IAEA-TECDOC-1868

TRANSPORT OF RADIOACTIVE MATERIAL 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. OBJECTIVES 2
   - 2.3. TASKS AND FUNCTIONS 2
   - 2.4. OUTCOMES 3

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

4. COLLECTING REQUIRED INFORMATION 3
   - 4.1. TRANSPORT CHARACTERIZATION 3
   - 4.2. TARGET IDENTIFICATION 4
   - 4.3. THREAT DEFINITION 4

5. CONDUCTING ASSESSMENT 6
   - 5.1. PROCESS FOR USING THE TABLETOP EVALUATION METHOD 6
   - 5.2. DEVELOPMENT OF SCENARIOS 7
   - 5.3. TABLETOP MODEL AND IMPLEMENTATION 10
   - 5.4. NUSAM TABLETOP RESULTS 11
     - 5.4.1. Scenario condition: theft scenario 1— steal transport vehicle 11
     - 5.4.2. Scenario results: theft scenario 1— steal transport vehicle 12
     - 5.4.3 Scenario condition: theft scenario 2— steal material container or materials 13
     - 5.4.4 Scenario results: theft scenario 2— steal material container or materials 14
     - 5.4.5. Scenario condition: sabotage scenario 1— radiological dispersion device with explosives 14
     - 5.4.6 Scenario results: sabotage scenario 1— radiological dispersion device with explosives 15

6. OVERALL ASSESSMENT OF SECURITY 16
   - 6.1. ASSESSMENT TOOL SUMMARY 16
     - 6.1.1 Tabletop observations 16
   - 6.2. EVALUATION AND REPORTING 17
     - 6.2.1. Prescriptive requirements 17
     - 6.2.2. Performance-based requirements 17
   - 6.3. COMBINED ASSESSMENT 17
   - 6.4. UNCERTAINTIES AND ASSUMPTIONS 18

APPENDIX I GAMMA SECURE P/L HYPOTHETICAL TRANSPORT SECURITY PLAN..... 19
I.1. INTRODUCTION 19
I.2. OBJECTIVES 19
I.3. APPLICABILITY 19
I.4. ADMINISTRATIVE REQUIREMENTS 20
I.4.1. Policies, procedures and operations 20
I.4.2. Testing and evaluation of the security plan 20
I.4.3. Review and update of the security plan 20
I.4.4. Readiness review and assessment 21
I.4.5. Reporting of threats and incidents 21
I.5. RESPONSIBILITIES 21
I.5.1. Allocation of responsibilities 21
I.5.2. GSPL organization structure 21
I.5.3. Trustworthiness 21
I.5.4. Training 22
I.6. INFORMATION MANAGEMENT 22
I.6.1. Information security 22
I.6.2. Records retention 22
I.7. TRANSPORT SECURITY MEASURES 22
I.7.1. Primary and alternative routes 22
I.8. DESCRIPTION OF THE SECURITY SYSTEM 23
I.8.1. Equipment and modes of transport 23
I.8.2. Operations command and control 24
I.8.3. Additional security measures 24
I.8.4. Maintenance and testing of security systems and equipment 24
I.8.5. Emergency response 24
I.8.6. Non-tactical and tactical emergency response 25
I.8.7. Incident communication 25
I.8.8. Notification of relevant agencies 25
I.9. SECURITY MEASURES OVERVIEW 25
I.10. ADDITIONAL SECURITY MEASURES 28
I.10.1. Procedures for normal operations 28
I.10.2. Procedures for security incidents (especially for unplanned stops) 28
I.11. RESPONSE FORCE DATA 28
I.11.1. State police escort 28
I.11.2. State police tactical response team 29
I.11.3. Local police 29
I.11.4. Response procedures 30
I.12. AVERAGE RESPONSE PERFORMANCE DATA 30

APPENDIX II 31

DESCRIPTION OF TABLETOP METHODOLOGIES 31
II.1. INTRODUCTION 31
II.2. OAK RIDGE NATIONAL LABORATORY BATTLEBOARD TABLETOP

METHODOLOGY 31
II.2.1. ORNL BattleBoard P_H/P_K 31
II.2.2. How the simulation progresses 31
II.2.3. ORNL BattleBoard tabletop methodology rules 32
II.3. SANDIA NATIONAL LABORATORIES TABLETOP METHODOLOGY 41
II.3.1. SNL TTX P_H/P_K 41
II.3.2. SNL TTX methodology process 43

REFERENCES 45

ABBREVIATIONS 47

LIST OF PARTICIPANTS 49

1. INTRODUCTION

1.1 BACKGROUND

This publication provides Member States with a hypothetical transport of radioactive material 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 transport of radioactive material. 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 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 transport of radioactive material.

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 transport of radioactive material. 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 conduct of the SA. Section 6 describes the overall summary of the security assessment for the SA.

Appendix I provides a hypothetical security plan containing detailed information that was used to conduct the SA. Appendix II provides a description of tabletop methodologies used for 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 that would be expected to be relevant for Member States, which are expected to participate in the NUSAM project, are nuclear power plants (Ref. [2]), spent fuel storage facilities, Category 1 source facilities (Ref. [3]), transport of Category 1 sources 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 included as security cases for the NUSAM project.

This case study will address transport. Transport of radioactive materials poses a different challenge for security than fixed sites containing these materials. While in transport, the adversary can choose any location on the transportation route to attack the transport vehicle and either sabotage the material or steal it. Much of the security results from the strength of the transport container and response forces. The container provides delay against the adversary gaining access to the material, as well as protection against projectiles that might be shot at the container/material. Other security measures that might be employed include escorts (armed or unarmed), communications, global positioning system (GPS) tracking, response from authorities in local law enforcement and safe havens.

2.2. OBJECTIVES

The transport of material case study working group needed to develop a detailed model of the facilities to demonstrate the use and applicability of the NUSAM methodological framework and the recommended information, tools and approaches developed by the methodological working groups. The development of transport of material case study 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.

The purpose of this transport of material case study is to guide an operator on how to assess their transport security of radioactive source by a performance-based approach using NUSAM methods. A performance-based approach is not required for radioactive sources, as documented in Ref. [4]. However, the Member State could use this method for high consequence materials, under a high-threat level, or in order to ensure the effectiveness of prescriptive measures against the threat. Transport of radioactive source material was selected for this case study because of its frequency of movement and significances to Member States. This method also can be applied to nuclear materials.

2.3. TASKS AND FUNCTIONS

To realize the objectives of the transport of material 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 list the Guidelines/ Regulations/ Policies applicable to the case study;
- Compiling and describing 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.

Throughout the project, the working group proposed and communicated any potential enhancements to the methodological framework to the Coordinating Group.

2.4. OUTCOMES

In order to produce the expected outcome, the transport of material case study working group:

- Deveoped a detailed transport model and associated information for the activity;
- Documented assessment of nuclear security systems using the NUSAM methodological framework, including assumptions 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 is extensive official documentation on the need for, and methods of achieving, the security of nuclear materials and processes from external threats. The documentation ranges 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 them. These procedures typically become formal regulatory requirements for the facility/activity.

The operator (i.e. shipper/carrier), is responsible and accountable for the security of the facility and its materials. The shipper/carrier 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 what they are intended to. Both the regulator and shipper/carrier have a common interest in identifying which elements of the security system are effective and also how efficient and cost effective they are.

3.2. REQUIREMENTS

The requirement to protect nuclear material against unauthorized removal and sabotage is based on Refs [5–7] The main objective to be fulfilled in this case study was to evaluate the effectiveness of the physical protection measures to prevent unauthorized removal and sabotage of material during transport.

4. COLLECTING REQUIRED INFORMATION

4.1. TRANSPORT CHARACTERIZATION

The description contained as part of the transportation security plan (TSP) is hypothetical and provided solely for use as a case study. This transport security plan was developed for the road transport of Category 1 radioactive source material. The material is transported from the sterilization factory of Gamma Secure P/L (GSPL) located in Central City, Lagassi to the warehouse of Kobalt Service P/L (KSPL) in Industrial City, Lagassi.

The transport vehicle is a 10-ton truck with the following security measures installed and, prior to shipment, verified the following items:

- Enclosed cargo compartment;
- Lockable doors;
- Barrier between driver’s compartment and cargo area;
- Communications to Gamma-Secure P/L Transport Command Centre (TCC); and
- Meets the European Agreement concerning the International Carriage of Dangerous Goods by Road standards.

A detailed characterization of the transport operation used in this analysis is contained within Appendix I.

4.2. TARGET IDENTIFICATION

The radioactive material contained within the transport are Category 1 Cobalt-60 (^{60}Co) pencils. The details of the package used to transport the fresh radioactive source(s) are:

- Activity: 100 Terabecquerel
- Chemical Nature: Metal
- Physical Form: Solid
- Hazard: Radiation
- Packaging: Type B
- Package Mass: 5445 kilogram
- Package Height" 1.456 metre
- Package Diameter: 1.013 metre
- Certificate: A/1002/B(U)
- No. of Packages: One

It was assumed that once the adversaries were able to stop the convoy and neutralize the transport escorts, a hypothetical sabotage task time of 120 seconds was required to complete their task.

4.3. THREAT DEFINITION

The National Alert Level as set by the Lagassi National Counter-Terrorism Committee shall be used for the shipment as the threat level in conjunction with the Design Basis Threat (DBT). Table 1 characterizes the DBT, as established by the Lagassi National Counter-Terrorism Committee. In the event that an elevated threat occurs, further implementation of appropriate additional security measures may be required by the competent authority.

TABLE 1. THREAT CHARACTERIZATION

Threat Characteristics	Protestors	Criminals	Terrorists	Insider
Motivation	Ideological	Economic	Political, Ideological	Economic, Ideological, or Ego
Intention	To disrupt operations, gain notoriety, and to recruit others to their cause.	Theft of radioactive material for extortion, coercion, or transfer to a third party for economic gain.	Theft of radioactive material with the intention to use it maliciously in-situ or elsewhere, transfer to a third party, or use for violence or threat of violence. To gain notoriety, disrupt operations, recruit others to their cause, and convince funding sources of capabilities and reach. May change strategies from	Individual in any position or role. Theft of radioactive material. Damage a source device. Revenge against co-worker or management. Disrupt operations by sabotaging process, equipment, or materials. Generally, to remain anonymous.
Number	Hundreds	3	3	1
Weapons	No	Pistols, vehicles	Rifles, vehicles, and grenades	No
Explosives	No	Yes	Yes	No
Tools	Yes	Tools for breaching barriers, locks, and communications equipment, etc.	Tools for breaching barriers, locks, and communications equipment. In some cases, acquisition of heavy vehicles or equipment (such as mobile cranes) is possible, etc.	Yes. Those available to a worker of noted position and capability, including all tools to secure, move, communicate, authorize, and change transport characteristics.
Transportation	Yes	A vehicle to transport personnel to the location, and/or provide radioactive source transport, and perhaps move material from one vehicle to another.	A vehicle to transport personnel to the location, and/or provide radioactive source transport, and perhaps move material from one vehicle to another.	Yes. Vehicles allowed for the insider position, such as site vehicles, transport vehicles, heavy vehicles, lifting vehicles, and perhaps police escort vehicles for theft and sabotage scenarios.
Technical Skills	No	Well trained in criminal trespass and in the use of tools Familiarity with handling of radioactive materials	Well trained in criminal trespass and in the use of tools Familiarity with handling of radioactive materials	Access to security information; technical data; movement schedules, personnel information; physical access to materials; vehicles; communications equipment, frequencies, and procedures; site and transport information; response information; locks and keys, etc. Familiar with handling radioactive material
Funding	Maybe	Yes	Yes	Yes

TABLE 1. THREAT CHARACTERIZATION (CONT.)

Threat Characteristics	Protestors	Criminals	Terrorists	Insider
Insider Collusion	Yes	Provides information about target, routing, timing for transport, physical security delay and detection information, and response information. May participate by, for example, facilitating entrance and exit, disabling alarms and communication Will not participate in violent activity.	Provides information about target, routing, timing for transport, physical security delay and detection information, and response information. May participate by, for example, facilitating entrance and exit, disabling alarms and communication Will not participate in violent activity	Single insider colluding with outsiders.
Support Structure	Yes	Yes	Yes	All internal privileges and access authorizations, up to and including tools, vehicles, communications, procedure, locks and keys, and personnel information
Willing to kill/die	No	Determined and willing to use violence. Not willing to die and will attempt to flee if interrupted with force.	Determined and willing to use violence. Willing to die and to kill others in all phases of the attack. May change strategies from theft to sabotage if threatened	Non-violent

5. CONDUCTING ASSESSMENT

Many tools can be used to evaluate the effectiveness of security at a fixed site. However, these tools do not lend themselves to evaluate the complexities of material in transport. These complexities include dynamic changes in the environment (i.e., road conditions, terrain, choke points, communication to responders, etc.). It was determined that due to the unique requirement of material in transport, the tabletop method would account for these various changing conditions.

5.1. PROCESS FOR USING THE TABLETOP EVALUATION METHOD

The analysis approach for the manual evaluation method of a tabletop exercise is depicted using a common diagram (Figure 1).

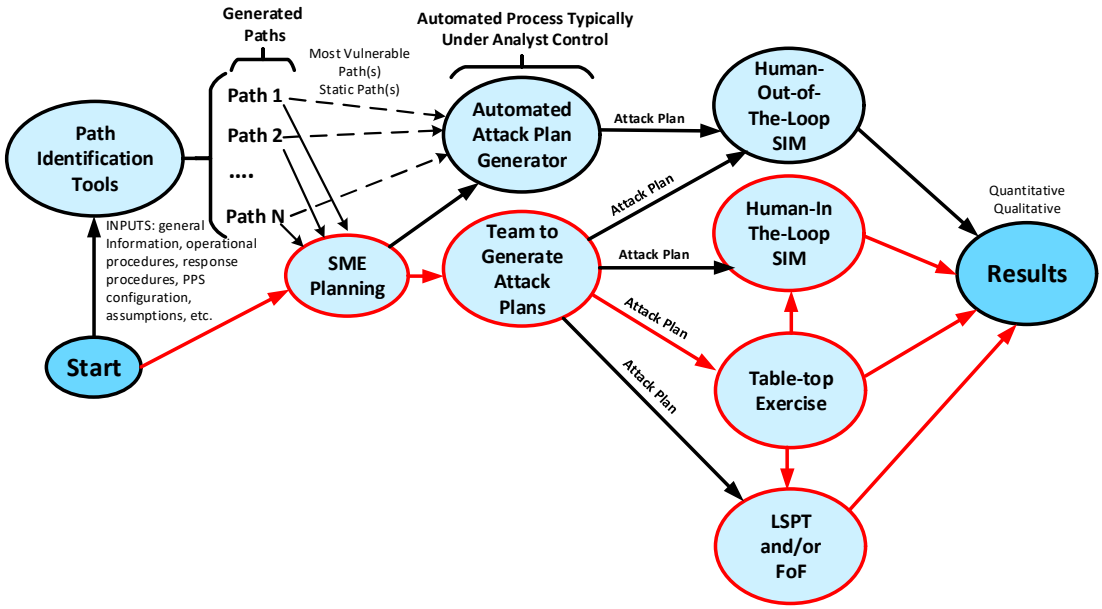


FIG. 1. Scenario analysis process overview for tabletops

The analysis process begins at the start node. Prior to the planning process, general information such as convoy configuration, route information, target configuration/packaging, etc., is gathered. Based upon the provided information, the description of the path can then be used by a subject matter expert to plan an adversary attack plan.

5.2. DEVELOPMENT OF SCENARIOS

The transport security working group developed three scenarios which test and demonstrate different considerations for basic, enhanced, and additional measures used and applied to the example case in NUSAM working materials. The working group identified two theft and one sabotage scenario, each with different characteristics according to the materials provided, the guidance received, and the working group discussions and decisions. They are based upon the threat characteristics outlined in Table 1. For details regarding the process for scenario selection, refer to Ref. [1].

Adversary characteristics were used to imply and develop general DBT capabilities, weapons, tools, and tactics. The DBT selected by the working group represents a blending of the above adversary characteristics, and should be considered credible (that is, the adversaries will be assumed to be proficient in all competencies necessary to complete the tasks of theft or sabotage). These were used to generate the scenarios summarized in Table 2.

TABLE 2. SCENARIO ATTRIBUTES/PARAMETERS

Considered parameters	Theft scenario I	Theft scenario II	Sabotage scenario I
1. Threat assessment			
a. Motivation	a. Ideological	a. Ideological	a. Ideological
b. Intention: theft or sabotage	b. Theft	b. Theft	b. Sabotage in-situ
c. Capabilities: insider collusion	c. Passive insider and small team tactics	c. Active insider, small team tactics, and additional technical skills	c. Small team tactics and explosives
2. Number of adversaries	3	3 + 1 (driver escort)	3
3. General objective	Theft of vehicle	Theft of package (or materials, as a blended scenario)	Dispersion of material in-situ
4. Strategy for initial attack			
a. Stop vehicle • Deceit:(demonstrator, ambulance, fire fighter) • Ambush • Force (e.g. crash and direct attack)	Rolling ambush Using force through directly engaging escort in a crash and with small weapons	Deceitful unplanned stop using road construction	Rolling ambush to block road, then use of small weapons to engage police
5. Strategy to Neutralize Personnel			
a. Neutralize guards	Neutralize police	Neutralize police	Block road between escort and transport vehicle
b. Neutralize driver	Neutralize driver and escort	Neutralize driver	
c. Separate escort vehicle			Neutralize police
6. Strategy to delay response			
a. Jamming to communication	Kill police, driver, and escort to minimize communication	Kill police and driver to minimize communication	Strategy includes encouraging expedited response at or near radiological dispersion device time detonation
b. Disable GPS	Jam communication	Driver escort reports OK to TCC	
c. Divert	Disable GPS	Disable GPS	
d. Block road			
7. Strategy to steal or to attack package			
a. Take control of transport vehicle	Take control of transport vehicle	Take control of transport vehicle	Take control of transport vehicle
b. Moving package to second vehicle	Escape along a different route from planned transport route	Moving package to second vehicle	Force driver to provide tools or use bolt extraction tools
c. Removing material from package	Escape along a different route from planned transport route	Escape along a different route from planned transport route	Remove material from package
			Attach explosive to material and detonate
			Escape not necessary, though possible

TABLE 2. SCENARIO ATTRIBUTES/PARAMETERS (CONT.)

Considered Parameters	Theft I	Theft II	Sabotage I
8. Weapons and Tools			
a. Vehicles	Car for initial crash	Fake construction vehicle with amber lights (could be the crane vehicle listed below)	Truck (for blocking)
b. Weapons	Rifles/Grenades	Second truck with mounted crane	Rifles/Grenades
c. Explosives	Tools to cut GPS transmitter	Rifles/Grenades	Explosives
d. Tools		Construction uniforms	Bolt extraction tools (backup)
		Radio/Cell-phone from driver	
		Tools to cut GPS transmitter	
		Bolt-cutter to remove locks and tie-downs	
9. Location of action			
a. Distance from city:	a. Far from city	a. Far from city	a. In city
Types of road:	b. Highway	b. Highway	b. Crossroad
• Highway	c. Mountain	c. Mountain	c. Flat
• Rural road	d. Moderate traffic	d. Low traffic	d. Forced traffic jam
• Unpaved road			
• Crossroad			
• Tunnel,			
• Bridge			
b. Topographic features:			
• Forest			
• Desert			
• Mountain			
• Near water			
c. Traffic conditions:			
• Traffic jam			
• Unpopulated road			
10. Time: day or night (Weather: Random)	Day	Night	Day

Tabletop Purpose: To demonstrate how a manual analysis process can be applied to determine quantitative and/or qualitative information about the effectiveness of a transport operation.

Scope: The simulation includes an evaluation of the designed physical protection system in conjunction with primary and secondary response forces as part of an overall response contingency.

Objectives: To determine how effective the transport operation is against an adversary profile and postulated scenarios.

Adversary objectives: Theft and/or sabotage of target material.

The following highlight the termination conditions for the tabletop:

- Adversaries win if they complete their theft or sabotage task OR response forces have been neutralized to the point there are no response forces that can engage the adversary for the rest of the scenario; or
- Response forces win if adversary forces are degraded to the point that they cannot complete their task.

5.3. TABLETOP MODEL AND IMPLEMENTATION

A tabletop (TT) exercise is an analysis methodology intended to determine how well a given protection system performs against a defined set of conditions as well as 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 against, 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.

Tabletop 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 changes to improve the system. Using the tabletop tool, 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 exercise 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 group's goals.

In a more advanced TT exercise, the level of detail required throughout is typically much more extensive. Significant detail is defined in the characterization process as well as the documentation and validation processes. These advanced TTs are more disciplined and more precise in their results and actions. 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 3-dimensional scaled model. The 3-dimensional 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.

Additionally, play can become more complex by introducing in-scenario cues. In these cases, play advances as players receive pre-scripted messages that may be in the form of statements of communications from the central alarm station or that events are happening on the site that persons leading the response are to consider. An example is communication received of an explosion in the vicinity of a building of concern. These cues can be additional information to carry out the scenario or they may be intended to be distractions for the response to measure their knowledge and training of a tactical plan. A facilitator usually introduces cues one at a time in the form of a written message, simulated telephone call, videotape, or other means. Players discuss the issues raised by each cue, referencing established authorities, plans, and procedures for guidance. Player decisions are incorporated as the scenario continues to unfold. Player reaction to the cues is recorded and later graded.

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.

The transportation security TT exercise provides the operator or regulator with a tool to assess and evaluate the effectiveness of personnel, physical protection equipment, inter-agency planning and response coordination and overall radioactive material transport security policies and procedures.

Aside from the TT exercise methods, there are several other tabletop tools available. Each have their value in evaluating a nuclear security programme, including:

- Vulnerability to Intrusion System Analysis (VISA); and
- Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability (CARVER).

All tabletop methods rely heavily on the expert judgement of the subject matter expert(s) 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.

5.4. NUSAM TABLETOP RESULTS

Two different TT exercise approaches were used to analyze the effectiveness of the transport operation. These approaches included the Oak Ridge National Laboratory (ORNL) BattleBoard tabletop and the Sandia National Laboratory (SNL) Tabletop Methodologies. Details on these approaches used, their rules of play, and associated data libraries, etc., are documented in Appendix II. The following summarizes the analysis of the scenarios developed by the NUSAM working group.

5.4.1. Scenario condition: theft scenario 1— steal transport vehicle

Theft scenario 1 is considered the most common transportation event: the theft of the vehicle containing a radioactive source during a planned or unplanned stop. This scenario recognizes the risk exposure of the transport vehicle to incursion by vehicles which may follow or join the convoy with the objective to disable the escort vehicle, engage police directly, and gain control of the shipping vehicle. This is a common theme throughout the scenarios as presented—the time required for transport personnel to recognize intentional accidents as a pre-cursor to attack.

This attack method appears to be accidental at first, and thus reduces the probability that police and transport vehicle personnel immediately call authorities. The adversary team plans to keep the distances for engagement relatively short to improve shooting accuracy. Under this circumstance, the adversaries have immediate awareness of convoy actions to notify response.

This scenario also presents a distinct advantage for the adversaries in planning and plan execution, in that they do not need to bring additional equipment as described in Theft scenario 2 (5.4.3). This plan may not strictly require an insider, though advance notification of the shipment timing and shipment

characteristics would be helpful. Careful adversary observation of previous transport mission routing and unscrupulous operational security factors (e.g. publicity about the transportation event) could also aid adversary planning efforts.

Vehicles are easy to obtain through rental, purchase, or theft, and using one to impact another vehicle is a common occurrence. The ability to obtain pistols, rifles, and grenades (grenades are not required as part of this scenario) through legal or illegal means varies in every country, but it is possible in most parts of the world based on crime studies. The effective use of small arms requires training and practice to be effective. Based on the availability of firearms and locations to train with them, adversaries could train with small arms in a separate location and travel to the area of operations with these skills intact.

Theft scenarios 1 and 2 do not make use of radioactive material handling skills. The win condition is if the adversaries successfully leave the scene without responders in direct contact with them. The material(s) may then be used or sold later as conditions permit based on the effectiveness of a national response strategy. Figure 2 reflects the area map used to evaluate the theft scenario.

FIG. 2. Area map: theft scenario 1—steal transport vehicle

5.4.2. Scenario results: theft scenario 1— steal transport vehicle

Scenario 1 concluded after 240 seconds as an adversary win. Sixty seconds into the attack, the adversaries engaged the escort vehicle and neutralized both the driver and passenger, leaving only one escort 'combat effective'. Within 30 to 60 seconds, the adversary team was able to engage the lead escort vehicle and neutralize both the driver and the passenger. At the 180-seconds time mark, the adversaries were able to gain access to the cabin of the transport vehicle and drive away at 240 seconds. In this scenario, communication to the TCC started at 90 seconds and resulted in the start of the secondary response at 120 seconds. Figure 3 illustrates the timeline of events for theft scenario 1.

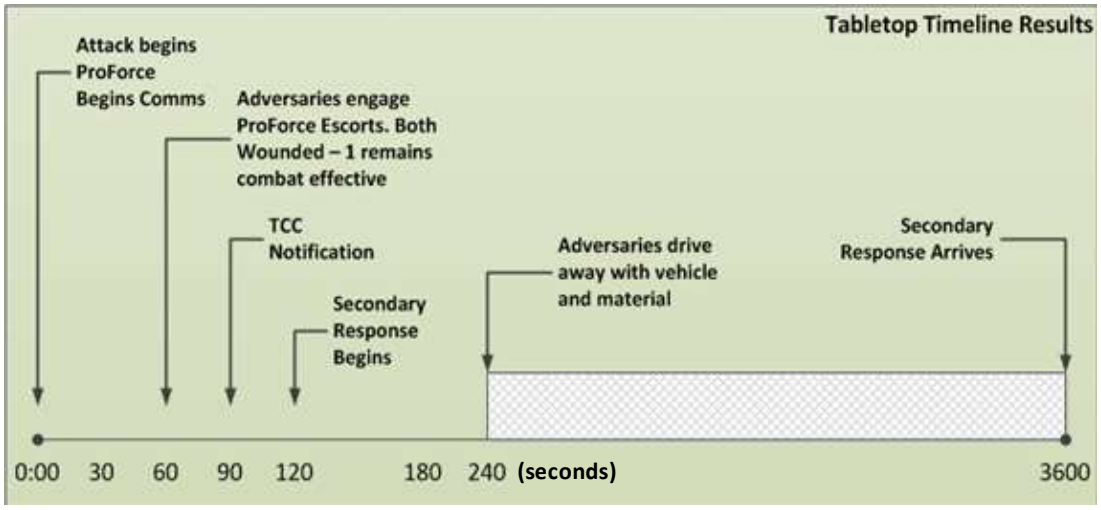


FIG. 3. Tabletop timeline for theft scenario 1-steal transport vehicle

5.4.3 Scenario condition: theft scenario 2— steal material container or materials

Theft scenario 2 was considered for an important reason: if the transport vehicle is damaged or is disabled and the container is heavy, the adversaries will be required to plan for and stage heavy equipment to unload, reload and escape the scene with the container and/or materials.

If just the materials are desired, shielding capable of blocking extensive gamma radiation would be required. This scenario requires considerably more skill to plan and execute because of the technical and deception requirements for the adversaries. For example, the adversary would need to pre-stage construction equipment and/or a crane to lift the package from the transport vehicle and place it in a second. Mobile cranes with five-ton capacity are available for rental or purchase in most countries, but may or may not require a license to operate prior to the sale of the machine. The staging for the deception portion requires that the adversaries know precisely when and where to establish a realistic construction zone, then use techniques to force the escort and shipping vehicle to a stop. When the vehicles are stopped, both escort and transport vehicles are expected to be front-to-back and in direct line-of-sight for relatively easy adversary engagement. This facilitates elimination of armed escorts and observation of the driver they attempt notification actions.

Since this scenario does not depend on the operation of the transport vehicle, it may be damaged or disabled as part of the action. Therefore, this scenario may be considered an appendage on theft scenario 1. Here, however, we are measuring the effectiveness of the delay of moving a second transport vehicle into position, defeating the attachment measures of the container to the vehicle, hoisting it out of the original transport, and moving it to the new vehicle. If only the materials are desired, mobile shielding, tools to open the package and move the materials and place them in a suitable improvised shielded container would be necessary, since the materials would be intended for use or sale elsewhere.

Depending on the transport vehicle type, it may be possible to attach a new truck to the trailer, or may require complete unloading of the container, as in this scenario example (scenario planners should not be constrained by our proposed scenarios). An insider was used to reduce probability of communication, to provide deceptive communications to the TCC to delay response, as well as to provide advance information to the adversaries as to the shipment time and route.

The availability and training for weapons and adversaries is equal to theft scenario 1, except for the training required to operate a mobile crane, move heavy loads, and drive heavy equipment, or conversely, to provide for opening the package, safely handling the materials, and providing shielding during and after the operation.

Victory conditions for the adversaries are successful theft of the package or materials and leaving the scene without responders in direct contact.

5.4.4 Scenario results: theft scenario 2— steal material container or materials

Three response members were neutralized by the adversary team within the first thirty seconds. Also within this timeframe, notification of the attack was communicated to local law enforcement by members of the public calling to report suspicious activity. At the 60-second time interval, the adversary team begins the task of breaching the rear door of the transport vehicle, completes the task, and enters the cargo area of the transport vehicle at the 90-second time interval. At 150 seconds into their mission, the adversary defeated the delay elements at the target and begins to remove the material to an awaiting transport vehicle, and drive away with the target material by 180 seconds, well before the arrival of the secondary response. Figure 4 depicts the events of theft scenario 2.

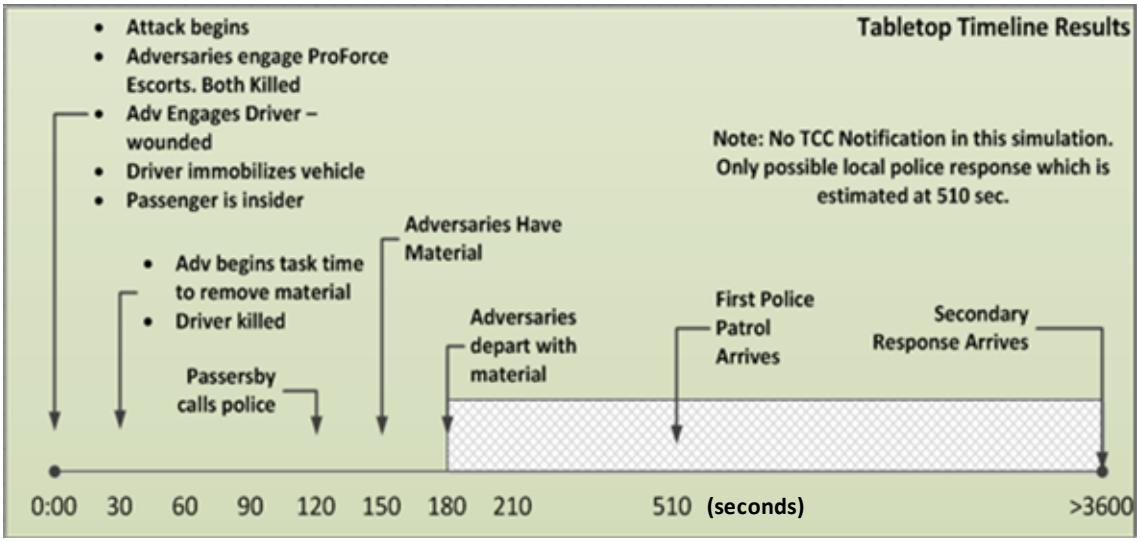


FIG. 4. Tabletop timelines for theft scenario 2—steal material container or material

5.4.5. Scenario condition: sabotage scenario 1— radiological dispersion device with explosives

Sabotage scenario 1 intends to evaluate what could be considered a 'worst-case' adversary attack plan—the attack elements of theft scenario 1 without the need to escape and sabotaging the materials in-place. Sabotage represents a 'one-way trip' for the adversary in which they wish to access materials for the purposes of dispersing it to create a denial weapon; causing terror and economic damage. Similar to theft scenarios 1 and 2, the adversaries would need to force the vehicles to stop and then eliminate police forces. However, in this scenario, the adversaries would need to open the package, expose themselves to the materials, and then detonate them in that exposed state (outside of the package). This is the defining scenario objective.

This scenario measures the effectiveness of the physical delay, the communication actions of the convoy, and of the rapidity of response by contingency personnel against an adversary with no intent to flee, but rather directly access the materials. It requires adversary skill to effectively shoot, open the container with provided tools (or if tools are not provided, to extract bolts using tap-and-die methods), and to place and detonate explosives. Depending on the exposure characteristics and feasibility of portable shielding, the adversaries may directly expose themselves to high doses of gamma radiation in the fulfilment of this plan. To facilitate more working time, adversaries could prepare explosives ahead of time, place the materials as a final step into the explosives, then detonate.

The threat of this type of attack could be mitigated by a route that does not move through major population areas. Any resulting contamination would affect roads, vehicles, structures, and personnel in the plume and fallout areas.

The victory condition for the adversaries is successful detonation of explosives on materials located outside of the package.

5.4.6 Scenario results: sabotage scenario 1— radiological dispersion device with explosives

Figure 5 depicts the terrain map used to evaluate the convoy attack of sabotage scenario 1.

FIG. 5. Sabotage scenario 1 area map

TT analysis of sabotage scenario 1 resulted in an adversary win in which the adversary was able to complete their mission at the 210-seconds time interval (Figure 6). Within the first 30 seconds, the adversaries neutralized the escorts and the driver and passenger of the transport vehicle. At the 90-seconds time interval, the adversary team began their task of breaching the cargo vehicle. Between the 90 and 210-seconds time interval, the adversary team was able to enter the cargo vehicle, set an explosive device, and detonate the device, thereby accomplishing their mission.

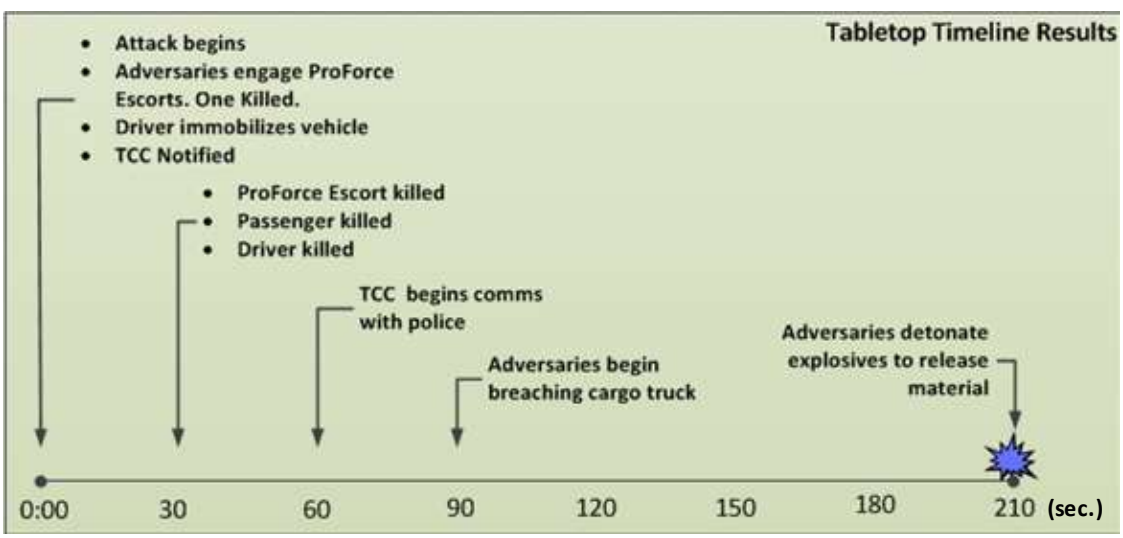


FIG. 6. Tabletop timelines for sabotage scenario 3, radiological dispersion

6. OVERALL ASSESSMENT OF SECURITY

6.1. ASSESSMENT TOOL SUMMARY

The intent of the transport case study was to evaluate the assessment methodology outlined in the NUSAM Methodological Framework. Although this case study focuses upon the use of a tabletop approach, which normally produces qualitative results, an alternate approach may include the use of a complementary tool for neutralization, which produces quantitative results.

Two different TT exercise approaches were used to evaluate the three theft and sabotage scenarios. Each approach had its own unique rules of play and data look-up tables. However, despite these differences, the methodologies produced similar results for all three scenarios. The most notable differences occur in the timeline of events, specifically, one method resulted in shorter scenario timelines compared to that of the other. These timeline differences ranged from 30 – 60 seconds, which translates into one to two game turns. The contributing factor for this is due to the rules of adopted play in which wounds are not considered for game play. Based upon this method, if a token is engaged, the resulting action is either a hit or miss compared to the method, whereas if a token is hit, and the dice roll is below the threshold for a kill, there is another roll of the dice to determine if the token is wounded. Given a wound, a determination is then required to identify if the token is combat effective or ineffective. In instances in which players were wounded, but combat effective, the timeline for the scenario increased by a minimum of an additional 30 seconds (or one game turn).

Another contribution to differences in timelines relates to the determination of communication, specifically to secondary responders. One method relies upon dice rolls to determine if communication can occur compared to the other method that relies upon the subject matter expert(s) to determine if and when communication occurs.

Despite the identified differences in game play, the ultimate results for the two TT exercises are extremely comparable in terms of system wins or losses.

6.1.1 Tabletop observations

Tabletops 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 issues, challenges and/or impact of analytical assumptions;
  - Identifies 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 for a defined scenario. Quantitative results requires many iterations of a single scenario which can be costly due to the numbers of people involved and the time required to complete each iteration of the scenario;
  - Only one scenario can be evaluated at one time, thus does not provide insight in terms of trends.

- Lessons Learned:
  - TTs provide excellent insight into plans, policies, and procedures as well as command and control;
  - Excellent method for getting key players into the room and promotes communication and planning amongst key participants;
  - TTs can be applied for training or be used as a training tool;
  - Quickly evaluates potential changes to protection strategies in order to identify effectiveness of enhancements;
  - Immediately demonstrates potential weaknesses and can be used to demonstrate proposed enhancements in a real-time environment;
  - TTs are a preferred method to evaluate material in transport as compared to many complex computer tools that are not suitable for transport;
  - Some of the complex computer tools can be used to evaluate the engagements during transport.

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 the high-level question of whether security requirements were met.

The security requirements may be prescriptive or performance based or a combination of the two. For the transport operation, the level of protection described reflects current IAEA guidelines.

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

6.2.1. Prescriptive requirements

For the transport case study, performance-based requirements were the focus, and no explicit assessment of the conformance with IAEA prescriptive requirements of any kind was conducted. Therefore, it is not possible to state if the transport operation meets the physical protection system (PPS) prescriptive requirements.

6.2.2. Performance-based requirements

To be able to answer the question if the performance-based requirement has been met, the tool would provide a result in a metric that can be compared with an appropriate acceptance criterion. However, in this case study, the regulator or State authority did not define a performance-based metric or criteria against which to assess the analysis results. Ref. [7] identifies the performance-based requirements to deter, detect and delay unauthorized access to the radioactive materials while in transport and during storage in transit to defeat any attempted malicious acts. This served as the basis to evaluate the effectiveness of the protection measures of the transport operation.

6.3. COMBINED ASSESSMENT

For the hypothetical transport case study, some issues were identified.

For the first issue, the evaluation did not include an assessment to determine if the transportation protection requirements met the IAEA prescriptive requirements. It is not advisable to conduct an assessment or to identify modifications without first ensuring the PPS design meets the minimum requirements. An additional evaluation of the transportation PPS design may be conducted, to determine

if the prescriptive requirements are met.

Due to the limitations of this case study, only three adversary scenarios were evaluated for theft and sabotage. A comprehensive assessment would be required to confidently determine the transportation 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 6.3, 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 transport overall protection effectiveness against the full range of DBT defined threat.

6.4. UNCERTAINTIES AND ASSUMPTIONS

The transport operations described in this case study are based on recommended requirements documented in Ref. [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 transport operation against the full range of DBT adversary capabilities. Further, the quality of performance data, such as delay and response times, was very limited because the operation described is notional.

Appendix I

GAMMA SECURE P/L HYPOTHETICAL TRANSPORT SECURITY PLAN

I.1. INTRODUCTION

This transport security plan accounts for the transport from the sterilization factory of Gamma Secure P/L (GSPL) at RR684 to the warehouse of Kobalt Service P/L (KSPL) at RR261. The GSPL repatriates the used ^{60}Co source to the production factory of Kobalt Service P/L (KSPL) in another country for recycling. The air transportation of the stored ^{60}Co to its original country will be followed after this transportation. The air transportation is not in the scope of the transport security plan.

This transport security plan was developed for the transport of Category 1 ^{60}Co radioactive sources requiring an enhanced security level including some additional security measures for a normal threat level as specified in Ref. [4].

The sources are to be transported individually:

- From Gamma Secure P/L (GSPL), located at RR681, Central City, Lagassi
- To Kobalt Service P/L (KSPL), located at RR261, Industrial City, Lagassi

GSPL is responsible for the determination and implementation of the security measures identified in this plan. The GSPL Transport Department will be the carrier (shipper) of the ^{60}Co radioactive sources. Thus, GSPL shall assume all carrier responsibilities and, as a result, will be transporting the sources by road vehicle from GSPL, 123 Gamma Road, Central City, Lagassi (in Province A); through Province B; to KSPL, 432 RR261, Industrial City, Lagassi (in Province C).

The transport security plan was developed in accordance with the hypothetical documents National Regulations for Transport Security of Radioactive Materials and guidance from the Lagassi Nuclear Regulatory Agency (LNRA) Code of Practice for Transport Security of Radioactive Material (CoPTSRM) 2007 for shipments of radioactive sources that require basic to selected additional security level measures for a normal threat level as specified in Ref. [4].

I.2. OBJECTIVES

The objectives of the transport security plan for radioactive materials are to:

- Ensure security to protect personnel and equipment;
- Provide clear direction and roles to personnel on actions to be taken to:
  - Ensure security of shipments;
  - Provide appropriate response to incidents.

I.3. APPLICABILITY

This security plan covers the transport security measures and activities of GSPL for the execution of this plan. Shipments made under this plan would contain an aggregate radioactivity per package to be categorized by *National Regulations for Transport Security of Radioactive Materials* and the IAEA guidance as a Category 1 source according to the *IAEA Code of Conduct*. If a consignment of one of these sources is to be undertaken when a threat level higher than normal exists, then further additional security measures as specified in Ref. [4] may be required and the plan will need to be modified accordingly.

The plan identifies security interfaces with the following companies and government entities:

- GSPL (Gamma Secure P/L);
- KSPL (Kobalt Service P/L);
- LNRA (LAGASSI Nuclear Regulatory Agency);
- State Police;

- NHT (National HAZMAT Team);
- Ambulance services;
- EPA (National Environmental Protection Agency).

The measures established in this transport security plan apply to transport staff: management personnel, vehicle drivers, shipping and receiving personnel, security personnel, as well as others who are, or may be deemed to be involved with the transport of the radioactive materials covered by this plan.

The radioactive material to be transported is a Category 1 ^{60}Co irradiation source. The details of the package used to transport the fresh radioactive source(s) are:

- Activity: 100 Terabecquerel
- Chemical Nature: Metal
- Physical Form: Solid
- Hazard: Radiation
- Packaging: Type B
- Package Mass: 5445 kilogram
- Package Height: 1.456 metre
- Package Diameter : 1.013 metre
- Certificate: A/1002/B(U)
- No. of Packages: One

I.4. ADMINISTRATIVE REQUIREMENTS

Information in this document and other associated documentation (i.e. security measures and procedures, transport documents, schedules, and routes) may be considered sensitive (see Section I.6). Such information, as determined by GSPL shall only be accessible to relevant entities and their contractors that have: (a) demonstrated need-to-know, (b) received appropriate training and (c) been individually determined to be trustworthy (see Section I.5.3).

At the discretion of GSPL, this document may be made available, upon request, to personnel with demonstrated need-to-know from GSPL, LNRA or EPA, or other provincial government agencies, local law enforcement or other emergency response agencies.

I.4.1. Policies, procedures and operations

The following GSPL policies and procedures apply:

- Gamma Secure P/L Corporate and Security Manual (CPSM1);
- Gamma Secure P/L Emergency and Contingency Plan (GSECP2007);
- State OH&S Policy and Arrangements.

I.4.2. Testing and evaluation of the security plan

This plan shall be tested and evaluated periodically, at least annually or when the TSP is modified, to ensure company employees, contractors, carriers, and others are performing responsibilities as outlined in this plan fully understand and execute their responsibilities.

I.4.3. Review and update of the security plan

In the event that a shipment of an IRRCO60/B source requiring enhanced security level and additional security measures is planned to occur at any time after one year of development, review, update or approval of this plan,

then GSPL shall update this plan; in addition, this plan shall be updated as otherwise needed based upon other activities associated with security of these radioactive sources during transport.

I.4.4. Readiness review and assessment

Immediately prior to each shipment, the GSPL transport manager shall perform a readiness review against this plan to assess any vulnerabilities and to demonstrate that all security measures, to include the availability of escort personnel and vehicles, are in place and functioning. All critical factors, including equipment operability, schedule, weather, and routes to be followed and any potential alternate routes shall be reviewed.

Prior to any shipment of an IRRCO60/B source, GSPL shall address all corrective actions that result from the readiness review. In some cases, and as needed, corrective actions may result in the delay or cancellation of the shipment until completed.

I.4.5. Reporting of threats and incidents

Threats or incidents shall be reported, according to the CoPTSRM 2007 regulations, to LNRA within 48 hours of occurrence. Initially, communications can be made by telephone or telefax and then followed in a timely manner by a written report within seven days, with a detailed description of the identified threat or incident.

I.5. RESPONSIBILITIES

I.5.1. Allocation of responsibilities

The general manager of GSPL has the overall responsibility for ensuring compliance of the security measures in this transport security plan. At the everyday working level, the GSPL transport manager, security manager and staff are responsible and accountable for security. GSPL, would ensure continuity of security until responsibility is transferred between GSPL and KSPL.

I.5.2. GSPL organization structure

Figure I.1 provides the organization structure of the GSPL:

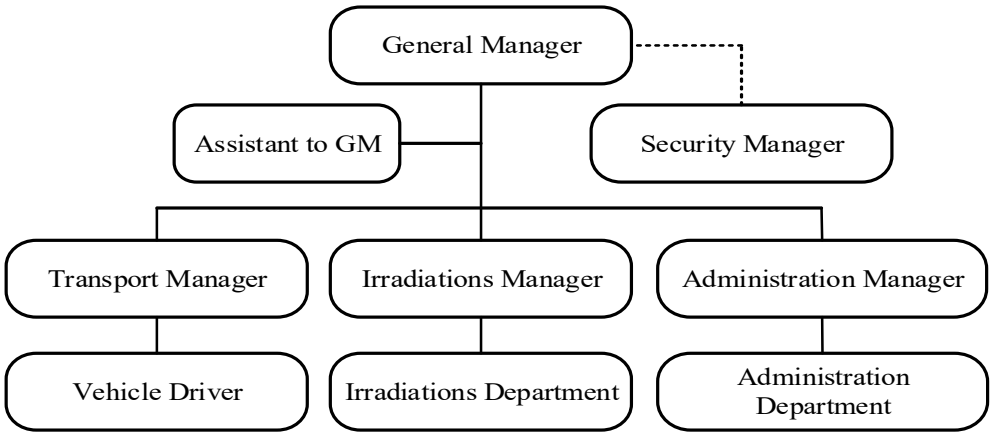


FIG. I.1. Organizational structure of GSPL

I.5.3. Trustworthiness

GSPL shall ensure that personnel involved in the shipments of sources are trustworthy. Trustworthiness shall be established by performing background checks (including police checks) prior to engagement, providing security and awareness training, and annual assessments of job performance. The GSPL administration manager is responsible for ensuring that the checks are performed. Identification badges with photo shall be provided and worn by authorized personnel.

I.5.4. Training

GSPL shall ensure that appropriate security training on responsibility, awareness and procedures is provided, according to current procedures of transportation personnel and guards. Training with response personnel shall be conducted at least annually. Records of all security training shall comply with LNRA CoPTSRS 2007 regulations and the CPSM1 Manual.

I.6. INFORMATION MANAGEMENT

This section describes the manner in which information will be managed prior to, during and following the transport of the radioactive sources.

I.6.1. Information security

GPSL shall notify each authorized recipient of this plan and of the emergency and contingency plan GSECP2007 not to distribute the plans to any other individual, inside or outside, the recipient's organization, without the approval of GSPL. All copies of these plans shall be controlled, managed and stored in accordance with GSPL CPSM1 Manual which shall be reviewed by LNRA on an annual basis. GSPL shall ensure that access to these plans is restricted to personnel on a need-to-know basis, who have been demonstrated to be trustworthy, and in accordance with the CPSM1 Manual. GSPL shall maintain a list of individuals and/or organizations that are authorized to receive or view this TSP and the GSECP2007.

I.6.2. Records retention

GSPL shall provide for retention of all applicable records according to current policies. The documentation that shall be retained shall include, but not be limited to training records, shipping documentation, and verification of sources (nuclides, activities and configuration of sources).

Information on the sources being transported shall be included in the GSPL inventory system. This information shall include location of storage and encoding of the source. Any records of accidents or incidents that occur during transport shall be included in the LNRA database for incidents.

The computer system containing the database for these records shall comply with the national requirements for information and computer security. Access to the database is limited to LNRA and GSPL personnel with respective clearance according to the GSPL CPSM1 Manual.

I.7. TRANSPORT SECURITY MEASURES

This section describes the specific security measures prior to, during and upon receipt of each source during transport. Information and communications required by this section, which is based in part upon the best-practice security measures outlined in Section I.9 of this plan, are considered sensitive and shall be handled according to procedures outlined in Section I.6.1.

I.7.1. Primary and alternative routes

GSPL has received approval from LNRA for the following primary and alternative routes to be used (without any planned stops):

Primary Route (southern route) 205.3 km

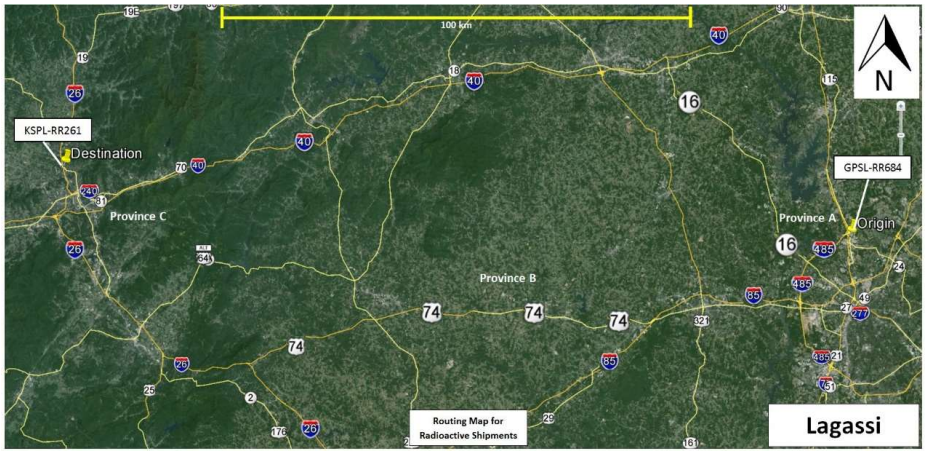
- RR684 to 485 W
- 485 W to 85 W
- 85 W to 74 W
- 74 W to 26 N
- 26 N to RR261

Secondary Route (northern route) 205.5 km

- RR684 S to 485 W

- 485 W to 16 N
- 16 N to 40 W
- 40 W to 240 W
- 240 W to 26 N
- 26 N to RR261

These routes were selected by GSPL considering road quality, distances and other geographic and ergonomic factors based on the map illustrated in Figure I.2.



Federal highway (multi-lane divided highway)

Regional highway (2-lane divided highway)

Regional route (2-lane bi-directional road)

FIG. I.2. Route map for radioactive source shipment

The actual transport time and route shall be selected at least one week in advance of the shipment in agreement with the police. This information shall only be distributed to other parties involved according to Section I.6.1.

I.8. DESCRIPTION OF THE SECURITY SYSTEM

I.8.1. Equipment and modes of transport

The package shall have the following security measure installed and, prior to shipment, verified:

- Tie-downs;
- Tamper indicating devices; and
- Secured transport truck.

The transport vehicle shall be a 10-ton carrying truck with the following security measures installed and, prior to shipment, verified:

- Enclosed truck;
- Lockable doors;
- Barrier between drivers compartment and cargo area;

- Communications to GSPL TCC; and
- Meets the European Agreement concerning the International Carriage of Dangerous Goods by Road standards.

I.8.2. Operations command and control

During normal operations, the communications for the transport of the radioactive material shall be conducted in accordance with the CPSM1 Manual.

Any threat, emergency, delay in transit, unusual situation, or incident shall be immediately reported, as appropriate, by the personnel in the transport vehicle or the escort vehicle to the TCC. Depending on the severity of event, the TCC personnel shall then first call the response forces and second inform LNRA. Dispatch of any needed additional security and/or emergency resources shall be initiated and coordinated through LNRA.

GSPL shall establish a TCC in a separate room with access control and staffed with two people during the transport. During operations associated with the transport of the sources, the chain of command shall be established by the designated supervisor at the TCC. The TCC shall have full responsibility and authority for the shipment and communicating with site responders for both normal operations and emergency situations.

I.8.3. Additional security measures

Due to the shipment being a Category 1 source, GSPL will follow the LNRA recommendations to invoke the following additional security measures in the vehicle:

- Equipped with appropriate redundent communications equipment (encrypted radio and mobile phone) capable of timely notification to the TCC and LNRA;
- Protocols for communications between personnel involved;
- Automatic GPS tracking with encrypted data transmission to TCC;
- Chain of command defining responsibilities for actions in the event of off normal situations;
- Written instructions;
- Training for emergencies;
- Thorough search of vehicle before shipment.

The transport vehicle will be accompanied by an escort vehicle with two armed police officers continuously observing the conveyance. The car will be equipped with equivalent redundant communication devices as in the transport vehicle.

I.8.4. Maintenance and testing of security systems and equipment

Maintenance and testing of the transport vehicle shall be performed in accordance with the CPSM1 Manual. Operability and functionality of all equipment and communication devices shall be performed in accordance with the CPSM1 Manual.

I.8.5. Emergency response

There are three key elements of response planning:

- Emergency response (if necessary tactical);
- Incident communications (including command and control); and
- Notification of relevant agencies.

I.8.6. Non-tactical and tactical emergency response

Upon notification by the transport vehicle crew and/or escort vehicle personnel of an incident, emergency or a security attack, the TCC shall follow its non-tactical or tactical emergency response procedures and actions, as applicable. This shall include coordinating, as necessary, with relevant regulatory bodies and law enforcement agencies including any communications with the State Police, provincial police, other potential first-on-the-scene emergency responders, National HAZMAT Team, and relevant ambulance services as applicable and as specified in the Radioactive Source Transport Emergency and Contingency Plan (GSECP2007).

I.8.7. Incident communication

For any incident, either non-tactical or tactical, the communication procedures specified in the Radioactive Source Transport Emergency and Contingency Plan (GSECP2007) shall be followed by the TCC and any other involved personnel, including any communications with the State Police, National HAZMAT Team, and relevant ambulance services as specified in the Response Plan.

I.8.8. Notification of relevant agencies

For any incident, either non-tactical or tactical, the notification procedures specified in the Radioactive Source Transport Emergency and Contingency Plan (GSECP2007) shall be followed including any notifications with the State Police, national HAZMAT team, and relevant ambulance services as specified in the Response Plan.

I.9. SECURITY MEASURES OVERVIEW

The Table I.1 identifies the recommended security measures to be implemented based on the material activity being shipped and threat level.

TABLE I.1. RECOMMENDED SECURITY MEASURES

SECURITY MEASURES	Basic or Enhanced Security Level	Additional Security Measures
Description of material:		
Verify shipping documentation is accurate: type, weight and form of material, hazards, number and type of packaging, other criteria information	X	
Radioactive contents of packaging require enhanced level of security/security plan	X	
Packages:		
Tamper indicating device	X	
Package lid fixed with special screws	X	
Tie downs:		
Normal tie down chains and locks	X	
Cargo over-pack fixtures in truck	X	
Transport vehicle:		
Truck cab:		
Separate cab and cargo area	X	
Cab door locks	X	
Standard safety glass	X	
Alarm panel	X	
Closed truck – freight door		
Locks:		
Standard vehicle door lock	X	
Additional security lock (key or combination)	X	
Door sensor	X	
Communications:		
Transport vehicle to guards:	X	
Walkie-Talkies	X	
Redundant communication (cell phone)		X
Transport vehicle to transport command centre:		
Encrypted radio and cell phone		X
Emergency alarm button		
Engine:		
Disablement system	X	
Vehicle Tracking:		
GPS real time tracking (encrypted data transmission)		X
Vehicle inspections and Driver Observations:		
Thorough inspection of vehicle prior to start of shipment		X
Driver or escort in vehicle maintain observance of vehicle at all times	X	

TABLE I.1. RECOMMENDED SECURITY MEASURES (CONT.)

SECURITY MEASURES	Basic or Enhanced Security Level	Additional Security Measures
Drivers & Escorts/Escort Vehicles:		
Driver and one escort in vehicle (unarmed)	X	
Guards:		
Police escort car with two armed police officers		X
Walkie-Talkie, encrypted radio and cell phone		X
Continuous surveillance of conveyance		X
Annual exercises with transport personnel	X	
Transport Command Centre:		
Advance notification of consignee KSPL	X	
Encrypted radio and cell phone		X
Periodic control of vehicle position		X
Periodic contact with vehicle driver/escort		X
Transport Personnel:		
Training:		
Annual exercises with response forces		X
Training of responsibility and procedures	X	
Trustworthiness		
National security clearance		X
Photo ID badges	X	
Licensing and Review:		
TSP approval and periodic review		X
Operation license for carrier and consignor (GSPL)		X
Confidentiality of Information:		
TSP:		
LNRA, GSPL management, transport and security personnel, police escort		X
Transport Time and Route:		
LNRA, GSPL management, transport and security personnel, TCC, police, KSPL: 7 days in advance		X
NHT, EPA: 48 h in advance		X
Contingency/Emergency Plan:		
LNRA, transport and security personnel, TCC, police, NHT, EPA, ambulance service		X

I.10. ADDITIONAL SECURITY MEASURES

I.10.1. Procedures for normal operations

Three transport phases are used to describe procedures for normal operations. These include prior to, during, and after the shipment.

Prior to the shipment, as noted in Section I.4, a readiness review will be conducted which details personnel (driver and/or passenger, police, and responder) training and fitness-for-duty; vehicle (shipping and police) availability and operability; technology functionality (all technologies identified in Section I.8); and awareness and appropriateness of procedures. Items found insufficient during the readiness review require corrective action. When identified items are resolved, material container(s) may be loaded and secured onto the conveyance and a safety inspection is performed, after which, a security inspection of locks, tie downs and seals is performed. At this point, chain-of-custody and continuous observation of the shipping vehicle would be maintained until the materials reach the final destination and the receiver formally accepts them. Immediately prior to transport, the TCC and receiver are notified that the shipment is ready to depart.

During transport, driver, passenger and escort personnel maintain continuous observation of the conveyance and situational awareness to report status, position, and any abnormal circumstances as detailed in Section I.8, within the convoy and to the TCC at intervals established in the Radioactive Source Transport Emergency and Contingency Plan (CSECP2007). The TCC monitors the shipment via GPS and communicates developing situations or threats to the convoy along the route, as well as notification of status to the receiver.

After the shipment arrives, the convoy notifies the TCC of arrival, the receiver verifies the integrity of locks and seals, and formally accepts the material. Personnel who took part in the transport mission then perform incident and after-action reporting, in order for lessons-learned to be applied to future personnel training, technology enhancements, and procedural changes.

I.10.2. Procedures for security incidents (especially for unplanned stops)

The procedures for security incidents are based on threat assessment and adversary task analysis. There are four basic documents which may be approved before the transport of the source:

- Transport plan including emergency transport plan;
- Physical protection plan (based on DBT);
- Radiation health protection plan ;
- Quality assurance.

I.11. RESPONSE FORCE DATA

I.11.1. State police escort

A police escort consists of two police officers in a squad car from the State Police. They are responsible for:

- Performing periodic communication with local police station and transport control center;
- Protecting the public from crime and safety hazards associated with transportation;
- Responding to assessed intrusion to delay intruders until the tactical response team arrives.

Note: Police escort are not trained on radioactive materials.

I.11.1.1 Equipment

The police escort are equipped with:

- Standard police car;
- 9 mm semiautomatic handgun with a fully loaded magazine;

- Spare magazine of 8 rounds;
- One set of handcuffs;
- Flashlight;
- Hand-held radio.

I.11.1.2. Training

The members of the local police receive training in the following areas:

- Legal basis for search and seizure;
- Use of force;
- Local statutes and laws;
- Firearms qualification training (four times per year).

I.11.2. State police tactical response team

There is one tactical response team in the central city and one in the industrial city on 24-hour alert. The teams have five members each. All members are trained in hostage situations and close-quarters combat.

I.11.2.1. Equipment

The tactical response team members are equipped with:

- 9 mm semiautomatic handgun with a fully loaded magazine;
- 5.56 mm assault rifle with a 25-round magazine;
- Two spare magazines of ammunition for each weapon. Both weapons are carried with a fully loaded magazine but without a round in the chamber;
- Straight baton;
- One set of handcuffs;
- Flashlight;
- Hand-held radio.

I.11.2.2. Training

The members of the military tactical response team receive training in the following areas:

- Firearms qualification training (12 times per year);
- Standard military combat training;
- Close quarters combat.

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

I.11.3. Local police

When incidents occur, local police officers are deployed from local police station located in nearby city. They consist of four police officers in two squad cars. They are responsible for:

- Protecting the public from crime and safety hazards associated with transportation;

- Responding to reported adversaries to neutralize or delay them until the tactical response team arrives;
- Communicating to the local police station and State Police;
- Controlling traffic.

They are not trained on radioactive materials. The equipment and training of local police is equal to police escort.

I.11.4. Response procedures

Police escort report any incidents to the local police station and TCC with the location of vehicle by a single channel. If the incident is severe, the local police patrol deployed. If the incident is assessed as an attack, the police escort immediately notifies the police dispatcher in the TCC, who then notifies the local police patrols and the commander of tactical response team in order for the appropriate tactical team to begin preparations for deployment to the GPS location. In case no communication is possible with police escort, the local police and tactical team could be deployed by the decision of police dispatcher.

When the first police patrol arrives, the officers receive a quick briefing from the police escort, and then begin to tactically assess the situation. Upon arrival of the second patrol, the two patrols deploy to neutralize the adversary and prevent employees and the public from injury.

Once the members of a tactical response team arrive, they deploy as a team and proceed with operations to protect material.

I.12. AVERAGE RESPONSE PERFORMANCE DATA

The tactical response team has conducted performance testing of preparation, travel, and deployment times in a regular basis. The average times are listed in Table I.12.1.

TABLE I.12.1. AVERAGE RESPONSE TIMES

Description	Average Performance Time
Communication time of police/driver/passenger escort to local police station and TCC	30 seconds
Communication time of police dispatcher in TCC to local police station and tactical response team	60 seconds
Local police preparation time	90 seconds
Local police response time. The local police is located in every city	Distance from the nearest local police station ÷ 108 km/h (30m/s)
Local police deployment time	30 seconds
Tactical response preparation time	1200 seconds (20 minutes)
Tactical response travel time. Tactical response team is located in central city and industrial city	Distance from the nearest tactical response team ÷ 108 km/h (30m/s)
Tactical response deployment time	30 seconds

Appendix II

DESCRIPTION OF TABLETOP METHODOLOGIES

II.1. INTRODUCTION

This section describes the tabletop methodologies for both the Oak Ridge National Laboratory BattleBoard Tabletop and the Sandia National Laboratories Tabletop approaches. For additional information concerning the comparison of these two approaches see Ref. [1].

II.2. OAK RIDGE NATIONAL LABORATORY BATTLEBOARD TABLETOP METHODOLOGY

The BattleBoard Tabletop Methodology was originally developed by the US Army for theatre-wide battle planning. That method was later modified by the US Department of Energy to reflect small unit tactics, engagements, and conflicts. A BattleBoard tabletop is a turn-based (adversary then protective force) simulation designed to evaluate the protection system's capability in response to an attack by an adversary force. The Battle Board tabletop helps stakeholders to identify whether or not weaknesses are present in a physical protection system that could result in a loss of material by unauthorized removal or by sabotage.

II.2.1. ORNL BattleBoard P_H/P_K

An important decision to be made is the use of a representative probability of hit/probability of kill (P_H/P_K) Table. Many of the decisions made in a BattleBoard tabletop are made based on the outcomes of dice rolls which correspond to a percentage of success or failure. The most common decision is whether a shot from one team upon the other results in a miss, wound, or kill. Outcomes of weapons engagements are decided based upon probability tables (probability of hit/probability of kill) based on shooter weapon, tactics proficiency, weapon type, distance, training effectiveness, and environmental factors.

II.2.2. How the simulation progresses

The following provides a brief description for each 'turn' played on the BattleBoard tabletop:

- The simulation begins with the adversary force. The adversary force will initiate each game turn by moving any, all, or none of their markers. All other forces will then move any, all, or none of their markers. Normally, the protective force has the second move. Each adversary and protective force turn represents activities happening in the same time increment being modeled;
- Time increments are typically played as 30 second real-time intervals. This means that each time a turn has been played, 30 seconds have elapsed on the scenario timeline;
- A five-minute time limit is allotted to each team to make their moves on their turn;
- Once a player makes a move and that move would be observed, such as during an engagement, all tokens that are involved in that move are moved to the board so that the opposing side can see them;
- All preplanned movements and engagements will be announced to and concurred by the facilitator prior to beginning the simulation;
- After all movements have been completed, results of engagements will be determined and the results will be recorded on the documentation forms included below (Tables II.10–13).

The rules of the tabletop methodologies are easy to understand and most participants are well versed in the methodology after a single simulation. However, the skill of the facilitator can greatly promote a successful process. With the rules as a basis and the ability to draw upon the expertise of the players as well as to reach out to others for technical analysis, results can be achieved which accurately reflect an actual situation. Poorly managed simulations can result in poor data and a loss of confidence in the analysis by everyone involved.

II.2.3. ORNL BattleBoard tabletop methodology rules

Below are the BattleBoard tabletop methodology rules:

- Engagement between forces:
  - Tokens represent people. Each token is uniquely identified for documentation and tracking purposes (i.e. PF 1 for protective force number 1);
  - Adversary plans that include hidden traps, explosives, snipers, etc. need to be announced to the facilitator prior to the simulation beginning;
  - A token may engage only one other token per turn;
  - A token firing from a hidden position becomes visible to those in line of sight and may be engaged in that same turn;
  - Multiple tokens may engage a single token during the same turn;
  - Variation of success of firearm engagements is determined by the roll of two six-sided dice. Possible outcomes of an engagement:
    - Miss;
    - Wound (wounded tokens cannot move but can communicate) dice roll to determine whether combat effective or not;
    - Kill.
  - Engagement outcomes are determined by P_H/P_K tables based on:
    - Type of weapon;
    - Distance from target;
    - Observation capability;
    - Firing from armored position;
    - Armor type if employed by the targeted token.
- Modeling Armor:
  - Vehicles:
    - No protection against explosives or rocket propelled grenades unless designed against those threats;
    - Armor piercing rounds' effectiveness based on type of armor deployed;
    - Firing small arms from a moving vehicle will not result in neutralization of tokens;
    - Soft vehicles offer no protection for tokens inside.
  - Personnel:
    - No protection achieved with body armor. Basis of the simulation is that both the adversary and the protective forces have the appropriate information to plan and select appropriate ammunition.
  - Hardened fighting positions:
    - No protection against explosives or rocket propelled grenades unless designed against those threats;
    - Armor piercing rounds' effectiveness based on type of armor deployed.
- Special weapons & equipment:
  - Bulk explosives:
    - Expert analysis is used to determine the amounts of explosives needed for each type of barrier to be explosively breached. Players may not attempt to use more explosives than is approved in the design basis threat. Players need to document their use of explosives in the scenario planning phase of the BattleBoard;

- Thirty seconds of task time is required complete a breach. This time includes:
  - Setting charge on barrier;
  - Retreat to safe location;
  - Detonate the charge;
  - Fifteen seconds to clear debris;
  - Fifteen seconds to enter breach.

- Fragmentation grenades:
  - Deployed accurately to a maximum of 30 metres;
  - Neutralization radius of 5 metres;
  - Casualty radius 15 metres. Roll dice for tokens 5–15 metres from device to decide if combat effective;
  - Probability of neutralization is 50% (dice roll of 7 or better);
  - Dice roll for each person in the radius.
- Rocket propelled grenades:
  - Not possible for targets less than 25 metres away;
  - One round per 30 second turn;
  - Engagement table used to determine hit or miss;
  - Controller makes decisions on combat effectiveness of tokens based on how the rocket-propelled grnade is used (against vehicles or structures).
- Distraction and disorientation devices:
  - Maximum accurate range of throw is 30 metres;
  - Effective range is a 5 metres radius;
  - Tokens are combat ineffective for 1 turn.
- Smoke grenades:
  - Maximum accurate range of throw is 30 metres;
  - Smoke dispenses for maximum of 60 seconds;
  - Effective obscure distance is 25 metres;
  - One game turn to become effective cover;
  - Effective only when wind is less than 40 kilometre/hour.

— Movement of tokens:
- Tokens may move ½ distance and engage a token in the same turn;
- Movement distances are based on:
  - Walking;
  - Running – defensive standard;
  - Running – offensive standard;
  - Tokens encumbered with weight (more than 20 kilogram) or awkward items will be slowed to at least half of maximum.
- Movements of tokens will be slowed based on barriers in their path. For example:
  - A token can move 100 metres in 30 seconds (offensive standard);
  - If that token would need to overcome a fence which takes 15 seconds then the movement will be limited to 50 metres.
- Vehicle movements:
  - Thirty seconds for tokens to mount and start vehicle;
  - Distance travelled based on actual speed assessed as realistic for conditions;
  - Fifteen seconds for tokens to exit a vehicle and ready weapons.

- Observation capabilities:
  - Tokens may be observed:
    - Up to 300 meters during daylight (clear) if line-of-sight is possible and no optics are used;
    - Up to 150 meters in dark but lighted conditions;
    - Up to 25 meters in darkness;
    - Vehicles may be observed:
      - Six hundred meters during daylight and at night with headlights on;
      - Two hundred meters at night in lighted conditions no headlights;
      - Fifty meters at night no headlights.
- Other Considerations:
  - Casualties (wounded):
    - A wounded token is laid on its side so that everyone knows the status of that position;
    - A wounded token may not move;
    - After a token has been wounded a decision is made to determine whether or not the token is still combat effective:
      - Dice role of 7 or better will permit the token to be combat effective (shoot);
      - Token can only communicate with dice roles of 6 or less;
    - Becomes neutralized (dead) after 5 turns;
    - Two hits result in the death of a token.
  - Man portable:
    - Items less than 70 kilogram is considered man portable by one person.
  - Other Considerations:
    - An advantage of the BattleBoard tabletop is its flexibility and ease to introduce new strategies for both protection as well as how a system might be attacked. When players devise a strategy not specifically governed by the rules, the facilitator will take measures to assure adequate understanding of the proposed action by conferring with the players involved and other experts at the site or elsewhere to determine the credible application of the approach and any outcomes derived from the use of the approach. Examples may include: use of radio jamming, explosive breaching techniques, force multipliers, as well as others.

Tables II.1–9 are hypothetical data tables for use during the BattleBoard tabletop analysis. These values were developed for training and demonstration purposes only.

TABLE II.1. PERSONNEL MOVEMENT TABLE — DEFENSIVE

Personnel Movement Table - Defensive															
	All Times in Seconds														
Metres	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300
Hard Surface	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Mixed Surface	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75

TABLE II.2. PERSONNEL MOVEMENT TABLE — OFFENSIVE

Personnel Movement Table - Offensive															
	All Times in Seconds														
Metres	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300
Hard Surface	3	6	9	12	15	18	22	25	28	31	34	37	40	43	46
Mixed Surface	4	7	11	15	18	22	25	29	33	36	40	44	47	51	55

TABLE II.3. P_H/P_K TABLE — HANDGUN/PISTOL

Handgun/Pistol					
	Range				
Yards	7	15	25	50	60
Metres	6.4	13.7	22.9	45.7	54.9
DAY	Total Dice Roll				
Miss	2-4	2-6	2-8	2-10	2-11
Wound	5-8	7-10	9-10	11	12
Kill	9-12	11-12	11-12	12	-
NIGHT					
Miss	2-6	2-8	2-10	2-12	-
Wound	7-10	9-10	11	-	-
Kill	11-12	11-12	12	-	-
From Armoured Vehicle					
DAY					
Miss	2-6	2-7	2-12	2-12	2-12
Wound	7-11	8-12	-	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-7	2-10	2-12	2-12	2-12
Wound	8-11	11-12	-	-	-
Kill	12	-	-	-	-

TABLE II.4. P_H/P_K TABLE SUBMACHINE GUN

9mm Submachine Gun					
	Range				
Yards	10	25	50	75	100
Metres	9.1	22.9	45.7	68.6	91.4
DAY	Total Dice Roll				
Miss	2-4	2-5	2-6	2-8	2-10
Wound	5-8	6-10	7-10	9-10	11
Kill	9-12	11-12	11-12	11-12	12
NIGHT					
Miss	2-5	2-6	2-8	2-10	2-12
Wound	6-10	7-10	9-11	11	-
Kill	11-12	11-12	12	12	-
From Armoured Vehicle					
DAY					
Miss	2-5	2-6	2-7	2-12	2-12
Wound	6-11	7-12	8-12	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-6	2-7	2-10	2-12	2-12
Wound	7-11	8-12	11-12	-	-
Kill	12	-	-	-	-

TABLE II.5. P_H/P_K TABLE — RIFLE (5.56 MM)

5.56 mm Rifle												
	Range											
Yards	25	50	75	100	125	150	175	200	225	250	275	300
Metres	23	46	69	91	114	137	160	183	206	229	251	274
DAY	Total Dice Roll											
Miss	2-3	2-4	2-6	2-6	2-6	2-7	2-8	2-9	2-10	2-11	2-11	2-11
Wound	4-8	5-10	7-10	7-10	7-10	8-10	9-10	10-11	11	12	12	12
Kill	9-12	11-12	11-12	11-12	11-12	11-12	11-12	12	12	-	-	-
NIGHT												
Miss	2-6	2-7	2-8	2-9	2-9	2-10	2-11	2-11	-	-	-	-
Wound	7-9	8-10	9-11	10-11	10-11	11	12	12	-	-	-	-
Kill	10-12	11-12	12	12	12	12	-	-	-	-	-	-
	From Armoured Vehicle											
DAY												
Miss	2-5	2-6	2-7	2-7	2-7	2-9	2-10	2-12	-	-	-	-
Wound	6-11	7-12	8-12	8-12	8-12	10-12	11-12	-	-	-	-	-
Kill	12	-	-	-	-	-	-	-	-	-	-	-
NIGHT												
Miss	2-7	2-9	2-10	2-12	-	-	-	-	-	-	-	-
Wound	8-12	10-12	11-12	-	-	-	-	-	-	-	-	-
Kill	-	-	-	-	-	-	-	-	-	-	-	-

TABLE II.6. P_H/P_K TABLE–RIFLE (7.62 MM)

7.62 mm Rifle							
	Range						
Yards	50	100	200	300	400	500	600
Metres	46	91	183	274	366	457	549
DAY	Total Dice Roll						
Miss	2	2-4	2-5	2-6	2-8	2-10	2-11
Wound	3-6	5-8	6-10	7-10	9-10	11	12
Kill	7-12	9-12	11-12	11-12	11-12	12	-
NIGHT							
Miss	2-4	2-6	2-8	2-10	2-12	-	-
Wound	5-8	7-10	9-11	11	-	-	-
Kill	9-12	11-12	11-12	12	-	-	-
	From Armoured Vehicle						
DAY							
Miss	2-5	2-6	2-6	2-7	2-10	2-12	-
Wound	6-8	7-11	7-12	8-12	11-12	-	-
Kill	9-12	12	-	-	-	-	-
NIGHT							
Miss	2-6	2-7	2-10	2-12	-	-	-
Wound	7-11	8-12	11-12	-	-	-	-
Kill	12	-	-	-	-	-	-

TABLE II.7. P_H/P_K TABLE - ROCKET PROPELLED GRENADE

Rocket Propelled Grenade				
		Range		
Yards	50	100	150	200
Metres	46	91	137	183
		Total Dice Roll		
Stationary Vehicles (Lightly Armoured)	7-12	9-12	11-12	12
Moving Vehicle	8-12	10-12	12	-

No Effect if Total Dice Roll is less than the lower range of values shown
1 Round Per Engagement, 1 Round per turn

TABLE II.8. P_H/P_K TABLE — SHOTGUN

Shotgun					
	Range				
Yards	7	15	25	40	60
Metres	6.4	13.7	22.9	36.6	54.9
DAY	Total Dice Roll				
Miss	2-4	2-6	2-8	2-10	2-11
Wound	5-8	7-10	9-10	11	12
Kill	9-12	11-12	11-12	12	-
NIGHT					
Miss	2-6	2-8	2-10	-	-
Wound	7-10	9-10	11	-	-
Kill	11-12	11-12	12	-	-
From Armoured Vehicle					
DAY					
Miss	2-6	2-7	2-12	2-12	2-12
Wound	7-11	8-12	-	-	-
Kill	12	-	-	-	-
NIGHT					
Miss	2-7	2-10	2-12	2-12	2-12
Wound	8-11	11-12	-	-	-
Kill	12	-	-	-	-

TABLE II.9. P_H/P_K TABLE — SNIPER RIFLE (M24)

M24 Sniper Rifle					
	Range				
Yards	50	100	150	200	300
Metres	46	91	137	183	274
	Total Dice Roll				
Personnel	4-12	6-12	7-12	8-12	-
Vehicle (non-armoured)	8-12	8-12	9-12	9-12	9-12
From armoured vehicle					
Personnel	6-12	8-12	9-12	10-12	-
Vehicle (non-armoured)	10-12	10-12	12	12	12
M24 vs Armoured Vehicle -- PK = 0.0 (can roll to cause a flat tire)					
No Effect if Total Dice Roll is less than the lower range of the values shown					
1 Round per engagement, 1 Engagement per turn					

The following forms can be used during the tabletop analysis (See Tables II.10 through II.13):

TABLE II.10. DATA COLLECTION TABLE — RESPONSE FORCE

Protective Force Unit Assignment				
Controller Name:			Page ____ of ____	
ID Number	Assignment	Equipment	Action	Turn

TABLE II.11. DATA COLLECTION TABLE — ADVERSARY ASSIGNMENTS

Adversary Assignments				
Controller Name:			Page ____ of ____	
ID Number	Assignment	Equipment	Action	Turn

TABLE II.12. SCENARIO DESCRIPTION FORMS

Tabletop Modelling Scenario Description
Scenario Description (Scenario #____)
Protective Force
Configuration:

Tabletop Modelling Scenario Description
Scenario Description (Scenario #____)
Adversary Force
Configuration:

TABLE II.13. TABLETOP DATA COLLECTION SHEET

BattleBoard Analysis Timeline				
Time (seconds)	Marker ID	Marker Action	Dice Roll	Result (Miss, Wound, Kill)

II.3. SANDIA NATIONAL LABORATORIES TABLETOP METHODOLOGY

The following describes the process used to conduct a scenario-based SNL TTX methodology.

II.3.1. SNL TTX P_H/P_K

The P_H/P_K calculation chart tool resolves engagements and other events between the adversary and the response force. In instances in which engagements occur the P_H chart(s) are consulted to determine the statistical probability of an event outcome based upon the weapon type, distance, and rate of fire using a roll of a ten-sided die. Tables II.14 and II.15 reflect hypothetical data P_H calculation charts used for human target and armoured vehicles.

TABLE II.14. SNL TTX P_H CHART FOR HUMAN TARGETS

Step 1	Find base P_H cross-referencing weapon type and range to target (rounds down range)								
	Weapons P_H Table								
Weapon Type	RANGE ->	10m	20m	30m	40m	50m	60m	70m	Max Eff.
	Rate of fire in 10 seconds # rounds fired								
Pistol (9mm)	2	7	5	3	1	x	x	x	50m
Assault Rifle (9mm)	2	7	5	3	3	2	1	1	100m
Weapon Type	RANGE ->	100m	300m	500m	700m	900m	1100m	1300m	Max Eff.
	Rate of fire in 10 seconds # rounds fired								
Assault Rifle (5.56)	2	7	5	3	1	x	x	x	600m
Light Machine Gun (5.56)	3	6	4	2	1	x	x	x	600m
Heavy Machine Gun (7.62)	3	6	4	2	2	1	1	x	1000m
Heavy Machine Gun (50 cal.)	3	5	5	5	3	3	3	1	1800m
Sniper Rifle (7.62)	2	7	7	5	3	1	1	x	1000m
Sniper Rifle (50 cal.)	1	7	7	5	3	3	3	1	1800m
Rocket Propelled Granade-7	1	6	3	1	x	x	x	x	500m
40 mm	1	6	3	x	x	x	x	x	350m
40 mm belted	3	6	4	4	3	3	2	2	1600m
Spotting only	n.a.	5	3	1	0	0	0	0	0

Modified spotting P_H +1 for target firing, +1 for target moving, +1 for large target, +1 fpr pos rep from friendly unit: all modifiers are cumulative. Example: P_H to spot a moving vehicle ay 700 metres is 0 + 1 + 1 = 2

* n.a.: not applicable.

TABLE II.15. SNL TTX P_H CHART FOR ARMOURED VEHICLES

Vehicle P_K Table							
Die Roll:	Vs. Armour*	5.56mm	7.62mm	.50 cal	40mm HEDP	RPG	9 mm (No effect on Armour)
1	Vk	Vk	VK 1 KIA	VK 2 KIA	VK 2 KIA	VK all KIA	1 KIA
2-3	1 KIA	1 KIA	VK	VK 1 KIA	VK 2 KIA	VK 2 KIA	1 KIA
4-5	No effect	1 KIA	VK	VK 1 KIA	VK 1 KIA	VK 2 KIA	No effect
6-7	No effect	1 KIA	1 KIA	VK 1 KIA	VK 1 KIA	VK 1 KIA	No effect
8-9	No effect	No effect	1 KIA	VK	VK	VK 1 KIA	No effect
10	No effect	No effect	1 KIA	1 KIA	1 KIA	VK 0 KIA	No effect

Vk = Vehicle Kill (or vehicle disabled)

KIA = Personnel in vehicle killed

Movement Table: Movement of humans and vehicles are an important element for any time-based analysis or analysis tool. There are various factors that determine the speed for which a TTX entity moves such as the rate of speed (slow, medium, fast, very fast), position (crawling or crouching) or method of movement (tactical). Movement speeds are disregarded in instances in which an individual is traversing large distances on foot, or is carrying a heavy load. Table II.16 is a hypothetical data movement table used during a TTX.

TABLE II.16. SNL TTX MOVEMENT RATES

TTX Movement Rate Table						
	10 Seconds		30 Seconds		60 Seconds	
	Personnel	Vehicle	Personnel	Vehicle	Personnel	Vehicle
Slow	7 m 2 kph (crawling or crouch)	27 m 10 kph	20 m 2 kph (crawling or crouch)	80 m 10 kph	40 m 2 kph (crawling or crouch)	160 m 10 kph
Medium	13 m 5 kph (tactical movement)	133 m 48 kph	40 m 5 kph (tactical movement)	400 m 48 kph	80 m 5 kph (tactical movement)	800 m 48 kph
Fast	26 m 10 kph (running)	266 m 97 kph	80 m 10 kph (running)	800 m 97 kph	160 m 10 kph (running)	1600 m 97 kph
Very Fast	N/A	400 m 145 kph	N/A	1200 m 145 kph	N/A	2400 m 145 kph

II.3.2. SNL TTX methodology process

The facilitator will initiate the assessment by asking the protective force team to lay the convoy's response force positions out on the map in a typical configuration and dispersion for the facility. Initially, the adversary team adversary positions will not be identified on the map. The facilitator will start the simulation by examining the first ten seconds of the attack beginning with the adversary team's intentions. The adversary team will state each adversary element's intentions for this block of time to the facilitator. The facilitator will tell the protective force team what each response force element is going to experience during this block of time and what each element will be able to see and hear as a result of the adversary's actions. Next, the facilitator will ask the protective force team to state response force element's reactions and intentions for the same ten second block of time. The facilitator will note all individual and vehicle movements, potential engagements, and other stated intentions on the white board for both teams. Once both commanders' intentions are fully understood, they are noted on the map and the facilitator looks for any adversary/protective force interactions or engagements that need to be further examined and evaluated. The arbitration team will examine each potential engagement individually and determine the following for each:

- Engagement feasibility
  - Line of site between shooter and target
  - Range of weapon system (distance in Table II.14)
- Characteristics of the shooter
  - Standing still, walking, running, prone, kneeling, in vehicle
  - Type of weapon and round, number of rounds, mounted, bipod, supported
- Characteristics of target
  - In/out of vehicle, level of armor on vehicle, speed of vehicle
  - Body armor/level, behind cover, in prepared fighting position
  - Prone, kneeling, standing, walking, running, low crawling.
- Run P_H/P_K calculations and declare the results of the engagement (see Tables II.14 and II.15)

Personnel casualties, personnel suppressed from fire, and vehicle kills are recorded for both teams. The facilitator along with the arbitration team will decide which adversary positions were exposed to the response force as a result of actions during the previous ten seconds. Those adversary positions will be noted on the map and pointed out to response force team elements that would have seen them.

The facilitator will briefly recap the actions and engagements of the previous ten seconds to the adversary and protective force teams, describing what each element would have experienced. Depending on how fast the scenario is moving, the facilitator will decide the amount of time to examine in each subsequent evolution. Typically, the initial moments of the simulation are examined in small time slices of ten or twenty seconds. As the action of the scenario starts to slow, the facilitator may increase the time increments to a longer duration of thirty seconds up to several minutes depending on progress of the assessment.

The facilitator will ask the adversary team to state each individual adversary element's intentions for the next time period being examined. The facilitator will then explain to the protective force team what each response force element is experiencing and ask for that element's actions or reactions for the time period being examined and the process repeats itself.

The assessment will continue until the facilitator and arbitration team decide that the analysis objectives have been met.

It is important to review necessary information so all stakeholders and supporting personnel thoroughly understand how the stage is set and what the parameters are prior to starting the tabletop exercise.

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, Nuclear Power Plant Case Study for the Nuclear Security Assessment Methodologies for Regulated Facilities, IAEA, Vienna (2019)

[3] 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)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No.14, IAEA, Vienna (2011).

[5] 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).

[6] 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).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

ABBREVIATIONS

Ci	Curie
CRP	Coordinated research project
DBT	Design basis threat
GPS	Global positioning system
GSPL	Gamma Secure P/L
IAEA	International Atomic Energy Agency
KIA	Killed in action
KSPL	Kobalt Service P/L
LNRA	Lagassi Nuclear Regulatory Agency
NUSAM	Nuclear security assessment methodologies
ORNL	Oak Ridge National Laboratory
P_H/P_K	Probability hit/probability kill
PPS	Physical protection system
SA	Security assessment
SNL	Sandia National Laboratories
TCC	Transport command centre
TSP	Transportation security plan
TT	Tabletop
TTX	Tabletop exercise

LIST OF PARTICIPANTS

Alam, B	Bangladesh Atomic Energy Commission, Bangladesh
Brüecher, W.	GRS, Germany 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