team Deployment Data

Military Tactical Response Team Deployment Data					
				Number Of Personnel	
Location	Description	Post	Personnel Type	Day Shift	Night Shift
Offsite	Military Tactical Response Teams (two teams of five personnel each)	N/A	Tactical Teams	10	10
			Totals	**10**	**10**

Table 6 LIMP Response Posture

Guard and Response Force Activities		
Location/Description:	**Post**	**Area of Responsibility:**
CAS	P-1	• Receives and assesses all alarms • Notifies RF Commander so preparations for deployment can begin • At least one guard is always present in the CAS • During workdays – the one additional guard is available to respond based on direction of GF Commander
RF team #1 (5 people)	P-1	• Respond and deploy based on direction form RF Commander
RF team #2 (5 people)	P-1	• Prepare, respond and deploy based on direction form RF Commander
RF team #3 (5 people)	P-1	• Prepare, respond and deploy based on direction form RF Commander
Institute personnel entrance	P-2	• Checks credentials and observes for unusual behavior • Operate badging station only during workdays • During workdays – one guard is available to respond based on direction of GF Commander
Institute vehicle gate	P-3	• On entry - Checks credentials and vehicle • On exit – observes vehicle and waves vehicle to leave • During workdays – one guard is available to respond based on direction of GF Commander
Institute delivery vehicle gate	P-4	• Gate is normally closed and locked • During workdays – on entry checks credentials of passengers, vehicle authorization papers, inspects vehicle, if all is acceptable then unlocks and opens the gate; on exit unlocks the gates, inspects vehicle, opens gate and allows vehicle to proceed • During workdays – the one guard is available to respond based on direction of GF Commander, the gate would be closed/locked

Guard and Response Force Activities		
Location/Description:	**Post**	**Area of Responsibility:**
PTR personnel/vehicle portal	P-5	• One guard present at all times, if a vehicle requires entry then another guard is called to assist • Personnel entry – on entry observes entry and if authorized will unlock gate for entry by a single person into the portal, guard checks picture badge and if ok then opens inner door to let person enter; on exit observes exit and if authorized will unlock gate for entry by a single person into the portal, guard checks picture badge and if ok then opens outer door to let person exit • Vehicle entry – two guards are present for entry, inspect vehicle paperwork, inspects vehicle, unlocks and opens inner vehicle gate, people go through personnel portal, vehicle is driven into the area and inner gate is closed and locked; two guards are present for exit, inspects vehicle, checks peoples badge and paperwork, unlocks and opens inner vehicle gate, vehicle goes into the portal, inner gate is closed and locked, outer vehicle gate is unlocked and opened, vehicle exits portal, outer gate is closed and locked. • Guard remains at portal at all times
Emergency PTR vehicle portal		• Only manned in times of emergency
PTR building personnel portal	P-6	• One guard is present whenever any person is inside the PTR, normally closed and locked during non-workdays • On entry – checks picture badge and exchanges for PTR badge, observes person going through metal detector, inspects as necessary, observes entry if ok; on exit – observes person leaving, re-exchanges the badge and observes exit. • Guard remains at portal at all times
SAS	P-7	• One guard is present in the SAS at all times • Verifies the CAS operator's assessment to ensure all alarms are properly assessed • During workdays the second guard is available to respond based on direction from GF Commander
NBR personnel/vehicle portal	P-8	• One guard is present at all times • Performs pedestrian and vehicle entry control, checks badges, paperwork, opens/locks personnel and/or vehicle entrances
Waste storage facility	P-9	• One guard is present at all times • Performs pedestrian and vehicle entry control, checks badges, paperwork, opens/locks personnel and/or vehicle entrances
RF roving patrol	P-10	• Responds to alarm based on directions from CAS

3.4 RULES OF CONDUCT

The following are some rules concerning conduct of the GF/RF:

- The GF/RF shall conduct itself in a professional manner at all times.
- The GF shall not engage in activities which would cause them to neglect or be inattentive to their duties.
- Whenever someone approaches the ECP the guards shall ascertain the person's intentions.
- The GF must be proficient in the proper operation of all issued equipment.
- The GF shall not allow entry to any individual without the appropriate credentials.

3.5 COMMAND AND CONTROL (C&C)

Command and control provides for clear, effective, in-depth coordination, and utilization of the on-site guard force. This includes fixed positions, roving patrols, response teams in ready positions, and other security assets in the pursuit of mission accomplishments. The RF leader exercises command over the actions of the GF/RF utilizing the Contingency Plan, which provides predetermined guidance for the orderly accomplishment of the security mission. All unforeseen circumstances will be resolved at the discretion of the RF leader.

The Contingency Plan is administered by the LIMP Security Operations Department. The primary mission is to provide physical protection of nuclear material, facilities and related property. The GF and RF organizations are part of this department. The department is also responsible for leading the development of the security/vulnerability assessments, operation and maintenance of the physical protection system, personnel security, badging/access control and coordination with outside security and emergency response organizations. The following provides details concerning GF/RF actions to security incidents.

- GF/RF shall immediately notify the appropriate supervisor for all security incidents or situations of uncertainty.
- The RF tactical leader will be the highest ranking GF/RF member onsite at the time of the event.
- Succession of command is:
    - RF Commander
    - GF Commander
    - Site/Facility Manager
    - CAS Operator

3.6 COMMUNICATIONS

The **Central Alarm Station** (CAS) is located in P1 and is staffed by two guards during the day and one guard at night. All alarms are received at the CAS. Alarms from the PTR facility are communicated and assessed by P1 using video. Alarms from the NBR are assessed by the guard at P8.

The **Secondary Alarm Station** (SAS) is located in P-7 and is staffed by two guards during the day and one guard at night. The SAS monitors the activities of the CAS to ensure appropriate actions are taken. The CAS only relinquishes monitoring and control during maintenance and other temporary facility outages.

Both the CAS and the SAS are equipped with:

- 100-watt radios that can communicate to all posts and patrols within the boundaries of the Institute.
- 2 telephone lines. One is linked to each fixed post via a buried telephone cable and the second telephone is a direct link to the Ministry of Interior headquarters located in the city.

Extensive testing of the communication system has shown that the radio communications are good throughout the Institute with the exception of the lower level interior of the NBR facility. Testing concluded that security personnel inside the NBR facility are able to monitor transmissions from both the CAS and the SAS but are unable to transmit to the CAS and the SAS with their handheld radios.

All handheld radios and fixed posts are equipped with a duress switch to allow a covert signal to the CAS and SAS of unauthorized activity. When the CAS or SAS receive a duress alarm, the response team is notified and the response force commander initiates a tactical response. The primary duress notification capability for the GF/RF is the duress notification feature of the hand-held portable and mobile radios. Fixed posts at the main gate and CAS have hard-wired duress capabilities.

All alarms are received and assessed at the Central Alarm Station. The CAS operator immediately notifies the Commander of the Response Force so preparations for deployment can begin by the appropriate response team.

3.7 GF/RF WEAPONS AND EQUIPMENT

Listed below is some of the equipment for the GF/RF.

All **guards** are equipped with:

- a straight baton
- one set of handcuffs
- a small flashlight
- a handheld radio

The **response force** team members are equipped with

- a Markov pistol with a fully loaded magazine but without a round in the chamber and
- a Kalashnikov assault rifle with a fully loaded magazine but without a round in the chamber
- two spare magazines of ammunition for each weapon and both weapons are carried with a fully loaded magazine but without a round in the chamber.
- a straight baton

- handcuffs
- flashlight
- handheld radio
- body armor is readily available in the response force building

3.8 GF/RF TRAINING

This section will describe the training required of the GF/RF. The GF/RF receives a wide range of training including physical fitness, weapons qualification and tactical training. Details of the training can be found in the LIMP physical security plan.

4.0 INCIDENT RESPONSE PROCEDURES

4.1 RULES OF ENGAGEMENT

The rules of engagement direct that the RF use the minimum amount of force necessary to control the situation, make the arrest or perform other actions to stop the action of the adversaries and prevent a malicious act. The force continuum to be followed is:

- Presence of the GF/RF
- Verbal commands
- Use of hands
- Less than lethal options
- Deadly force

The Use of Force authority is as follows:

- If the individuals identified as suspicious are outside the PTR area outer chain-link fence, but inside the site limited access area:
    - The guards/responders shall dispatch a patrol to challenge the individuals.
    - If necessary, a guard/responder will give a verbal warning and attempt arrest if necessary.
- If The intruders breach the outer PTR chain-link fence:
    - Given Hostilities (e.g. Shots Fire, Explosive Event, Physical Barrier defeated [given an ignored warning]), a guard/responder is authorized to use force.
    - If Hostilities are yet to be determined, a guard/responder must decide authority based on:
        - A guard/responder shall give a verbal warning (e.g. an order to halt), if feasible.
        - A guard/responder will use his less-than-lethal equipment (baton or handcuffs), if in close proximity to the unauthorized personnel, if feasible.
- If there is an individual in a higher security area (e.g., inner or vital area):
    - Given Hostilities (e.g. shots fired, explosive event, physical barrier defeated [given an ignored warning]), a guard/responder is authorized to use force.

- If Hostilities are yet to be determined, a guard/responder must decide authority based on:
  - A guard/responder shall give a verbal warning (e.g. an order to halt), if feasible.
  - A guard/responder will use his less-than-lethal equipment (baton or handcuffs), if in close proximity to the unauthorized personnel, if feasible.
  - A guard/responder will shoot to Prevent/Stop an adversary from continuing with deadly force actions; either a brandished weapon or explosive device.

An unannounced landing on site should be considered suspicious and is technically a trespassing incident. Immediately announce any aircraft sightings to the CAS operator to include location, vector, and approximate altitude. The response will follow the phased responses described in the sections below.

4.2 RESPONSE PROCEDURES

All alarms are received and assessed at the Central Alarm Station (CAS). The Secondary Alarm Station (SAS) verifies the CAS operator's assessment to ensure all alarms are properly assessed. The CAS operator immediately notifies the Commander of the Response Force so preparations for deployment can begin by the appropriate response force team. The CAS operator will provide the tactical information that the responders will need, such as number of adversaries, direction of travel, and any other visual clues. This communication will be via the standard radio system. In addition, institute procedures require that the nearest guard also be dispatched to the point of the alarm to provide additional assessment and to observe and report any unauthorized activity. The appropriate response force:

- collects their firearms from the armory,
- puts on their body armor, and
- prepares to respond either by foot or vehicle as directed by the response force commander.
- Once an alarm is announced, the frequency will remain clear for the response force commander and the positions in the alarmed area.
- The first person to determine that there are unauthorized personnel in the security area, will state their call sign, number of adversaries, the adversary location, and direction of travel.

Once the response force team arrives at the appropriate facility, they deploy as a team and proceed with operations to enter the facility and ensure the protection of material and assets.

4.2.1 RESPONSE/DEFENSIVE STRATEGY

The GF/RF Contingency Plan provides security support to the LIMP in an appropriate manner that will not disrupt the site's conduct of operations. The following section will outline the concept of normal operations.

The Licensee of the LIMP uses a balanced, graded, integrated, and cost-effective approach to determine levels of protection that are commensurate with the threat and risk. The operator of the LIMP has designed and integrated protection strategies into its overall Security Plan in accordance with the regulations and oversight of the Competent Authority.

Protection strategies are employed to protect the State's security interests based on the nature of the threat, the vulnerability of the potential target, and the potential consequences of an adversary act. In accordance with the State's policy, Category I NM targets described in this plan are protected using a containment strategy with locate and recovery strategies incorporated in the LIMP protection strategy to protect NM from unauthorized removal or sabotage.

In addition to the existing security technology associated to the LIMP's physical protection system (PPS), this plan addresses the deployment of LIMP security forces to defend the site against an adversary force attempting to steal nuclear material or sabotage nuclear material or facilities. Concept of the defensive strategy is to tactically deploy an internal roving patrol to actively patrol the site and the deployment of a dedicated response force to aggressively interdict and contain intruders at critical operating components. The strategy for the on-site GF focuses on detection, assessment, reporting, response, delay, and resolution containment. The on-site RF focus on the interruption and neutralization to mitigate malevolent acts. Off-site armed RFs will be notified of a security incident and be prepared to respond under the direction of the highest ranking site GF/RF member onsite at the time of the event.

Protection is provided to the site across the entire threat spectrum. The GF is prepared to deal with security incidents at the low end of the spectrum where stop and apprehend techniques for ordinary criminals are adequate. At the high end of the spectrum where defensive tactics must be employed to respond to the most sophisticated threat the RF will be deployed. The objective will be to defend the site's personnel, critical operating components, and critical production facilities.

The GF/RF will take reasonable and prudent action within the constraints of its strength and tactical capability to stop and apprehend persons who have committed serious offenses on LIMP property. In enforcing the trespass policy, the GF will defend against unauthorized access using the measured, minimum force necessary to challenge, control, apprehend, and if necessary, arrest unauthorized intruders.

Defense in depth is achieved by detecting and engaging adversaries as soon and as far away from protected assets as possible. Dependent on the tactical situation, forces which have deployed in depth may be redeployed to protect the interior of the site or other sectors, if these areas are significantly threatened.

4.2.2 PHASED ALERT RESPONSE

The phased alert response is implemented to differentiate security states and to provide the response appropriate to the situation.

- There are offsite security incidents that could affect site operations. This early warning results in site security preparation. However, once a security incident has been confirmed and there is a sense that an asset is being targeted, the guard force has plans that require a response to pre-designated positions that provide the best observation and/or protection.
- The incident information will reflect the specific actions guard force personnel take for enhanced protection.

Phase alerts are intended to be sequential, but depending on the escalation of activities the GF/RF could immediately move to Phase II or Phase III.

These phase alerts will apply to either an attempted theft or sabotage event while the intruders are on the LIMP site.

4.2.2.1 PHASE I ALERT

GF/RFs do not have Use of Force Authorization. Alert result of:

- Notification of a potential threat condition or a security concern taking place at another off-site location, but could eventually impact on site operations, i.e. at another energy entity, public disturbance and/or demonstration, etc.
- Intruders are onsite, an alarm has been generated, and however the assessment is not complete.

4.2.2.2 PHASE I RESPONSES

All units notified, and remain at post. One on-site GF/RF patrol, based on sector alarm, will be dispatched to assess the alarm. Redundant assessment is to be provided by PPS as available.

4.2.2.3 PHASE II ALERT

GF/RFs do not have Use of Force Authorization. Alert result of:

Notification of an actual threat condition that has resulted in a verifiable site intrusion. The actual target and/or intentions of the intruders are not known. However, the asset protection strategy is implemented. This means that guard force personnel initiate movement to their designated asset protection positions.

- Onsite alarm has been assessed, and unknown individuals are in the security area.
    - Alarm to PPS with assessment.

4.2.2.4 PHASE II RESPONSES

The LIMP Response Posture is initiated. All forces move to primary positions, and RF Teams gather for deployment.

4.2.2.5 PHASE III ALERT

RFs do have Use of Force Authorization. Alert result of:

- Notification of an actual threat condition where an asset is specifically targeted.
- Onsite alarm has been assessed, individuals are in the security area, hostilities confirmed.

4.2.2.6 PHASE III RESPONSES

The RF Commander coordinates the deployment of the GF/RF personnel and possible engagement of the adversaries. The specific tactical plans will be different for the possible scenarios and will be based on plans developed as part of exercises. If the RF Commander determines that the capabilities of the site's GF/RF are not adequate then the off-site security forces will be requested. The CAS will notify offsite security organizations of any security incident involving inner or vital areas.

4.2.3 RESPONSE FORCE TIMES

The Institute has conducted extensive performance testing of the response force in the areas of alarm assessment, alarm communication, preparation, travel and deployment times to alarms at the research reactor and the NBR facility. The average times are listed in the table below. Institute procedures require that all tactical responders be available to respond to an alarm from P-1. All tactical responders are fully equipped with their duty gear with the exception of their rifles, which are kept in storage in the armory until needed.

Table 7 Average Response Times for Physical Protection System Functions

Description	Research Reactor	NBR Facility
Alarm communication time	1 second	1 second
Alarm assessment time	45 seconds	45 seconds
Response force communication time	18 seconds	18 second
P-1 Response force preparation time	90 seconds	90 seconds
P-1 Travel time by vehicle	75 seconds	65 seconds
P-1 Travel time by foot	250 seconds	200 seconds
P-1 On-site deployment time (after arrival)	90 seconds	90 seconds
P-10 Preparation time	0 seconds	10 seconds
P-10 On-site deployment time (after arrival)	20 seconds	30 seconds
P-10 Travel time by vehicle	45 seconds	45 seconds
Offsite police patrols response	300 seconds	300 seconds
Offsite MTR team response	900 seconds	900 seconds

4.3 RECAPUTURE AND RECOVERY

It has been confirmed that there are intruders on the facility. The deployment for the response forces is as described in the Phase III response above, the RFs respond to the previously identified theft targets. As the CAS gathers more data about the direction and intent of the intruders, some or all of the RFs may be redeployed to protect specific targets or deploy to contain the adversaries.

The GF personnel located at specific posts will respond to a possible intrusion in accordance with direction from the GF and/or RF Commanders. In some cases the GF may secure and remain at their posts and if they are needed to provide additional surveillance of the intruders some may be deployed. The P-10 random patrol will generally move towards the last known location of the intruders but will not engage unless directed to do so by the RF Commander.

If the adversary's remove the target from the facility site, the RF Commander will notify the local law enforcement (police) agencies along with the MTR teams and provide them information concerning the nuclear material that is now out of control. Additional support will be provided by the LIMP security organization based on agreements with the offsite organizations. The primary responsibility to locate and recover the nuclear material which is no longer on the LIMP sites rests with the offsite security/emergency forces. Once the item has been recovered, the site safety and security will work with the local law enforcement and military teams to transfer the item back to the site.

4.4 MINIMIZE AND MITIGATE

It has been confirmed that there are intruders on the facility. The deployment for the response forces is as described in the Phase III response above. Again the GF personnel located at specific posts will respond to a possible intrusion in accordance with direction from the GF and/or RF Commanders. In some cases the GF may secure and remain at their posts and if they are needed to provide additional surveillance of the intruders some may be deployed. The P-10 random patrol will generally move towards the last known location of the intruders but will not engage unless directed to do so by the RF Commander. If it is determined that the adversary objective may be sabotage then the RF will if possible deploy to positions to allow them to deny access of the intruders to the possible sabotage location. If this is not possible then, then the RF will implement pre-planned actions to prevent the sabotage act from occurring and also begin measures to help mitigate and minimize the effects of a potential radiological release.

Contingency and response plans must be developed to limit the consequences of a radiological sabotage attack. Emergency management may present some unique problems in the case of malevolent attacks. Therefore it is necessary that security contingency plans and safety and emergency plans are compatible and complementary. Care should be taken to verify that activities of the security forces do not jeopardize safety and likewise that security is not jeopardized during the implementation of safety measures.

5.0 COORDINATION

Implementation of the Contingency Plan and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions. Security, contingency plans and emergency plans should be comprehensive and complementary. Contingency Plans and associated procedures must include measures which focus on preventing further damage, on securing nuclear facilities, and on protecting emergency equipment and personnel. The LIMP Security Operations Department will coordinate with off-site security (e.g., police, military tactical response teams) and emergency service (medical, fire, radiation protection) organizations and develop agreements on the support to be provided to the LIMP site as well as support from LIMP organizations. Off-site organizations should be familiar with the LIMP facility and particularly any hazards to their personnel. They should participate in training exercises with the LIMP facility.

Coordination with other LIMP organizations (e.g., safety, safeguards, and operations) should also be done and specific actions identified for these organizations if a security incident occurs. For example, placing operations in a "safe condition" could be initiated if certain alarms occurred or mobilizing the emergency response teams.

6.0 PROTECTION OF INFORMATION

The material within this Contingency Plan along with other parts of the LIMP Security Plan contains sensitive information which must be protected. The State will specify the necessary requirements and LIMP will develop and implement the necessary plans and procedures for making sure the information is adequately protected.

APPENDICIES - ACRONYMS

C&C	Command and Control
CAS	Central Alarm Station
ECP	Entry Control Point
GF	Guard Force
RFT	Response Force Time
IA	Inner Area
LAA	Limited Access Area
MTR	Military Tactical Response
NM	Nuclear Material
PA	Protected Area
PPS	Physical Protection System
RF	Response Force
VA	Vital Area