IAEA-TECDOC-1868

# NUCLEAR POWER PLANT CASE STUDY FOR THE NUCLEAR SECURITY ASSESSMENT METHODOLOGIES FOR REGULATED FACILITIES

COORDINATED RESEARCH PROJECT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

**CONTENTS**


1. INTRODUCTION....1
   1.1 BACKGROUND....1
   1.2 OBJECTIVE....1
   1.3 SCOPE....1
   1.4 STRUCTURE....1

2. TERMS OF REFERENCE....1
   2.1. RATIONALE....1
   2.2. OBJECTIVE....2
   2.3. TASKS AND FUNCTIONS....2
   2.4. OUTCOMES....2

3. PREPARATION AND PLANNING....3
   3.1. REGULATION/POLICIES/GUIDELINES....3
   3.2. REQUIREMENTS....3

4. COLLECTING REQUIRED INFORMATION....3
   4.1. BACKGROUND....3
   4.2. CASE STUDY FACILITY CHARACTERIZATION....3
   4.3. CASE STUDY TARGET IDENTIFICATION....6
   4.4. CASE STUDY THREAT DEFINITION....6

5. CONDUCTING THE SECURITY ASSESSMENT....6
   5.1. PROCESS FOR USING SOFTWARE TOOLS AND EVALUATION METHODS....6
   5.2. COMPARISON OF TOOLS....7
   5.3. SIMULATION SPECIFICATION....11
   5.4. VISA MODEL AND IMPLEMENTATION....11
      5.4.1. VISA background and overview of method....11
      5.4.2. Scenario conditions....13
      5.4.3. Modelling information....13
      5.4.4. Results....13
      5.4.5. VISA observations....15
   5.5. SAVI MODEL AND IMPLEMENTATION....15
      5.5.1. SAVI background and overview of software....15
      5.5.2. Scenario conditions....16
      5.5.3. Modelling information....16
      5.5.4. Results....17
      5.5.5. SAVI observations....18
   5.6. PROEV MODEL AND IMPLEMENTATION....18
      5.6.1. ProEv background and overview of software....18
      5.6.2. Scenario conditions....19
      5.6.3. Modelling information....19
      5.6.4. Results....20
      5.6.5. ProEv observations....21
   5.7. STAGE MODEL AND IMPLEMENTATION....22
      5.7.1. STAGE background and overview of software....22
      5.7.2. Scenario conditions....23
      5.7.3. Modelling information....23
      5.7.4. Results....24
      5.7.5. STAGE observations....24

5.8. VEGA 2 MODEL AND IMPLEMENTATION ..... 25
5.8.1. VEGA-2 background and overview ..... 25
5.8.2. Scenario conditions ..... 25
5.8.3. Modelling information ..... 26
5.8.4. Results ..... 27
5.8.5. VEGA 2 observations ..... 27
5.9. SIMAJIN/VANGUARD MODEL AND IMPLEMENTATION ..... 28
5.9.1. Simajin/Vanguard background and overview of software ..... 28
5.9.2. Scenario conditions ..... 29
5.9.3. Modelling information ..... 30
5.9.4. Results ..... 30
5.9.5. Simajin/Vanguard observations ..... 31
5.10. AVERT MODEL AND IMPLEMENTATION ..... 33
5.10.1. AVERT background and overview of software ..... 33
5.10.2. Scenario conditions ..... 34
5.10.3. Modelling information ..... 34
5.10.4. Results ..... 35
5.10.5. AVERT observations ..... 36
5.11 TABLETOP METHOD AND IMPLEMENTATION ..... 38
5.11.1. Tabletop background and overview of method ..... 38
5.11.2. Scenario conditions ..... 39
5.11.3. Modelling information ..... 39
5.11.4. Results ..... 40
5.11.5. Tabletop observations ..... 43

6. OVERALL ASSESSMENT OF SECURITY ASSESSMENT METHODS ..... 43
6.1. ASSESSMENT TOOL SUMMARY ..... 43
6.2. EVALUATION AND REPORTING ..... 44
6.3. PRESCRIPTIVE REQUIREMENTS ..... 44
6.4. PERFORMANCE-BASED REQUIREMENTS ..... 45
6.5. COMBINED ASSESSMENT ..... 45
6.6. UNCERTAINTIES AND ASSUMPTIONS ..... 45

APPENDIX I LONE PINE NUCLEAR POWER PLANT HYPOTHETICAL FACILITY SECURITY PLAN ..... 47

I.1. INTRODUCTION ..... 47
I.1.1. Facility overview ..... 47
I.1.2. Facility location ..... 47
I.1.3. PPS description ..... 50
I.1.4. Access control ..... 51
I.1.5. Radioactive material locations ..... 64
I.1.6. Computer security ..... 64
I.1.7. Nuclear Material Accounting and Control system description ..... 66
I.1.8. Stakeholders identification ..... 70
I.1.9. Management of security ..... 71
I.1.10. Detailed LPNPP technology description ..... 73
I.1.11. Detection component data ..... 78
I.1.12. Delay component data ..... 81

ABBREVIATIONS ..... 89
LIST OF PARTICIPANTS ..... 91

# 1. INTRODUCTION

## 1.1 BACKGROUND

This publication provides Member States with a nuclear power plant (NPP) case study that demonstrates the standard nuclear security assessment (SA) methodology that was developed by the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP), Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities.

## 1.2 OBJECTIVE

The objective of this publication is to demonstrate the risk informed, performance based methodological framework in a systematic, structured, comprehensive and appropriately transparent manner for a hypothetical NPP. While the NUSAM project explored new approaches to nuclear security assessment, the established framework contained in Ref. [1] is consistent with recommendations and guidance provided in current IAEA Nuclear Security Series (NSS) publications.

## 1.3 SCOPE

This publication utilizes the methodology framework contained in Ref. [1] to assess the performance of defined protection measures as described in the security plan in Appendix I. The emphasis is on the methodological aspects of SA and is illustrated by the application of the methodological framework to a hypothetical NPP.

It is not appropriate to use this methodology where the security risks to materials and facilities are judged as requiring no more security than similar industrial and technological facilities that do not handle nuclear or radioactive materials.

## 1.4 STRUCTURE

This publication demonstrates the assessment methodology and compares various methods for assessment security performance for a hypothetical NPP. It is intended to be a practical reference. This publication contains two main sections and three annexes.

Section 2 provides the terms of reference for the case study. Section 3 discusses the preparation and planning for an SA. Section 4 discusses the collection of required information for an SA Section 5 discusses the tools and methods used for the conduct of the SA. Section 6 describes the overall summary of security assessment methods utilized for the SA.

Appendix I provides a hypothetical security plan containing detailed information that was used to conduct the SA.

References in this publication provide links to important international publications, standards and other guidance publications relevant to NUSAM.

# 2. TERMS OF REFERENCE

## 2.1. RATIONALE

In order to illustrate the application of the methodological framework, a number of security case studies were considered. Each security case study had a dedicated working group to develop a model and perform a nuclear security assessment using the recommended methodological framework on that model. This provides Member States with detailed examples to illustrate the nuclear security assessment process.

The highest consequence facilities/activities expected to be relevant for Member States are nuclear power plants, spent fuel storage facilities, Category 1 source facilities (see Ref. [2]), transport of

Category 1 sources (see Ref. [3]) and low enriched uranium fuel cycle facilities. These facilities/activities tend to have significantly different approaches for security. As a result of both of these factors, they were considered for inclusion as security cases for the NUSAM project.

This case study will address a Nuclear Power Plant (NPP). NPPs have very complex security systems and have potentially high radiological consequences as a result of sabotage. They tend to have an on-site guard force, multiple alarm stations, and multiple layers of security and access controls. In addition, a large percentage of Member States, which are expected to participate in the NUSAM project, have these facilities within their boundaries. NPPs have possible complex adversary targets/target sets (for additional information, see Refs. [4, 5]). Targets are generally nuclear safety systems that allow safe operation of the NPP. If a group of these systems can be disabled, this group is called a target set. Essentially if the adversary is able to compromise all of the targets within a target set, the result will be core damage likely resulting in an unacceptable radiological consequence. An additional target at the NPP would be the spent fuel pool. If the adversary attacked this target, the goal would be to drain the spent fuel pool which would cause the fuel to overheat resulting in radiological dispersal.

## 2.2. OBJECTIVE

The NPP case study working group needed to develop a detailed model of the facility to demonstrate the use and applicability of the NUSAM methodological framework and the recommended information, tools and approaches developed by the methodological working groups. See Appendix I. The development of the security case provides a basis for discussion of the many practical issues encountered when undertaking a nuclear security assessment, with the aim to reach broad consensus in as many areas as possible.

## 2.3. TASKS AND FUNCTIONS

To realize the objectives of the NPP case study working group within the overall objectives of the NUSAM project, the following broadly defined activities included:

- Defining each security case study in more detail and listing the guidelines/regulations/policies applicable to the case study;
- Compiling and describe the information needed for the security assessment;
- Developing detailed models and facility/activity specific information in a report based on the recommendations of the methodological working groups;
- Encouraging participation from each security case study working group in a methodological working group;
- Defining, considering and documenting information security concerns;
- Performing the security assessment for each security case study; and
- Documenting lessons learned in terms of the application of the methodological framework to each security case study.

## 2.4. OUTCOMES

In order to produce the expected outcome, the NPP case study working group:

- Produced a detailed model and information for the facility/activity; and
- Documented assessment of nuclear security systems using the NUSAM methodological framework, including assumption and rationales used in the assessment process.

# 3. PREPARATION AND PLANNING

## 3.1. REGULATION/POLICIES/GUIDELINES

The Regulator should ensure that the current regulations in a State are appropriate and reflect both international standards and best practices. A security assessment takes place within that regulatory framework and there will be a significant amount of pre-existing information of direct relevance to the assessment.

There are extensive official publications on the need for, and methods of achieving, the security of nuclear materials (NMs) and processes relative to outsider threats. Publications range from the obligations included in Conventions to advice and guidance based on expert experience. Included in this range of material are recommendations for security assessment. Based on these regulations, policies and guidelines, facilities are required to develop plans and procedures to implement these guidance and recommendations. These procedures typically become formal regulatory requirements for the facility/activity.

The operator is responsible and accountable for the security of the facility and its materials. The operator will wish to ensure that security measures, as well as being compliant with regulations, are genuinely appropriate and effective. The regulator may wish to initiate security assessments for similar reasons to be assured that the regulatory standards achieve their intended objectives. Both regulator and operator have a common interest in identifying which protection elements of the security system are effective and also how efficient and cost effective they are to implement and operate.

## 3.2. REQUIREMENTS

For these purposes of this case study, it is assumed that the fundamental principles and the recommended requirements in Refs [6, 7] have been adopted as prescriptive requirements. The main performance-based requirement is the effective prevention of high radiological consequences at the hypothetical facility. The acceptance criteria for physical protection system (PPS) effectiveness will be determined by the State or competent authority of the hypothetical country named the Republic of Lagassi.

# 4. COLLECTING REQUIRED INFORMATION

## 4.1. BACKGROUND

Assessment of an effective nuclear security system includes the determination of the nuclear security system objectives, the proposed design or characterization of an existing nuclear security system, the evaluation of the design, and possibly a redesign or refinement of the system. To assess the objectives or the facility/activity, characterization involves gathering information about facility/activity operations and conditions, and nuclear security requirements as well as the regulatory requirements. The assessment considers the effectiveness of a system of elements that work together to ensure protection rather than regarding each element separately.

The assessor **identifies targets** including vital areas. Determination of whether nuclear/radioactive materials are attractive targets is based mainly on the type of material and the ultimate goal of the adversary. Target identification allows the assessor to know the objectives of the nuclear security system (what to protect against whom).

Following the facility characterization and target identification processes, the assessor uses the competent authority provided designed basis threat (DBT) and other considerations, such as local conditions and factors about potential adversaries including: intent, motivation, types, capabilities and the range of tactics.

## 4.2. CASE STUDY FACILITY CHARACTERIZATION

The description of this country and facility is purely hypothetical. The Lone Pine Nuclear Power Plant (LPNPP) is a nuclear power plant located just to the east of the Lagassi Institute of Medicine and Physics

facility on a tributary of the Upper Lagassi River. The LPNPP was built in 1972 to produce 1150 Megawatts electrical for the Lagassi power grid. The LPNPP is located in the Republic of Lagassi, approximately 30 km (18 mi) east of Hashbakar.

There are 3 main areas in the LPNPP – the Limited Access Area, the Protected Area and the Vital Area (Fig. 3). The LPNPP Limited Access Area is surrounded by an unalarmed 2.5 m high chain-link fence with outriggers to keep out trespassers. There are two entrances into the area, P3 Employee Vehicle Entrance in the northern part of the area and the P9 Vehicle Entrance in the southern part. The LPNPP Protected Area is surrounded by two 2.5m high chain-link mesh fences with outriggers 4 mm x 50 mm mesh. There is an intrusion detection system between the two fences. There are five guard towers (T1-T5) located around the perimeter. There is one main personnel and vehicle entrance to the Protected Area - P2 (Secondary Alarm Station - SAS) and 3 other vehicle gates P4-P6. The LPNPP Vital Area walls, roof and floors are thick reinforced concrete construction. Personnel and vehicle gate access is mainly through steel-plate water tight doors with access controls. A 24-hour guard and response force (RF) is provided to ensure an adequate and timely response to prevent an adversary from completing an act of sabotage.

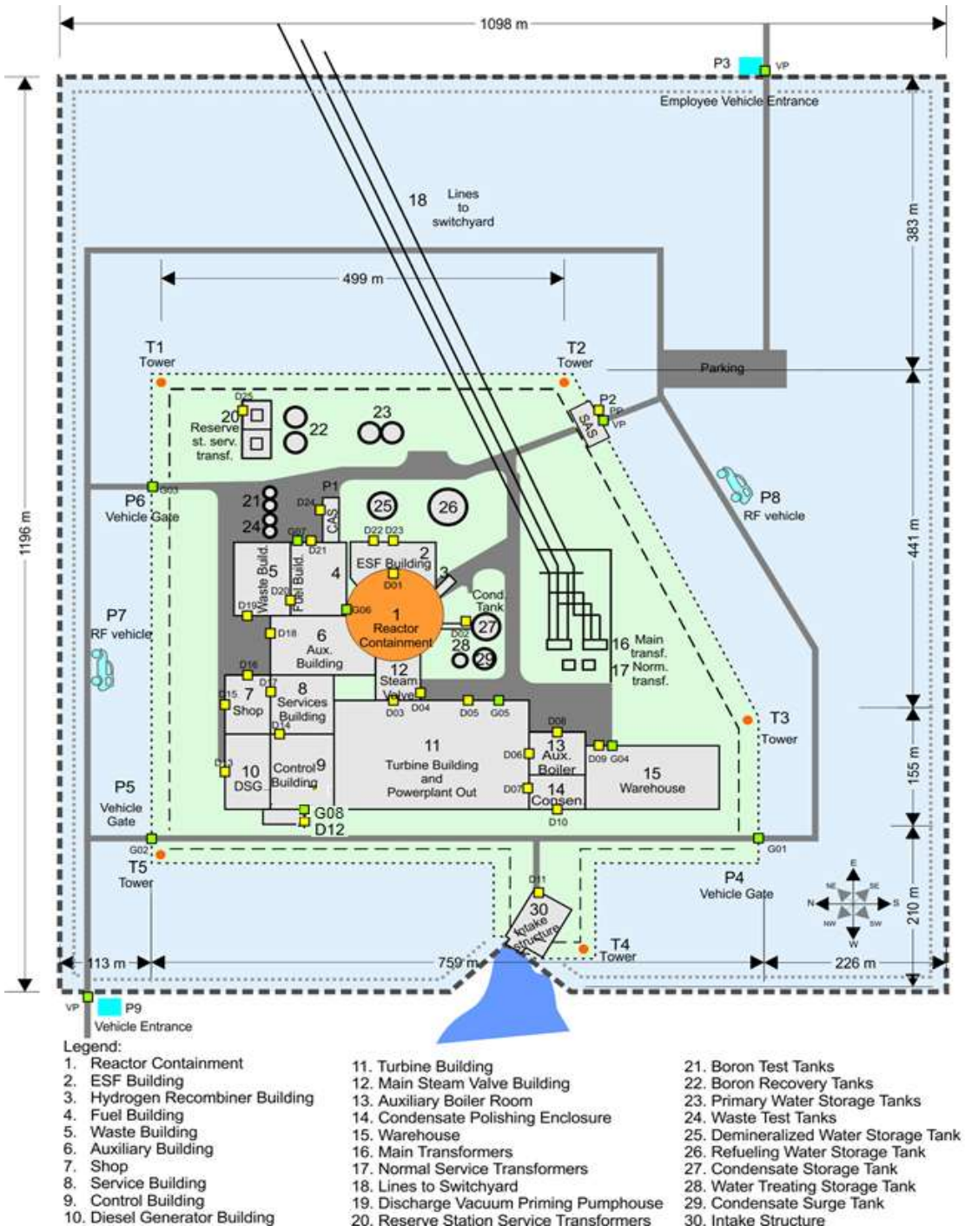



*FIG. 3. Facility site plan*

A detailed facility description used in the various analyses methods is contained in Appendix I.

NOTE: The NPP PPS was developed to address recommendations as outlined in Refs [6, 7] for requirements of measures against sabotage of nuclear facilities and nuclear materials in use and storage. When needed, PPS prescriptive requirements were stated as PPS capabilities and, if needed, revised to state how the prescriptive requirements were implemented as PPS capabilities based on generally accepted security practices.

### 4.3. CASE STUDY TARGET IDENTIFICATION

A hypothetical vital area identification (VAI) was conducted. Based on the results, the control room was determined to be the hypothetical target location to demonstrate the modelling/simulation methodologies for sabotage analysis. It was assumed that once the adversaries gained access to the control room location, a sabotage task time of 20 minutes (1200 seconds) was required. For additional details concerning the description of the control room, see Appendix A.

### 4.4. CASE STUDY THREAT DEFINITION

The PPS of nuclear facilities within the Republic of Lagassi shall be designed and evaluated to defeat the following adversary acts:

(1) Radiological sabotage and direct physical attack that could cause high radiological consequences by a determined violent external assault or attack by stealth or deceptive actions. The following capabilities, numbers, equipment and assistance apply:

- 5-6 outsider adversary personnel who are determined and violent;
- Outsider adversary personnel are well trained to include advanced military training and skills with the ability to operate in two or more teams;
- Insider assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g. provide facility information to the outsider);
- Weapons to include pistols, hand-held automatic rifles with or without silencers, belt-fed machine guns, hand grenades and precision (sniper) weapons. Weapons mounted night sites and night vision goggles are available to the adversaries during night-time conditions;
- Irritating (e.g. tear gas, pepper spray, riot control agents) and incapacitating (lethal and non-lethal agents) chemical agents. Adversaries will have protective equipment. Commercial grade explosives, sophisticated explosive and breaching charges, and tools for use in breaching barriers, facilitating entry or for otherwise destroying reactor, facility, transporter or container integrity features of the safety system or other vital equipment of the facility;
- A land or sea vehicle for transporting personnel and their equipment to the site and to the proximity of vital areas.

(2) An insider threat including an employee in any position.

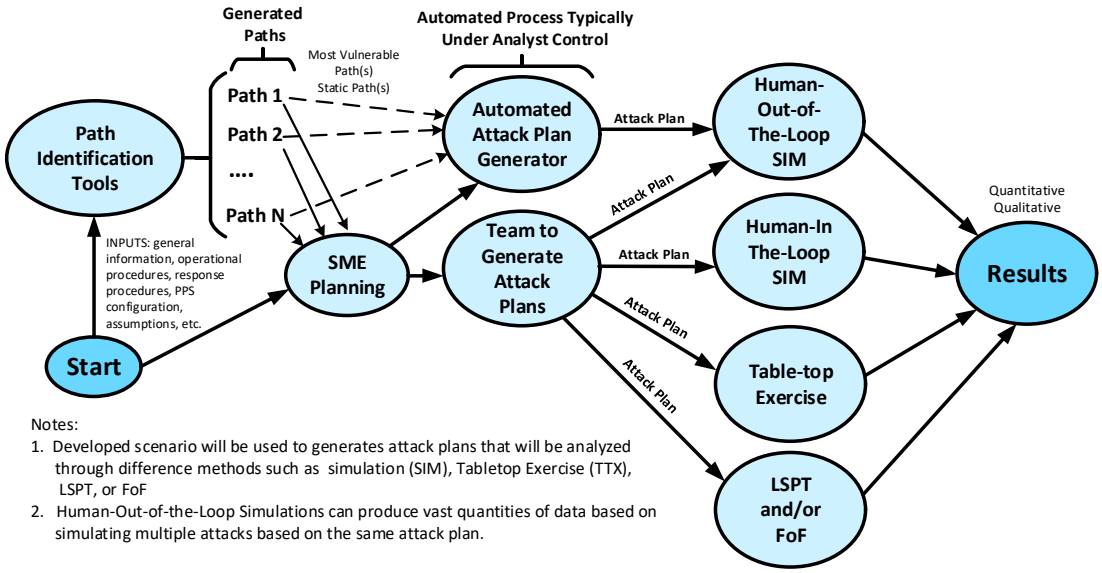
(3) A high mobility land vehicle bomb containing up to 50 kg of trinitrotoluene (TNT) equivalent explosive.

## 5. CONDUCTING THE SECURITY ASSESSMENT

Many tools and methods can be used to evaluate the effectiveness of security at a fixed site. These tools range from simple pathway analysis to complex computer modelling and simulations. Each category of tool is unique in terms of its analysis method, analysis output (probability of interruption ($P_I$), probability of neutralization ($P_N$), or probability of system effectiveness ($P_E$)), model inputs, and algorithms. For the purpose of conducting this case study, a variety of tools were utilized using the same hypothetical facility description, for comparative purposes. Where gaps in information existed, analysis teams needed to make assumptions, as necessary, to complete their analysis. The following represent descriptions of the tools/methods, observations of their usage, and overall results and initial findings. The documentation within this section is not a critical evaluation of the tools, but the information provided is intended to show the process, results, and capabilities of the specific tools.

### 5.1. PROCESS FOR USING SOFTWARE TOOLS AND EVALUATION METHODS

The analysis approaches for all of the tools and methods described within this report can be depicted using a common diagram (see Fig. 4).




*(Courtesy of M. Snell, Sandia National Laboratories)*

*FIG. 4. General scenario analysis process using software tools and effectiveness methods*

The analysis process begins at the start node. If the tool or method uses a path analysis approach, the node 'path identification tools' would be highlighted along with the paths Path 1, Path 2, …, Path N. The description of the path can then be used by a subject matter expert (SME) to plan an adversary attack plan or can be used internally by software to identify an adversary attack plan automatically. Some tools do nothing more than generate paths.

SME-planned attack plans can be used in human-in-the-loop simulations, in tabletop exercises, or as part of limited-scope-performance-tests or force-on-force exercises.

## 5.2. COMPARISON OF TOOLS

The software tools and methods used in this assessment are listed and compared in the Table 1 below:

TABLE 1. SOFTWARE AND TOOL COMPARISON

| **Software/Method Name** | **Tabletop*** | **VISA** | **SAVI** | **ProEv** | **STAGE** | **VEGA-2** | **Simajin** | **AVERT** |
|---|---|---|---|---|---|---|---|---|
| Type (S = Software, M = Method) | M | M | S | S | S | S | S | S |
| Performs Path Analysis | Yes | Yes | Yes | Yes | Yes | Yes | Under development | Yes |
| Metrics Calculated: $P_I$ | No | Yes | Yes | Yes | Yes | Yes | Under development | Yes |
| Performs Scenario Analysis | Yes | Yes | No | No | Yes | Yes | Yes | Yes |
| Metrics Calculated: $P_N$, $P_E$ | $P_N$ | $P_N$, $P_E$ | No | No | Yes | Yes | Yes | Yes |
| Simulation | No | No | No | No | Yes | Yes | Yes | Yes |
| Human in the Loop | | | | | No | No | Yes | Yes |
| Human out of the Loop (Constructive) | | | | | Yes | Yes | Yes | Yes |
| **Facility Representation** | | | | | | | | |
| Adversary Sequence Diagram (ASD) | No | Layer | Yes | No | No | No | No | No |
| Representation of Site and Building Floors | Yes | No | No | 2D+ | 3D | 2D + Floors | 3D | 3D |
| Path Network on representation Determined: | No | No | ASD | By Mixed Approach | By User | By Mixed Approach | Automatically | Automatically |
| Adversary Penetration Points on Barriers and Waypoints Are Determined: | | | | Automatically or by user | By User | By User | Mixed | Automatically determined |
| **Input Data** | | | | | | | | |
| Detection | | | | | | | | |
| $P_D$ Values | Fixed | Fixed | Fixed | Fixed | Fixed | Fixed | Fixed or Sampled | Sampled |
| Sensor/Camera Area Coverage Maps Represented | No | No | No | No | Yes | Yes | Yes | Yes |
| Delay values for barriers | Fixed | Fixed | Fixed | Fixed | Fixed | Fixed | Fixed or Sampled | Fixed or Sampled |
| **Software/Method Name** | **Tabletop** | **VISA** | **SAVI** | **ProEv** | **STAGE** | **VEGA-2** | **Simajin** | **AVERT** |
| Probability Hit/Probability Kill ($P_H/P_K$) | $P_H/P_K$ | No | No | No | $P_H/P_K$ | Physical | $P_H/P_K$ | $P_H/P_K$ |
| Patrol Routes | No | No | No | No | Yes | Yes | Yes | Yes |

TABLE 1. SOFTWARE AND TOOL COMPARISON (CONT.)

| Software/Method Name | Tabletop | VISA | SAVI | ProEv | STAGE | VEGA-2 | Simajin | AVERT |
|---|---|---|---|---|---|---|---|---|
| **Results** | | | | | | | | |
| Path Description | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Scenario Description | Yes | Yes | Tactics | Tactics | Yes | Tactics | Yes | Yes |
| Scenario Representation on Maps | Yes | No | No | Yes | Yes | Yes | Yes | Yes |
| Sampled Input Data | No | No | No | No | Yes | Yes | Yes | Yes |
| Replications performed for each set of input data | No | No | No | No | Yes | Yes | Yes | Yes |
| Data Analysis Tools | No | No | No | No | Yes | No | Yes | Yes |

* The tabletop methodology was included for comparative purposes against analysis results from the simulation tools.

Table 2 shows notes explaining the entries in Table 1.

TABLE 2. EXPLANATION OF ENTRIES FOUND TABLE 1 – SOFTWARE AND TOOL COMPARISON

| FIELD | DEFINITION/EXPLANATION |
|---|---|
| Type (S = Software, M = Method) | Approach is a method (implemented manually) or a software tool |
| PERFORMS PATH ANALYSIS | |
| Metrics Calculated (e.g., $P_I$) | $P_I$, Path Delay Time, Path Probability of Detection ($P_D$), $P_N$, and/or $P_E$ |
| PERFORMS SCENARIO ANALYSIS | |
| Metrics Calculated (e.g., $P_N$, $P_E$) | See above |
| SIMULATION | |
| Human in the Loop | Human operator makes decisions for and controls entities such as guards, adversaries, vehicles, cameras |
| Human out of the Loop (Constructive) | Program makes decisions for and controls entities |
| FACILITY REPRESENTATION | |
| Adversary Sequence Diagram (ASD) | |
| Representation of Site and Building Floors | 2D means that the site is represented by layers, one being the site and facility ground level, and others layers representing floors. 3D means that buildings and terrain are modelled to some level of fidelity. 2D+ assumes that each 2D layer representation is accurate between adjacent layers (e.g., if floors 2 and 3 are at 10m and 15m, respectively, then the floor 2 layout is valid between 10m and 14.99m). 2D and 2D+ typically assume terrain is flat. |
| Path Network on representation of Site and Buildings Determined | Paths in 2D or 3D are defined on networks that consist of r nodes (typically specific locations where the adversary can go) and arcs allowing routes to travel between nodes. Nodes are defined by Penetration Points and Waypoints (see next item). Arcs can either be determined automatically by software, by the user, or in a 'mixed approach' where some arcs can be set automatically while the user typically defines others, for example, traversals between layers. ASDs represent the facility in terms of protection layers which otherwise have no association with specific facility locations. |
| Adversary Penetration Points on Barriers and Waypoints Are Determined | Approach used for placing these penetration points and waypoints for the adversary/defenders to move between. These points may be defined by the user, automatically, or a 'mixed approach' may be used where the user defines penetration points on barriers and the software automatically places waypoints at corners of objects such as walls or terrain obstacles so that entities can move around these objects when moving between penetration points. |
| INPUT DATA | |
| Detection | DEFINITION/EXPLANATION |
| $P_D$ Values | Fixed or Sampled depending upon whether the value is a point values or sampled from a distribution |
| Sensor/Camera Area Coverage Maps Represented | Does the tool attempt to model the actual coverage map covered by the sensor and/or camera |
| Delay values for barriers | Fixed or Sampled depending upon whether the value is a point values or sampled from a distribution |
| $P_H/P_K$ | $P_H/P_K$ =Probability of Hit, Probability of Kill (given hit); Physical = Model actual round fired. |
| Patrol Routes | Patrol routes specifically defined |

TABLE 2. EXPLANATION OF ENTRIES FOUND TABLE 1 – SOFTWARE AND TOOL COMPARISON (CONT.)

| FIELD | DEFINITION/EXPLANATION |
|---|---|
| RESULTS | |
| Path Description | Yes = describes where the adversary group(s) went and what tactics they used. Otherwise: Partial |
| Scenario Description | Yes = Tool provides a description of the adversary attack plan (to some level of detail); otherwise: Partial. |
| Scenario Representation on Maps | Does the tool/approach result in a description of the scenario that specifies where the adversary group(s) go? |
| Sampled Input Data | Yes if input parameters such as $P_D$, delay values, response locations, and/or response times that are used in a software tool or method can be chosen (sampled) from probability distributions as opposed to just using point values; otherwise, No. |
| Replications performed for each set of input data | Two or more simulated adversary attacks are said to be replications if they are based on identical analysis assumptions and input variables are sampled from the same input distributions in such a way that all input variables are statistically independent (meaning that knowing the specific input variable values used in one simulated attack does not improve one's ability to predict the values used in another simulated attack). Yes means that multiple replications can be performed; otherwise, No. |
| Data Analysis Tools | Yes = Simulation/Method results can be stored in dedicated relational databases; otherwise, No. Note that such databases can then be queried using specialized database analysis and visualization tools to help understand the data. |

## 5.3. SIMULATION SPECIFICATION

- Simulation purpose: The following sections reflect the evaluation of various human in the loop and human out of the loop tools. These tools were evaluated to identify the overall operational process, characterize observations, strengths, and weaknesses, and the overall usage of the tool for determining $P_E$, for training, or to validate a security plan.
- Scope: Information regarding the modelling of the response and force (on and offsite responders) and adversary team were documented within a site characterization document which is included as an appendix. For each tool included as part of the evaluation, the level of resolution required for different entities (e.g., doors could be defined merely in terms of delay times versus detailed representations of the hardware) were captured for the purpose of comparison.
- Adversary objectives: Sabotage of control room - Stopping conditions for completing the scenario: e.g., completing the task of placing a bomb at a sabotage target (facility loss), the actual explosion of that bomb at the target (facility loss), incapacitation of the single adversary expert who can place the bomb at the target (facility win), adversary still on task when 100 off-site responders arrive at the site (facility win).

## 5.4. VISA MODEL AND IMPLEMENTATION

### 5.4.1. VISA background and overview of method

Vulnerability of Integrated Security Analysis (VISA) tabletop methodology was developed by Science Applications International Corporation (SAIC) for the U.S. Nuclear Regulatory Commission (NRC) in 1976-1977. The VISA methodology can systematically evaluate effectiveness of nuclear security through the use of SMEs. (See Ref. [8]) The methodology is a scenario-based approach based on subject matter expert opinion, published values or a combination of both.

- Performance metrics: $P_E$ (typically VISA results in an overall probability of system effectiveness (SE) determination. For this evaluation, $P_E$ will be used to be consistent with other evaluation tool terminology).
- Process for use: The VISA process consists of four phases: 1) development of a general adversary scenario, 2) expansion of the scenario into logical steps (sensing and assessment opportunities), 3) analysis of the effectiveness for each individual step and 4) determination of the overall scenario protection system effectiveness.

Phase 1 is a general attack strategy description for theft or sabotage (numbers of adversaries with specific capabilities and equipment, weapons and intent).

Phase 2 expands the attack strategy from Step 1 into logical steps (or events) based on site characteristics and credible scenarios that gives the adversary the best chance for success.

Phase 3 utilizes professional judgment by SMEs and is used to determine each of the adjectival values (qualitative approach) or numerical values (quantitative approach) for the probability of sensing (Ps), probability of assessment ($P_A$), $P_I$, and $P_N$. $P_S$ and $P_A$ are step dependent while $P_I$ is dependent on the adversary overall task/timeline versus the response force time. $P_N$ is dependent on the response force size and capability to defeat the adversary assuming interruption occurs.

Within each step, each element is evaluated individually; $P_S$ is first assigned for the step, then $P_A$ is assigned 'given sensing has occurred' for that step, therefore, $P_S$ and $P_A$ are a chain of events, each of which would need to occur to provide detection in that step.

Phase 4 using the qualitative approach as discussed in Phase 3 assigns percentage values for $P_S$, $P_A$, $P_I$ and $P_N$. Take the lowest adjectival score (value) horizontally for each step and record it in the step score column (weakest link in the chain). Once each step score is determined, use the highest step score value (strongest link in the chain) to determine the scenario $P_E$. The $P_E$ step qualitatively summarizes the probability that the overall protection system of procedures, equipment, guards and barriers will defeat the assumed adversary threat.

These adjectival ratings are based on a percentage scale from 0.0 to 1.0, as follows:

| | |
|---|---|
| Very Low (VL) | = 0.00 – 0.20 = midpoint = 0.10 |
| Low (L) | = 0.21 – 0.40 = midpoint = 0.30 |
| Moderate (M) | = 0.41 – 0.60 = midpoint = 0.50 |
| High (H) | = 0.61 – 0.80 = midpoint = 0.70 |
| Very High (VH) | = 0.81 – 0.99 = midpoint = 0.90 |

The scenario analysis process using VISA is illustrated in Fig. 5.

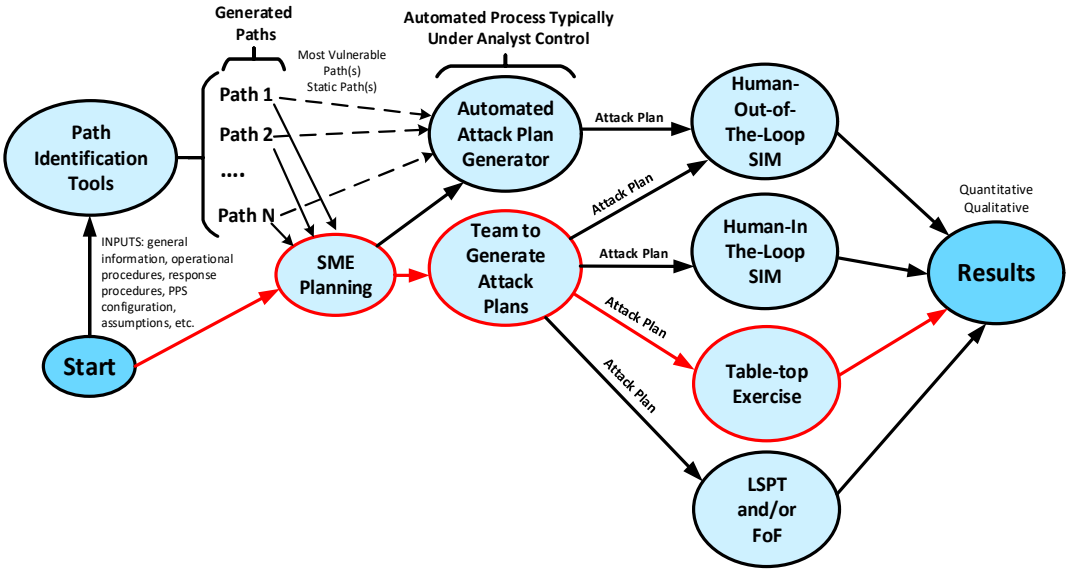



*FIG. 5. Scenario analysis process using VISA*

### 5.4.2. Scenario conditions

- General scenario description: Adversaries will attack the LPNPP with the goal of accessing the control room where they will set up their sabotage mission;
- Design basis threat: All adversaries are armed with AK-47 assault rifles, hand tools (manual bolt cutter), and explosive breaching charges;
- Adversary assumptions:
  - Adversary will attack on foot;
  - Adversary traversal distances included in analysis are minimal to represent that shortest paths will be taken (i.e. adversary will minimize delay);
- Response force assumptions: n.a.
- Attack conditions: Closed condition non-operational (1:00 am); clear weather conditions;
- Other model assumptions:
  - Delay times for barriers encountered along adversary path represent times outlined in the facility description document. Any deviations will be noted as part of the analysis;
  - The likelihood that the adversary will be detected by roving response force patrol(s) is considered to be minimal, and thus not considered within the VISA analysis.

### 5.4.3. Modelling information

- Model used to represent the facility: LPNPP Facility Map (see Fig. 3);
- Facility layout features: n.a.
- Initial conditions for adversaries: Adversaries start at the offsite area;
- Data:
  - Detection: Used values found in the facility description document. Any deviations will be noted as part of the analysis;
  - Delay for Barriers: Used values found in the facility description document. Any deviations will be noted as part of the analysis;
  - Movement speeds and/or traversal speeds: Based upon SME judgment;
  - Probability of hit/probability of kill values: Values are used indirectly in support of SME estimation of $P_N$.

### 5.4.4. Results

#### *5.4.4.1. Scenario description*

In order to minimize detection, the adversary team will attack the LPNPP during non-operational hours. The adversaries climb the Limited Access Area (LAA) fence line and traverse to the Protected Area (PA) perimeter fence line. Using hand tools, the adversary team (six members) breaches the outer chain-link mesh fence to the PA perimeter. Once the fence is cut, the team enters and moves across the perimeter detection zone (triggering infrared sensor alarm) and proceeds to the inner fence which they also breach with hand tools, subsequently causing a second alarm (vibration sensor). The combined $P_S$ for both sensors is very high as well as the $P_A$ due to the CCTV in the perimeter.

The adversary team immediately proceeds to the door (D12) near the northwest corner of the Vital Area and set an explosive charge. The team retreats, detonates the charge, returns to the breach point, clears debris and enter the Vital Area. Moving up the stairs, the team moves toward the door of the control room (D34), breaches the door, enters the room and initiate their sabotage task (20 minutes). Table 3 below represents the individual step scores for the described scenario.

### *5.4.4.2. Scenario representation*

TABLE 3. VISA TABLETOP RESULTS

**Lone Pine Nuclear Power Plant**
**Outsider – Radiological Sabotage**
**Control Room Task**

| Step | Step Time ..(Sec.) | Cuml Time (Sec.) | RF Time (Sec.) | Step Description | $P_S$* | $P_A$* | $P_I$** | $P_N$** | Step …Score |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 10 | | | LAA - No Sensor ($P_S$ is VL- Adversaries climb the fence. If seen by roving patrol then assessment is High – (10 sec to climb fence). | VL | H | VH | H | **VL** |
| 2 | 30 | | | Traversal Time from LAA to PA fence (30 sec) | VL | H | VH | H | **VL** |
| 3 | 160 | 95 | | PA - Adversaries cut outer Fence (60 sec) - Cross Zone (10 sec), Cut inner fence (60 sec) - Complimentary Sensors Detection VH, CCTV provides VH assessment – time starts following detection – an additional delay of 30 seconds is required to defeat the guard in the guard tower. | VH | VH | VH | H | **H** |
| | | | 30 | *CAS Assessment (15 sec) and notification time (15 sec)* | | | | | |
| 4 | 35 | 130 | | Distance from PA to Control Stairwell Door (90 metres at 2.6 m/s = 35 sec), No sensors or CCTV inside area in this location. Detection from tower guards assumed M, Assessment if detected is assumed M from tower guards and patrols. | M | M | VH | H | **M** |
| | | 90 | 60 | *Response Team Muster time (60 s)* | | | | | |
| | | 150 | 60 | *Response Team traversal time is 60 s for a total response time of 150 s.* | | | | | |
| 5 | 30 | 160 | | Building surface (door – D12) - Adversaries set explosive charge and retreat (15 sec) – Door is breached and adversaries re-enter stairwell (15 sec). Detection assumed H from explosive noise and door BMS. Assessment is assumed to be VH from CCTV outside of building door. | H | VH | VH | H | **H** |
| 6 | 50 | 210 | | Adversary team traverses the stairwell to the control room door D34 (20 sec) and set explosive charge and retreat (15 sec) - Door is breached and adversaries approach the control room door (15 sec). Detection assumed H from explosive noise and door BMS. Assessment is assumed to be VH from CCTV inside stairwell. | H | VH | VH | H | **H** |
| 7 | 10 | 220 | | Adversaries enter the control room (10 sec). Detection assumed VH from control room personnel. Assessment assumed H from control room CCTV. | VH | H | VH | H | **H** |
| 8 | 1200 | 1420 | | Adversaries complete sabotage target task (1200 sec). Detection and assessment assumed L due to adversary's defeat of alarms and CCTV during task. | L | L | VH | H | **L** |
| Response Force Time = 150 seconds | | | | Probability of System Effectiveness ($P_E$): | | | | | **H** |

* $P_S$ and $P_A$ are step dependent. $P_S$ is first assigned for the step, then $P_A$ is assigned 'given sensing has occurred' for that step.

** $P_I$ is dependent on the adversary overall task/timeline versus the response force time. $P_N$ is dependent on the response force size and capability to defeat the adversary assuming interruption occurs.

Note 1: $P_I$ is assumed Very High since the total adversary task time is 1340 seconds following detection at the perimeter (step 3) versus the response force time (RFT) of 150 seconds (as defined in Appendix I)

Note 2: $P_N$ is assumed High due to six adversaries versus eight response team members

Qualitative results: $P_E$ = High

### 5.4.5. VISA observations

- General:
  - Intuitive approach using logic process;
  - Single path analysis tool provides $P_S$, $P_A$, $P_I$;
  - Identifies the weakest link in the chain of $P_S$, $P_A$, $P_I$ or $P_N$;
  - The qualitative approach is less accurate than a quantitative approach;
  - The method can be converted to quantitative approach if desired;
  - Easier and quicker than other analytical modelling methods;
  - Manual method limits analysis to a few scenarios;
  - Is highly dependent on SME capability;
  - Need other method to evaluate neutralization;
  - Provides an assumed vulnerable path based on SME opinion;
  - Can analyse the results of $P_I$ over the range of response force times (RFT);
  - Is a qualitative approach that can be used to analyse the insider threat;
  - Can be used for abrupt and protracted theft evaluations;
  - Can be used to account for PP, material control (MC) and material accounting (MA) protection elements;
  - Sensitivity analysis is possible;
  - Minimal training required;
  - No specialized software required.

- Strengths:
  - Less data and set up requirements than other analytical methods;
  - Simple to provide results in a very short time;
  - Reasoned approach to determine logical paths;
  - VISA is currently widely taught internationally.

- Weaknesses:
  - Only as good as data input;
  - Limited number of scenarios generated;
  - Results may be driven by strong work group personality.

## 5.5. SAVI MODEL AND IMPLEMENTATION

### 5.5.1. SAVI background and overview of software

Developed in the 1980s, the Systematic Analysis of Vulnerability to Intrusion (SAVI) creates a pathway analysis to determine the ordered series of potential adversary actions (called an adversary path) and calculates the probability that a response force will interrupt this adversary before the task is completed. SAVI was developed to determine the effectiveness of a site's physical protection and material control and accounting system to protect against a spectrum of insider and outsider threats.

- Performance metrics: SAVI calculates the $P_I$, the probability that a response force will interrupt this adversary before the task is completed. SAVI does not address $P_N$.

- Process for use: Merely identifies paths with the lowest $P_I$ (See Fig. 6). Paths may be used by an SME to develop scenarios.

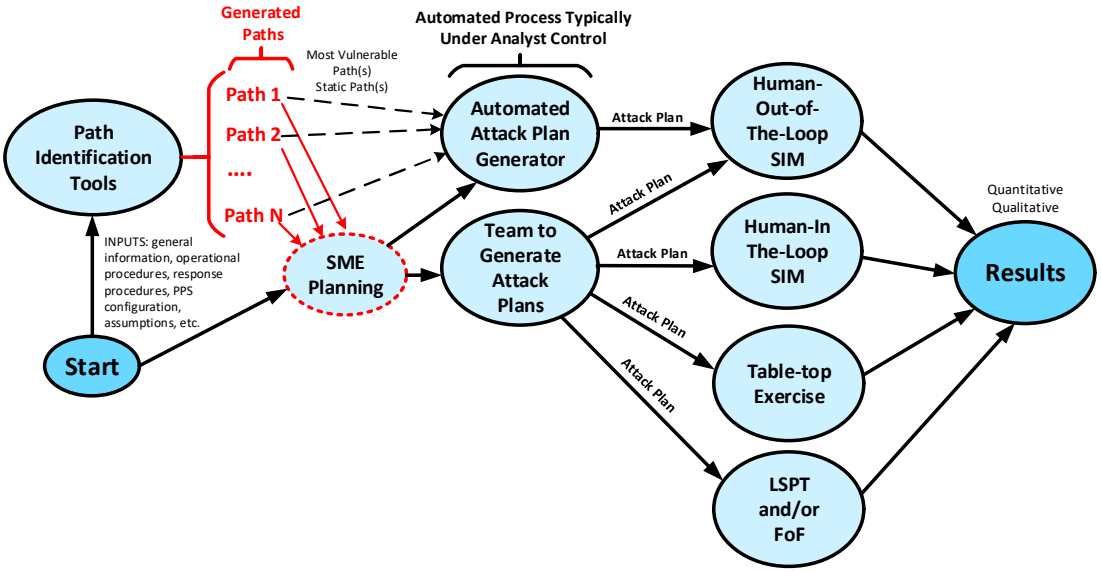



*FIG. 6. Scenario analysis process using SAVI*

### 5.5.2. Scenario conditions

- General scenario description: Adversaries will attack the LPNPP with the goal of accessing the control room where they will set up their sabotage mission;
- Design basis threat: Tool only uses information: All adversaries are armed with automatic weapons, hand tools, and explosive breaching charges;
- Adversary assumptions: Adversary will attack on foot;
- Response force assumptions: N/A
- Attack conditions: Closed condition non-operational (1:00 am); clear weather conditions;
- Other modelling assumptions:
  - The likelihood that the adversary will be detected by roving response force patrol(s) is considered to be minimal, and thus not considered within the SAVI analysis.

### 5.5.3. Modelling information

- Model used to represent the facility: SAVI represents a PPS using what is called an adversary sequence diagram (ASD). The ASD represents the concentric layers of protection elements (detection and delay features) and path segments. Detection features on a layer might include intrusion sensors, response force personnel, prohibited item checks, and access control procedures. Performance databases in the software describe the effectiveness of these detection and delay features against adversary threats. The ASD represents the target at the bottom of the ASD and offsite, where there is no physical protection, at the top. Adversary sabotage paths move from offsite to the sabotage target.
- Facility layout features: ASD includes areas and elements, each describing physical protection measures and minimal traversal distances across that area or element;
- Initial conditions for adversaries: Adversaries start at the offsite area;
- Data:
  - Detection: Probabilities of detection were selected from a database used in international SAVI courses;

- Delay for barriers: Used values found in the facility description document. Any deviations will be noted as part of the analysis;
- Movement speeds and/or traversal speeds: Adversary traversal distances included in analysis are minimal to represent that shortest paths will be taken (i.e. adversary will minimize delay);
- Probability of hit/probability of kill values: Not used in SAVI.

### 5.5.4. Results

#### *5.5.4.1. Scenario description*

In order to minimize detection, the adversary team will attack the LPNPP during non-operational hours. Using hand tools, the adversary team (6 members) breaches the outer chain link mesh fence to the isolation zone. Once the fence is cut, the team enters and moves across the isolation zone (triggering infrared sensor alarm 0.8) and proceeds to the inner fence which they also breach with hand tools, subsequently causing a second alarm (vibration sensor). The adversary team immediately proceeds to the door (D12) near the northwest corner of the Vital Area and set an explosive charge. The team retreats, detonates the charge, returns to the breach point, clears debris and enter the Vital Area. Moving up the stairs, the team moves toward the door of the control room (D34), breaches the door, enters the room and initiate their sabotage task (20 minutes). The Fig. 7 depicts the ASD for the described adversary scenario.

#### *5.5.4.2. Scenario representation*

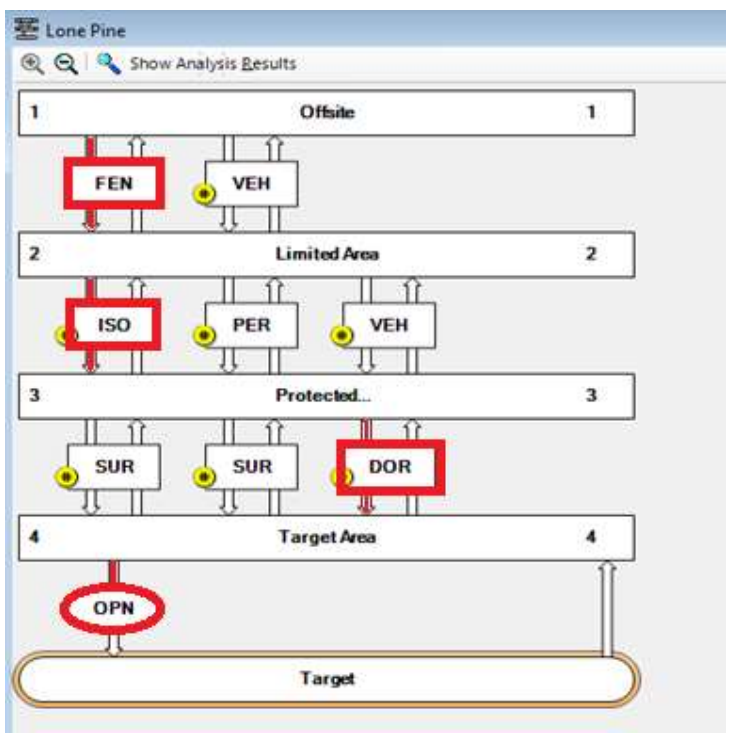



*FIG. 7. SAVI adversary sequence diagram for the adversary scenario*

Quantitative results: $P_I = 0.49$

### 5.5.5. SAVI observations

- General:
  - Multi-path analysis tool provides $P_I$;
  - Need other method to evaluate neutralization;
  - Provides a set of most critical paths in one dimensional space;
    - Tool does not provide continuous path, only shortest distance. Would need to piece each path together to create one path. Moves one element at a time and you would need to connect them;
    - Tool provides an analytical worst case path which would need to be verified based upon actual facility layout (for distances…) to determine if it is a valid path.
  - Analyzes results for a single RFT;
  - Allows for RF sensitivity case for analysis;
  - Purely an analytical tool – not suitable for RF training purposes;
  - Lower level of configuration and level of details;
  - Lower level of maintenance by SME and site;
    - Analytic skills required.
  - Much less training required.
- Strengths:
  - Less data and set up requirements than simulations;
  - Simple to provide results in a very short time (conservative estimates of $P_I$);
  - Reasoned approach (human in the loop) to determine logical paths.
- Weaknesses:
  - Only as good as data used for population;
  - Library of values are generated by the user for the current version;
  - Results in ASD need to be translated/compared to the applicable facility;
  - Limited number of reports generated.

## 5.6. PROEV MODEL AND IMPLEMENTATION

### 5.6.1. ProEv background and overview of software

ProEv is a multi-path analysis tool. It was developed in the Czech Republic by the EBIS Company. ProEv is designed to balance the need for data inputs to develop a realistic model. The tool focuses primarily on the evaluation of $P_I$ independently of attack neutralization. The neutralization part of the PPS effectiveness analysis is represented by RFT. ProEv is suitable for facilities, where detection and delay are the key aspects of protection. The tool provides the set of most critical paths and represents these continuous realistic paths in maps or drawings of the analyzed facilities. The tool searches for critical paths from all points on the facility perimeter and therefore truly provides the most critical path. The tool also searches for critical paths from selected point on the facility perimeter or calculates $P_I$ for user selected path. Paths are described in a detailed tabular form that includes the overview of different layers of a protective element as well as critical detection point (CDP) for each path. The tool allows for the detailed description and presentation of sensitivity analysis for various metrics such as RFT, $P_D$, and delay for the selected $P_I$. ProEv makes it feasible to model different types of attacks – sabotage, theft as well as an escape from a facility. The tool is designed to perform upgrades to the facility in real time and evaluate the cost effectiveness of such changes during the facility design, upgrade and optimization of the current PPS installation. Furthermore, it is designed to provide a well-documented proof for authorities that a PPS is effective against a given threat.

- Performance metrics: ProEv calculates the $P_I$;
- Process for use: Identifies paths with the lowest $P_I$ in 2D+ dimension. Paths may be used by an SME to develop scenarios (See Fig. 8).

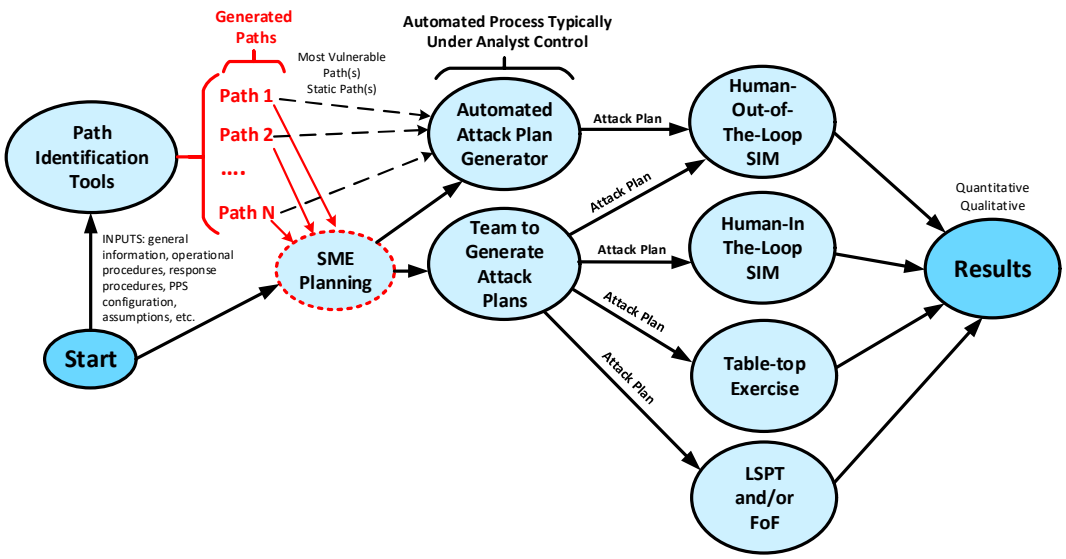



*FIG. 8. Scenario analysis process using ProEv*

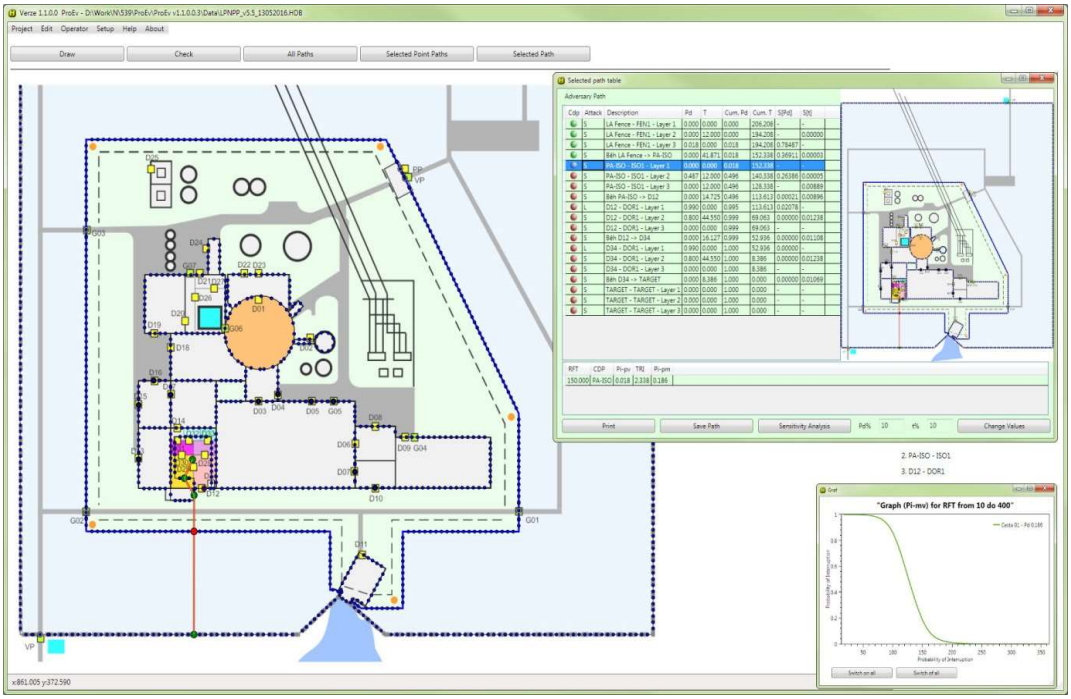
### 5.6.2. Scenario conditions

- General scenario conditions: Adversary uses stealth tactics to gain access and sabotage target, fast surprise attack;
- Design basis threat: Defined in hypothetical facility description;
- Adversary assumptions: The adversary uses vehicle only to get access to the off-site area. Further, adversary uses information gained from a passive insider, the information concern technical-level details about sabotage of the control room;
- Response force assumptions: The response forces may use weapons only in self-protection or if ordered from the commander. Only response force team may engage with the adversaries. Guards may shoot in self-protection only;
- Attack conditions: off-shift;
- Other modelling assumptions:
    - LPNPP delay and detection data were used (conservative); if no data were available, expert opinion was used (e.g. detection of explosives use);
    - Due to insufficient $P_I$ data, there were some simplifications assumed in the model (some door or rooms were not modelled in details e.g. first floor Control Building).

### 5.6.3. Modelling information

- Model used to represent the facility: 2D model (See Fig. 9);
- Facility layout features: Analyst describes terrain and building;
- Initial conditions for adversaries: Adversaries start offsite;

- Data:
  - Detection: Probability of detection values were selected from database;
  - Delay for barriers: Used values from facility description;
  - Movement speeds and/or traversal speeds can be changed depending on facility location:
  - Probability of hit/probability of kill values: Not used in ProEv.




*(Courtesy of the EBIS Company, Czech Republic)*

*FIG. 9. Scenario 2D graphic using ProEv*

### 5.6.4. Results

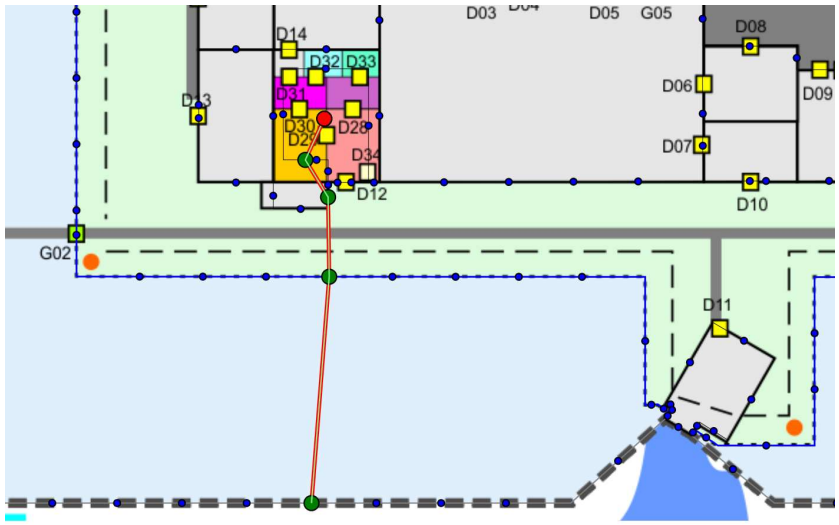
#### *5.6.4.1. Scenario description*

The team of five adversaries approaches the facility from the western part of the facility at the point marked by the picture. Adversaries are trying to go unnoticed as long as possible, so they wait for the patrol to pass that area, once out of sight they use hand tools to cut through the fence, run through the limited access area and breach the isolation zone fences using hand tools. They further proceed to door D12, use mechanical tools to cut through the door to avoid the detection of the BMS. The team approaches the control room door D34 and uses explosives to gain access to the control room.

The adversary path, illustrated in Fig. 10 below, leads through the following protective elements:

- Fence
- Isolation Zone
- Door D12
- Door D34
- Control Room

*5.6.4.2. Scenario representation*




*(Courtesy of the EBIS Company, Czech Republic)*

*FIG. 10. Selected path for the scenario using ProEv*

Quantitative results: $P_I = 0.99$

### 5.6.5. ProEv observations

- General:
  - Multi-path analysis tool;
  - ProEv focuses primarily on the evaluation of $P_I$ independently of attack neutralization;
  - Provides a set of most critical paths in two-dimensional space, continuously represents adversary paths, shows real paths (bypass objects) and other results on actual maps of a facility;
  - 2D+ tool - the 3rd dimension is modelled by the possibility of the change of adversary movement speed, different facility area can have different speeds of adversary movement;
  - Calculates $P_I$, critical detection point (CDP) and standard metrics for detection, delay and response;
  - Conducts analysis utilizing the possibilities of an up-to-date graphical interface;
  - Results are provided in a graphical environment, provides clearly arranged detailed tabular path description including the critical detection point depiction in facility maps;
  - Clearly-arranged multilayer all-purpose protective element that makes it feasible to model common PPS protective elements, easy modification during analysis;
  - Allows for a detailed description and presentation of sensitivity analysis for various metrics (RFT, $P_D$, Delay for selected $P_I$);
  - Allows for modelling of different types of attacks (sabotage – from offsite to the target, theft – from offsite to the target and back, escape – from a selected point from inside the facility to an offsite area);
  - Supports simple insider analysis, providing, we assume, that an insider adversary behaves from a certain point as an outsider. This can be utilized, for example, while conducting an insider theft analysis;
  - Makes it feasible to user-select specific path and specific point outside the facility to determine the most vulnerable paths;

- Analysis and upgrades to the facility in real time;
- Allows for cost optimization during the facility design, upgrade and optimization of the current PPS installation as well as to provide a proof for authorities that a PPS is effective against the DBT;
- ProEv is designed in such a way as to balance the need for significant data input and neglecting unnecessary data and at the same time it maintains the possibilities to develop a realistic model;
- Allows for the direct use of facility maps/blueprints for graphical model creation;
- Lower level of maintenance by SME and site;
- Analytic skills required;
- Interactive tool that supports an effective and economically-optimized analysis of a PPS;
- Extensive validation and verification process was conducted.

— Strengths:
  - Presents realistic continuous paths in 2D+;
  - Detailed overviews of paths, protective elements, sensitivity analysis;
  - Balances the use of data to create a realistic model (suitable both for newcomers as well as advanced users);
  - Approximately one-week training course for a security professional with no modelling and simulation experience;
  - Reasoned approach (human-in-the-loop) to determine logical paths.

— Weaknesses:
  - Only as good as data used for population;
  - Library of values are generated by the user;
  - Does consider only RFT for $P_I$ evaluation, doesn't simulate neutralization;
  - Purely an analytical tool – not suitable for RF training purposes.

## 5.7. STAGE MODEL AND IMPLEMENTATION

### 5.7.1. STAGE background and overview of software

The Simulation Toolkit and Simulation Environment (STAGE) is a modelling and simulation tool developed in Canada that provides users with the ability to generate and execute complex scenarios for training and analysis. The tool uses an integrated simulation environment to build dynamic and interactive tactical and operational scenarios.

— Performance Metrics: STAGE is a simulation that calculates $P_N$ and $P_E$;

— Process for Use: SME develops attack plan that is then used in a human-out-of-the-loop simulation (see Fig. 11).

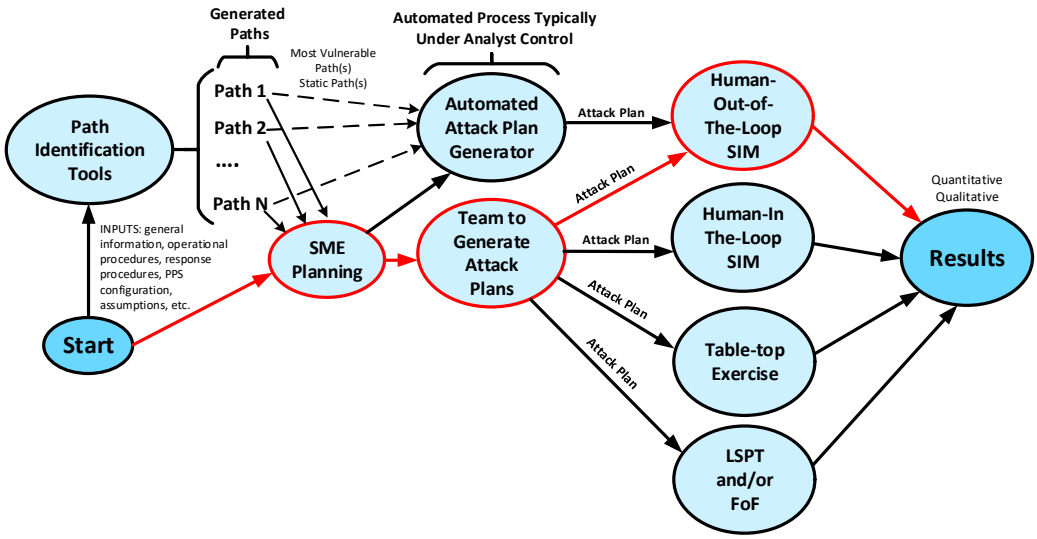



*FIG. 11. Scenario analysis process using STAGE*

### 5.7.2. Scenario conditions

- General scenario description: Adversary use of stealth and/or force to obtain access to target;
- Design basis threat: Defined in hypothetical facility description;
- Adversary assumptions: Basic mechanical breaching tools, explosive charges (for door breach), AK-47 7.62 mm rifles, 180 rds ammunition each, radios;
- Response force assumptions:
  - Equipment/Weapons: Radios, 5.56 mm rifles, 180 rds ammunition each, light armoured vehicle (for patrols);
  - The response force consists of two groups, divided into three teams. The patrol group consists of four individuals and split into two vehicles. These two teams patrol the site on the inside of the PIDAS and one outside. Upon alarm, the outer team proceeds to secure the exterior of the breach, while the inner team moves to secure the interior. The other RF team is based in the CAS and moves upon assessed detection of an alarm. It consists of four individuals; they do not have a vehicle, andwould need to proceed on foot. In this scenario, they are dispatched to the control room (due to alarms along the adversary path) after meeting a 60-second muster time. Upon arrival, they clear the exterior of hostiles and stack up outside the build and make entry to remove hostiles from the control room.
- Attack conditions: Closed condition non-operational (1:00 am); good weather conditions;
- Other modelling assumptions: None.

### 5.7.3. Modelling information

- Model used to represent the facility: 3Dimensional model;
- Facility layout features: Analyst describes terrain and buildings;
- Initial conditions for adversaries: Adversaries start at the offsite area;
- Data:
  - Detection: probabilities of detection were selected from a database used in international SAVI courses;
  - Delay for barriers: Used values found in the facility description. Any deviations will be noted as part of the analysis;

- Movement speeds and/or traversal speeds: Predetermined by the user;
- Probability of hit/probability of kill values: Used values from an unclassified demonstration database that is based upon SME and open source data.

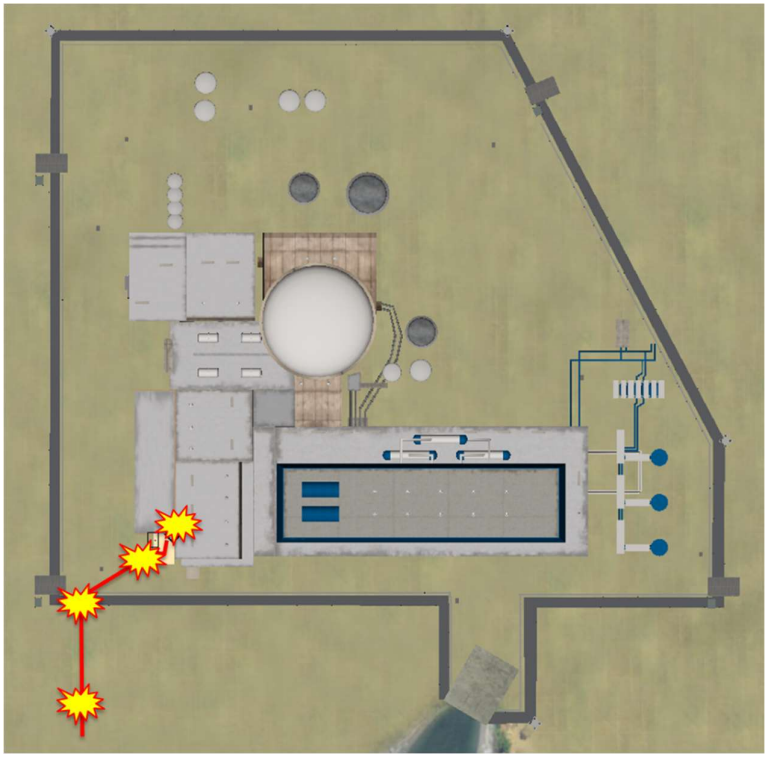
### 5.7.4. Results

#### *5.7.4.1. Scenario description*

An adversary team of five approaches the facility perimeter wall surrounding the LPNPP. Five members climb the outer wall and set up an ambush for the RF patrol vehicle in their sector. As the RF vehicle enters the ambush zone, they engage with small arms fire. They will not proceed with their attack until the RF team has been neutralized. Once the area is secure, one individual approaches and breaches both PIDAS fences mechanically, while the remainder provide cover. Once the PIDAS is breached, the team moves into the protected area and proceeds to the outer skin of the complex on the southwest side. One adversary approaches an exterior door and breaches explosively, while the remainder provide cover. Upon breach completion, two adversaries enter the building interior and proceed to the control room. Upon entering the control room, they proceed with their sabotage task.

#### *5.7.4.2. Scenario representation*

Figure 12 represents the adversary path modelled within STAGE.



*(Courtesy of Sandia National Laboratories)*

*FIG. 12. Adversary path modelled using STAGE*

Quantitative results: $P_N = 0.80$

### 5.7.5. STAGE observations

— Strengths:
- High flexibility;
- High traceability;

- Open code if desired, very little coding required;
- Standard model format;
- Customizable data report.

— Weaknesses:
  - High level of vulnerability analysis (VA) training;
  - Out-of-the-box customization to run with high fidelity;
  - Requires multiple tools to go from source data to simulation.

## 5.8. VEGA 2 MODEL AND IMPLEMENTATION

### 5.8.1. VEGA-2 background and overview

VEGA-2 is a modelling and simulation software tool developed by the Federal Centre of Science and High Technologies (Eleron) of the State Corporation Rosatom to support PPS effectiveness assessments at Russian nuclear sites. VEGA-2 calculates a PPS effectiveness index, measuring the probability of system effectiveness for a given PPS against a specified design basis threat.

— Performance metrics: $P_I$, $P_N$ and $P_E$;

— Process for use: The operator enters site information, such as a terrain map, response force information and DBT information into VEGA-2. The software will then automatically generate path and associated attack plans and then simulate the scenario in a human-out-of-the-loop simulation (see Fig. 13).

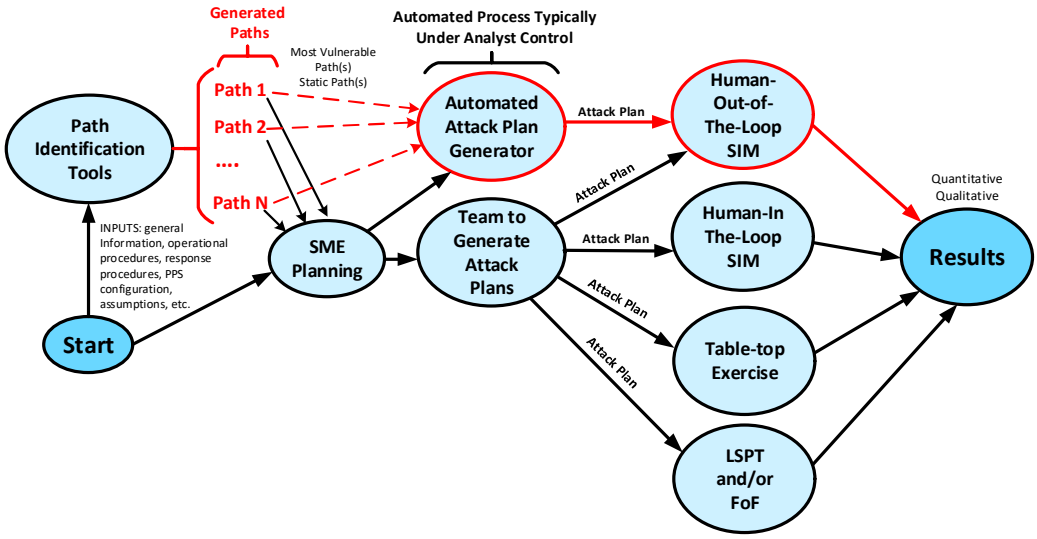



*FIG. 13. Scenario analysis process using VEGA-2*

### 5.8.2. Scenario conditions

— General scenario description: Adversaries will attack the LPNPP with the goal of accessing the control room and completing their sabotage mission;

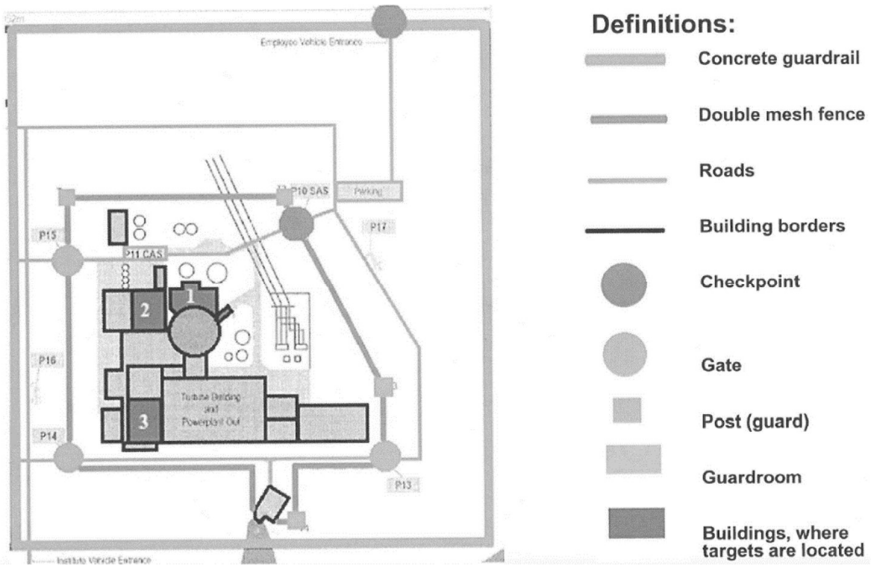
— Design basis threat: Team consisting of four individuals and equipped with guns, explosives (16 kg), available tools, mobile phones, and two vehicles;

— Guard/response force information: Two patrols with two guards per vehicle and a four-person response force. Guards are armed with submachine guns and pistols. Response forces have handcuffs, flashlights, and portable radios. There are two guard vehicles, one for each patrol;

- Attack conditions: Closed condition non-operational (1:00 am); clear weather conditions;
- Other modelling assumptions:
  - The description of LPNPP protected area buildings, objects, and physical barriers lacked information, thus assumptions were made to fill gaps;
  - The interior of the control building was not fully documented as part of the facility description and assumptions were made to fill in the floorplan to include points of movement between floors (stairs), for example;
  - Some buildings included in the general LPNPP facility description lacked necessary modelling information, thus these buildings were not taken into account for modelling purposes;
  - Guard force performance tactics were not defined, nor were patrol routes assigned; assumptions were made for the purpose of analysis in VEGA-2;
  - Passage times through gates at checkpoints were assumed.

### 5.8.3. Modelling information

- Model used to represent the facility: The software utilizes a series of basic inputs such as a graphical representation of the site, description of the PPS elements and a description of the DBT;
- Facility layout features: The site description includes identification of barriers, modes of overcoming elements (i.e. force or stealth) and building and facility entry points (see Fig. 14). Based upon this information in the site description, VEGA-2 identifies all the probable intrusion paths.




*(Courtesy of the Federal Centre of Science and High Technologies (Eleron) of the State Corporation Rosatom)*

*FIG. 14. VEGA-2 2D map of LPNPP*

- Initial conditions for adversaries: Adversaries start at the offsite area;
- Data:
  - Detection: Probabilities of detection were selected from the VEGA-2 database;
  - Delay for barriers: Used values found in the facility description. Any deviations will be noted as part of the analysis;

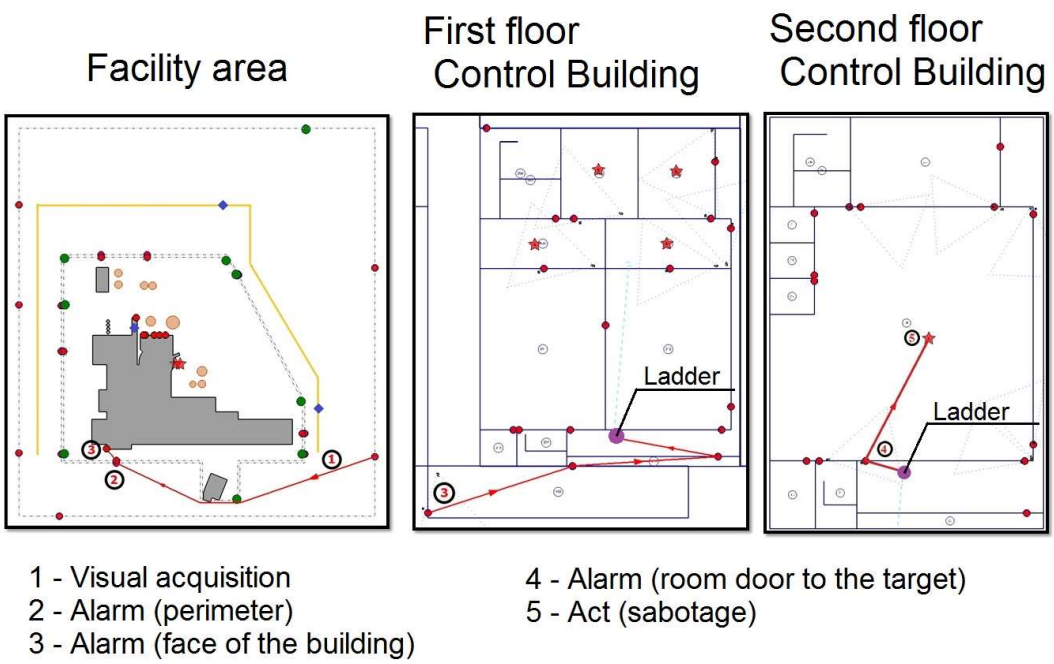
- Movement speeds and/or traversal speeds: Adversary traversal distances included in analysis are minimal to represent that shortest paths will be taken (i.e. adversary will minimize delay);
- Probability of hit/probability of kill values: When an intruder is visually detected, a skirmish is simulated based on the number, armaments and protection means of the parties. $P_H/P_K$ values are thereby determined by VEGA-2 database.

### 5.8.4. Results

#### *5.8.4.1. Scenario description*

The adversary team starts at the limited access area boundary on the facility area map shown below (see Fig. 15). They then move along the route (1-2-3) to a location (3) just to the left of the Control Building. Moving from the same location (3) on the first-floor map, they move to some stairs to the second floor, indicated by (4) and referred to with the label 'ladder.' Once on the second floor the adversaries move to the target location (5) and complete their mission.

#### *5.8.4.2. Scenario representation*




*(Courtesy of the Federal Centre of Science and High Technologies (Eleron) of the State Corporation Rosatom)*

*FIG. 15. Adversary path modelled using VEGA-2*

Quantitative results:

- $P_D$: 0.99
- $P_I$: 0.99
- $P_N$: 0.46

### 5.8.5. VEGA 2 observations

- General:
  - Each path is divided into segments (steps) made by the intruder at a definite time length (time step);

- At each step, the software identifies the PPS response to the intruder actions (generation of the alarms, assessment by CCTV and visual intruder detection by the guards etc.);
- Since the intruder and the protection force speed, delay times at physical barriers, detection by sensors, and weapons effects on their target are probabilistic, multiple simulations are performed using Monte Carlo techniques to produce estimates of performance measures. These simulations are performed independently for every adversary path. The path with the lowest estimate of $P_E$ is reported as the worst-case path;
- If the protection force succeeds the simulation ends, otherwise it is continued till the adversary attack is completed;
- This software allows an assessment of the site protection from both the insider and outsider threats.

— Strengths:
  - Low-level user qualification;
  - Addresses both insider and outsider attacks;
  - Insider analysis takes into account access rights of the particular type of insider;
  - Automatically generates any path and attack plan through a 2D space;
  - Software is capable of modelling multi-story buildings with complex interiors as well as various terrain conditions to include water features;
  - Multiple target locations are analyzed simultaneously;
  - Calculates overall $P_D$, $P_I$, and $P_N$ and $P_E$;
  - During the analysis, users can obtain information on how the adversary defeated each PPS elements, the adversary tools used, detection probability, and identify system effectiveness failure causes and enhancements for improvement.

— Weaknesses:
  - Requires high expertise to properly interpret the output;
  - The program does not take into account sniper support outside site territory;
  - Needs to be adopted for other countries.

## 5.9. SIMAJIN/VANGUARD MODEL AND IMPLEMENTATION

### 5.9.1. Simajin/Vanguard background and overview of software

The Vanguard modelling and simulation tool utilizes the Simajin Application Suite of models to provide quantitative and qualitative analysis of physical security scenarios. The fully automated force-on-force simulation tool enables physical security analysis to model a range of environments with a number of threat vectors and variables. The fully automated representation of human behaviour in a combat environment provides statistically significant results with only limited user interaction. Vanguard allows analysts to conduct risk assessments and quantify how well protective measures will repel, or defeat, a suite of tailored threats; further, it allows for the analysis of countermeasures whether they be personnel, equipment, tactical, technical, or procedure based to reduce risk to manageable levels. Vanguard helps decision makers make truly effective physical security planning decisions that are backed by solid, intelligence-based scenarios, and statistically valid analysis.

— Performance metrics: Simajin/Vanguard is a simulation that calculates $P_I$, $P_N$ and $P_E$;

— Process for use: Tool will generate pathways and SME will enhance pathways to develop a high fidelity, possibly multi team, coordinated attack plan that is then used in a human-out-of-the-loop simulation (see Fig. 16). This attack plan may also be reused for tabletop simulations in which 1-n simulated players are controlled by humans; this can include offensive or defensive players and also allows for users to command subordinates in the command chain.

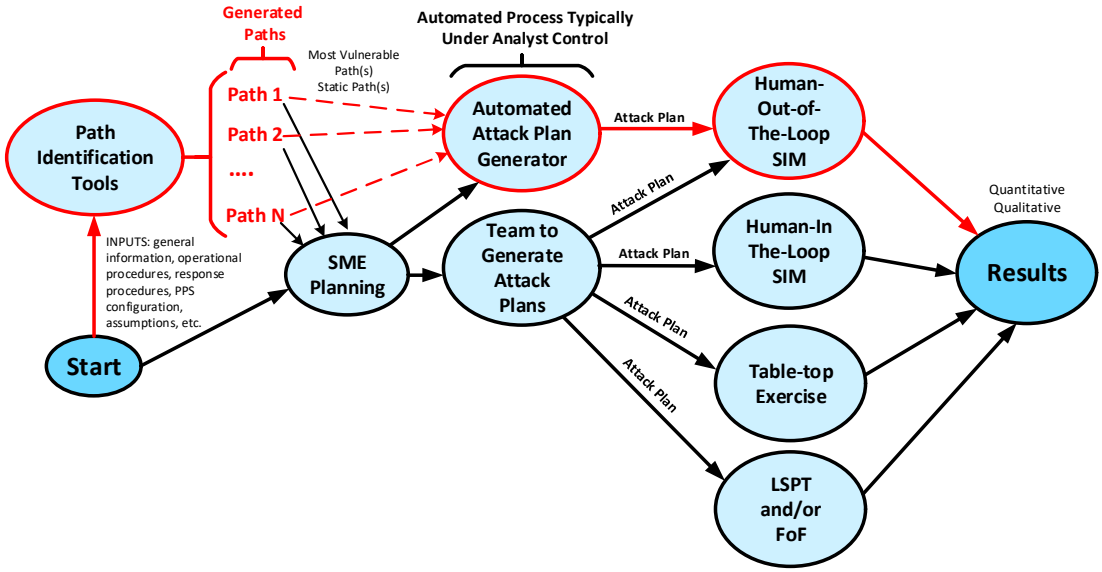



*FIG. 16. Scenario analysis process using Simajin/Vanguard*

### 5.9.2. Scenario conditions

- General scenario description: Adversary use of stealth and/or force to obtain access to target;
- Design basis threat: Defined in hypothetical facility description;
- Adversary assumptions:
  - Design basis threat was for 5-6 people and the case study uses 6 people in each scenario;
  - Adversary were assigned Ak-47 assault rifles and handguns with ammunition as specified in this publication. The DBT also allowed for the use of belt-fed machine guns and precision rifles. For this case study, the M240 machine gun and .50 caliber sniper rifle are selected.
- Response force assumptions:
  - Armed RF were assigned M4 assault rifles and handguns with ammunition as specified in this publication;
  - Towers utilized by RF were assumed to be unprotected based upon visual 3D models, and bullet resistant enclosures (BRE) were placed upon ground to support RF operating gates at the vehicle portals.
- Attack conditions: Closed condition non-operational (1:00 am); good weather conditions;
- Other modelling assumptions:
  - Breach and sabotage times were used from this publication, however, a few barriers were matched to the closest barrier type in delay tables. The sabotage task is assumed to require a single person with a single tool kit in order to complete;
  - For one of the attack plans, the vehicle-borne improvised explosive device (VBIED) utilized at vehicle gate (northwest) was able to neutralize RF personnel in Tower 5. This is an example of using an independent blast analysis to support simulations of combat;
  - The infrared (IR) sensor coverage around the perimeter fence is assumed to completely cover that perimeter. The drawings could be interpreted as showing gaps in coverage at some corners and towers, however, for the case study the infrared sensor coverage is assumed to be complete;
  - According to the publication drawings there are two areas lacking camera coverage along the perimeter. These areas without camera coverage utilized a lower $P_D$ (0.4) associated with breaching with hand tools;

- The scenarios were only executed against the Work Days RF configuration because the off-shift RF configuration only eliminated unarmed guards. Guards listed as unarmed are assumed to have no access to weapons;
- The main buildings of the power plant were modelled with limited interior detail due to lack of data availability. The Control Building was modelled with two floors and basic room structure with limited clutter. Other target locations used an empty shell with the target located on the first floor and only an exterior door to control entry;
- Exterior vehicle gates, P3 and P9, perform badge checks to control access. The adversary use counterfeit badges to pass through these gates undetected;
- The visual models are rotated 90º from the facility description drawings. The facility model used in the case study was rotated to match the publication drawings.

### 5.9.3. Modelling information

- Model used to represent the facility: 3Dimensional model;
- Facility layout features: Analyst creates terrain and buildings;
- Initial conditions for adversaries: Eight unique attack plans were created based upon SME input, in each case adversaries started outside the perimeter fencing; vector of attack included: VBIED, water approach, steam towers and frequently includes a sniper position to the northwest of the facility;
- Data:
  - Detection: probabilities of detection were selected from the facility description;
  - Delay for barriers: Used values found in the facility description. Any deviations were noted as part of the analysis;
  - Movement speeds and/or traversal speeds: Movement speeds for all transport means (foot, vehicle, etc.) are controlled by the user. For this analysis, the protective and adversary forces were prescribed the same nominal 8.0 km per hour (kph) for pre-alarm conditions and 11.2 kph after alarm conditions. They both also had similar scalars for 'sprint', 'hurry' and 'slow' conditions (190%, 150% and 50%, respectively) that might be used on a per task basis as appropriate;
  - Probability of hit/probability of kill values: Used values from an unclassified demonstration database that is based upon SME and open source data.

### 5.9.4. Results

#### *5.9.4.1. Scenario description*

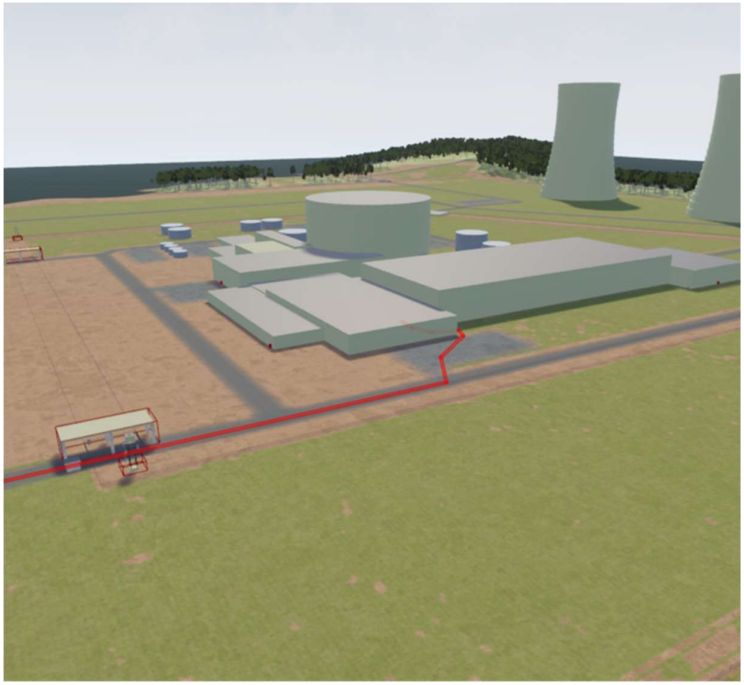
These baseline scenarios included: (1) VBIED, (2) VBEID with Sniper, boat-based intake assault, foot-based aux/intake assault and foot-based steam tower assault. Two variants of the defence were also created; one with nominal weapons and another with a weapons upgrade to the tower positions. The following is a detailed scenario description for the VBEID with sniper pathway.

Two adversary vehicles are positioned west of gate P9 and enter using counterfeit credentials. The lead vehicle is driven by a single person and is carrying an improvised explosive device (50 kg TNT equivalent). This vehicle proceeds to vehicle gate P5, while the second vehicle carrying four people lingers at P9. A sniper is positioned to the west side of the facility and is at least 500 m from towers T5 and T4 and is outside of engagement range for the RF positioned in those towers.

The driver of the lead vehicle detonates the improvised explosive device once they arrive at gate P5. The improvised explosive device is expected to neutralize RF in Tower 5 and destroy the exterior gate at P5. The sniper begins to engage Tower 4 at the point of detonation, and continues to engage responding RF in vehicles and on foot. The second vehicle proceeds to P5 and crashes the remaining gate at the vehicle portal, and then proceeds to parking lot adjacent to the control room building. The vehicle is positioned in front of the control room building entrance to provide cover.

The four adversaries exit the second vehicle and use explosives to breach gate G08. After the breach is completed they proceed upstairs to the control room entrance and breach the door into the control room using explosives. The adversaries then proceed into the control room and attempt to sabotage control room equipment (See Fig. 17).

*5.9.4.2. Scenario representation*



*(Courtesy of RhinoCorps)*

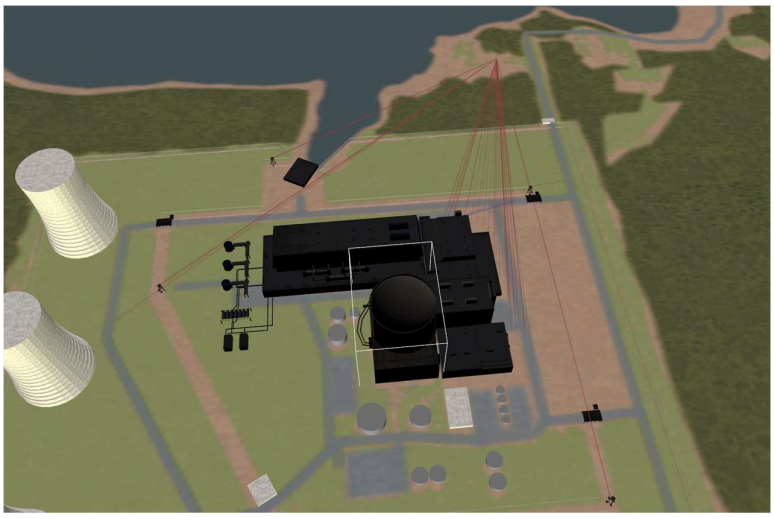
*FIG. 17. Adversary attack path as analyzed in Simajin/Vanguard*

Quantitative results: $P_N = 0.70$

### 5.9.5. Simajin/Vanguard observations

- General:
  - Task lines are determined by the SME flexibility programmed in based upon attack plan;
    - SME driven attack plan with option for tool generated pathways.
  - Vanguard can set rules of engagement for nonviolent interdictions;
  - Automated behaviour in simulation supports team collaboration, movement in complex spaces, use of weapons and tools, communication of status and intelligence information, and operating vehicles;
  - Task model supports rapid construction of attack plans that include complex coordination and contingency planning and can represent real world attack scenarios;
  - AB studies based upon number of defined runs to get statistical sampling;
  - Can account for delay times (requires input into the simulation);
  - Can account for degradation of speed due to terrain and ground cover based upon user-defined graphical areas;
  - Can model health (account for tiredness);
  - Can create task assignments for ‘players’;
  - Speed is affected by load-outs;
  - Need to define anticipatory actions for RF;

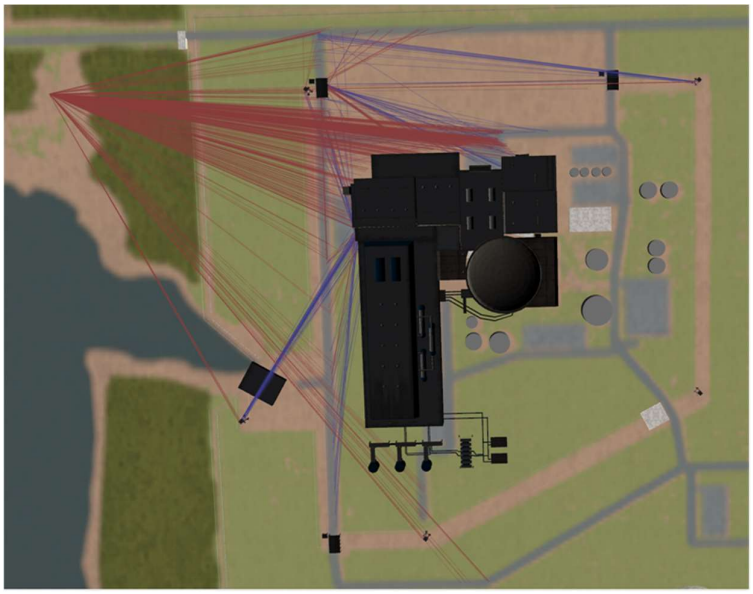
- Does not account for wounds;
- Analysis output report of 'human reportable actions' provides information of individual experiences – timeline based / detection events are logged;
- Standard library format of $P_H/P_K$ and other data (barrier delay) – user is responsible for populating site specific or more accurate data (this generic information is available to an international audience);
- Simulation output – provides report of data for each run (data comes from shot list or event list) RF/ADV deaths, number of shots, target work times, number of adversaries that gained access by layer (everything that is defined in the simulation):
  - Produces 3D Shot Plots© illustrating the origin and termination, and death, for each weapons use in a simulation execution (See Fig. 18);



*(Courtesy of RhinoCorps)*

*FIG. 18. 3D Shot Plot© for individual run*

  - Produces 3D Death Plots© (aggregation death locations and kill shots for a series of simulations using the same simulation initial conditions) (See Fig. 19);



*(Courtesy of RhinoCorps)*

*FIG. 19. 3D top down Death Plot© for study cell of 25 executions*

- Produces Lethal Force Reports© (tabular reports in both detailed and summary form, covering data regarding use of weapons);
- Produces Breach Time Report (documents the obstacle/barrier, time destroyer, breaching player, breaching tool used, and breach duration);
- Produces Player Action Log© (documents by time/player performed key actions, task completion, weapon selection, weapons fire, alarm conditions, and initial observations for each player);
- Produces Personnel Reports (documents post/player names, team ID, training level, weapons, tools and equipment for RF/ADV personnel and vehicles);
- Provides statistical confidence level based upon number of runs conducted;
- Fifteen standard reports and other customizable reports available.

o Can evaluate detection results per layer;

o Line of sight is accounted for;

o Supports use of smoke, use of flares, day/night conditions, weather conditions;

o Usability – need expertise for developing an attack plan;

o Tool specific skills – five-day course to develop proficiency;

o Helps if individual using the tool has a modelling and simulation background.

— Strengths:

o Can distribute runs using multi-servers (i.e. need one station to run on multiple machines) to generate statistical confidence using multiple variables;

o Once defensive posture is developed, it can be used for multiple adversary attack plans.

— Weaknesses:

o High-level of configuration required to run;

- Large overhead for building the defence posture.

o Maintenance and operation requirements – likely needs permanent dedicated staff to maintain proficiency;

o Not necessarily a site-training tool;

o Highly specific tool;

o Each run is based upon a specific adversary plan;

## 5.10. AVERT MODEL AND IMPLEMENTATION

### 5.10.1. AVERT background and overview of software

AVERT is a modelling and simulation tool designed to enable risk-informed decision making based upon quantitative risk assessments. The software analyzes the performance of current facility and security design and interrogates 'what if' scenarios to asses and prioritize future investments and operational procedures. The AVERT tool suite has the ability to model a variety of risks including intentional acts, natural disasters and other disruptive events to address the needs of a variety of operations. AVERT can also be utilized as a human-in-the-loop tool by placing 'destination' targets anywhere in a model.

— Performance metrics: AVERT calculates $P_I$, $P_N$ and $P_E$;

— Process for use: AVERT utilizes a 3D terrain and building model as well as Monte Carlo simulation to visualize adversarial attempts to defeat security and safety systems by determining the pathways of adversaries via a human-out-of-the-loop simulation (see Fig. 20).

The scenario analysis process using AVERT is illustrated in Fig. 20.

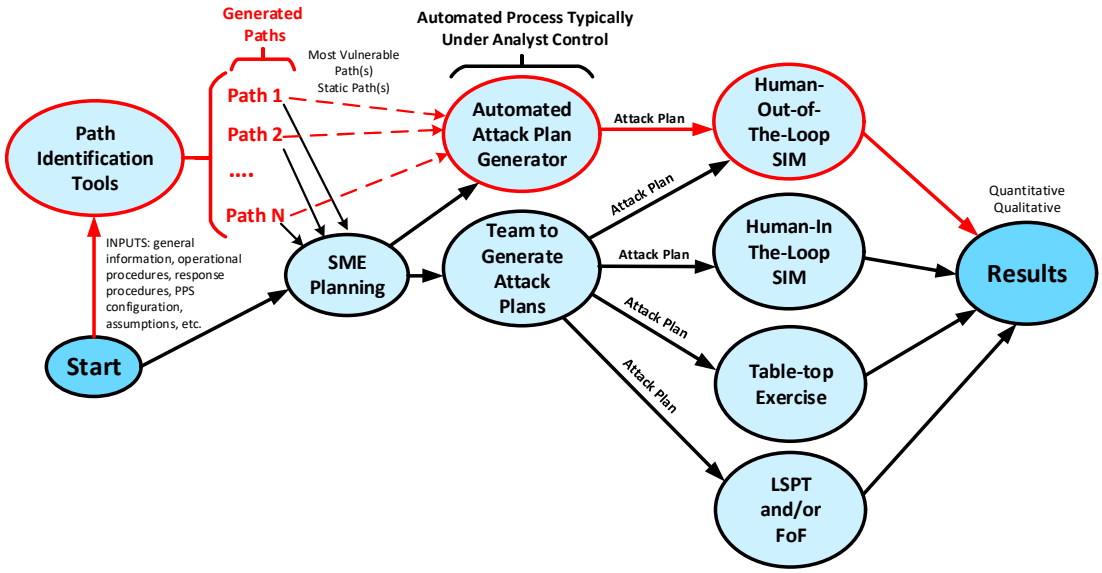



*FIG. 20. Scenario analysis process using AVERT*

### 5.10.2. Scenario conditions

- General scenario description: Adversaries utilize stealth, line of sight blockage, sniper support and explosive breaching to gain access to facility and access vulnerable targets;
- Design basis threat: Six-person adversary team as equipped and defined in the hypothetical facility description;
- Adversary assumptions: None;
- Response force assumptions: Guards, patrols and weapons as defined in hypothetical facility description;
- Attack conditions: Open condition (daytime) – operational hours;
- Other modelling assumptions:
  - Vehicles cannot drive around the full perimeter of the facility, adversary foot travel is required when off roadways;
  - Adversaries will not launch an assault from the water;
  - All fence gaps are properly closed and connected to walls or gates;
  - All facility doors are locked. Guards require keys and adversaries are required to breach based on pathing strategy used;
  - Delay times and equipment are as listed in in hypothetical facility description;
  - BREs are equipped with 7.62mm rated glass and 25.4 x 25.4 cm sliding firing ports;
  - New wall and door barrier was added on the southeast open wall of the intake structure;
  - PA fence is equipped with multiple complimentary sensors as defined in the in hypothetical facility description.

### 5.10.3. Modelling information

- Model used to represent the facility: 3Dimensional;
- Facility layout features: Analyst creates terrain and buildings;.
- Initial condition for Adversaries: Adversaries move from offsite to initiate the attack;

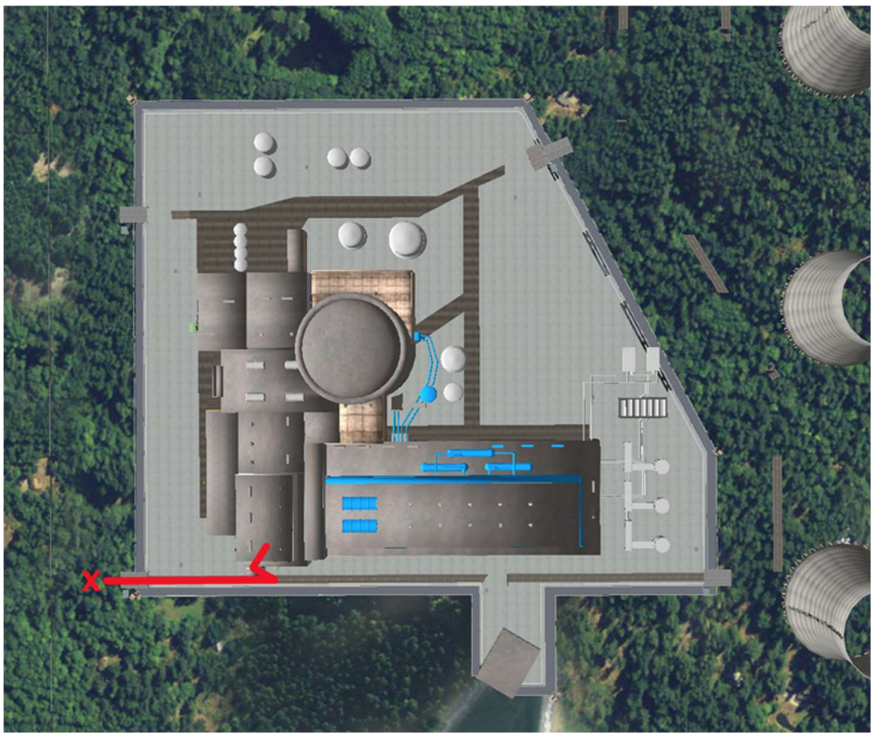
- Data:
  - Detection: $P_D$ for PA fence sensors is 95%;
  - Delay for barriers: Used values found in the facility description. Any deviations noted as part of the analysis;
  - Movement speeds and/or traversal speeds: AVERT uses different speeds for different terrain types. A terrain of 'pavement' was used in these scenarios. Agents 'on foot' utilized a randomly selected traversal speed of 1.11 to 2.24 metres per second (MPS);
  - Probability of hit/probability of kill values: Used open-source $P_H/P_K$ data.

### 5.10.4. Results

#### *5.10.4.1. Scenario description*

Five adversaries use a direct attack to gain entry into the facility with an initial surprise attack killing P5 then completing an explosive breach of the North Gate at T5. The adversaries proceed approximately 205 metres entering the Control Building using the door nearest the outer PA Fence. Adversaries are supported by a single sniper who remains in place and initially concentrates firepower on T5, then attempts to engage any available targets for the duration of the scenario (See Fig. 21).

#### *5.10.4.2. Scenario representation*



*(Courtesy of the ARES Corporation)*

*FIG. 21. Adversary attack path – AVERT*

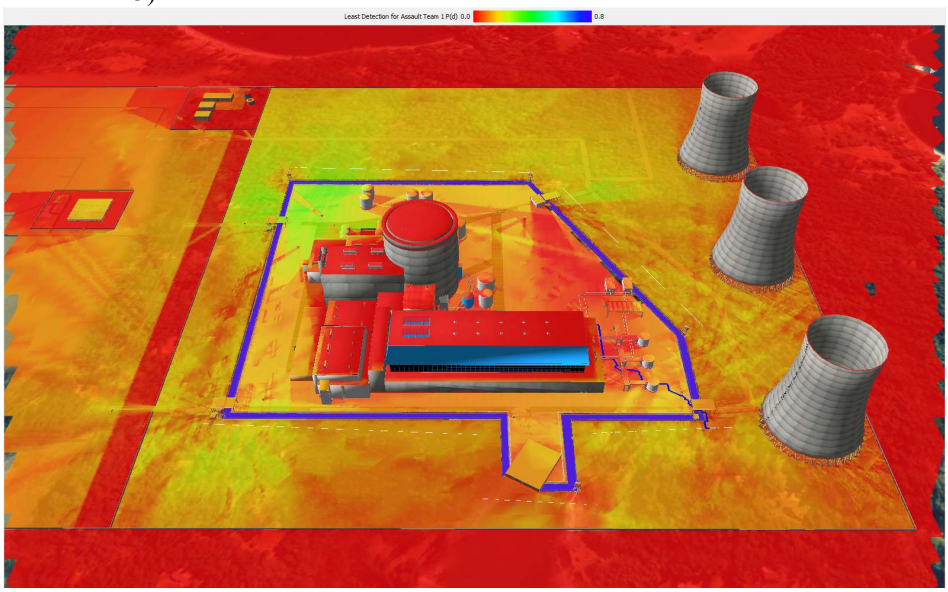
Quantitative results:

- $P_D$: 1.00*
- $P_N$: 1.00*
- $P_E$: 1.00*

* A result of 1.00 may be attributed to the tool rounding up a 0.999 calculated value.

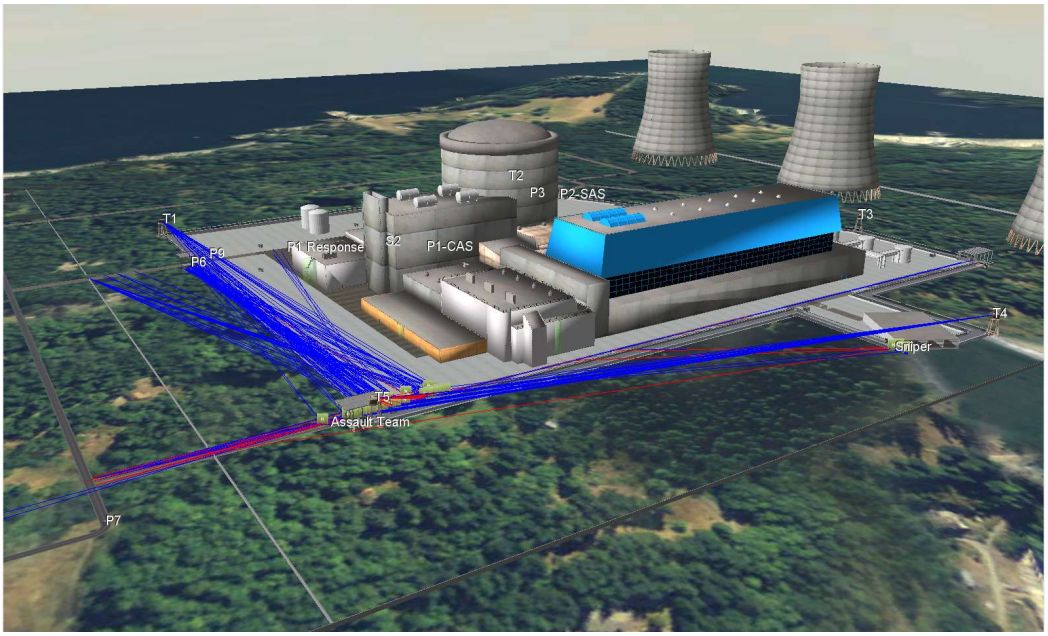
### 5.10.5. AVERT observations

- General:
  - Needs definitive data for population for both adversary and RF;
  - Very close results to the tabletop (TT) exercise;
    - Results comparisons similar ~ 250 runs on Avert;
    - Validation.
  - Sensitivity analysis;
  - Develop scenarios independently to provide validation between both TT exercise and Avert;
  - When combined with other tools, it gives validation;
  - Both tools allow for many iterations to provide input for the next run and subsequent runs;
  - Supports security awareness. Provides great visual of the simulation;
    - Development for better response strategy;
    - Useful for training RF;
    - Demonstrates (follows) response paths for observation by RF.
  - Informs DBT development/identifies worst case scenario for those who create DBT;
  - Avert does not require adversary path prior to population:
    - Can create and analyse all pathways; or
    - Analyse complete facility based on path type.
  - Heat Maps;
    - Visual heat maps of weapons, detectors, guard line of site (eyes on) (See Figs 22-23).




*(Courtesy of the ARES Corporation)*

*FIG. 22. Adversary path to avoid detection heat-map – AVERT*




*(Courtesy of the ARES Corporation)*

*FIG. 23. Adversary to responder neutralization average – AVERT*

- Billboards can display event in time hacks/slices that are equivalent to the time hacks in the TT exercise;
- Does not account for wounded adversaries or reponse force members;
- Able to simulate less lethal, physical arrest (unarmed adversary armour). Allows for RF to adversary verbal commands (protestor) Models nonviolent interdiction;
- High level of configuration and level of details;
- High level of maintenance by SME and site;
  - Dedicated staff required.
- Overhead for initial facility characterization;
- 5-day class to train operator to user level;
- It is estimated to need 6 weeks of training for operator with high experience in security principles, assuming the operator already has 3D geometry computer skills;
- Ability to use random seeds or same seeds to reproduce results;
- Similar to Simajin.

— Strengths:

- Measures many inputs and outputs at the same time… (i.e. TT exercise looks at segments of time and moves from icon to icon in determining actions. The tool allows all icons to act/react during time segment);
- Visual tool (only tool with heat map view);
- Library of values (single file you can import into Avert);
- Comes with default values for data base/data input;
- Ability to use random seeds or same seeds to reproduce results;

- Weaknesses:
  - Requires a high expertise to properly interpret the output;
  - Only as good as data used for populations;
    - RF procedures, adversary task times, DBT, etc.;
    - Requires intellectual honesty.

## 5.11 TABLETOP METHOD AND IMPLEMENTATION

### 5.11.1. Tabletop background and overview of method

A TT exercise is an analysis methodology intended to generate discussion of various issues regarding a particular facility or transport configuration. TT exercises have many benefits. They can be used to enhance general awareness of all parties responsible for the protection of assets or response to events. TT exercises are used to validate security plans and procedures, tactical response plans, rehearse planned changes or upgrades, and assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined security incident. TT exercises are an excellent tool to facilitate nuclear security system or programme understanding. This method identifies strengths as well as areas for improvement. During a TT exercise, stakeholders are encouraged to discuss issues in depth and collaboratively examine areas of concern in order to solve problems. The effectiveness of a TT exercise is derived from the energetic involvement of participants and their assessment of recommended revisions to current policies, procedures, and plans.

TT exercises can range from basic to complex depending on the goal of the simulation and the desired accuracy in the outcomes. In a basic TT exercise, the goals are typically higher level in nature to discover obvious issues or to promote common understanding of the processes and plans to all stakeholders. Participants apply their knowledge and skills to a list of issues identified by stakeholders, site/transport management and agency or national oversight organizations. The issues are systematically presented by a facilitator where the problems are discussed as a group who then simulate current methods for protection to determine if the issue(s) are factual and where the group could introduce change to improve the system. Using the TT exercise, the group 'upgrades' the system from the baseline then carries out additional simulations to evaluate the upgraded systems response. The results and upgrades are documented for more analysis as needed. Basic TT exercises can range from 4 hours (baseline) to 16 hours (or more) for a single scenario depending on how well the group works together and how many simulations are needed to meet the groups' goals.

In more advanced TT exercises, the level of detail in the characterization process as well as the documentation requirements and validation of results process are more disciplined and precise. From an evaluation perspective, there are literally unlimited ways to evaluate the nuclear security programme and its people's knowledge. Often the more advanced TT exercises are needed when the results would need to yield high confidence that the outcomes of the analysis are accurate. In many cases, individual actions of the protective system would need to be validated as accurate before the simulation can proceed to the next step. These more complex versions utilize a very accurate and detailed 3D scaled model. The 3D models help confirm player actions, movements and response timelines. Before the simulation begins, it is common that the facilitator confirms the physical locations of response forces and the time required to respond to a specific event from those locations. Response times are confirmed either by the site's test data or by asking the 'real' players to perform an activity and collecting data on their actions.

During a TT exercise, all participants are encouraged to contribute to the discussion and be reminded that they are making decisions in a no-fault environment. Effective TT exercise facilitation is critical to keeping participants focused on exercise objectives and associated capability targets. Further, all TT exercise methods rely heavily on the expert judgement of the SME and the integrity of all persons involved to conduct the analysis based on the facts of the actual facility/transport system or on the defined parameters of an upgrade. The facilitator is ultimately responsible for ensuring the best possible outcome.

The scenario analysis process using a tabletop is illustrated in Fig. 24.

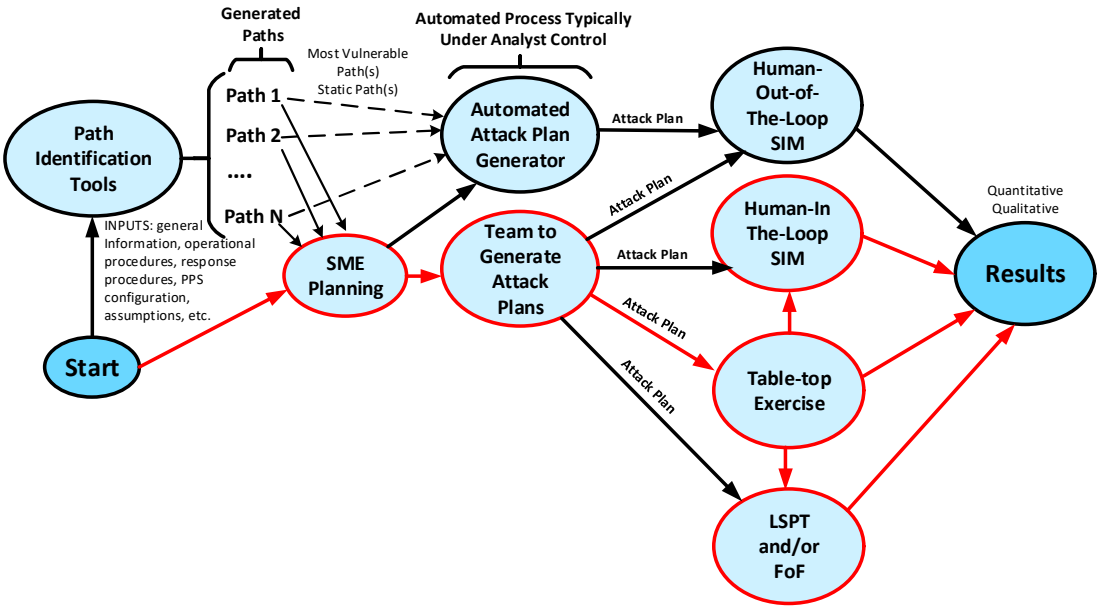



*FIG. 24. Scenario analysis process overview for tabletops*

### 5.11.2. Scenario conditions

- Adversary Scenario Conditions:
  - General scenario description: Adversary use of stealth and/or force to obtain access to target;
  - Design basis threat: Six-person adversary team as equipped and defined in the hypothetical facility description;
  - Adversary assumptions: None;
  - Response force assumptions: Guards, patrols and weapons as defined in in hypothetical facility description;
  - Attack conditions: Closed condition non-operational (1:00 am); good weather conditions;
  - Other modelling assumptions: None.

### 5.11.3. Modelling information

- Model used to represent the facility: 2D map;
- Facility layout features: Analyst creates terrain and buildings;
- Initial condition for adversaries: Adversaries move from offsite to initiate the attack;
- Data:
  - Detection: $P_D$ for PA fence sensors is 95%;
  - Delay for barriers: Used values found in the facility description. Any deviations noted as part of the analysis;
  - Movement speeds and/or traversal speeds: based upon distance-based look-up tables;
  - Probability of hit/probability of kill values: based upon $P_H/P_K$ look-up tables;

### 5.11.4. Results

#### *5.11.4.1 Scenario description*

The adversary team approaches the facility perimeter wall surrounding the LPNPP. Five members climb the outer wall, and await the approach of the RF patrol vehicle. As the RF vehicle approaches, the adversary team engages and neutralizes the patrol. The team then moves to breach the PIDAS and once complete, the team moves into the PA and proceeds to the building housing the control room. One adversary approaches the exterior facility door and breaches explosively, while the other adversary team members provide cover. Upon breach completion, two adversaries enter the building interior and proceed to the control room. Upon entering the control room, they proceed with their sabotage task.

#### *5.11.4.2 Scenario representation*

Figure 25 depicts the facility map used as part of the TT exercise with indications of the starting position for both the adversary and response teams.

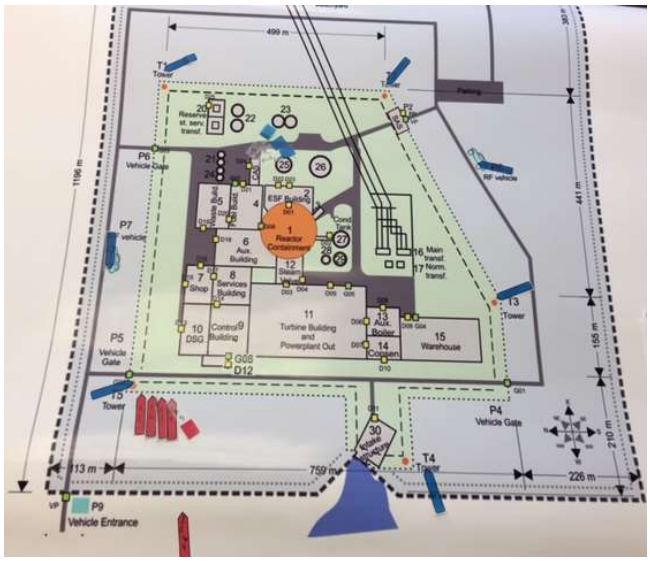



*FIG. 25. Tabletop image – time zero*

Table 4 details the step-by-step events for each predefined measures of time for the scenario previously described.

TABLE 4. TABLETOP RESULTS

| Time (seconds) | Marker ID | Marker Action | Event Details |
|---|---|---|---|
| 00 | A1 | Sets breaching charge and detonates | Creates breach in perimeter fence |
| | | Sets up for second breach | |
| | | Alarm on G02 | |
| | | P9 radios explosion | |
| 10 | A2 | Move to engage | None |
| | A3 | Move to engage | None |
| | A4 | Move to engage | None |
| | A5 | Remain in place | None |
| | CAS | Radio Communication – maintain positions and begin assessment | |
| 20 | A3 | Engages P7A | Kill |
| | A4 | Engages P7B | Miss/Suppressed |
| | T5 | Sees man | |
| | T4 | Confirms explosion | |
| | S2 | Muster | |
| | PIA | Muster | |
| | P2C | Muster | |
| | P8 | Move to interior | |
| 30 | A3 | Engages P7B | Kill |
| | A2 | Engages T1 | Miss (600 metres) |
| | A5 | Engages T4 | Miss (550 metres) |
| | T1 | Engages A2 | Miss (600 metres) |
| | T4 | Engages A5 | Miss (550 m) |
| | P8 | Moves north | Fast |
| 40 | A1 | Detonates second breaching charge, Moves south fast | |
| | A2 | Moves south fast | |
| | A3 | Moves south fast | |
| | A4 | Moves south fast | |
| | A5 | Moves south fast | |
| | CAS | Off-site call | |
| | P8 | Moves 200 metres N | |
| | T1 | Engages A1 | Miss (550 m) |
| | T4 | Engages A1 | Kill |
| 50 | A6 | Engages T5 | KIA (300 m) |
| | A2 | Moves south fast | |
| | A3 | Moves south 26 metres | |
| | A4 | Moves south 26 metres | |
| | A5 | Moves south 26 metres | |
| | P8 | Moves 266 metres north | |
| | T1 | Engages A2 | Kill |

TABLE 4. TABLETOP RESULTS (CONT.)

| Time (seconds) | Marker ID | Marker Action | Event Details |
|---|---|---|---|
| 60 | A3 | Moves south 26 metres | |
| | A4 | Moves south 26 metres | |
| | A5 | Moves south 26 metres | |
| | P8 | Moves 266 metres north | |
| | T1 | Engages A4 | Miss (600 m) |
| | T4 | Engages A5 | Miss (450 m) |
| 70 | A3 | Moves south 26 metres | |
| | A4 | Moves south 26 metres | |
| | A5 | Moves south 26 metres | |
| | P8 | Moves 200 metres west | |
| | T4 | Engages A5 | Miss (300 m) |
| 80 | A3 | Engage T4 | Miss |
| | A4 | Engage T4 | Miss |
| | A5 | Engage T4 | Miss |
| | T4 | Engages A5 | Miss (300 metres) |
| | P8 | Moves to P6 to open gate | |
| | S2 | Move 26 metres north | |
| | PIA | Move 26 metres north | |
| | PI6 | Move 26 metres north | |
| 90 | A3 | Moves fast in cover | |
| | A4 | Moves fast in cover | |
| | A5 | Moves fast in cover | |
| | S2 | Move 26 metres north | |
| | PIA | Move 26 metres north | |
| | PI6 | Move 26 metres north | |
| 100 | A3 | Moves south 26 metres | |
| | A4 | Moves south 26 metres | |
| | A5 | Moves south 26 metres | |
| | T4 | Engages A5 | Kill |
| | S2 | Move 26 metres north | |
| | PIA | Move 26 metres north | |
| | PI6 | Move 26 metres north | |
| 110 | A3 | Moves south 26 metres | |
| | A4 | Engages T4 | Miss |
| | T4 | Engages A3 | Miss |
| | S2 | Move 26 metres north | |
| | PIA | Move 26 metres north | |
| | PI6 | Move 26 metres north | |
| 120 | A3 | Engages T4 | Miss |
| | A4 | Engages T4 | Miss |
| | T4 | Engages A3 | Kill |
| 130 | A4 | Engages T4 | Miss |
| | T4 | Engages A4 | Kill |

Quantitative Results: $P_E$: Win

### 5.11.5. Tabletop observations

Tabletop exercises are excellent tools for training and for assessments and have inherent advantages and disadvantages, some of which have been captured below:

- Strengths:
  - Requires modest commitment in terms of time, cost, and resources;
  - Effective method for reviewing situational command and control;
  - Effective method for reviewing plans, procedures, and policies by revealing shortcomings in documentation;
  - Familiarize key personnel with their roles and responsibilities, procedures, and other emergency response elements;
  - Focuses the evaluation team within a specific situation/scenario;
  - Identifies any issues, challenges and / or assumptions;
  - Identify resources necessary to overcome any issues, challenges and / or assumptions.

- Weaknesses:
  - Does not provide insight into probability of detection or assessment;
  - Method only provides qualitative information of overall scenario result;
  - Only one scenario can be evaluated at a time, thus does not provide insight in terms of trends.

# 6. OVERALL ASSESSMENT OF SECURITY ASSESSMENT METHODS

## 6.1. ASSESSMENT TOOL SUMMARY

The security assessment of the LPNPP was conducted using a range of analysis tools, many of which are available to the international community. Analytical tools utilized in this report included a range of path analysis and computer simulations.

Path analysis tools utilized included SAVI, ProEv and VISA. These tools create a pathway analysis to determine the ordered series of potential adversary actions and calculate the probability of interruption for the most vulnerable paths. Path analysis is based on two sub-analyses: timely detection and overt attack analysis. Timely detection analysis determines whether $P_I$ is adequate along all adversary paths. Overt attack analyses determines whether there are paths that are susceptible to overt attacks that reduce $P_N$. Both analyses focus on adversary paths within a stated DBT and account for facility response requirements. Path analysis tools are useful because they provide insight into the performance of a system across a spectrum of possible paths and scenarios. Path analysis tools such as SAVI and ProEv only provide $P_I$ values, thus a neutralization tool is needed in conjunction in order to determine $P_E$. For detailed and sophisticated adversary scenarios that could include diversion, SAVI and ProEv may not be appropriate.

Computer simulation tools utilized included STAGE, VEGA-2, Simajin, and AVERT some of which are capable of path analysis (such as VEGA-2 and AVERT) and neutralization analysis using simulated adversary attack scenarios. These tools are sophisticated enough that they are capable of running hundreds of engagement iterations, thereby greatly increasing the amount of data that the analyst can review; on the other hand, such tools generally require more training and logistical support than the path analysis tools. In terms of the analysis, tool results were not expected to be comparable due to differences in assumed adversary team size, ranging from four (VEGA-2) to six (Simajin) individuals. Despite these differences, in most instances, the likelihood of adversary neutralization was high due to the fact that the response force outnumbered the adversary team. Further, once in the control room, the adversary team had a sabotage task time of 1200 seconds (1340 seconds overall), considerably larger than that of

the RFT, thereby ensuring a high likelihood for an adversary/response engagement. As such, the results of overall PPS effectiveness were comparable despite these differences.

One other analysis method was applied based on using TT exercises which simulate the adversary attack manually. A TT exercise was conducted to compare and contrast the differences between that method and the AVERT computer simulation, using the attack plan identified by AVERT and the same scenario assumptions so as to evaluate how similar the results were for identical assumptions. The TT exercise methodology result for PPS effectiveness was comparable with the AVERT end result.

TABLE 5. ANALYSIS METHODS SUMMARY TABLE

| | $P_E$ | $P_D$ | $P_I$ | $P_N$ |
|---|---|---|---|---|
| Tabletop | Win | | | |
| VISA | High | | | |
| SAVI | | | 0.49 | |
| ProEv | | | 0.99 | |
| STAGE | Win | | | 0.70 |
| VEGA-2 | Win | 0.99 | 0.99 | 0.46 |
| Simajin | Win | | | 0.70 |
| AVERT | Win | 1.00* | 1.00* | 1.00* |

* A result of 1.00 may be attributed to the tool rounding up a 0.999 calculated value.

As shown in Table 5, the tools evaluated did not produce the same numerical result; however, the tools demonstrated generally similar outcomes in the upper range for system effectiveness for the specific adversary and scenario class analyzed for the hypothetical LNNPP. The numerical outcomes differences may be attributed to variations in modelling assumptions and virtual environment conditions associated with each tool. For example, some tools used simple two-dimensional maps while other tools used three-dimensional environments where fields of view, field of fire, and building obstructions may have affected final numerical values. Additionally, the lower SAVI results may be attributed to the tool evaluating the shortest distances, least detection, least assessment along an assumed normalized pathway in determining the probability of interruption. The VEGA-2 result for probability of neutralization may be attributed to modelling assumptions and model-specific combat engagement differences along the specific path analyzed as compared to the other tools. The AVERT result of 1.00 for all probabilities may be attributed to tool rounding up the 0.999 calculated value since an assurance of a 100 percent system effectiveness is generally never assumed.

## 6.2. EVALUATION AND REPORTING

The activities included in the key step ‘conducting the assessment’ aims at providing input to the step ‘overall assessment of security’. The main task now is to summarize all relevant evidence in a comprehensive manner, to be able to answer whether security requirements are met.

The security requirements may be prescriptive or performance-based or a combination of the two. For the hypothetical facility, the prescriptive requirements are not very specific, used only to design physical protection according to IAEA guidelines. The performance-based requirement is to prevent high radiological consequence for malicious acts included in the threat definition.

Below are example assessment evaluation and reporting statements based on this LPNPP case study analysis.

## 6.3. PRESCRIPTIVE REQUIREMENTS

For the LPNPP hypothetical facility, the performance-based requirements were the focus. Although it was stated in Section 3.2 that the PPS was developed to address IAEA prescriptive recommendations, no explicit assessment of the conformance with them was conducted. Therefore, it is not possible to state if the LPNPP meets the PPS prescriptive requirements.

## 6.4. PERFORMANCE-BASED REQUIREMENTS

For the LPNPP hypothetical facility, a number of assessment tools and methods were compared. To be able to answer the question if the performance-based requirement has been met, the tool/method would need to provide a result in a metric that can be compared with an appropriate acceptance criterion. However, since this case study does not define a performance-based metric or criteria to assess the analysis results against, no claim can be made if the protection is acceptable or not. Instead, performance measures were estimated and recorded for the range of tools and methods discussed in this publication based upon the individually described scenarios. Output examples for several assessment models presented in Table 5 reflect quantitative ranges from 0.49 – 1.00 and qualitative terms such as high/win to describe PPS effectiveness. Additionally, since only a limited adversary scenario class was evaluated for sabotage, no claim can be made as to the overall protection effectiveness against the range of scenarios that could be performed by the DBT defined threat. A potential security issue has been identified. Refs [6, 7] identify the performance-based requirements to deter, detect, delay, and respond to unauthorized access to NMs. These publications served as a basis to evaluate the effectiveness of the protection measures at the LPNPP facility.

## 6.5. COMBINED ASSESSMENT

Some issues were identified for the LPNPP hypothetical facility.

For the first issue, the evaluation did not include an assessment to determine if the LPNPP met the IAEA prescriptive requirements. It is not recommended to conduct an assessment or to identify modifications without first ensuring the PPS design meets the minimum requirements. It is highly advised that an additional evaluation of the PPS design be conducted to determine if the prescriptive requirements are met.

Due to the limitations of this case study, a single adversary scenario class for sabotage was conducted. A comprehensive assessment would be required to confidently determine if the LPNPP PPS effectiveness against the full range of DBT adversary capabilities.

Another observation is the lack of a regulatory standard or criteria to establish PPS effectiveness values. As discussed in Section 6.1, the assessment methods produced both quantitative and qualitative values but without a defined performance-based metric or criteria, no final determination can be made as to the LPNPP overall protection effectiveness against the full range of DBT defined threat.

## 6.6. UNCERTAINTIES AND ASSUMPTIONS

Since the LPNPP is a hypothetical facility based on recommended requirements outlined in Ref. [6], the assumptions varied by assessment method input requirement and are documented in Section 5. As a result of evaluating a very limited number of adversary scenarios, other types of adversary attack tactics were not evaluated resulting in a high uncertainty for confidently determining the effectiveness of the LPNPP PPS against the full range of DBT adversary capabilities. Further, the quality of performance data, such as delay and response times, was very limited because this is not an actual facility.

# Appendix I

## LONE PINE NUCLEAR POWER PLANT HYPOTHETICAL FACILITY SECURITY PLAN

### I.1. INTRODUCTION

The following information represents the hypothetical facility information for the LPNPP. Note that not all details provided within this section were used to conduct the analysis documented in Section 5. Rather, the information provided reflects the level of detail needed to properly characterize a facility and provide for reference purposes.

#### I.1.1. Facility overview

The LPNPP consists of one reactor unit. The unit is equipped with a nuclear steam unit that employs a pressurized water reactor and a once-through cooling system. The LPNPP generating system is a dual-cycle plant consisting of a closed, pressurized, reactor coolant system (primary) and a separate power conversion system (secondary) for the generation of electricity. The use of a dual cycle keeps the potentially radioactive reactor coolant separate from the main turbine, condenser, and other secondary plant components. The LPNPP has a generating capacity of 1,150 megawatts of electrical power.

#### I.1.2. Facility location

The LPNPP is located in the country of Lagassi (see Fig. I.1. and I.2) It is 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 defence 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 neighbouring states and other foreign powers. Ref. [9].

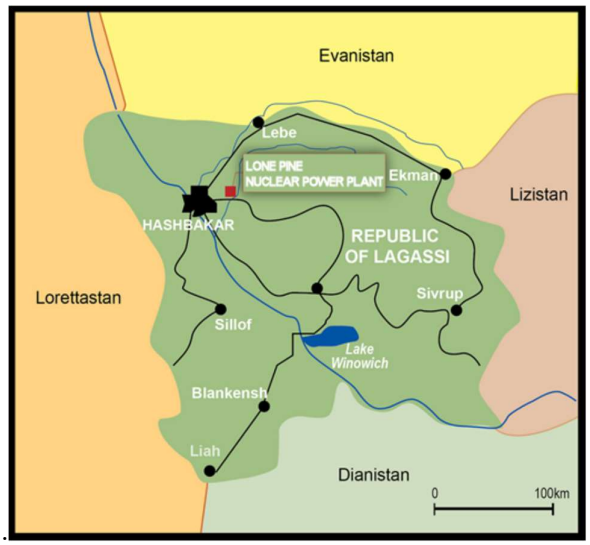



*FIG. I.1. Country map of Lagassi*

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.

*FIG. I.2. Hashbakar city map*

### *I.1.2.1. Environmental and physical conditions*

The LPNPP is a hypothetical nuclear power plant. It is located just to the east of the Lagassi Institute of Medicine and Physics facility on a tributary of the Upper Lagassi River. The LNPP was built in 1972 to produce 1150 Megawatts electrical for the Lagassi power grid. The LPNPP is located in the Republic of Lagassi, approximately 30 km east of Hashbakar.

- Topography
  - LNPP 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.

The Lone Pine NPP facility site plan is shown in Fig. I.3.

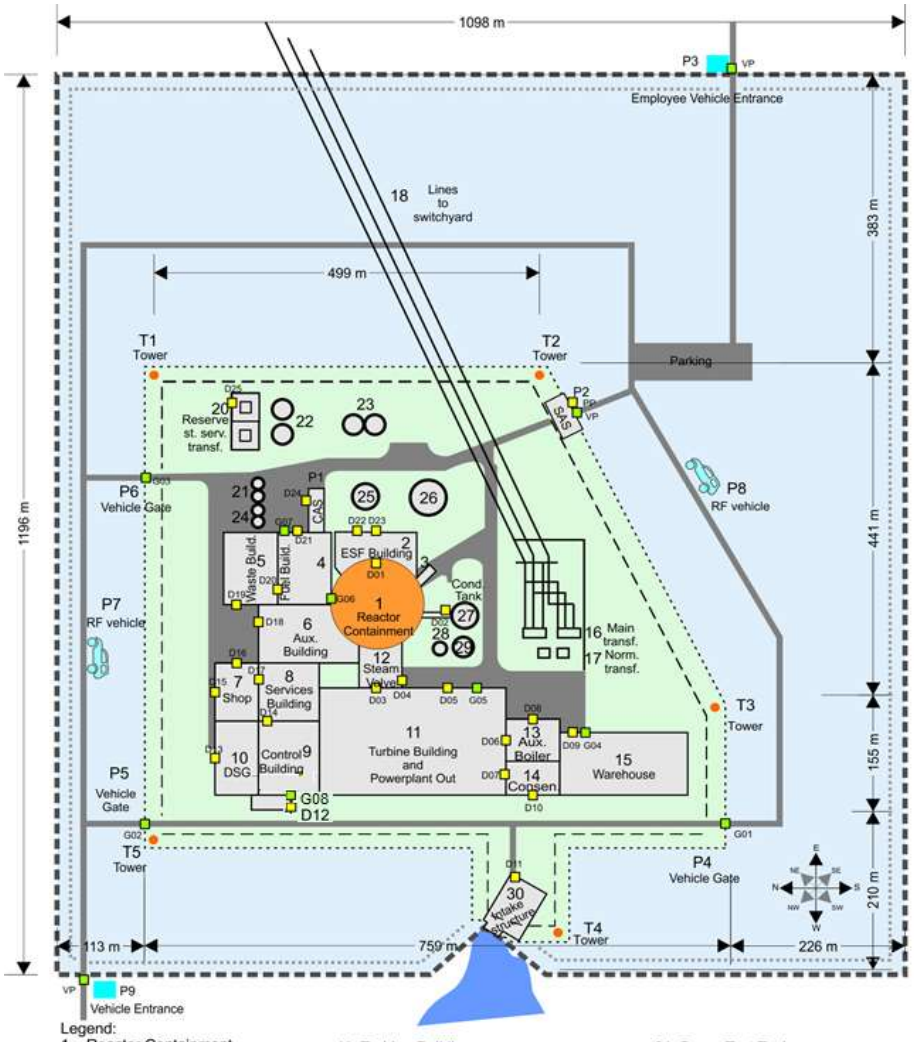



*FIG. I.3. Facility site plan*

To aid in visualizing the layout of the Lone Pine NPP, Fig. I.4 provides a three-dimensional presentation of the site layout looking from the Northwest and Southeast. This drawing shows the major features of the plant.

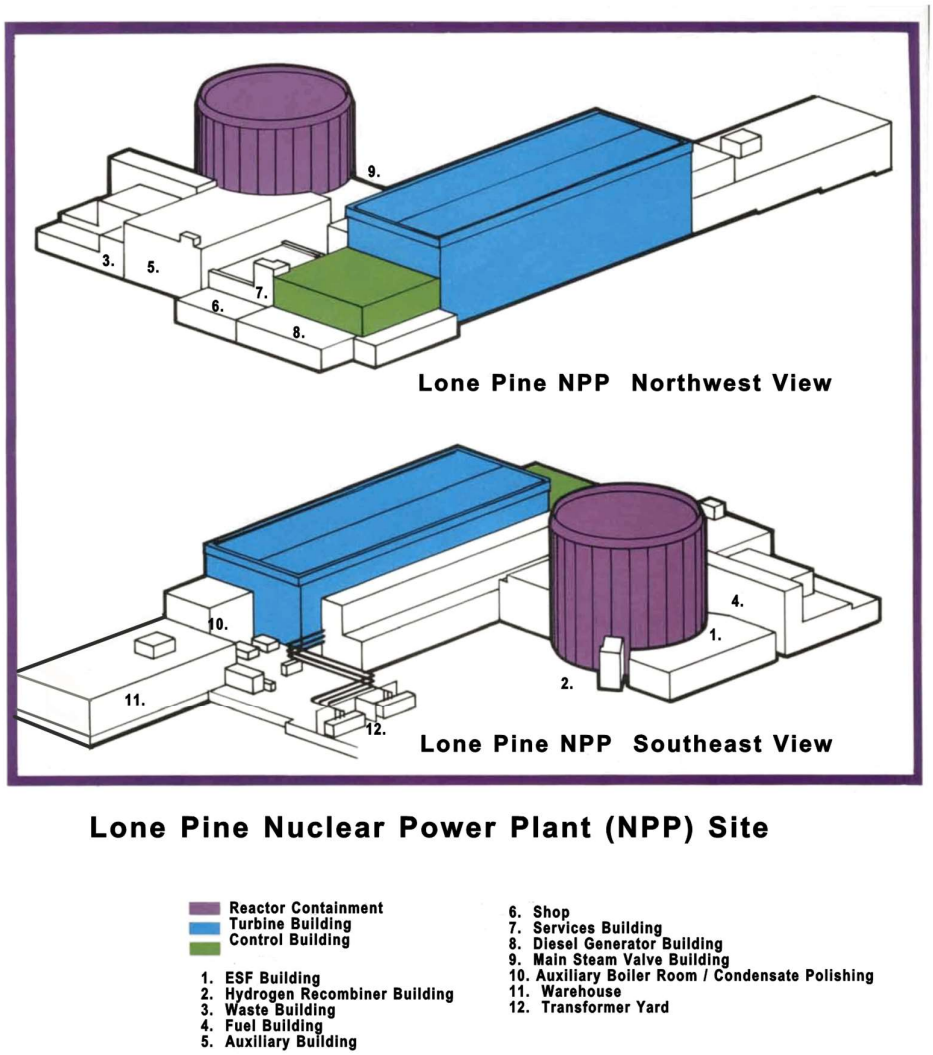



*FIG. I.4. Facility 3D plan*

### I.1.3. PPS description

There are three main areas in the LPNPP — the limited access area, the protected area and the vital area.

#### *I.1.3.1. Limited access area*

The LPNPP limited access area is surrounded by an unalarmed 2.5m high chain link fence with outriggers to keep out trespassers. Adjacent to the exterior concrete fence is a concrete block vehicle barrier designed to withstand the impact of vehicles weighting up to 40 tons, travelling at speed up to 40 km per hour. The terrain in the limited access area is mainly desert sand, except marked asphalt roads.

There are two entrances into the area, P3 employee vehicle entrance in the northern part of the area and the P9 vehicle entrance in the southern part. Both entrances are equipped with a road stop active barrier, designed to withstand the impact of vehicles weighing up to 40 tons, travelling at speed up to 40 km per hour from the inner as well as the outer side of the gate. The inner vehicle gates are equipped with a BMS.

#### *I.1.3.2. Protected area*

The LPNPP protected area is surrounded by two 2.5m high chain-link mesh fences with outriggers 4 mm x 50 mm mesh. There is an intrusion detection system between the two fences. The sensors in the isolation zone consist of active infra-red sensor in a self-protecting pattern and are in close proximity to

the inner fence vibration sensor to be considered a complimentary sensor configuration. Alarm assessment is provided by closed-circuit television (CCTV) cameras, augmented by visual assessment by guards in 5 towers on the protected area perimeter (T1-T5). The guard towers are small arms resistant. There is lighting around the inner perimeter in the protected area side of the isolation zone. Lights are distributed within 50 metres from each other. There is one main personnel and vehicle entrance to the protected area - P2 (secondary alarm station - SAS) and three other vehicle gates P4-P6. Vehicle gates are equipped with high security padlocks and a BMS. When not in use, the vehicle gate areas are protected by the active infrared sensors. See Fig. I.5 for the layout of the facility physical protection system.

#### *I.1.3.3. Vital area*

The LPNPP vital area exterior walls and roof are 30 cm thick reinforced concrete (210 kg/cm2 one layer, No. 4 rebar, 15-cm on centre) to provide some resistance to stand-off attack. The floors and ceilings are 20 cm thick reinforced with one layer of No. 5 rebar 15-cm x 15-cm on centre. All vital area interior walls are 10 cm thick, reinforced concrete with one layer, 6.4-mm dia., 15-cm x 15-cm mesh. Personnel and vehicle gate access is mainly through 0.75 cm steel-plate water tight doors. Whenever personnel are present in the vital areas, they are under CCTV surveillance for timely detection of unauthorized actions. All vital area equipment locations are under video motion alarm coverage to ensure timely detection of tampering or interference.

### I.1.4. Access control

#### *I.1.4.1. Limited access area - access control*

On entry to the limited access area, the vehicle's driver drives the vehicle up to the outer gate. The driver can push an electric buzzer at the gate to alert the guard. The sensor is put in 'access' mode and then the guard at P3 (or P9) unlocks and opens the outer gate. The vehicle enters the portal and then the driver leaves the vehicle and goes back outside. The guard shuts and locks the outer vehicle gate. The driver enters the pedestrian portal, is subjected to the same checks as all personnel entering the protected area, and remains in the portal until the vehicle has been inspected. The guard inspects the vehicle for prohibited items while it is still in the vehicle portal. When the inspection is complete the guard unlocks and opens the inner vehicle gate. The driver exits the personnel portal, re-enters the vehicle, and drives into the area. The inner gate is closed and locked by the guard. The gate BMS is put in 'active' mode.

On exit from the limited access area, the process is reversed. The vehicle's driver drives the vehicle up to the inner gate. The driver may push an electric buzzer at the gate to alert the guard. The gate BMS is put in 'access' mode and the guard at P3 (or P9) unlocks and opens the inner gate. The vehicle enters the portal and then the driver leaves the vehicle and goes back inside the area. The guard shuts and locks the inner vehicle gate. The driver enters the pedestrian portal, is subjected to the same checks as all personnel leaving the protected area, and remains in the portal until the vehicle has been inspected. The guard visually inspects the vehicle for unauthorized material while it is still in the vehicle portal. When the inspection is complete, the guard unlocks and opens the outer vehicle gate. The driver exits the personnel portal, re-enters the vehicle, and proceeds. The guard shuts and locks the outer gate. The gate BMS is put in 'active' mode.

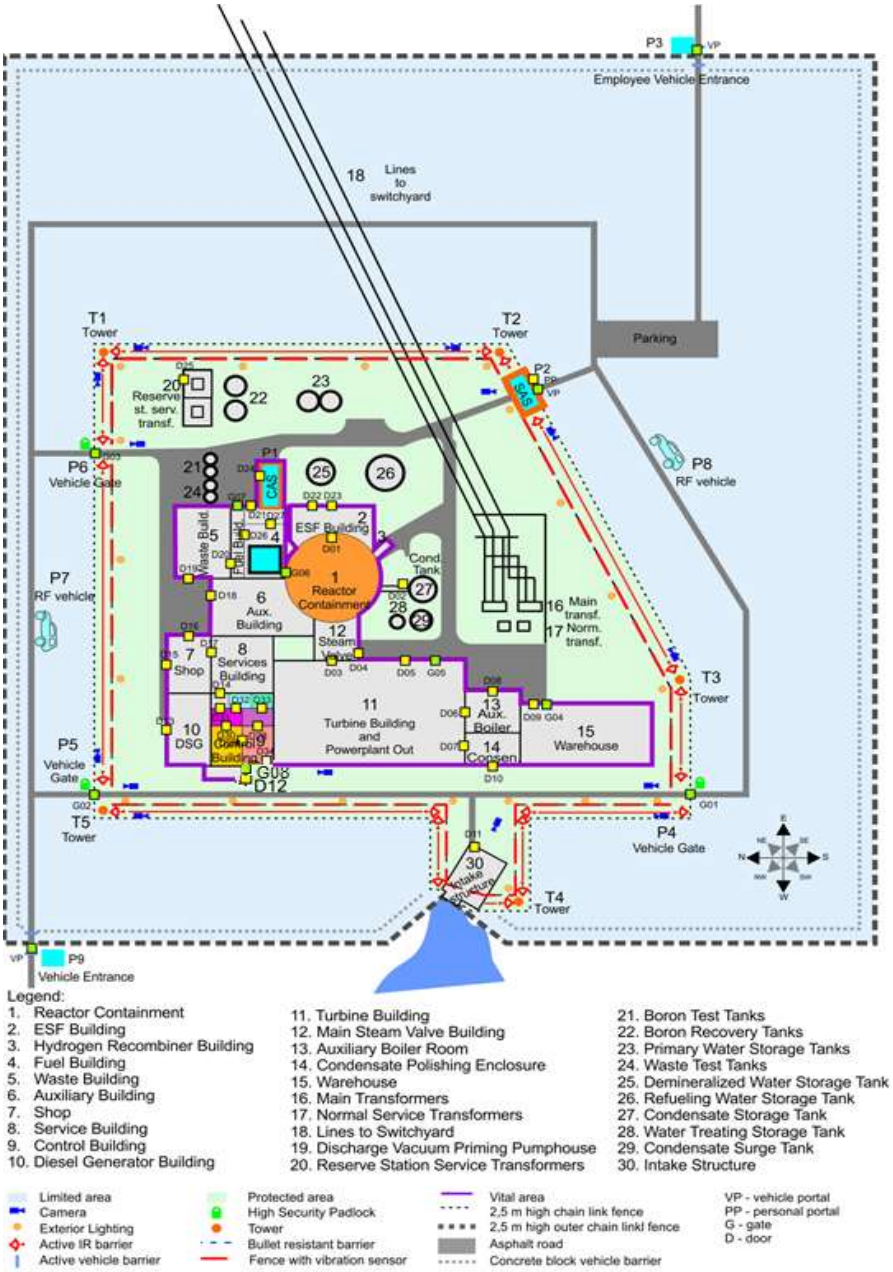



*FIG. I.5. Facility PPS layout*

### *I.1.4.2. Protected area — access control*

All access points are secured and fitted with alarms. Vehicles, persons, and packages entering the protected area are subject to search for detections and prevention of unauthorized access and of the introduction of prohibited items. Entry of vehicles into the protected area are strictly minimized and limited to designated parking areas. Only authorized persons should have access to the protected area and should be kept to a minimum. Authorized unescorted access to the protected area is limited to authorized personnel. Personnel how are not cleared for protected area access, such as temporary repair, services or constructions workers and visitors are escorted by cleared authorized personnel. The identity of authorized personnel entering the protected area is verified and badges would need to be issued and visually displayed inside the protected area.

**Main protected area access control point for vehicles and personnel (P2)**

Guard Force Staffing: One guard is present at all times. If a vehicle requires entry, the guard at P2 calls another guard to assist with the PA vehicle entry. The SAS is also located in P2.

Personnel entering the protected area undergo a search for prohibited items by passing through metal detectors and randomly checked with a hand-held explosives detection device. Hand carried items are X-rayed and passed through metal detectors. Suspicious items are physically searched and individuals who fail the metal detector search are 'wanded' with hand-held metal detectors or subjected to a pat down search. If items are too large to pass through the x-ray unit, they are visually searched by the guards. After verification that individuals are not carrying prohibited items, they undergo a badge exchange, turning in their NPP picture badges and picking up their LNPP picture badges and key cards. The personnel then enter the LNPP Protected Area via a turnstile operated by their key cards. The guards who perform the badge exchange are in small arms protected enclosures and have a 'panic' button that will override the key card reader, freezing the turnstiles and precluding any entry to the protected area. In a site emergency, the turnstiles can also be reconfigured to permit egress from the protected area to facilitate evacuation. The layout of the entry control section of the LPNPP main protected area access control point is shown below in Fig. I.6.

Personnel exiting the protected area turn in their LPNPP picture badges and key cards and picking up their NPP picture badges then undergo a search for NM by passing through metal and NM monitors. Hand carried items are X-rayed. Suspicious items are physically searched and individuals who fail the metal detector search are 'wanded' with hand-held metal detectors and NM detectors or subjected to a pat down search. The personnel then exit the LPNPP protected area via unlocked doors.

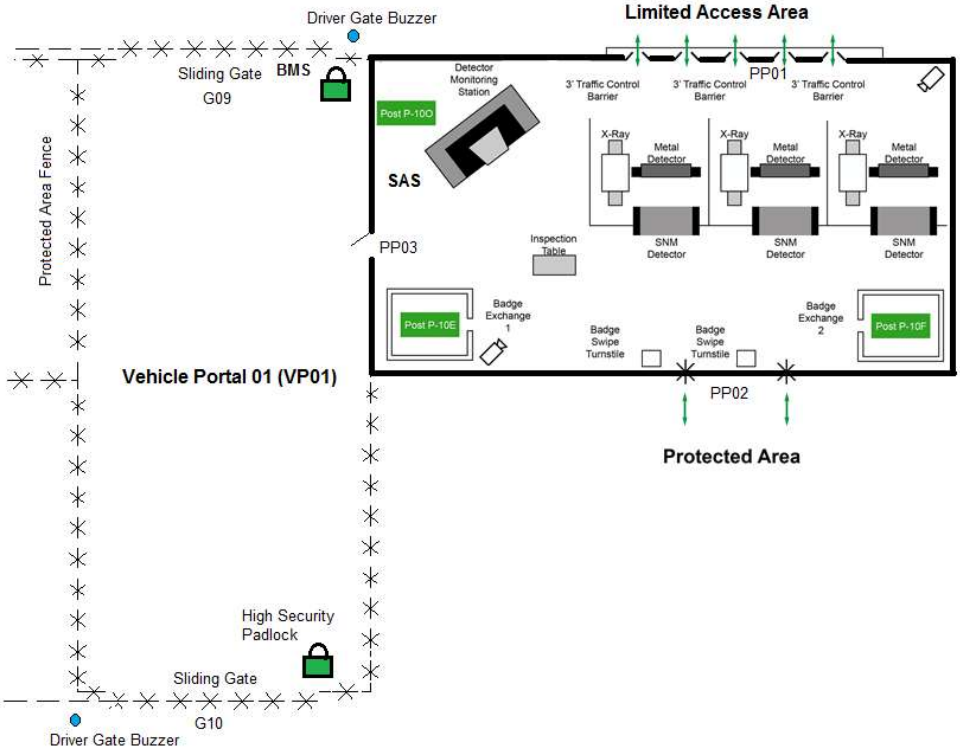



*FIG. I.6. Main protected area access control point for both personnel and vehicles*

**Protected area vehicle gates (P4-P6)**

These gates are normally closed and locked with high security padlocks with BMS detection (See Fig. I.7). When a delivery vehicle arrives, four guards are dispatched to the gates. They verify that the individuals driving the vehicle have LPNPP badges (exchange badges) permitting access to the LPNPP protected area or have the required guard force escorts. They review the manifest or other documents to verify that the vehicle requires entry to the LPNPP. The guards then contact the LPNPP control room and verify that the vehicle is expected. Once they have verified that the vehicle is expected, they inspect it for prohibited items. If the vehicle passes inspection, the guards contact the central alarm station (CAS) requesting that the protected area intrusion detection system zone at the gates be placed in the access mode. The guards then unlock the vehicle gates to permit the vehicle entry to the LPNPP protected area. After the vehicle has entered the protected area, the gates are locked and the protected area intrusion

detection system zone at the gates is returned to the secure mode. When a vehicle needs to exit the protected area, the driver notifies the CAS, which dispatches four guards to the gate. On exit, vehicles are scanned with a hand-held radiation monitor to ensure that there is no contamination and searched for NM. Once vehicles are verified not to be contaminated and not to have unauthorized NM, they are permitted to exit. The contamination scan and NM search are performed inside the protected area with the vehicle gates locked.

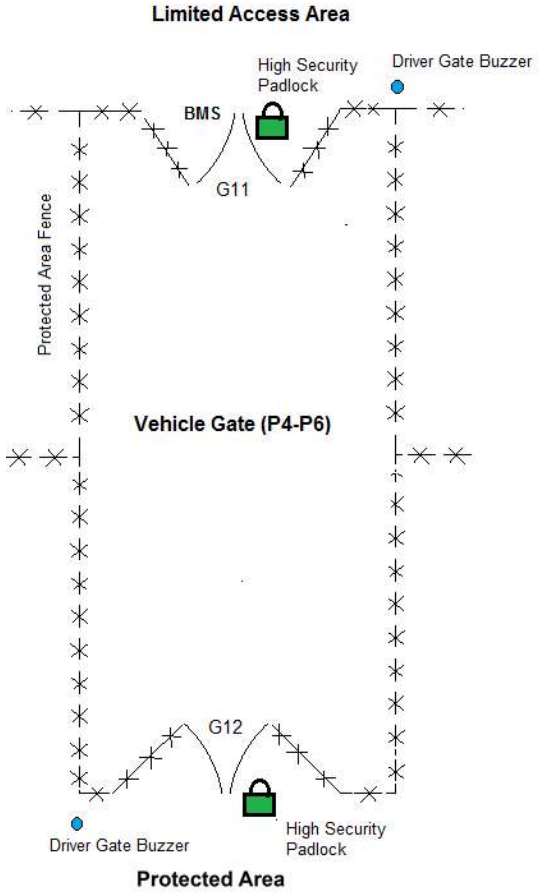



*FIG. I.7. Protected area vehicle gate*

### *I.1.4.3. Vital area — access control*

A computerized access control system maintains records of all personnel who access the vital areas or have access to or possession of keys, key cards, and/or other systems, including computer systems that control access to the vital areas.

Private vehicles are prohibited from accessing the vital areas. Vital area equipment and interface systems and devices are equipped with timely detection against tampering. All suspected malicious activities are reported in a timely fashion to facility management and the competent authorities.

Access to the vital areas is maintained at all times including during periods of shutdown and maintenance periods. Prior to reactor start-up, searches and testing is conducted to detect any tampering that may have been committed during shutdown or maintenance.

Vital area access requires combination of a key card and fingerprint biometric authorization. All personnel doors are equipped with an electric lock. All vehicle gate doors are padlocked from the inside. In addition, each door leading to the vital area is alarmed with a BMS and CCTV to assess an unauthorized entry. CCTV is also located throughout the vital area rooms to assess unauthorized activities. Unless noted otherwise, building gates are 0.75 cm steel-plate doors, equipped with interior high security padlock, a BMS and CCTV.

Access to the control building, CAS, steam valve building, ESF building and reactor containment requires a CAS operator to visually verify the person through CCTV prior to releasing the door electric lock. Access to fuel building where the spent fuel pool is located requires two-person rule — i.e. two key cards and two fingerprints would need to be presented. Access requires a guard to be present. Reactor containment entrance is equipped with a radiation interlock and bullet resistant barriers and doors. The interlock consists of two 0.75 cm steel plate doors. Condensate storage tank and piping have lock and key access control to valves and other insider sabotage targets.

The second floor of the control room building requires combination of a key card and fingerprint plus an operator is required to visually verify the person through CCTV. The control room is enclosed by 20 cm thick reinforced concrete walls, floors and ceiling. The entry doors are 1.5 cm steel-plate and the window is bullet resistant glass.

Refer to Fig. I.8 and Table I.1 for additional information.

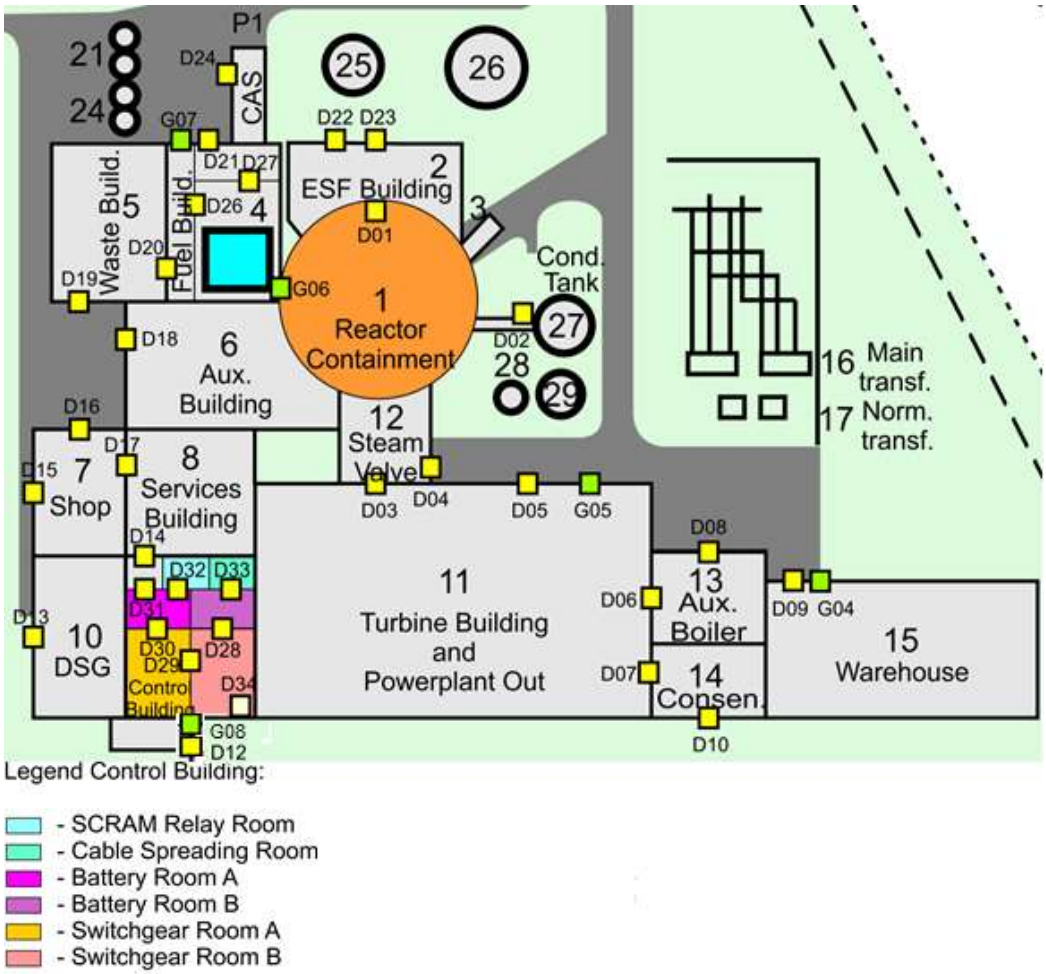



*FIG. I.8. Entrances and door locations in detail*

### *I.1.4.4. Entrance areas and portals*

Table I.1 describes doors and personnel entrances in the facility. Table I.2 lists door locations, door numbers and access controls and door barrier details.

TABLE I.1. FACILITY DOOR AND PERSONNEL ENTRANCES

| Location | Door No. | Access Controls and Physical Barriers |
|---|---|---|
| Reactor Containment | D01 | Key card access + fingerprint biometric reader control with radiation interlock, bullet resistant barriers and doors; interlock consists of two .75 cm steel-plate doors, two-person rule, visual verification through CCTV |
| Condensate Storage Tank | D02 | Lock and key card access control to valves and other targets, CCTV assessment, 0.75 cm steel-plate door |
| Main Steam Valve Building | D03 | Key card access, electric lock, BMS, standard industrial pedestrian door, visual verification through CCTV |
| Main Steam Valve Building | D04 | Key card access + fingerprint biometric reader control, electric lock, BMS, 0.75 cm steel-plate water tight door, visual verification through CCTV |
| Turbine Building and Power Plant Out | D05 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Auxiliary Boiler Room | D06 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Condensate Polishing Enclosure | D07 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Auxiliary Boiler Room | D08 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Warehouse | D09 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Condensate Polishing Enclosure | D10 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Intake Structure | D11 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building, First Floor | D12 | Key card access + fingerprint biometric reader control, electric lock, BMS, visual verification through CCTV, 1.5 cm steel-plate door |
| Control Building - First floor, Switchgear Rooms | D12A<br>D12B | Key card access + fingerprint biometric reader control, electric lock, BMS, visual verification through CCTV, 0.75 cm steel-plate water tight door |
| Diesel Generator Building | D13<br>D13A | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Diesel Generator Building | D13B<br>D13C | Standard industrial pedestrian door, no lock |
| Services Building | D14<br>D14A | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Shop | D15, D16 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Services Building | D17 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Auxiliary Building | D18 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Auxiliary Building Interior | D18 A-J | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |

TABLE I.1. FACILITY DOOR AND PERSONNEL ENTRANCES (CONT.)

| Location | Door No. | Access Controls and Physical Barriers |
|---|---|---|
| Waste Building | D19 | Key card access + fingerprint biometric reader control, electric lock, BMS, CCTV assessment, 0.75 cm steel-plate water tight door |
| Fuel Building | D20 | Key card access + fingerprint biometric reader control, electric lock, BMS, two-person rule, guard presence, CCTV assessment, standard industrial pedestrian door |
| Fuel Building | D21 | Key card access + fingerprint biometric reader control, electric lock, BMS, two-person rule, guard presence, CCTV assessment, 0.75 cm steel-plate water tight doors |
| ESF Building | D22, D23 | Key card access + fingerprint biometric reader control, electric lock, BMS, 0.75 cm steel-plate water tight doors, visual verification through CCTV |
| ESF Building | D22A-B<br>D23A-D | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Central Alarm Station | D24 | Key card access + fingerprint biometric reader control, electric lock, BMS, 1.5 cm steel-plate door, visual verification through CCTV |
| Reserve Station Service Transformers | D25 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Fuel Building | D26,<br>D26A D27<br>D27A | Key card access, electric lock, BMS, two-person rule, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor, Switchgear Room B / Battery room B | D28 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor, Switchgear Room A, B | D29 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor, Switchgear Room A | D30 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor | D31 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor, (SCRAM) system | D32 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 1st floor, Cable Spreading Room | D33 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Control Building - 2nd floor, Control Room | D34 | Key card access + fingerprint biometric reader control, electric lock, BMS, 1.5 cm steel-plate door, walls, windows, visual verification through CCTV |
| Control Building – 2nd floor, Control Room Computer Room | D34A | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Main Protected Area Access Control Point | PP01 | Standard industrial pedestrian door, no lock |
| Main Protected Area Access Control Point | PP02 | Key card access, locking turnstile |
| Main Protected Area Access Control Point | PP03 | Key card access, electric lock, BMS, CCTV assessment, standard industrial pedestrian door |
| Shop | G01 | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS and CCTV |
| Diesel Generator Building | G02<br>G03 | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS and CCTV |

TABLE I.2. VEHICLE GATE DESCRIPTION

| Location | Gate No. | Controls and Physical Barriers |
|---|---|---|
| Warehouse | G04 | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS and CCTV |
| Turbine Building | G05 | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS and CCTV |
| Reactor Containment | G06 | Radiation interlock doors. The interlock consists of two .75 cm steel plate doors a BMS and CCTV. |
| Fuel Building | G07<br>G07A | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS, two-person rule, guard presence, CCTV assessment |
| Control Building | G08 | 0.75 cm steel-plate doors, equipped with interior high security padlock and a BMS and CCTV |
| Protected Area Vehicle Portal | G09-G10 | Sliding fence gate with high security padlock and a BMS (G10 only) and CCTV |
| Protected Area Vehicle Gates | G11-16 | Swinging fence gate with high security padlock and a BMS |

### *I.1.4.5. Guards and response force*

A 24-hour guard and response force is provided to ensure an adequate and timely response to prevent an adversary from completing an act of sabotage. See Table I.3 for the response force staffing locations. The response strategy is the denial of the adversary task completion at the sabotage target locations. The guard and response force consists of four types of security personnel:

(1) Unarmed guards;

(2) Armed guards in protected area perimeter towers;

(3) Onsite tactical response force; and

(4) Offsite response team.

All posts and patrols have defined policies and procedures with which the security personnel would need to comply.

For each shift, two supervisors are present:

- Supervisor 1 supervises the guards that conduct administrative duties, guard tower duties and access control;
- Supervisor 2 is the commander of the tactical response team and their duties include shift change access control, random patrols and alarm assessment and response.

All guards and response force personnel are equipped with:

- a straight baton;
- one set of handcuffs;
- a small flashlight; and
- a hand-held radio.

**Unarmed guards**

Unarmed guards are responsible for:

- assessment of alarms in the CAS/SAS;
- administrative duties such as access control and key service.

**Armed guards**

Armed guards are responsible for:

- assessment of alarm; and
- in-place response in protected area guard towers.

The armed guards are equipped with a .38 calibre revolver with six rounds with a total of twenty-four rounds and an automatic submachine gun with a total of five magazines with thirty rounds each. Both weapons are carried fully loaded but without a round in the automatic submachine gun chamber.

**On-site tactical response team**

On-site tactical response team is responsible for:

- administrative duties such as access control and key service;
- routine patrols in the protected area;
- staffing of vehicle access control points as needed;
- staffing of personnel access control points during shift changes; and
- armed response to all intrusion alarms.

The onsite tactical response team has eight members (including the commander of the tactical response team), present during operational as well as non-operational hours. Four of these eight members are deployed in two two-person response teams that are on random patrol in unarmoured vehicles at all times. The main function of the random patrol is to deter and adversary, detect intrusion, visually inspect physical protection components, supplement existing physical protection measures and to provide initial alarm response. The random patrol also provides surveillance of tampering of physical barriers not covered by an intrusion detection system.

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.

The tactical response team members are equipped with:

- a .38 calibre revolver with six rounds with a total of twenty-four rounds and an automatic submachine gun with a total of five magazines with thirty rounds each (5.56x45 mm). Both weapons are carried fully loaded but without a round in the automatic submachine gun chamber; and
- two vehicles not armoured.

**Off-site response force**

A 15-person off-site response team is deployed from the Regional Army Base near Hashbakar. This force is Special Weapons and Tactics trained and can arrive in 120 minutes after being notified. The CAS communicates with the offsite response force on a routine interval.

**Response force training**

- Classroom training (all security staff) includes the following topics:
    - Access control procedures;
    - Use of force continuum;
    - Target locations;
    - Response procedures;
    - Chain of command; and
    - Other administrative responsibilities.

- Tactical response team personnel receive additional training on:
  - Close quarters combat;
  - Recapture and recovery of nuclear material/facilities; and
  - Advanced firearms training for both the revolver and the automatic submachine gun.
- Firearms training:
  - The tactical response team personnel are required to qualify with their firearms four times a year; and the
  - Tactical response teams are provided with firearms training each month to ensure proficiency.

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

*I.1.4.6. Alarm stations*

**Central alarm station**

A hardened and permanently staffed 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 (P1) and SAS (P2). The CAS provides for a complete and continuous alarm monitoring, assessment and communications with guards, facility management and response force. Information acquired at the CAS is stored in a secure manner in the CAS. The PPS system is designed and operated to maintain alarm communications and display system integrity during nuclear events. Access control to the CAS is strictly minimized and controlled. All CAS functions are redundantly maintained in the SAS. All alarm equipment, alarm communications paths are redundant and diverse and the CAS is equipped with an uninterruptable power supply and is tamper protected against unauthorized monitoring, cyber-attack, manipulation and falsification. The guard is responsible for assessing alarms and communicating them to the response forces.

**Secondary alarm station**

The SAS is located in P2, the Main Access Control Point 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 SAS can take over the CAS functions in the event of hardware or personnel failure at the CAS, in the case of an attack on the CAS, or during maintenance and other temporary facility outages. Both the CAS and the SAS are equipped with:

- A dedicated, redundant, secure transmission system for two-way voice communication between the CAS and the guard and response force members is provided;
- 100-watt radios that can communicate to all posts and patrols within the boundaries of the NPP. The guards and response force members are equipped with 5 watt radios – non-encrypted; and
- Two 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 NPP with the exception of the lower level interiors of the LPNPP facility buildings. Testing concluded that security personnel on these lower levels 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.

Supervisor 1, the guard force commander, is normally located in the CAS during the day shift. See Table I.3 for the response force staffing locations.

TABLE I.3. GUARD AND RESPONSE FORCE STAFFING LOCATIONS

| Post No. | Description | Security Personnel | Armed | No. of Personnel | | |
|---|---|---|---|---|---|---|
| | | | | Work days | Shift Change | Non-work days |
| S2 | Tactical Response Force Commander (Supervisor 2) | Captain | Yes | 1 | 1 | 1 |
| S1 | Guard Commander (Supervisor 1) | Lieutenant | No | 1 | 1 | 1 |
| P2 | Access to Protected Area | Guard | No | 4 | 4 | 3 |
| P2 | Access to Protected Area | Response Force | Yes | 0 | 6 | 3 |
| P2 | Secondary Alarm Station | Guard | No | 2 | 2 | 1 |
| P1 | Central Alarm Station | Guard | No | 2 | 2 | 1 |
| P1 | Onsite Tactical Response Forces Stationed in the CAS | Response Force | Yes | 3 | 0 | 3 |
| P3 | Lone Pine Employee Vehicle Entrance | Guard | No | 2 | 1 | 1 |
| P7 | First two-person vehicle patrol | Response Force | Yes | 2 | 2 | 2 |
| P8 | Second two-person vehicle patrol | Response Force | Yes | 2 | 0 | 2 |
| T1-T5 | Guard Towers | Guard | Yes | 5 | 5 | 5 |
| P9 | Lone Pine Vehicle Entrance | Guard | No | 2 | 1 | 1 |
| Offsite | Offsite Response Force | Response Forces | Yes | 15 | 15 | 15 |
| | | Totals | | 41 | 40 | 39 |

The protected area main access control point (P2) staffing is increased from four to ten beginning forty-five minutes before each LPNPP shift change and reduces back to four guards at thirty minutes after the LPNPP shift change. The six guards are re-deployed to other plant duties.

**Alarm communication procedures**

All alarms are received and initially assessed at the CAS. The SAS verifies the CAS operator's assessment to ensure all alarms are properly assessed.

For all alarms, NPP procedures require the CAS operator notify the nearest roving vehicle patrol to respond to the alarm location to provide additional alarm assessment and report back to the CAS operator. If an unauthorized activity is identified by the CAS operator on the CCTV or by the dispatched roving patrol, the CAS operator immediately notifies the Commander of the Response Force for deployment of the full tactical response team. The three response force members (equipped with pistols at all times) stationed in the Security Building and the tactical response force commander collect their firearms from the armoury in the Security Building, and prepare to respond either by foot or vehicle to a location directed by their commander. During periods of shift change, the tactical response team members assigned to P2 for access control duties are assigned firearms.

The farthest of the two-man vehicle patrols also responds. Both two-person patrols have their weapons with them in their vehicles.

Once all eight of tactical response team members arrive at the appropriate location, they deploy as a team and proceed with operations to enter the facility and ensure the protection of material and assets.

### *I.1.4.7. Response force performance data*

The NPP has conducted extensive performance testing of the CAS/SAS in the areas of alarm assessment, alarm communication, and response force notification and has recorded preparation, travel and deployment times for onsite tactical response forces alarms at the Lone Pine Nuclear Power Plant. The average times are listed in the table below. Procedures require that all tactical responders be available to respond to an alarm from P-2. All tactical responders are fully equipped with their duty gear with the exception of their rifles, which are kept in storage in the armoury until needed.

The CAS provides information to the tactical response force during a security incident. Should the CAS operator become unable to continue to direct the response, the SAS operator takes his place.

Note that the first two-person vehicle patrol can arrive in 30-60 seconds.

The average PPS response times for the entire eight-man tactical response team is listed below (See Table I.4).

TABLE I.4 RESPONSE FORCE TIMES

| Alarm Location | Response Time |
|---|---|
| Protected Area Fence | 60-150 seconds |
| Control Building | 120-150 seconds |
| Engineered Safety Features Building | 60-90 seconds |
| Condensate Storage Tank | 60-90 seconds |
| Reactor Containment | 5-10 minutes |

**NOTE:** Response times may be different from those listed in Table I.4 if the analytical tools calculated response force timelines as part of the simulation capability.

### *I.1.4.8. Insider protection measures*

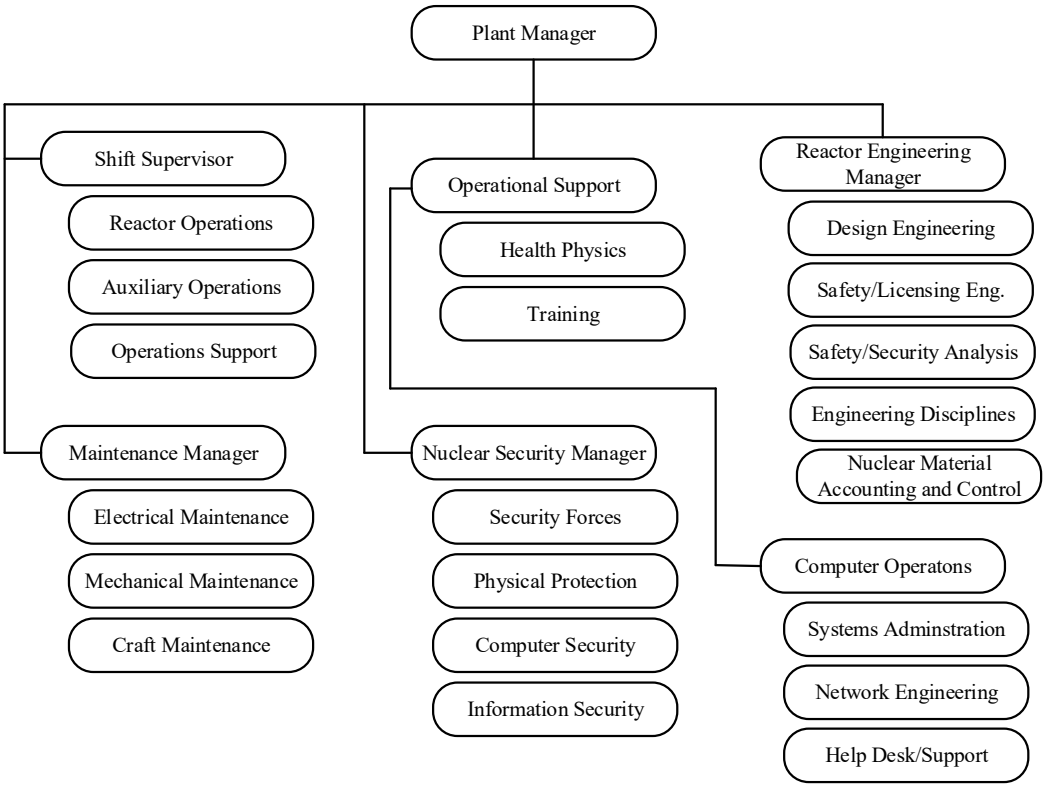



*FIG. I.9. LPNPP management structure*

The measures at LPNPP against insider threats include both preventive measures as well as protective measures. The LPNPP conducts regular self-assessments and is also controlled by the regulatory body. During normal operation, 750 full-time employees work at the LPNPP operations, maintenance, engineering, technical support, management and administrative support positions (See Fig. I.9).

Among preventive measures the following actions are conducted:

- Filtering potential insiders before they have authorized access to LPNPP through pre-employment screening that includes following:
  - Person's identity verification;
  - Work history check to determine past work practices;
  - Acquiring references to identify possible past undesirable behaviours;
  - Background checks to identify criminal activity;
  - Credit checks to evaluate financial situation;
  - Drug screening to identify substance abuse;
  - LPNPP also includes in the pre-employment process psychological exams and medical exams to reduce the risk of psychological instability and possible abuse.
- Further exclusion of potential insiders after a new employee is given access include the following:
  - Nuclear security culture in LPNPP has been improved over the past three years. Previously two security culture incidents were accounted. Both resulted in economic loss to the operator. These actions included disciplinary actions and prosecution followed. Employment was terminated in both cases. These cases are believed to serve as deterrence for other employees and raise awareness. For the past three years, regular assessments, observations and inspections have been frequently conducted to reveal any further risks. Emphasis has been put on trustworthiness and observation programmes and to raise employee awareness to ensure that the implementation of nuclear security measures receives the attention warranted by their significance;

    Employees have been trained to detect and report inadequate security conditions and to report suspicious acts or behaviour in several trainings. These included the spectrum of areas of security concern such as computer security, physical security and information security. A programme to protect employees who report violations has been introduced. Training of selected employees has been conducted in various levels from the top-management to workers;
  - An employee satisfaction programme has been introduced last year to support Nuclear Security Culture in the LPNPP. This mainly included the introduction of benefits, improvement in working environment and increased access to training;
  - Trustworthiness programmes in operation at LPNPP include periodic screening of drug/alcohol abuse, financial checks of employees, psychological exams and regular performance reviews;
  - Observation programmes include continuous tests including abiding security measures and procedures, disregarding LPNPP policies, changes in behaviour or personality; and
  - LPNPP updates an employee's file every five years from the hire date or if there is a significant security incident or event during that five year period.
- LPNPP is minimizing the opportunity of potential malicious insider actions in the following ways:
  - Limiting individual access (need-to-access rule) and limits persons empowered to give access authorization;
  - Limiting roles or assigned functions within the computer system users and administrators to only those required to perform the task;
  - Some types of information are available only to those employees who need it to perform their duties and some duties are separated to ensure that one person does not have sufficient access, authority, and knowledge to conduct activities without detection;

- A quality assurance programme is in place; and
- Visitors and other personnel who do not have authorized access are escorted to protect against unapproved access or actions.

Protective measures including detection and delay of potential insider threats are described throughout the LPNPP security plan description. The management of the plant considers these among the main measures:

- LPNPP's PPS should prevent unauthorized access or unscheduled access to various protection layers. In the fuel building and spent fuel pool areas a two-person rule is in place to minimize insider actions. Biometrics identification is also in place at all vital area exterior personnel entry door locations;
- Regular PPS tests are conducted to indicate possible system tampering. These tests include testing after maintenance, periodic functional and performance testing of components, and sub-systems of PPS. All alarm maintenance activities are conducted under a two-person rule control;
- Prohibited items detection is in place at entry points to detect any unwanted substances or items to be brought into the LPNPP;
- Surveillance that includes observation by personnel and by CCTV is in place;
- Nuclear material accounting and control (NMAC) system is an important detection if theft of NM should occur;
- The plant has indicated a risk in the area of maintenance. Not sufficient skills and spare parts are present to ensure all PPS components and subsystems are operational at all times;
- The plant has introduced a 'clean facility policy' and strictly controls leaving any material or tools freely available or unlocked; and
- Daily facility walk-downs are performed to detect tampering of safety systems. In case of tampering with safety systems, personnel observations and safety alarms are the first-line of detection.

### I.1.5. Radioactive material locations

#### *I.1.5.1. Materials and their enrichment*

Table I.5 provides the list and amounts of NMs present at the LPNPP.

TABLE I.5. NUCLEAR MATERIALS LIST

| Location | Form of Material | Amount of Material on Site (wt% enrichment) | Total Isotope Amounts | Level of Radiation |
|---|---|---|---|---|
| Reactor | $UO^2$ | 78 ton $UO^2$ ( 3.5% $^{235}U$) | 2.4 ton $^{235}U$ | High |
| Spent Fuel Pool | $UO^2$ | 500 ton $UO^2$ ( 0.8% $^{235}U$) | 3.5 ton $^{235}U$ | High |
| Fresh Fuel | $UO^2$ | 26 ton $UO^2$ ( 3.5% $^{235}U$) | 0.8 ton $^{235}U$ | Low |

I.1.5.1.1. Other nuclear materials

Experiment Materials

(1) 3 kg total of highly radioactive medical radionuclides, including Cesium, Americium, and Strontium-90.

(2) Experiments and metal are used in other irradiation and activation experiments.

### I.1.6. Computer security

An NPP has many types of network which independently support the function in the control room, process control, safety, data acquisition, and shared information server(s). An example of overall digital

I&C systems in NPP is shown in Fig. I.10. There are four types of networks in this figure, e.g. visual display units, safety network, process control network, and engineering processing network. An adversary's assault against I&C systems of NPP may/might give rise to some events, e.g. delaying or blocking the flow of information through control networks, unauthorized changes made to programmed instructions in programmable logic controllers, false information sent to control system operators, and malicious software introduced into the system. (See Fig. I.10 and I.11)

Moreover, other computer functions associated with security or security related systems need to be concerned. There is no established security classification for security systems comparable to the safety classification; however, control and data processes functions related to security require protection. Examples of those systems are; physical access control systems; voice and data communication infrastructure; security clearance database; security alarm monitoring and control systems; computer and network security components; and nuclear material accounting and control systems.

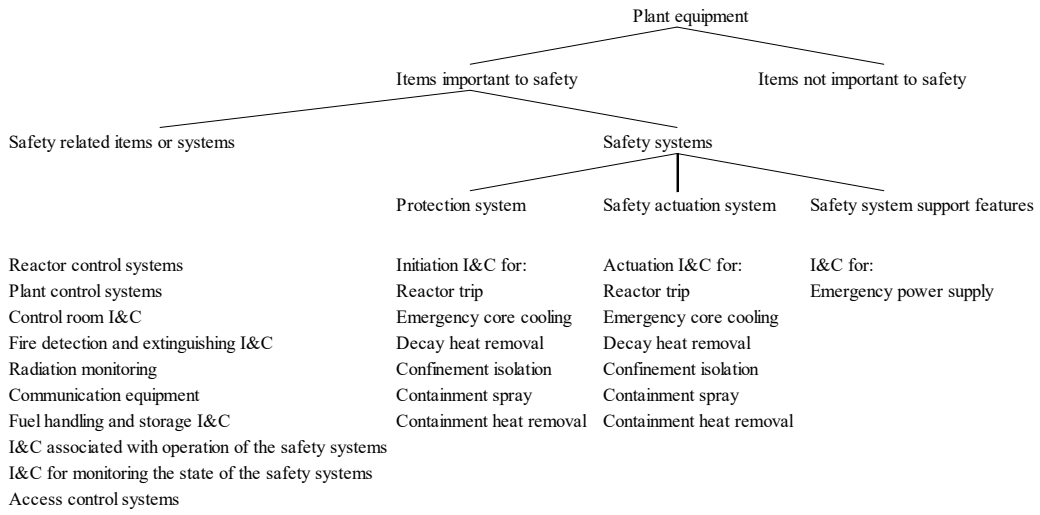
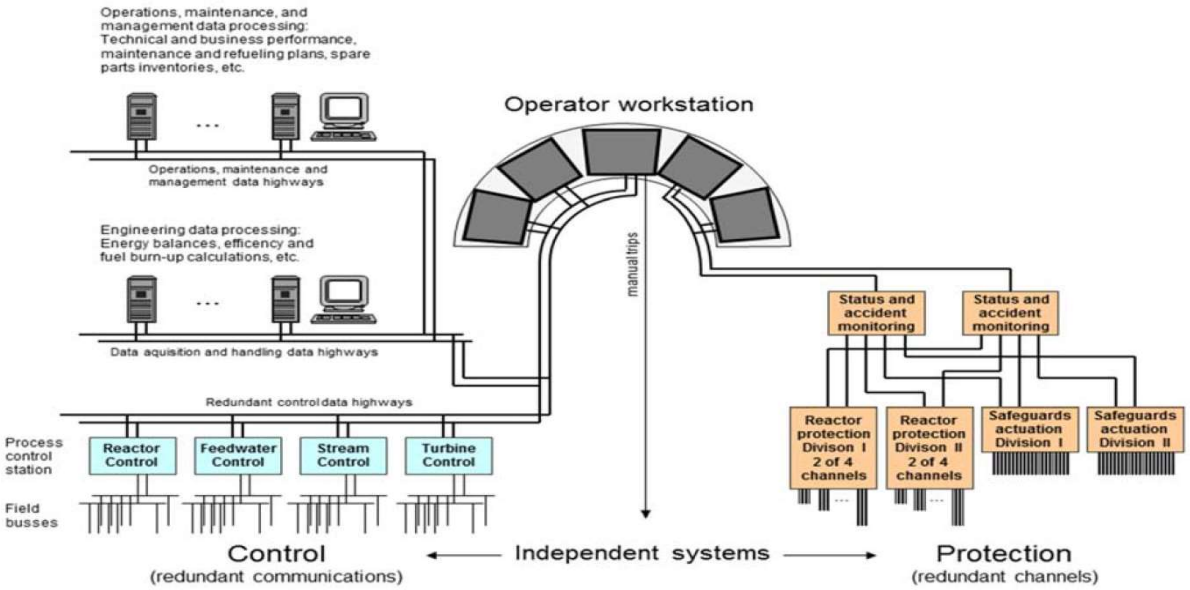



*FIG. I.10. I&C systems important to safety*[1]

[1] For additional information, refer to Ref. [10]




*(Courtesy of Sandia National Laboratories)*

*FIG. I.11. Digital instrumentation and control systems in NPPs*[2]

### I.1.7. Nuclear material accounting and control system description

The LPNPP NMAC system has two purposes, as does the NMAC system at all nuclear facilities. One purpose is to provide the information necessary for reporting NM types and quantities to the regulatory authority of the country of Lagassi. The information is subsequently reported to the IAEA in accordance with the Lagassi Safeguards Agreement. The other purpose is to maintain control of and to be able to account for all the LPNPP's NM at all times as recommended in Paragraph 3.26 of Ref. [6]. Since the threat of insider theft or diversion was not analyzed in this case study, no other NMAC details are addressed in this publication. This description of the NMAC system addresses the aspects of the NMAC system that are pertinent to the second purpose, i.e. the physical protection of NM. Therefore, specific parts of the NMAC system e.g. description of material balance areas (MBAs) and key measurements points (KMPs), as well as details of periodically reporting activities to the State Authority are not included in this description.

The LPNPP nuclear security management is assigned responsibility for protecting both the facility and its nuclear material and other radioactive material. Protecting the NM requires knowledge of the quantities and locations of all NM items. NMAC provides this knowledge. In the event of loss, theft, unauthorized removal or unauthorized use of NM, LPNPP relies on NMAC system information to identify what is missing and to aid in locating the missing material.

Responsibility for NMAC at the LPNPP resides in the reactor engineering department. The reactor engineering department, with the cooperation of the operations department, maintains accounting records of the location of all NM received, used and stored at the facility, and of all NM shipments from the facility. The reactor engineering department, in cooperation with the nuclear security department and operations, maintains control of all NM.

Reactor engineering is assigned direct responsibility for NMAC because it is responsible for all activities involving NM and the reactor, e.g. designing the placement of fuel assemblies in the reactor and the spent fuel pool, approving all movements of fuel assemblies, estimating NM quantities based on burn-up and production, and preparing State reports of NM quantities and locations. A senior member of the reactor engineering is appointed NMAC Manager, and this individual is given authority and responsibility for ensuring that all NMAC activities are carried out.

---

[2] For additional information, refer to Ref. [11].

#### *I.1.7.1. Nuclear material*

Nuclear material used and stored at the LPNPP includes fresh fuel (new assemblies and occasionally new rods), irradiated fuel (spent and partly spent assemblies and rods), and sources and instruments containing small quantities of NM. The LPNPP also utilizes transport containers (casks) containing depleted uranium shielding range in size from 25 to 100 tons. The smallest casks can be transported by truck, but the largest cask would need to be shipped by rail. The types, general locations and typical quantities of NM at the LPNPP are presented in Section I.1.5.

#### *I.1.7.2. Nuclear material receipts*

The NMAC management has established procedures for activities that are undertaken when NM is received at LPNPP. Nuclear material items received may include fresh (new) fuel assemblies, fresh fuel rods (in case of damage to or reconstitution of an assembly), and new sources or instruments which contain small amounts of NM. Upon receipt, the documents provided by the shipper are reviewed and compared to the actual receipt. The integrity of the shipping container is verified. Tamper indicating devices (seals) that were applied to the shipping casks by the shipper are checked for tampering and their identification numbers are compared with those in the shipper's documents. When shipping casks are opened, the assembly identification numbers (or other item identification numbers in case the items received are rods, instruments or sources) are compared with those in the shipping documents. Any irregularities, damage or other problems are investigated and resolved. These steps are performed by physical protection, NMAC, warehouse or operations personnel, or some combination of the staffs. NMAC staff has direct responsibility for assuring that the items received were the items shipped and for preparing and maintaining the LPNPP records that document the receipt. Items received are transferred to specially designated locations in the Fuel Building (or other storage locations, in the case of sources or instruments).

A record is prepared for each item received using the forms shown in Sections I.1.7.9 and I.1.7.10. Form 1 is the item history form. As the name of the form indicates, it documents the entire history of a single item at the LPNPP. In the case of an assembly, its history would begin with receipt and includes its location in the Fuel Building, its transfer into and out of the reactor, its movement within the spent fuel pool, any movement to an inspection station in the spent fuel pool, preparation for shipping, and final disposition. Form 2 is the Internal Transfer Form. It is used in conjunction with Form 1 and documents the movement of item from one location to another. Forms 1 and 2 are not official NMAC accounting documents but are designed to be completed by facility operations personnel when moving an item containing NM. When an item is relocated (assemblies, rods separated from their assemblies, instruments, etc.), the information about material quantities may not be available for inclusion on the forms. The information in these forms is essential to nuclear security to describe material current location if the need arises. For the improvement of nuclear security, the operations staff would complete the forms, providing location information, and NMAC staff (who is also responsible for maintaining safeguards records) would make certain that the completed forms became part of the facility's permanent historical record.

The LPNPP accepts values assigned to NM items by the shipper, which is usually the fuel fabrication facility, and there is no shipper-receiver difference. In rare cases where the shipper value is not accepted, the difference between the shipper's assigned value and the LPNPP's measured value is evaluated and significant differences are investigated.

#### *I.1.7.3. Accounting for nuclear material*

Accounting for NM at the LPNPP starts with the records prepared when NM items are first received. Complete and up-to-date records are essential for resolving questions of loss or theft of NM. Every movement of NM from one location to another is documented in the accounting records, providing for continuity of knowledge. The current location of every NM item is available in the accounting records.

### *I.1.7.4. Control of nuclear material*

LPNPP maintains basic control of NM by requiring that NM items be stored only in designated areas and by limiting access to those areas. (As noted in the PPS description sections, physical protection staff has direct responsibility for access control.) Written approval is required for access to locations where NM is stored and to the NM. Fuel building and spent fuel room access controls include key card and fingerprint biometric, electronic control for two-person rule entry, electromagnetic locks, BMS, guard presence and CCTV assessment. Equipment items such as cranes used to move assemblies are locked when not in use, and keys are controlled by nuclear security. Work is performed by teams with at least one person performing the actual activity and another person observing, verifying, and recording the activity. If it is possible containment and surveillance methods are also applied for controlling of NMs. Controls are 'layered' and the NMAC staff-members cooperate with the physical protection, operations and radiation safety departments to ensure that layers are in place. Examples of 'layers' of control used at the LPNPP are procedures for monitoring and controlling access to the spent fuel pool and equipment, use of cameras to monitor activities in the area, use of teams to perform activities, and radiation monitoring of the spent fuel pool area (so that removal of NM from the spent fuel pool causes an alarm to sound). Handling of non-NM is also controlled in areas that contain NM, to preclude the possibility that NM might be mistaken for non-NM and removed by accident. (Specific controls related to receipts and shipments are discussed in the sections covering those topics.)

### *I.1.7.5. Nuclear material use and storage*

Procedures are in place for documenting use and storage of NM at LPNPP. All activities involving NM items require prior written approval. For example, written approval is required before a NM item can be moved from fresh fuel storage to the reactor, from the reactor to the spent fuel pool, from one location in the spent fuel pool to another location, etc. To assure that all NM is accounted for, any activity conducted in an area of LPNPP where there is access to NM is approved in writing by the manager responsible for NMAC. Because the approval process is part of the facility's general procedure approval process, the NMAC manager's signature is required on most facility procedures. The NMAC manager is notified prior to the start of any activity involving an item of NM.

When a NM item is moved from one location to another, the movement is documented for NMAC by the staff performing the activity using Forms 1 and 2. This is in addition to the records made for operations and the notes in the reactor operator's log-book or the fuel building supervisor's log-book. Activities are documented as they occur by at least two people who have witnessed the activity, usually the person performing the activity and a person verifying the activity. Records of internal re-locations and other activities involving NM items are part of the LPNPP general historical record.

If two activities involving a single NM item are performed within a short time span, each activity is documented for the historical record. For example, if a spent fuel assembly discharged from the reactor is moved to an inspection station in the spent fuel pool and shortly thereafter is moved to a storage location in the spent fuel pool rack, two records are created to document the movements.

Infrequent activities, such as reconstitution of a damaged fuel assembly or clean-up of the spent fuel pool, are performed in accordance with written instructions. These instructions are followed line-by-line and the activities are documented in detail. Special attention is given to documenting activities that occur infrequently. If a fuel rod is removed from an assembly or part of a fuel rod separates from its assembly, Form 1 is used to create an item history of the new item and a record is made of its re-location in the spent fuel pool using Form 2. LPNPP has established technically justified procedures for determining the isotopic composition and NM quantities of individual rods or fragments of rods that have been removed from their assembly during reconstitution or separated from it by accident. Parts are placed in storage containers and the identity and location of the storage container is documented. If multiple rods or pieces are stored in a single container and treated as one item, the historical record of each individual rod is maintained along with the historical record of the container.

### *I.1.7.6. Physical inventory taking*

A physical inventory of all NM is conducted at the LPNPP at least every twelve months. The physical inventory taking has two purposes, namely, to confirm that all items listed in the records are physically

present and to confirm that there are no unrecorded items. The written procedure for the physical inventory taking requires that each NM item listed in the LPNPP records is visually verified. Both fuel and non-fuel items containing NM (sources and instruments) are included in the physical inventory taking. Verification of items and their locations is performed by inventory teams consisting of two members, at least one of which is well-acquainted with the area being inventoried and the items stored there. In accordance with the inventory procedure, any differences between the records and the results of the physical inventory taking are investigated and resolved within 30 days after the start of the physical inventory.

The LPNPP procedure for physical inventory taking requires that items be verified as follows: For fresh fuel assemblies and separated rods (if any are present), 100 % item counting is carrying out by visual verification of identification numbers and locations. Moreover, randomly selected items are measured by NDA techniques. For irradiated fuel assemblies stored in the spent fuel pool, an item count is acceptable along with comparison of locations to a map of assembly locations in the spent fuel and visual verification of the identification numbers of a small random sample of assemblies. For other NM items (such as individual rods and instruments) stored in the spent fuel pool, visual verification is required. For containers of rods or other components stored in the spent fuel pool, procedures are in place to visually ensure the contents of a container and to account for its contents when it is first prepared so that visual verification of the container is sufficient if measures (such as use of a tamper-indicating device) have been put in place to ensure the integrity of the container's contents. An operating reactor is considered a single item for the physical inventory taking and operating records are used to confirm that the reactor is operating as designed, which implies that no fuel has been removed from it.

#### *I.1.7.7. Shipment of nuclear material*

Nuclear material items and irradiated items designated for shipping are placed in approved shipping casks or containers. LPNPP procedures require that the contents of shipping containers be accurately recorded. Before a shipping cask is closed and sealed with a tamper-indicating device or welded shut, NMAC staff verify that the documentation accurately lists its contents and that nothing has been shipped inadvertently or substituted. The identification number of each item shipped is verified prior to closing the cask. In addition to the shipping documents, Forms 1 and 2 are completed to provide a historical record of NM items in the shipment. A video record is prepared of the contents of a shipping cask as part of the historical record.

Information concerning a shipment is treated as 'sensitive' and is not made public until after the shipment is complete and the receiver has acknowledged receipt of the shipment.

#### *I.1.7.8. Unusual events*

The NMAC system has written procedures that cover potential unusual events that might occur. The discovery of any theft, unauthorized removal, diversion or loss of 1 gram or more of NM would need to be reported immediately to NMAC management and LPNPP upper-level management. Instructions for responding to unusual events include steps to take in investigating and resolving such problems as lack of agreement between the results of physical inventory taking and the records, discovery by any means that an item is not in its recorded location, discovery that an item has been tampered with, unauthorized activities in an area where NM is used or stored, or an allegation of theft. Steps to be taken include isolating the area where the problem occurred; checking accounting records and source information; reviewing operating records; conducting a physical search of the area; determining the type, identity, and quantity of NM involved; establishing the most likely reason for the problem; and making a determination that the problem is or is not resolved. The procedures require that no individual with possible responsibility for the theft, unauthorized removal, diversion or loss under investigation is involved in the resolution. The investigation is to be conducted in a timely manner and documented.

*I.1.7.9. Form 1 – Item History Form*

Item Identification Number

Or Other Identification _____

| Date | Activity | Location From | Location To | Signature of Person Updating History Form |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Note: Location identities are specific. An example of a specific fuel bundle (ID: XYZ123) location is position A7 in the spent fuel pool storage rack.

*I.1.7.10. Form 2 – Internal Transfer Form*

| Item Identification Number or Other Identification | Location From | Location To | Date | Time | Signature of Person Performing Work | Signature of Person Observing Work |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Signature of Manager Authorizing Work _____ Date _____

Signature of NMAC Staff Verifying Completion_____ Date _____

Note: Location identities are specific. An example of a specific fuel bundle (ID: XYZ123) location is position A7 in the spent fuel pool storage rack.

### I.1.8. Stakeholders identification

In the LPNPP stakeholders can be divided into internal and external stakeholders. Internal stakeholders are those involved in the decision-making process or directly involved in the implementation of the LPNPP project. External stakeholders are those without direct involvement in the implementation of the LPNPP project but with a direct interest in the outcomes and impact of the project. The stakeholders can be local or regional organizations or national or international bodies. The relationship of the operator organization with the stakeholder can also vary from unofficial and informal to official and formal.

Internal stakeholders in the LPNPP include: operator organization, public authorities/elected representatives, regulators, ministries, construction, emergency management, and NPP support organizations.

External stakeholders can include the Lagassi city and state population and businesses, LPNPP employees, educational institutes, news media, environmentalists and bordering States and international organizations such as the IAEA and World Association of Nuclear Operators (WANO).

### I.1.9. Management of security

The nuclear security management system of the LPNPP was established by following the relevant international guidelines and national regulations. In this section, the relationship of the nuclear security management system to international and national legally binding and non-binding publications is shown. Moreover, some of the most important features of the nuclear security management system of the LPNPP will be described, e.g. nuclear security policy, nuclear security culture, structure of the security management system as part of the whole management system of the plant etc.

#### *I.1.9.1 Relevant Lagassi national regulation*

In general, Lagassi has the responsibility for establishing the legal and regulatory framework to foster an effective nuclear security regime including nuclear security culture. Lagassi established nuclear security regulations, which includes requirements for the following aspects:

- Identifying the security significance of individual systems;
- Specifying threat levels;
- Developing performance standards and periodic performance testing programmes;
- Reporting;
- Designing physical protection systems;
- Licensing of organizations for particular activities;
- Accounting and record keeping;
- Enforcement regarding non-compliance with regulations or failure of performance testing;
- Protection of sensitive information; and
- Measures for the detection (inspection).

The State's legal and regulatory framework establishes the basis for an organization's security policies, which determine the nuclear security management system.

#### *I.1.9.2 Features of the model LPNPP's security management*

As defined in international and national publications, the LPNPP general management has four main responsibilities by establishing the nuclear security system in order to ensure the appropriate nuclear security culture, which includes:

- Development of a nuclear security policy;
- Establishment of a nuclear security management structure;
- Allocation of the necessary resources; and
- A continuous review and improvement process.

#### *I.1.9.3 Nuclear security policy*

The policy declares a commitment to quality of performance in all nuclear security activities, making it clear that security has high priority, even overriding operational demands. If there is a conflict regarding the relative priorities of safety, security or operations, senior management would need to be authorized to resolve the conflict taking into account the overall impact of risk. This policy forms the foundation of the management systems that are an integral part of the security culture of the organization. It is important to highlight that the nuclear security policy is posted in facilities and offices, and it is familiar to staff as well.

#### *I.1.9.4 Nuclear security management structure*

The management of LPNPP had defined the responsibilities and accountability for each level of the organization, including security and other interfaces. In addition, the management of LPNPP appointed an individual responsible for nuclear security who has sufficient authority, autonomy and resources to implement and oversee nuclear security activities, called the Nuclear Safety and Security Director. The director is required to report directly to the director general of the organization with the responsibility defined and documented in sufficient detail to prevent ambiguity.

LPNPP follows the main pillars of the security management structure. The following list shows some examples for that:

- Visible security policy;
- Clear roles and responsibilities;
- Performance measurement;
- Work environment;
- Training and qualification;
- Work management;
- Information security;
- Operations and maintenance;
- Determination of staff trustworthiness;
- Quality assurance;
- Change management;
- Feedback process;
- Contingency plans and drills;
- Self-assessment; and
- Interface with the regulator;

These topics are fully covered by the nuclear security related description of the LPNPP:

#### *I.1.9.5 Resources*

The LPNPP allocates sufficient financial, technical and human resources to implement assigned security responsibilities. It is also ensured that all security personnel have the necessary qualifications and that these qualifications are maintained by an appropriate training and development programme. Personnel have the necessary equipment, adequate work areas, up to date information and all other necessary support to effectively discharge their security responsibilities.

#### *I.1.9.6 Review and improvement*

Arrangements were made by the management of the LPNPP for the regular review of their nuclear security practices and systems.

This regular review takes into account e.g. experiences collected during the operation of the system, lessons learned from both internal and external reviews (e.g. results of inspection conducted by the competent authorities or findings from the regular internal inspections). Moreover, all discrepancies detected relating to nuclear security system are followed by corrective actions at the adequate level of the management system.

As one of the most effective tools for continuous improvement of the system at all levels of the organization the management ensures that training is conducted to develop skills and provide tools to promote and implement security culture.

### I.1.10. Detailed LPNPP technology description

The LPNPP is a two-loop pressurized light water reactor with a reactor power level of 1,150 megawatts electric at full power. LPNPP is a dual cycle nuclear power plant consisting of a reactor, a closed primary coolant loop connected to the reactor vessel, and a separate power conversion system (secondary coolant) for the generation of electricity. The primary coolant is light water under pressure (typically 15.4 megapascals) containing chemicals to control the nuclear reaction (boric acid, referred to as 'chemical shim') and corrosion. The secondary coolant is also light water containing chemicals to control corrosion. The primary coolant system transfers heat from the reactor core to the steam generators, which transfer heat to the secondary coolant, causing it to boil. The steam passes from the steam generators to the turbine generator where the thermal energy of the steam is converted into mechanical and then electrical energy. The steam is condensed in the main condenser and the secondary coolant is returned to the steam generators by the feed water pumps. The use of a dual cycle minimizes the quantities of fission products released to the main turbine, condenser and other secondary plant components and subsequent release to the atmosphere. The reactor is equipped with a once-through cooling system.

The entire reactor coolant system (RCS), including the steam generators, is located in the containment building, which isolates the radioactive RCS from the environment in the event of a leak. The basic arrangement is shown in the figure below. However, the LPNPP is a once-through cooling system so the cooling tower was never built and the river supplies the cooling.

The intake structure houses the circulating water system, the service water system, and the screen wash system. The intake structure consists of six intake bays, each with a traveling water screen and a circulating water pump. The capacity of this pump house is approximately 1,000,000 gallons per minute (GPM).

The following major systems are included in the intake structure:

- Circulating water system: The six pumps of this system take water from the river and provide cooling to the main condenser. This cooling water is then discharged via a cooling canal to the river;
- Service water system: The four pumps of this system also take water from the river and discharge via the cooling canal to the river. Service water is used to cool other systems, such as the primary and secondary (steam) system, component cooling system, containment cooler, diesel generators and other heat exchangers; and a
- Screen wash system: Six traveling water screens are provided to remove trash and foreign matter from the water used to supply the service and circulating water systems.

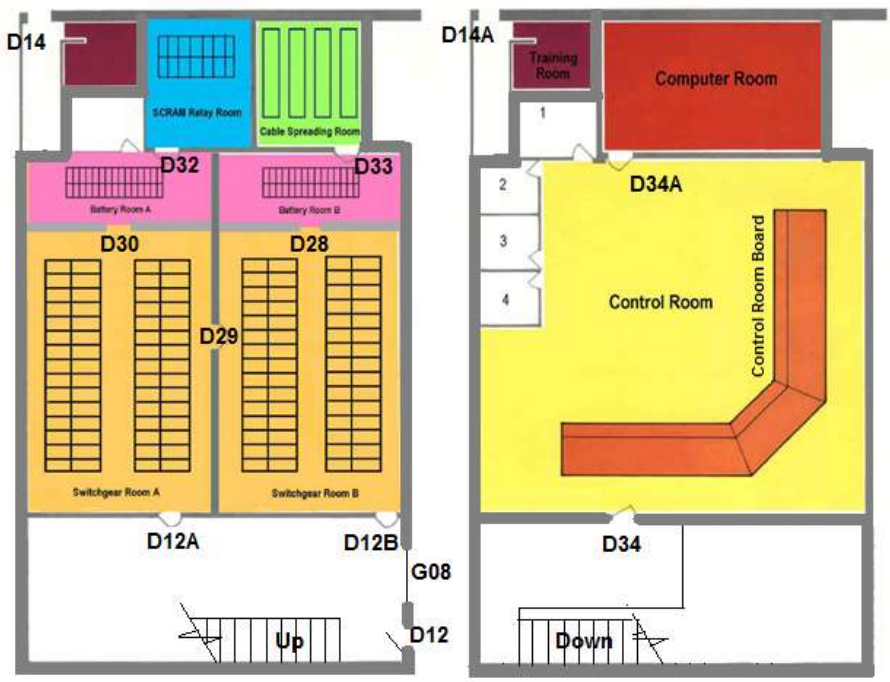
The containment building is designed to contain the pressure produced by a complete rupture of an RCS loop. All potentially radioactive auxiliary systems needed for normal operations are located in the auxiliary building, which is located adjacent to the containment building. Systems which need to be available to shut down the reactor and/or mitigate the consequences of an accident are located in the ESF building, which is also located adjacent to the containment building.

#### *I.1.10.1. Control room*

The control building is a two-level structure (See Fig. I.12). The lower level houses the switchgear and motor control centres that control and power motor-driven pumps, motor-operated valves and other electrical plant electrical equipment. The lower level also contains the battery rooms that supply backup instrumentation and control power, the electronics that control the reactor protection system (in the SCRAM relay room), and the cable spreading room where the instrumentation and control cables from the control room are routed to the appropriate instruments, motor control centres and other control equipment. The lower level also contains (in the SCRAM relay room) the auxiliary shutdown panel from which the reactor can also be monitored, controlled and safely shutdown should the control room become damaged or unavailable.

The upper level of the control building houses the main control board and the plant computer. Control of both the reactor and turbine generator can be accomplished from the control room, which contains all

instrumentation and control equipment required for start-up, operation, and shutdown under both normal and accident conditions.




*(Courtesy of Sandia National Laboratories)*

Control Building – First Floor
Electrical Equipment Room

Control Building – Second Floor
Control Room

*FIG. I.12. Lower and upper control building plan view*

### *I.1.10.2. Containment building technology*

A containment building is a reinforced steel or lead structure enclosing a nuclear reactor. The containment building houses the reactor and the reactor coolant system, including the steam generators, reactor coolant pumps, pressurizer, and some of the engineered safety features. The following major systems are included in the containment building: reactor coolant system, low pressure safety injection system, containment recirculation system and containment spray system.

The containment building contains a polar crane for movement of equipment and a fuel canal for reactor vessel refueling. The containment building also contains secondary system components including the steam generators and the main feed water and main steam lines that connect to the steam generators.

### *I.1.10.3. Turbine building technology*

The turbine building houses the main and auxiliary equipment required to transform the energy of steam into electrical energy and to condense the steam back into water for return to the steam generators for reheating. The turbine building is a two-story building with the turbine and generator on the upper level and the condenser and feed water pumps on the lower level.

The following major systems and components are included in the turbine building:

— Main steam system (MSS): This system is designed to direct the steam produced in the steam generators into the main turbine to produce electricity in the generator;

- Moisture separator reheaters (MSR): Two reheaters, which are part of the MSS, are used to warm up steam between the high pressure and low pressure portions of the turbine;
- Condensate system: Three pumps and three strings of five-point feed water heater strings comprise this system;
- Feed water system (FWS): Feed water pumps (two turbine driven and one motor driven) supply water to the steam generators from the condensate system via feed water regulating valves;
- Turbine plant component cooling water system: This closed system, consisting of three pumps and three heat exchangers, provides cooling water for numerous components located in the turbine building; and
- Air systems (SA, IAS): Instrument air (IAS) is provided by two compressors and stored in two receivers that normally supplies to instruments in all locations except the containment building.

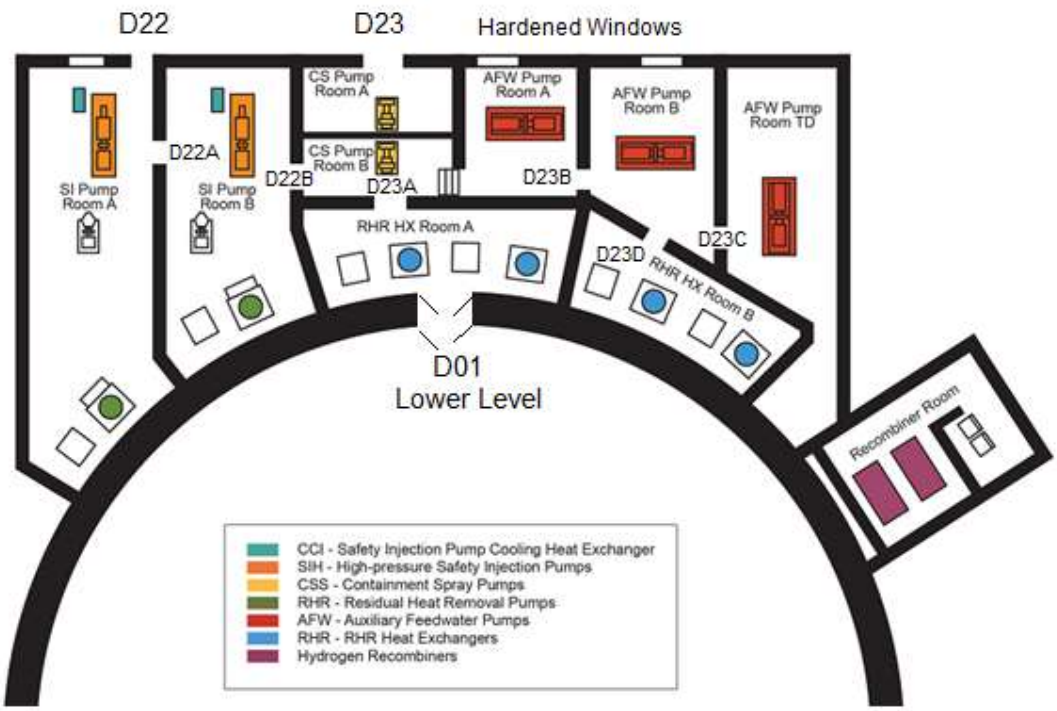
*I.1.10.4. Engineered safety features (ESF) building technology*

The systems in the ESF building are designed to mitigate the consequences of loss of coolant accidents (LOCAs) and plant transients. The ESF is designed to provide emergency cooling water to the reactor core to maintain fuel rod integrity in the event that normal cooling water (the river) is lost. This prevents the release of radioactive fission products to the containment and possibly to the environment. The ESF systems also serve to maintain the structural integrity of the containment if the pressurized primary coolant were released into the containment atmosphere during a LOCA. The ESF building also houses the auxiliary feed water system (AFW) that provides feed water to cool the steam generators during very low power operations and during transients that cause the main feed water system to be unavailable.

The following systems are housed in the ESF building:

- High pressure safety Injection system (SIH): Two safety injection pumps are designed to take suction on the 1.2 million gallon RWST located east of the ESF building to provide high pressure cooling water for the core in an emergency situation;
- Containment spray system (CSS): Two containment spray pumps are designed to provide water to a 360° circular spray header located on the inside of the containment dome to reduce the pressure in the containment in the event of a LOCA;
- Residual heat removal system (RHR): This system, consisting of two independent loops each containing a pump and heat exchanger, is primarily designed for the long term cool down of the reactor coolant system during shutdowns; and
- Reactor plant aerated drains (DAS): Various sumps and pumps are located in the ESF and containment building to transfer potentially radioactive leak off water to tanks for processing.

The ESF building houses the AFW which is the vital equipment in the ESF (see Fig. I.13.). This system, consisting of two motor-driven and one turbine-driven pump takes suction from the condensate storage tank and supply feed water to the steam generators to remove heat from the primary coolant system during very low power operations and during transients that cause the main feed water system to be unavailable.




*(Courtesy of Sandia National Laboratories)*

*FIG. I.13. ESF building and hydrogen recombiner plan view*

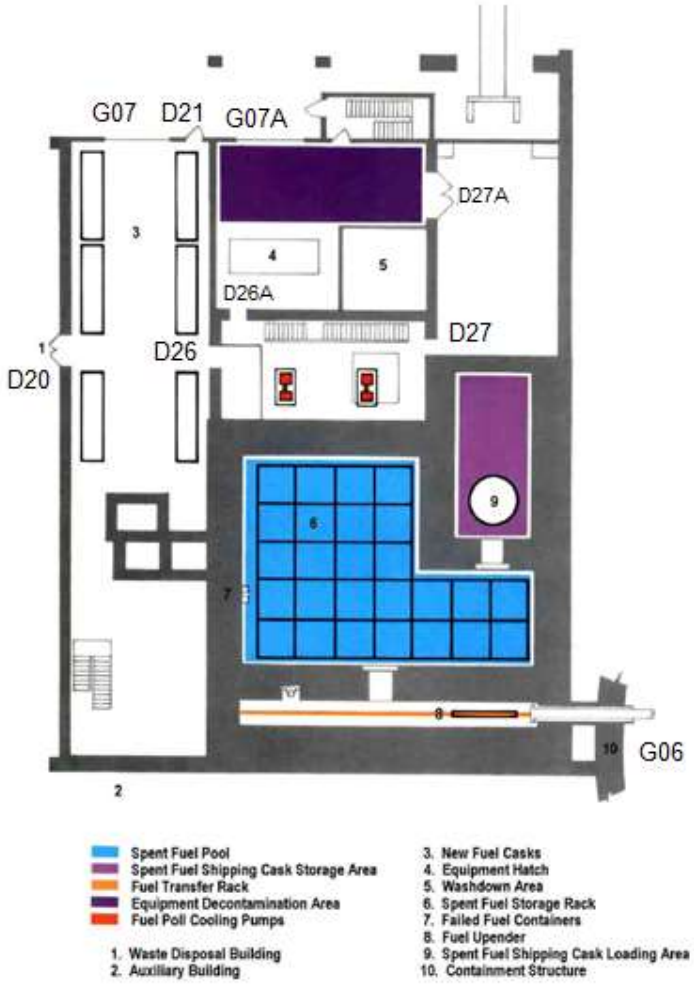
### *I.1.10.5. Fuel building*

The fuel building is designed as a transfer and storage area for new and used fuel. The average residence time of fuel in the core is about three years and the reactor is refuelled annually. After removal from the reactor, the fuel is handled remotely using special underwater fuel handling equipment. The spent fuel is placed in the spent fuel storage pool for at least six months until the radioactivity level is reduced by 99.9 percent. The fuel can then be shipped to another storage facility or a reprocessing plant in specially designed shipping casks made of steel and lined with lead.

All of the fuel assemblies in the core are of a similar design. The fuel rods in an assembly are arranged in a square array. Each fuel rod contains uranium oxide fuel pellets. The uranium-235 enrichment in the fuel assemblies is either 2.1, 2.6, or 3.1 weight percent. A core loading consists of 193 fuel assemblies. With the zircaloy clad and other mechanical components, each fuel assembly weighs about seven hundred kilograms.

The fuel pool cooling and purification system, consisting of cooling and purification pumps, heat exchangers, filters and demineralizers, is designed to maintain clarity and purity of the fuel pool water and to keep the stored spent fuel at a cool temperature.

The arrangement of the equipment in the fuel building is shown in Fig. I.14.

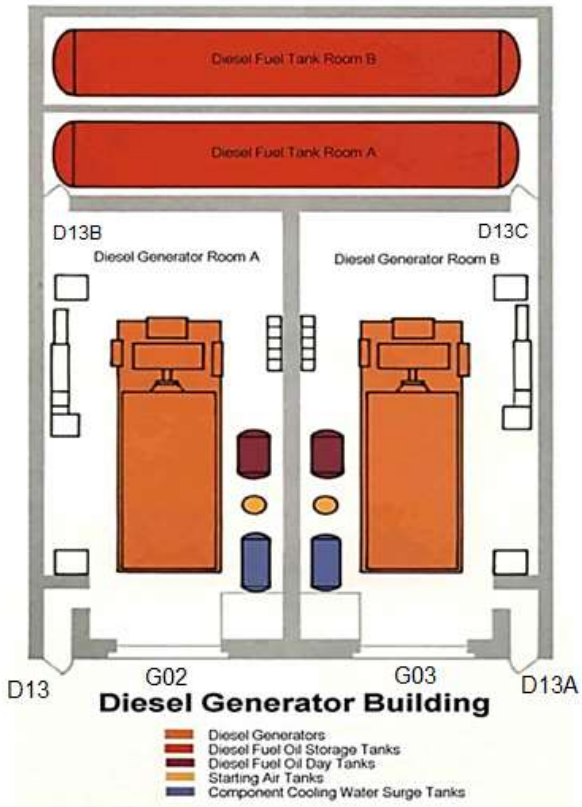



*(Courtesy of Sandia National Laboratories)*

*FIG. I.14. Fuel building plan view*

### *I.1.10.6. Diesel generator building*

This building houses two V-14 Colt diesel engines rated at approximately 7,000 HP each. Under reactor accident conditions, or should off-site power be lost during a plant shutdown, the two diesel generators are designed to handle vital safety loads (See Fig. I.15).




*(Courtesy of Sandia National Laboratories)*

*FIG. A-15. Diesel generator building plan view*

*I.1.10.7. Auxiliary building*

The auxiliary building contains reactor plant auxiliary equipment and components to accomplish the following:

- CVCS chemical and volume control: Periodically, changes in the reactor plant operating conditions or minor adjustments in reactor water inventory require the addition of make-up water using one of three charging pumps. This system also purifies the reactor coolant water, removing corrosion products and other impurities; and the
- CCW component cooling water: The component cooling water system is a closed-loop cooling system consisting of pumps, heat exchangers and piping that is designed to cool various reactor plant components, many of which are safety related. The service water system transports the heat from the heat exchanges to the ultimate heat sink.

*I.1.10.8. Condensate storage tank and piping from condensate storage tank*

The condensate storage tank serves as the normal supply to the auxiliary feed water pumps.

In the event that the condensate storage tank is damaged or destroyed, the Seismic Category I service water system is available as a backup suction for the auxiliary feed water pumps.

### I.1.11. Detection component data

Tables I.6–8 represent a hypothetical detection component class. Within each table the component types and descriptions are listed with the probability of detection by adversary defeat method or adversary attribute.

*I.1.11.1. Intrusion detection component class*

TABLE I.6. SAMPLE INTRUSION DETECTION VALUES

| Component Type | Component Description | No Equipment $P_D$ | Hand Tools $P_D$ | Power Tools $P_D$ | High Explosives $P_D$ | Land Vehicle $P_D$ |
|---|---|---|---|---|---|---|
| Exterior Sensors | Seismic buried cable | 0.5 | 0.5 | 0.5 | 0.5 | 0.9 |
| | Electric field | 0.5 | 0.3 | 0.3 | 0.5 | 0.9 |
| | Infrared | 0.8 | 0.4 | 0.4 | 0.5 | 0.8 |
| | Microwave | 0.8 | 0.7 | 0.7 | 0.7 | 0.9 |
| | Video motion | 0.8 | 0.6 | 0.6 | 0.7 | 0.9 |
| | Multiple non-complementary | 0.9 | 0.8 | 0.8 | 0.8 | 0.99 |
| | Multiple complementary | 0.99 | 0.95 | 0.95 | 0.99 | 0.99 |
| Interior Sensors | Sonic | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Capacitance | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Video motion | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Infrared | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Ultrasonic | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Microwave | 0.5 | 0.5 | 0.5 | 0.5 | N/A |
| | Multiple non-complementary | 0.75 | 0.75 | 0.75 | 0.75 | N/A |
| | Multiple complementary | 0.9 | 0.9 | 0.9 | 0.9 | N/A |
| Position Sensors | Position switch | 0.5 | 0.2 | 0.2 | 0.2 | N/A |
| | Balanced magnetic switch | 0.8 | 0.8 | 0.8 | 0.8 | N/A |
| Fence Sensors | Taut wire | 0.5 | 0.25 | 0.25 | 0.75 | 0.85 |
| | Vibration | 0.5 | 0.1 | 0.1 | 0.75 | 0.85 |
| | Strain | 0.1 | 0.1 | 0.1 | 0.1 | 0.9 |
| | Electric field | 0.5 | 0.4 | 0.4 | 0.75 | 0.9 |
| | Multiple sensors | 0.75 | 0.5 | 0.5 | 0.8 | 0.9 |
| Barrier Sensors | Vibration | 0.9 | 0.4 | 0.4 | 0.9 | N/A |
| | Glass breakage | 0.9 | 0.6 | 0.6 | 0.9 | N/A |
| | Conducting tape | 0.8 | 0.2 | 0.2 | 0.9 | N/A |
| | Grid mesh | 0.9 | 0.6 | 0.6 | 0.95 | N/A |
| | Multiple sensors | 0.99 | 0.9 | 0.9 | 0.99 | N/A |
| Helicopter Detector | Radar | 0.1 | | | | |
| | Sonic | 0.1 | | | | |

*I.1.11.2. Access control detection component class*

TABLE I.7. SAMPLE ACCESS CONTROL DETECTION VALUES

| Component Type | Component Description | Independent $P_D$ | Land Vehicle $P_D$ |
|---|---|---|---|
| ID Verification | Casual Recognition | 0.02 | |
| | Key Card | 0.05 | |
| | Key Card and PIN | 0.35 | |
| | Picture Badge | 0.1 | |
| | Picture Badge and PIN | 0.6 | |
| | Exchange picture badge | 0.5 | |
| | Exchange picture badge and PIN | 0.8 | |
| | Retinal scan and PIN | 0.99 | |
| | Hand geometry and PIN | 0.95 | |
| | Speech pattern and PIN | 0.95 | |
| | Signature dynamics and PIN | 0.95 | |
| | Fingerprint and Key Card | 0.95 | |
| | Fingerprint and Key Card and visual verification | 0.99 | |
| Personnel Access Authorization Check | General observation of authorization | 0.1 | |
| | Authorization verification each time location is accessed | 0.6 | |
| Two -Person Rule | Presence in area | 0 | |
| | Within sight | 0.1 | |
| | Dedicated observation | 0.5 | |
| | Dedicated observation with alarm | 0.95 | |
| Vehicle Authorization Check | Authorization form check | | 0.35 |
| | Serial number verification | | 0.45 |
| | Visual check of insignia/ license plate | | 0.15 |

*I.1.11.3. Human surveillance detection component class*

TABLE I.8. SAMPLE HUMAN SURVEILLANCE DETECTION VALUES

| Component Type | Component Description | No Equipment $P_D$ | Small Arms $P_D$ | Light Antitank Weapons (LAW) $P_D$ | Independent of threat attribute $P_D$ |
|---|---|---|---|---|---|
| Guard at Post Observation | Duress, LAW protected | 0.8 | 0.8 | 0.8 | |
| | Duress, small arms protected | 0.8 | 0.8 | 0.45 | |
| | Duress, small arms protected: LAW protected on alert | 0.8 | 0.8 | 0.45 | |
| | Duress, unprotected | 0.8 | 0.45 | 0.45 | |
| | Duress, unprotected: LAW protected position on alert | 0.8 | 0.45 | 0.45 | |
| | Duress, unprotected: small arms protected position on alert | 0.8 | 0.45 | 0.45 | |
| | No duress, LAW protected | 0.8 | 0.8 | 0.45 | |
| | No duress, small arms protected | 0.8 | 0.45 | 0.45 | |
| | No duress, small arms protected: LAW protected position on alert | 0.8 | 0.45 | 0.45 | |
| | No duress, unprotected | 0.8 | 0 | 0 | |
| | No duress, unprotected: LAW protected position on alert | 0.8 | 0 | 0 | |
| | No duress, unprotected: small arms protected on alert | 0.8 | 0 | 0 | |
| Guard in Tower Observation | LAW resistant tower | 0.05 | 0.05 | 0.02 | |
| | Small arms resistant | 0.05 | 0.05 | 0.02 | |
| Guard on Patrol | Random | | | | 0.02 |
| | Scheduled | | | | 0.01 |
| General Observation | Personnel always in vicinity | | | | 0.02 |
| | Personnel generally in vicinity | | | | 0.01 |

## I.1.12. Delay component data

Tables I.9–13 represent a hypothetical delay component class. Within each table the component types and descriptions are listed with the delay times by adversary defeat method.

*I.1.12.1. Barrier delay component class*

TABLE I.9. SAMPLE BARRIER DELAY VALUES

| Component Type | Component Description | No Equipment (seconds) | Hand Tools (seconds) | Power Tools (seconds) | Explosives (sec) | | Land Vehicle (seconds) |
|---|---|---|---|---|---|---|---|
| | | | | | Stage 1 | Stage 2 | |
| Walls | 60 cm reinforced concrete wall | Infinite | Infinite | 900 | 180 | 300 | Infinite |
| | 30 cm reinforced concrete wall | Infinite | Infinite | 840 | 120 | 54 | N/A |
| | 20 cm reinforced concrete wall | Infinite | Infinite | 600 | 120 | 0 | N/A |
| | Wood studs and sheetrock | 60 | 30 | 30 | 30 | 0 | N/A |
| Doors | 60 cm steel and concrete rolling door | Infinite | Infinite | 930 | 200 | 300 | N/A |
| | 30 cm steel and concrete rolling door | Infinite | Infinite | 640 | 160 | 54 | N/A |
| | 30 cm wood door with metal sheeting | Infinite | Infinite | 530 | 160 | 30 | N/A |
| | 10 cm wood door with metal sheeting | Infinite | 300 | 180 | 30 | 0 | 5 for large vehicle door |
| | 5 cm wood door | Infinite | 12 | 12 | 12 | 0 | N/A |
| | 5 cm wood door with glass panel | Infinite | 12 | 12 | 12 | 0 | N/A |
| | 1.5 cm steel plate door | Infinite | 300 | 60 | 30 | 0 | N/A |
| | .75 cm steel plate door | Infinite | 300 | 30 | 30 | 0 | N/A |
| | Class V or VI vault door | Infinite | 480 | 60 | 60 | 0 | N/A |
| | Steel turnstile | Infinite | 72 | 18 | 18 | 0 | N/A |
| Miscellaneous Barriers | High security padlock | Infinite | 90 | 60 | 30 | 0 | N/A |
| | Concrete Block Vehicle Barrier | 0 | 300 | 300 | 30 | 0 | 5 |
| | 2.5 m chain link mesh fence | 10 | 10 | 10 | 10 | 0 | 1 |
| | Welded wire fabric fence | 10 | 10 | 10 | 10 | 0 | 1 |
| | 2.5 m concrete panel wall | 10 | 10 | 10 | 10 | 0 | N/A |
| | Tempered glass window | 5 | 5 | 5 | 5 | 5 | N/A |
| | Electromagnetic Strike Lock | 15 | 10 | 5 | 5 | 2 | N/A |

### *I.1.12.2. Guard delay component class*

TABLE I.10. SAMPLE GUARD DELAY VALUES

| Component Type | Component Description | No Equipment (seconds) | Small Arms (seconds) | Light Antitank Weapons (LAW) (seconds) |
|---|---|---|---|---|
| Guard at Post Delay | Unprotected post | 30 000 | 0 | 0 |
| | Small arms protected post | 30 000 | 30 | 0 |
| | Unprotected post normally but moves to small arms protected position on alert | 30 000 | 30 | 0 |
| | LAW protected post | 30 000 | 125 | 125 |
| | Unprotected post normally but moves to LAW protected position on alert | 30 000 | 125 | 125 |
| | Small arms protected post normally, but moves to LAW protected position on alert | 30 000 | 125 | 125 |
| Guard in Tower Delay | Small arms resistance | 60 | 30 | 0 |
| | LAW resistant tower | 125 | 125 | 60 |

### *I.1.12.3. Penetration times - fences*

TABLE I.11. SAMPLE FENCE PENETRATION TIMES

| | | | Penetration Time (Minutes) | | | |
|---|---|---|---|---|---|---|
| Barrier Description | Penetration Equipment | Equipment Weight (kg) | Min. | Mean | Max. | Standard Deviation |
| 2.5-m chain-link mesh with outriggers 4-mm x 50-mm mesh | Ladder | 5.0 | 0.1 | 0.2 | 0.3 | 0.04 |
| | Tarpaulin | 2.0 | 0.1 | 0.2 | 0.3 | 0.04 |
| | Pliers | 1.0 | 1.0 | 2.0 | 3.0 | 0.41 |
| | Manual bolt cutters | 3.0 | 0.5 | 1.0 | 1.5 | 0.20 |
| | Circular saw | 10 | 0.5 | 1.0 | 1.5 | 0-20 |
| | Manual bolt cutters, gloves (more cuts) | 3.5 | 0.75 | 1.5 | 2.25 | 0.31 |
| | Circular saw (more cuts) | 11.0 | 0.75 | 1.5 | 2.25 | 0.31 |
| | Gloves | 0.5 | 0.1 | 0.2 | 0.3 | 0.04 |
| Vinyl-coated 3-mm x 50-mm mesh | Manual bolt cutters | 3.0 | 0.5 | 1.0 | 1.5 | 0.20 |
| | Pliers | 1.0 | 1.0 | 2.0 | 3.0 | 0.41 |
| | Circular Saw | 11.0 | 0.75 | 1.5 | 2.25 | 0.31 |
| 2.5-m chain-link mesh without outriggers vinyl-coated, 1.8-mm x 40-mm mesh | Ladder | 5.0 | 0.1 | 0.2 | 0.3 | 0.04 |
| | No equipment | 0.0 | 0.05 | 0.10 | 0.15 | 0.02 |
| | Manual bolt cutters | 3.0 | 0.5 | 1.0 | 1.5 | 0.20 |
| | Pliers | 0.5 | 1.0 | 2.0 | 3.0 | 0.41 |
| | Vise-grip pliers | 0.5 | 0.30 | 0.60 | 0.90 | 0.12 |

### *I.1.12.4. Penetration times – gates*

TABLE I.12. SAMPLE GATE PENETRATION TIMES

| | | | Penetration Time (Minutes) | | | |
|---|---|---|---|---|---|---|
| Barrier Description | Penetration Equipment | Equipment Weight (kg) | Min. | Mean | Max. | Standard Deviation |
| Chain-link mesh pipe 2.4-m x 4-m chain-link gate on metal pipe frame, chained and padlocked | Truck | 1,500 | 0.05 | 0.1 | 0.15 | 0.02 |
| | Pliers | 1.0 | 1.0 | 2.0 | 3.0 | 0.41 |
| Chain-link mesh pipe 1.2-m x 2.4-m gate, 11-gauge x 5-cm mesh on 4.8-cm metal pipe frame, chained and padlocked | Sledgehammer | 5 | 0.5 | 1.0 | 1.5 | 0.20 |
| | 1.8-m pry bar | 10 | 1.0 | 2.0 | 3.0 | 0.41 |
| | Bolt cutters | 3 | 0.75 | 1.5 | 2.25 | 0.31 |
| | Hacksaw | 0.2 | 1.0 | 2.0 | 3.0 | 0.41 |

### *I.1.12.5. Penetration times - walls*

TABLE I.13. SAMPLE WALL PENETRATION TIMES

| | | | Penetration Time (Minutes) | | | |
|---|---|---|---|---|---|---|
| Barrier Description | Penetration Equipment | Equipment Weight (kg) | Min. | Mean | Max. | Standard Deviation |
| Concrete-10 cm Thick, Reinforced Concrete-210 kg/cm$^2$ one layer, 6.4-mm dia., 15-cm x 15-cm mesh | Sledgehammer, hand bolt cutters | 10 | 2.0 | 4.0 | 6.0 | 0.82 |
| | Sledgehammer, cutting torch | 30 | 2.5 | 5.0 | 7.5 | 1.02 |
| | Circular saw, sledge-hammer | 5 | 4.3 | 8.6 | 12.9 | 1.76 |
| | Roto-hammer, chisel, punch, sledgehammer, hand bolt cutters, generator | 50 | 3.2 | 6.4 | 9.6 | 0.57 |
| | Explosives (1.0), sledgehammer, manual bolt cutters | 20 | 2.3 | 3.5 | 5.25 | |
| | Explosives (3.0), hand bolt cutters | 10 | 1.2 | 2.5 | 3.7 | |
| | Explosives (5.0), hand bolt cutters | 7 | 1.2 | 2.3 | 3.4 | |
| | Explosive (10) | 10 | 1.0 | 2.0 | 3.0 | |
| | Sledgehammer, hand hydraulic bolt cutters | 20 | 2.4 | 4.8 | 7.2 | 0.98 |

TABLE I.13. SAMPLE WALL PENETRATION TIMES (CONT.)

| Barrier Description | Penetration Equipment | Equipment Weight (kg) | Penetration Time (Minutes) Min. | Mean | Max. | Standard Deviation |
|---|---|---|---|---|---|---|
| Concrete-20 cm Thick, Reinforced Concrete-210 kg/cm$^2$ one layer, No. 5 rebar, 15-cm centers | Rotohammer, drill, sledge, chisel, punch, cutting torch, generator | 65 | 7.0 | 14.0 | 21.0 | 2.86 |
| | Explosives (2.0), sledgehammer, hand hydraulic bolt cutters | 30 | 4.3 | 6.5 | 9.7 | |
| | Explosives (3.0), hand hydraulic bolt cutters | 20 | 2.5 | 3.75 | 5.6 | |
| | Explosives (5.0), hand hydraulic bolt cutters | 22 | 2.5 | 3.75 | 5.6 | |
| | Explosives (12) | 12 | 1.5 | 3.0 | 4.5 | |
| Concrete-30 cm Thick, Reinforced Concrete- 210 kg/cm$^2$ one layer, No. 4 rebar, 15-cm centers | Explosives (5.0), hand bolt cutters | 8 | 2.2 | 3.25 | 4.9 | |
| | Explosives (7), hand bolt cutters | 9 | 2.3 | 3.5 | 5.2 | |
| | Explosives (12), hand bolt cutters | 14 | 2.5 | 3.8 | 5.6 | |
| | Explosives (16), hand bolt cutters | 18 | 2.5 | 3.8 | 5.6 | |

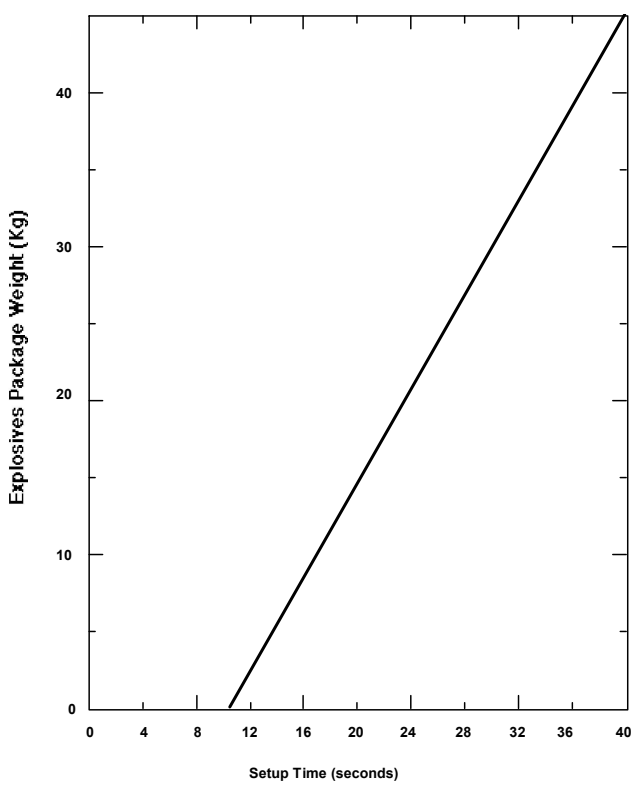



*FIG. I.16 Time required to set an explosives package as a function of package weight*

## REFERENCES


[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Final Report - Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Medical Irradiator Facility Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Coordinated Research Project, J02004, Transport of Radioactive Material Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage, Nuclear Security Series No. 4, IAEA, Vienna (2008).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Nuclear Security Series No. 16, IAEA, Vienna (2012).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Rev. 5), Nuclear Security Series No. 27-G, IAEA, Vienna (in preparation).

[8] H. Donnelly, Fullwood, R., and Glancy, J. et al,. VISA – A Method for Evaluating the Performance of Integrated Safeguards Systems at Nuclear Facilities, NUREG-0317, Vol. 1 and 2, Science Applications, Inc., (1977)

[9] Sandia National Laboratories, The Hypothetical Facility Exercise Date - Lone Pine Nuclear Power Plant - The Twenty-Sixth International Training Course (2016)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[11] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues), National Academy Press, Washington, DC (1997).

## ABBREVIATIONS

| | |
|---|---|
| 3D | Three dimensional |
| ASD | Adversary sequence diagram |
| BMS | Balanced magnetic switch |
| CAS | Central alarm station |
| CCTV | Closed-circuit television |
| CRP | Coordinated research project |
| DBT | Design basis threat |
| DOR | Door |
| H | High |
| IAEA | International Atomic Energy Agency |
| KIA | Killed in action |
| L | Low |
| LAA | Limited access area |
| LPNPP | Lone Pine Nuclear Power Plant |
| M | Moderate |
| NM | Nuclear material |
| NMAC | Nuclear material accounting and control |
| NPP | Nuclear power plant |
| NUSAM | Nuclear security assessment methodologies |
| $P_A$ | Probability of assessment |
| $P_D$ | Probability of detection |
| $P_{DET}$ | Probability of deterrence |
| $P_E$ | Probability of system effectiveness |
| $P_I$ | Probability of interruption |
| $P_N$ | Probability of neutralization |
| $P_S$ | Probability of sensing |
| PA | Protected area |
| PER | Personnel portal |
| $P_H/P_K$ | Probability hit/probability kill |
| PPS | Physical protection system |
| R | Measure of risk |
| RF | Response force |
| RFT | Response force time |
| SA | Security assessment |
| SAS | Secondary alarm station |
| SAVI | Systematic analysis of vulnerability to intrusion |
| SME | Subject matter expert |
| STAGE | Simulation toolkit and generation environment |
| SUR | Surface element |
| TA | Threat assessment |
| TNT | Trinitrotoluene |
| TT | Tabletop |
| TTX | Tabletop exercise |

| | |
|---|---|
| URC | Unacceptable radiological consequences |
| VEH | Vehicle portal element |
| VH | Very high |
| VISA | Vulnerability to intrusion system analysis |
| VL | Very low |
| VVL | Very very low |

## LIST OF PARTICIPANTS

| | |
|---|---|
| Alam, B | Bangladesh Atomic Energy Commission, Bangladesh |
| Brüecher, W. | GRS, Germany |
| Chetaine, A. | University of Mohammad V Rabat, Morocco |
| Contri, A | Rhino Corps, United States of America |
| Edwards, J. | National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland |
| Garrett, A. | International Atomic Energy Agency |
| Greenhalgh, D. | Oak Ridge National Laboratory, United States of America |
| Hall, C. | Expert, United States of America |
| Hill, S. | Sandia National Laboratories, United States of America |
| Hogan, T. | Sandia National Laboratories, United States of America |
| Hwang, M. | Korea Atomic Energy Research Institute, Republic of Korea |
| Iwuala, E. | Nigerian Nuclear Regulatory Authority, Nigeria |
| Izmaylov, A. | State Co. Scientific Production Union "Eleron", Russian Federation |
| Jang, S. | International Atomic Energy Agency |
| Jones, B. | Rhino Corps, United States of America |
| Jung, W. | Korea Atomic Energy Research Institute, Republic of Korea, |
| Kawata, N. | Japan Atomic Energy Agency, Japan |
| Kibria, F. | Bangladesh Atomic Energy Commission, Bangladesh |
| Knight, J. | ARES Security Corporation, United States of America |
| Leach, J. | Sandia National Laboratories, United States of America |
| Lee, J. | Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea, |
| Legoux, P. | World Institute for Nuclear Security |
| Lindahl, P. | OKG AB, Sweden |
| Little, R. | Quintessa Ltd., United Kingdom |
| Mahmood, R. | Pakistan Nuclear Regulatory Agency, Pakistan |
| Malach, J. | EBIS, Czech Republic |
| Malachova, T. | EBIS, Czech Republic |
| Mahdi, A. | Iraqi National Monitoring Authority |
| Malik, S. | National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland |
| Martin, K. | Oak Ridge National Laboratory, United States of America |
| Naoko, N. | Japan Atomic Energy Agency, Japan |
| Norichika, T. | Japan Atomic Energy Agency, Japan |
| Reynolds, J. | National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland |
| Rivers, J. | Nuclear Regulatory Commission, United States of America |
| Rodger, R. | National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland |
| Scott, J. | National Nuclear Laboratory, United Kingdom of Great Britain and Northern Ireland |
| Sergovantsev, P. | State Co. Scientific Production Union "Eleron", Russian Federation |
| Shaheen, H. | Egyptian Nuclear and Radiological Regulatory Authority, Egypt |
| Shakoor, A. | Pakistan Nuclear Regulatory Agency, Pakistan |
| Shridhar, A. | Bhabha Atomic Research Centre, India |
| Shull, D. | International Atomic Energy Agency |
| Snell, M. | Sandia National Laboratories, United States of America |
| Stangebye, J. | SKB, Sweden |
| Stefanka, Z. | Hungarian Atomic Energy Authority, Hungary |
| Terao, N. | Japan Atomic Energy Agency, Japan |
| Vaclav, J. | UJD SR, Slovakia |
| Yamaguchi, T | Japan Atomic Energy Agency, Japan |
| Zahnle, P | ARES Security Corporation, United States of America |
| Zielman, B | URENCO Nederland B.V., Netherlands |

## Consultants Meeting

Vienna, Austria: 6–8 March 2013, 3–4 February 2014, 17–21 March 2014, 2–3 September 2014, 13–17 October 2014, 16–20 March 2015, 13–17 April 2015, 10–14 August 2015, 27 June–1 July 2016

Preston, United Kingdom: 9-13 February 2015

Albuquerque, New Mexico, United States of America: 2-6 November 2015

Daejeon, Republic of Korea: 14-18 March 2016