SAND2017-11121C

SUMMARY OF ANALYSIS METHODOLOGY RESULTS OF THE NUCLEAR SECURITY ASSESSMENT METHODOLOGIES (NUSAM) COORDINATED RESEARCH PROJECT

M.SNELL
Sandia National Laboratories
Albuquerque, United States of America
Email: mksnell@Sandia.gov

J. RIVERS
Nuclear Regulatory Commission
Rockville, United States of America

D. SHULL
International Atomic Energy Agency
Vienna, Austria

Abstract

The paper reports on analysis methodology results developed and documented during the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP), the Development of Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities. The main objective of the NUSAM Project was to establish a risk-informed, performance-based methodological framework, addressing both insider and outsider threats to facilities and transport involving nuclear material. One of the NUSAM Working Groups, the Analysis Working Group (AWG) looked specifically at analysis techniques and methods. The paper discusses and compares several types of modeling and simulation tools that exist today and are used internationally to support physical protection system effectiveness evaluation, as part of risk-informed security. The AWG worked directly with the developers of these different methods and tools to document the strengths and weaknesses of each. With its technical expertise, the AWG documented the technical and mathematical basis for several of the different techniques, at a level that has not been published to date. The AWG developed summary diagrams that relate how the tools to date can best be used in conjunction with one-another.

1. INTRODUCTION

The paper reports on analysis methodology results developed and documented during the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP), the Development of Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities. The NUSAM CRP held its first meeting in April 2013. The main objective of the CRP was to develop a performance-based, risk-informed methodological framework for assessing security effectiveness at a broad range of facilities and transport activities involving nuclear material against both insiders and outsider threats. After 3 years, the NUSAM CRP has developed and validated such a methodology. The paper reports one aspect of that methodology, the modelling and simulation tools of relevance to that methodology that exist and are used internationally to support physical protection system (PPS) effectiveness evaluation, as part of risk-informed security.

The paper starts with an overview of the NUSAM methodology framework and process in Section 2. Section 3 describes different categories of methods and tools that were applied to analyse security for several case studies during the CRP. This section also describes a process for using modelling and simulation (mod/sim) tools and methods. Section 4 describes other technical and mathematical results produced by the NUSAM Analysis Working Group (AWG), while Section 5 presents conclusions.

2. NUSAM METHODOLOGICAL FRAMEWORK AND PROCESS

The NUSAM methodology is used to perform a Security Assessment (SA) of an entire security system. Figure 1 provides a high-level summary of the methodology and of the key milestones/activities in an SA. This methodology can be applied to support evaluations of security measures against unauthorized removal and/or

sabotage. The methodology is intended for use with fixed site facilities that handle, store, or manage nuclear and high-activity radiological materials and the transport of these materials.

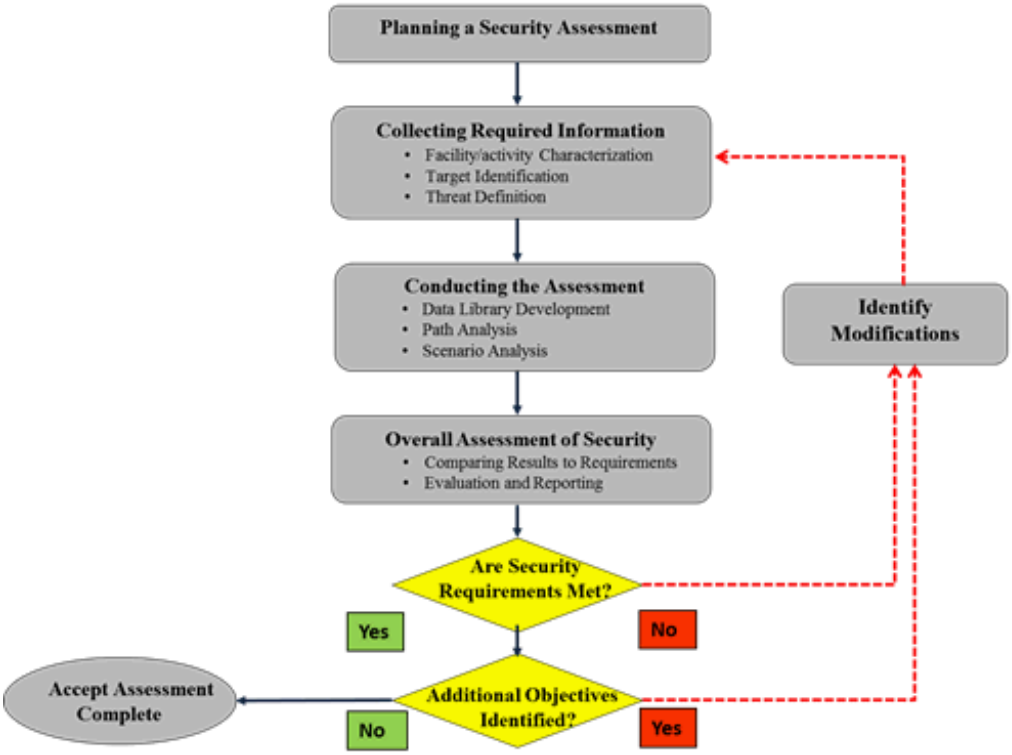

FIG. 1. The NUSAM Methodological Framework

The first milestone in the methodology is to plan the SA. Planning identifies the purpose of the SA; the security requirements, such as regulations, policies and guidelines, to be addressed as part of the SA; and how the SA will be managed. The primary purpose of a SA is to determine if the applicable security requirements are met. These requirements can be prescriptive, performance-based or a combination of the two, as defined by the relevant competent authority or State body. In addition, the assessment may also be intended to provide insight into the strengths and weaknesses of the PPS under evaluation. The regulations, policies and guidelines applicable to a facility will determine the security objectives that must be met and the type of assessment that will need to be performed. Note that the focus of the paper is on performance-based aspects of SA's.

The next milestone in the methodology is to collect the information required for the SA. The process for collecting required information consists of several steps: first, characterize the facility or activity; next, identify targets associated with that facility or activity; and finally, define the threat to be used for the assessment. The facility/activity characterization involves gathering information, such as a comprehensive description of the facility/activity, operation conditions, and nuclear security requirements as well as regulatory requirements. Targets are identified based on relevant requirements to protect the facility/activity against unauthorized removal and sabotage. A performance-based SA requires the threat and associated capabilities to be specified, as defined by the State's competent authority in the form of a threat assessment (TA) and, if appropriate, a Design Basis Threat (DBT). At the facility level, the TA/DBT may be augmented by assumptions associated with the approved security plan concerning how the threat might be addressed. For example, there may be assumptions about whether the adversary has the expertise to disable certain safety systems or to find the right NM container in a large, crowded vault. These additional assumptions are documented in a scoping document for the SA.

The third milestone in the methodology is to conduct the assessment itself. The three steps that make up a nuclear SA are: to develop data libraries that indicate how effective the physical protection measures are, both individually and as parts of subsystems and actual systems; to perform path analysis; and to perform scenario analysis. Depending upon the nature and objectives of the SA not all of these steps may need to be performed;

for example, facilities with simple layouts may not be a need to perform path analysis. This milestone is the focus of the paper so these three steps will described in detail in section 3.

The last milestone is to perform an overall assessment of security. The main task during this milestone is to summarize all relevant evidence in a comprehensive manner, to be able to answer the high-level question "Are Security Requirements Met?" The purpose of the assessment, agreed upon earlier, will determine the nature of the results and how they will be evaluated. In the overall assessment it may be helpful to report results differently depending upon whether a particular requirement is prescriptive or performance-based. If the assessment results reflect that security requirements are not met, a more detailed analysis of the assessment outcome(s) should be provided. This analysis should focus on the significant issues and problems associated with the facility/activity. The results of the SA should then be reported to relevant management responsible for protecting the facility/activity and to the competent authority, as appropriate. If the security requirements have not been met then it might be necessary to make modifications to the facility design, etc., and start the SA again. If the security requirements have been met, and there are no additional objectives that are identified, then the SA is accepted.

3. CONDUCTING THE ASSESSMENT

The three NUSAM assessment steps are described in more detail below in subsections 3.1 to 3.3. Steps 3.2, path analysis, and 3.3,scenario analysis are both used to determine 3 performance measures for each scenario:

- Probability of System Effectiveness (P_E): The probability that the PPS will defeat the adversary;
- Probability of Interruption (P_I): The probability that the response force arrives in time to stop the adversary;
- Probability of Neutralization (P_N): The probability that the response force defeats the adversary, given interruption occurs.

The three measures are related as follow: $P_E = P_I \times P_N$. A generalization of this formula will be presented in a later section.

3.1. Develop Data Libraries

Data libraries are historical collections of performance test data that can be used as a basis to justify nuclear security element probabilities of detection (P_{DS}) as well as assessment and delay times used in modelling and simulation activities. Data libraries should be developed and maintained as part of any assessment programme or process. Six categories of information may be included in a data library: detector performance (such as P_D), tools/equipment weights and delay times, weapon effectiveness, transit speeds for people and vehicles; building barrier information (e.g., construction, transparency, effects due to weapons), and terrain data.

Data library values can be derived from state sponsored or other site testing, facility specific performance testing, SME judgment, and other sources such as state law enforcement, military experience, and insurance industry information. Manufacturer specifications or testing data may be used initially, until other user performance data can be developed. The data should be retained for quality control purposes regardless of the specific methods used to select and reduce the data.

3.2. Path Analysis

A path is a time-ordered sequence of adversary tasks or actions where each adversary action/task is associated with a facility location that the adversary moves through as they perform that action/task. The definition of a location associated with a task may be very general, such as "climb somewhere over the (2-km long) north fence of the Protected Area," more specific such as "Penetrate door 42 of Building XYZ," or it may be very specific, for example, "steal can 1234 at location (X, Y, Z) in Vault 32."

Path analysis is an evaluation method to determine whether the PPS is simultaneously effective across the many possible paths that the adversary might take to cause theft or sabotage at a facility. Performed properly, path analysis can also very quickly determine which paths provide the lowest Probability of Interruption P_I against the TA/DBT. Such paths, termed most-vulnerable paths, help the analyst determine if the facility design performance is balanced or unacceptable and in need of improvement. Most-vulnerable paths may also serve during scenario analysis as the basis from which to develop detailed adversary attack plans.

Note that some activities, such as transportation, are not associated with a path and for that reason do not need formal path analysis when the vehicle is outside of a protected facility.

P_I is calculated for a single adversary path by comparing an adversary timeline, based on delay times and detection probabilities associated with that path, to a response timeline, which consists of the times needed by the PPS to assess and respond to an alarm (see Figure 2). Sensing opportunities are places along the path where the adversary may generate alarms or be observed by surveillance CCTV or by people.

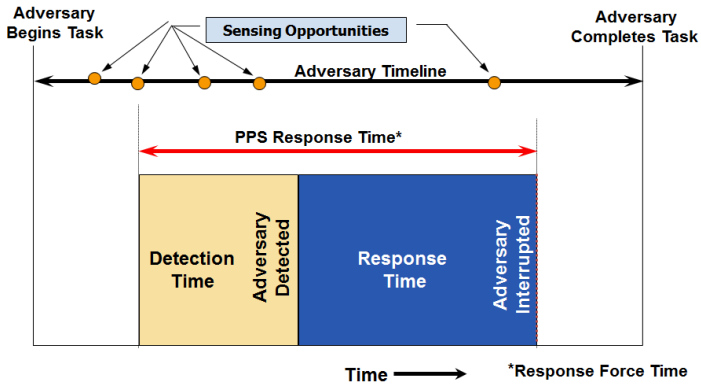

FIG. 2. Adversary Timeline and Response Timeline

During path analysis each sensing opportunity is evaluated to determine if the adversary delay after that opportunity exceeds the PPS Response Time (PRT) or not. If the remaining delay after that opportunity exceeds the PRT then that opportunity is judged to be timely. The last sensing opportunity on the path that is timely is called the Critical Detection Point (CDP). In the example in Figure 2, the CDP is the third sensing opportunity. Then P_I is defined to be the cumulative probability of detection on the path up to and including the CDP. CDPs are only defined if delay times, detection times and response times are point values. This assumption is true for the two software tools described here, Systematic Analysis of Vulnerability to Intrusion (SAVI) developed for the U.S. Department of Energy and ProEv (ProEv) developed in the Czech Republic by the EBIS Company, which both calculate P_I. Some scenario analysis tools, such as VEGA-2 and AVERT, have built in path models which determine not only P_I but P_N and P_E for paths; AVERT also allows delay times, etc., to have distributions.

Both SAVI and ProEv were created as "multipath tools" meant to determine those paths with the lowest P_I using networks that represent all of the paths through a facility. By considering all the paths, SAVI and ProEv can determine whether the PPS has balanced protection and is simultaneously effective across many paths that might be taken to cause unauthorized removal or sabotage at the facility. Both software tools develop a network model for the facility, from the point that the adversary starts the attack offsite to the end of the path where the adversary has completed their task. For SAVI the facility is represented as an adversary sequence diagram; ProEv uses two-dimensional representation of the facility.

Multipath tools require less training and facility modelling than computer simulations and can readily be taught in a week to security professionals who have no Mod-Sim experience. ProEv, being a more detailed tool than SAVI, can more directly and realistically represent the actual facility. If it turns out that the P_I for the most-vulnerable path is unacceptable, this fact can be identified and potentially fixed before the analyst performs more costly scenario analysis. The major weakness of path analysis P_I tools are that they do not model neutralization nor can they capture physical protection effectiveness beyond what can be assigned to detection probabilities, delay times, and PRTs.

3.3. Scenario Analysis

Nuclear security scenarios can be divided into several component stages, each addressing sub-objectives that the adversary has. The paper will refer to the scenario as that phase where a facility or transport activity is being attacked by adversaries intent on unauthorized removal or sabotage. Scenarios can be described as having attributes, such as the type of adversary involved (outsider/insider), the target location(s), facility/transport operating condition(s), whether part of the attack includes cyber-attacks or the use of Vehicle Borne Improvised Explosive Devices and avenue of approach (e.g., from the sea or by land).

The NUSAM CRP described scenario analysis is composed of four sub-steps:

(a) Identify scenario sets to analyse. During this step the analyst determines what set of scenario classes to evaluate. A scenario class conceptually includes scenarios that have the same scenario attributes. Thus one can speak about the class of scenarios involving unauthorized removal from vault 62 by terrorists during off shift operating conditions;

(b) Develop detailed scenarios. Scenarios selected within each scenario class might be chosen to be most-vulnerable and might be developed based on a most-vulnerable path generated by path analysis software or by a team of subject matter experts (SMEs);

(c) Select final scenarios to evaluate. Either while the scenario is being developed or at the end of that process, the scenarios need to be reviewed to determine what scenarios will be evaluated or not. This selection process may involve input from stakeholders, such as staff from the competent authority or facility management or it may be performed internally within the software itself;

(d) Determine effectiveness against final scenarios. NUSAM has identified four performance assurance methods that can be used singly or in combination to evaluate scenarios: Human-in-the-Loop Simulations, Human-out-of-the Loop Simulations, Table-Top Exercises (TTXs), and Limited Scope Performance Tests/Force-on-Force Exercises (LSPTs/FoF's).

The scenario analysis process for using the software tools and evaluation methods found in the paper is reflected in Fig. 3. The analysis process begins at the Start Node. If the tool or method applies a path analysis approach, the node "Path Identification Tools" would then be highlighted along with the resulting paths Path 1, Path 2, …, Path N. Some tools, such as SAVI or ProEv, do nothing more than generate paths. Detailed attack plans would then be generated, either by a specialized team of SMEs or by the software itself using an automated process. Note that in the latter case typically the analyst will interact with the attack plan generator to influence what scenarios are developed.

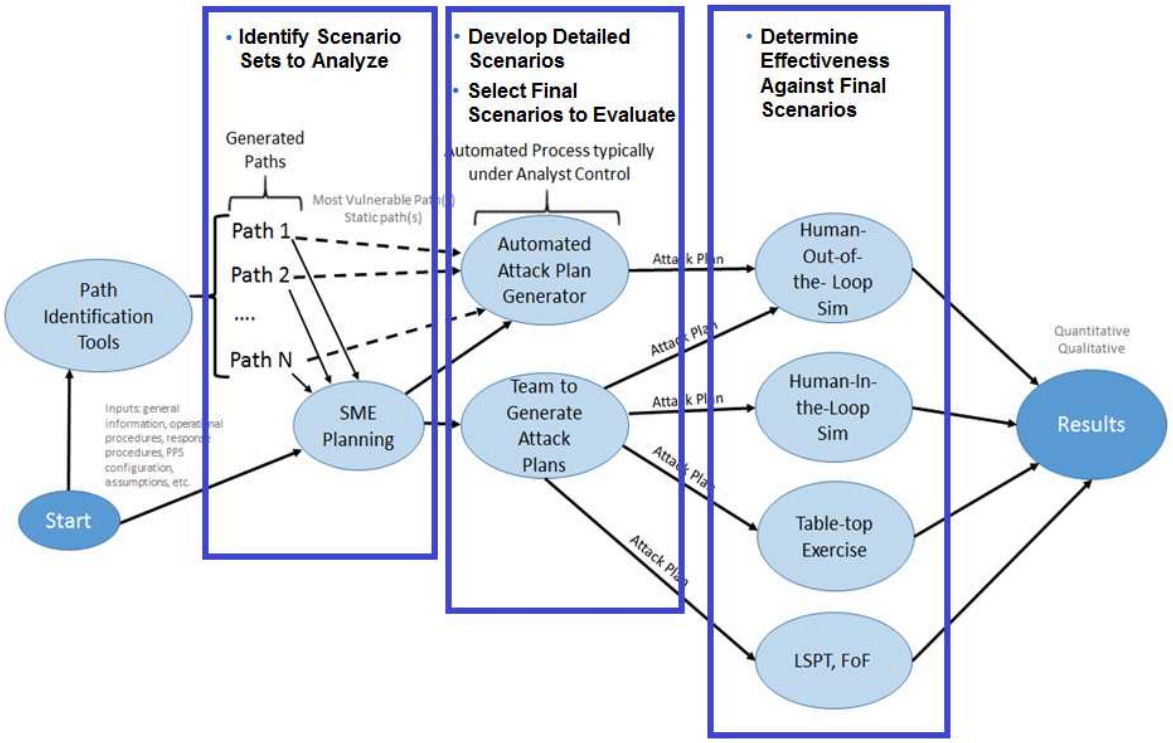

FIG. 3. Process for Using Evaluation Tools and Methods Combined with Four Scenario Analysis Sub-Steps

The last activity in Figure 3 is to determine effectiveness against the selected scenarios. SME-developed attack plans may be evaluated using

— Human-in-the-Loop Simulations, in which human operators directly control one or more entities such as guards and adversaries during a computer simulation of a scenario;

— Human-out-of-the-Loop Simulations, in which behaviour modules in the simulation control all entities during computer simulation of a scenario with limited human intervention;
— Table-Top Exercises (TTXs), in which humans perform all the steps needed to simulate the scenario using facility or terrain maps, to include making adversary and response force decisions and recording data during the TTX;
— Limited-Scope-Performance-Tests (LSPTs) or Force-on-Force (FoF) exercises, where the attack is simulated in the field using humans to perform adversary and response force activities and using simulated weapons.

FoF exercises are valuable because they evaluate the collective effectiveness of the complete PPS, including the actual protective force. These exercises are very resource intensive, requiring shadow forces, controllers, etc. FoF exercises were outside the scope of the NUSAM CRP.

Table 1 compares various characteristics of 5 scenario analysis tools that were applied during the NUSAM project to a notional Nuclear Power Plant, Lone Pine. *Note: The documentation within the paper in no way should be construed as a critical evaluation nor as an endorsement for the identified tools. Rather, the information provided here is intended to show the process, results, and general capabilities of the tools.*

TABLE 1. COMPARISON OF SCENARIO ANALYSIS TOOLS

Software/Method Name	TTX	STAGE	VEGA-2	Simajin	AVERT
Type (S = Software, M = Method)	M	S	S	S	S
Performs Path Analysis	Yes	No	Yes	Being developed	Yes
Metrics Calculated: P_I	No	Yes	Yes	Being developed	Yes
Metrics Calculated: P_N, P_E	Win/Loss Only	Yes	Yes	Yes	Yes
Computer Simulation	No	Yes	Yes	Yes	Yes
Human in the loop	-	No	No	Yes	Yes
Human out of the loop (Constructive)	-	Yes	Yes	Yes	Yes
Representation of Site and Building Floors	2D Maps	3D	2D+	3D	3D
Delay and Probability of Detection Values	Fixed	Fixed	Fixed	Sampled	Sampled
Data Analysis Tools	No	Yes	No	Yes	Yes

Figure 4 shows how facility sites and buildings are represented in each tool. Note: "2D+" in the table refers to facility representations where building floors are individually modelled in 2 dimensions and the building layout is assumed to be the same between two adjacent floors.

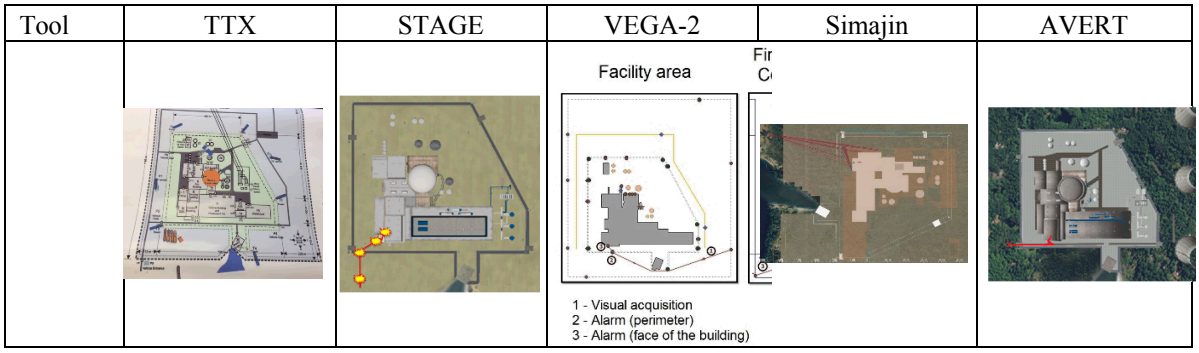

FIG. 4 Representation of Sites and Buildings in Scenario Analysis Tools

Additional information about these 5 scenario analysis tools is provided in 3.3.1-3.3.5.

3.3.1. Table-Top Exercise (TTX) Method

A Table-top Exercise is a manual analysis methodology intended to generate discussion of various issues regarding a particular facility or transport activity based on interactions between the PPS response forces and adversaries. The concept of the TTX is familiar to anyone who has engaged in a turn-based combat-oriented board games. Two methods were documented: the Oak Ridge National Laboratory Battleboard Table-Top Methodology and the Sandia National Laboratories Table-Top Methodology.

- Scenario Analysis Process Steps for Using a TTX: Start, SME Planning, Team to Generate Attack Plans, Table-top Exercise, then results.
- Process for Use: SMEs develop attack plan that is then simulated by hand in a facilitated manner as a group exercise with data recorded manually
- Some Strengths: Requires modest commitment of time and resources; good at replicating decision making; observers can easily see how events are handled and tactical decisions are made; can be stopped for discussion; no need for computers.
- Some Weaknesses: Results are qualitative; simulating one scenario may take hours; limited capability to model technical systems, determine weapon effects and check weapon line of sight with targets; expertise is needed to facilitate and manage the exercise.

3.3.2. STAGE

The Scenario Toolkit and Generation Environment (STAGE) is a Canadian-developed modelling and simulation tool that provides users with the ability to generate and execute complex scenarios for training and analysis. The tool, which was developed by Presagis, uses an integrated simulation environment to build dynamic and interactive tactical and operational scenarios. STAGE serves as the core simulation tool that was customized by adding capabilities that model an adversary/response force engagement to determine P_N and P_E.

- Scenario Analysis Process Steps for Using STAGE: Start, SME Planning, Team to Generate Attack Plans, Human-out-of-the-Loop simulation, then results.
- Process for Use: SME develops attack plan that is then simulated in a Human-Out-of-the-Loop simulation (see steps in Figure 3).
- Some Strengths: High flexibility, open code if modifications are desired, can be used by single analyst
- Some Weaknesses: The analyst(s) need a high level of training to go from source data to the simulation, then to run the simulation and to interpret the result. The basic STAGE simulation package also needs to be customized to support vulnerability assessments.

3.3.3. VEGA-2

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

- Scenario Analysis Process Steps for Using STAGE: Start, Path Identification Tools, Automatic Attack Plan Generator, Human-out-of-the-loop simulation, then results.
- Process for Use: The analyst enters facility and adversary information; the software then automatically generates each path and associated attack plans and finally simulates the scenario in a Human-Out-of-the-Loop simulation.
- Some Strengths: Addresses both insider and outsider threats; automatically generates and evaluates all paths through a model of the facility based on automatically-generated attack plans for each path; can be used by single analyst
- Some Weaknesses: The analyst(s) need a high level of training to interpret the output; does not take into account sniper support outside the site territory; and would need to be adapted for use by other countries.

3.3.4. Simajin/Vanguard Simulation Tool

The Vanguard modelling and simulation tool, developed by RhinoCorps Ltd. utilizes the Simajin Application Suite of models to provide quantitative and qualitative analysis of physical security scenarios. The fully automated force-on-force (FoF) simulation tool enables physical security analysis to model a range of environments with a number of threat vectors and variables. The fully automated representation of human behaviour in a combat environment provides statistically significant results with only limited user interaction. Vanguard allows analysts to conduct risk assessments and quantify how well protective measures will repel, or defeat, a suite of tailored threats; further, it allows for the analysis of countermeasures whether these be personnel, material, tactics, techniques, or procedures to reduce risk to manageable levels. Vanguard helps decision makers make physical security planning decisions that are backed by valid scenarios and statistically significant analysis results. Simajin/Vanguard is a simulation that calculates P_I, P_N, and P_E.

- Scenario Analysis Process Steps for Using Simajin: Start, SME Planning, Automatic Attack Plan Generator, Human-out-of-the-Loop simulation, then results.
- Process for Use: The analyst enters facility and adversary information; the tool will generate pathways based on SME inputs and a SME may enhance those pathways to develop high fidelity, possibly multi-team coordinated attack plans that are then simulated. The attack plan may also be reused in a table top human-in-the-loop simulation (which was not used or evaluated as part of the NUSAM analysis).
- Some Strengths: Automated behaviour in simulation supports adversary/response team collaboration and coordination, movement, use of weapons and tools, communications, and vehicles; Simajin is part of larger modelling and simulation suite with other capabilities; highly detailed models of the facility.
- Some Weaknesses: Maintenance and operational requirements are fairly high: a permanent dedicated staff to will probably be needed to maintain proficiency; developer support may be necessary; a fairly high level of effort is needed to build behaviours associated with the defence posture.

3.3.5. AVERT Modelling and Simulation Tool

AVERT is a modelling and simulation tool designed by ARES Security Corporation to enable risk-informed decision making based upon quantitative risk assessments. The software analyses the performance of current facility and security design and interrogates “what if” scenarios to assess and prioritize future investments and operational procedures. The AVERT tool suite has the ability to model a variety of risks including intentional acts, natural disasters, and other disruptive events to address the needs of a variety of operations. AVERT can also be used as a Human-In-The-Loop simulation by placing “destination” targets anywhere in a model. AVERT is a simulation that calculates P_I, P_N, and P_E.

- Scenario Analysis Process Steps for Using AVERT: Start, SME Planning, Automatic Attack Plan Generator, Human-out-of-the-Loop simulation, then results.
- Process for Use: The analyst builds a very detailed 3D terrain and building model; AVERT then creates a very detailed network of the facility and determines most-vulnerable paths through that network. It then automatically generates attack plans based on these pathways and models them in a Human-out-of-the Loop simulation. Finally, AVERT orders the attack plans in terms of increasing P_E, starting with the most-vulnerable P_E paths.
- Some Strengths: Combines path analysis seamlessly with scenario analysis within the tool; part of larger modelling and simulation suite with other capabilities; highly detailed models of facility.
- Some Weaknesses: Maintenance and operational requirements are fairly high: a permanent dedicated staff to will probably be needed to maintain proficiency; developer support may be necessary; a fairly high level of effort is needed to build 3D terrain and building models.

3.4. Application of Path and Scenario Analysis Tools and Methods

Table 2 indicates methods and tools that NUSAM researchers would recommend be used for different types of facilities and activities. For example, the CRP concluded that computer simulations and path analysis are probably not appropriate for evaluating a Spent-Fuel Storage facility. Computer simulations are listed as optional for NPP/Cat I Facilities and Transport; this is not meant to imply that they are of marginal benefit merely that the

recommendation to use them would be best made on a case-by-case basis by considering the benefit of using a computer simulation versus the costs in data and training required to use the simulation. Note that the computer simulation category includes both Human-in-the-Loop and Out-of–the-Loop simulations.

TABLE 2. SUGGESTED METHODS AND TOOLS TO USE FOR EVALUATING DIFFERENT TYPES OF FACILITIES/ACTIVITIES

Performance Assurance Methods	NPP/Cat I Facilities	Irradiator Facility	Transport	LEU Fuel Fabrication	Spent-Fuel Storage
Checklists Against Prescriptive Requirements	X	X**	X	X	X
Path Analysis	X**	X**	Parked at facilities	Optional	
Tablet-Top Exercises	X**	X**	X**	X	X
Computer Simulations	Optional**	***	Optional		
LSPTs	X	X	X	X	X
RF Tests, including Force-on-Force (FoF)	X (including FoF)	Optional	X (including FoF)	Optional	X

Entries in Table 2 with "**" indicate combinations of methods and facilities that were used for the 3 NUSAM CRP Case Studies: A nuclear power plant (Lone Pine), an irradiator facility, and a Category 1 radioactive source transport activity. There is also one combination indicated with "***" corresponding to the use of a computer simulation at an Irradiator Facility; in this case a computer simulation was applied to an irradiator facility but the case study participants subsequently decided that other tools with smaller resource requirements were adequate.

4. OTHER TECHNICAL RESULTS

The NUSAM CRP also produced a number of separate technical and mathematical results that will be summarized here.

NUSAM participants documented of a number of mathematical models that can be used as part of nuclear SAs, either by themselves or as part of simulation tools:

- Communications models;
- Line of sight models between an observer or camera and some entity being observed;
- Hearing models for guards, response forces, and intruders;
- Weapons effects models, including a description of both standard Ph/Pk models and physics-based models that track the flight of the bullet and round and determine whether it hits the target;
- Probability models used for calculating the probability of several OR'd and/or AND'd events. The NUSAM research addressed how to put lower bounds on probabilities for non-independent events. For example, if E_1 and E_2 are two different events and $P\{E_2|\overline{E_1}\} \leq P\{E_2\}$ then $P\{E_1 \text{OR } E_2\} \geq$ the larger of $P\{E_1\}$ and $P\{E_1\}$ while if $P\{E_2|\overline{E_1}\} \geq P\{E_2\}$ then $P\{E_1 \text{OR } E_2\} \geq P\{E_1\} + P\{E_2\} * (1 - P\{E_1\})$ which is the probability model assuming E_1 and E_2 are independent. Thus, it is possible to usefully bound $P\{E_1 \text{OR } E_2\}$ from below even if it can't be calculated explicitly. As an example of the second case, where $P\{E_2|\overline{E_1}\} \geq P\{E_2\}$, this may occur if E_1 and E_2 represent detection on one or the other of two complementary sensors. For $P\{E_1 \text{AND } E_2\}$ all that can be said is that $P\{E_1 \text{AND } E_2\} \geq 0$.

The general formula, $P_E = P_I \times P_N$, can be made more precise by conditioning on the sensing opportunity j which leads to the adversary being detection. If P_{Dj}, P_{Ij}, P_{Nj} are the probabilities of detection, interruption (given detection), and neutralization (given interruption), respectively, based on detection at sensing opportunity j, then:

$$P_E = \sum_{j=1}^{J} P_{FDj} P_{Ij} P_{Nj}$$

where P_{FDi} is the probability that the adversary is detected for the first time at sensing opportunity j:

$$P_{FDj} = P_{Dj} * \left\{ \prod_{i=1}^{j-1} (1 - P_{Di}) \right\}$$

NUSAM documented the two TTX methods on paper, with associated hypothetical supporting data, so that they can be used directly by Member States without needing software, etc. There was also an analysis that showed that the approaches could result in very different estimates of P_N for the same scenario.

A manual method for evaluating a scenario, Vulnerability of Integrated Security Analysis (VISA), developed by Science Applications International Corporation (SAIC), was also applied to the Lone Pine nuclear power plant. VISA was evaluated in a similar way to the other scenario analysis tools, with strengths and weaknesses identified, but was not included here due to space considerations. VISA has the virtue of being easy to apply, without needing software or TTX tools.

An approach to evaluating effectiveness against insider sabotage attacks was documented and an example provided. P_E equations were also developed to reflect the fact that the facility staff might actually fix some of the insider tampering (while mistakenly thinking it was assumed to be accidental) during a protracted sabotage attack. A mathematical model found in reference [1] for calculating P_E for violent insider attacks was also described.

A simple security risk analysis approach was proposed that attempts to harmonize security risks with safety risk models described in [2].

A game theory model for adversary deterrence was outlined, along with a hypothetical example.

Outsider path analysis approaches were developed from first principles, based on what are called adversary action sequences. An adversary action was originally defined in [3] as “any action conducted by an adversary in the course of perpetrating an event” (an “event” meaning a malicious act in current jargon). An adversary action sequence is a time-ordered sequence of adversary actions.

5. CONCLUSIONS

The paper reports on analysis methodology results developed and documented during the IAEA NUSAM CRP. The paper first presents a general methodology for performing security assessments and then discusses and compares several types of modelling and simulation tools and methods that exist today and are used internationally to support PPS effectiveness evaluations as part of risk-informed security. The NUSAM AWG also developed a general process showing how to use these analysis tools and methods sequentially as part of an security assessment. Finally, the AWG documented the technical and mathematical basis for several of the different techniques, at a level that has not been published to date.

REFERENCES

[1] BUSHUEV, A., GLEBOV, V., GERASKIN, N., IZMAYLOV, A., KRYCHUCKOV, E., KONDAKOV, V., FUNDAMENTALS OF NUCLEAR MATERIALS PHYSICAL PROTECTION, CONTROL AND ACCOUNTABILITY, Department of Education and Science of the Russian Federation, National Research Nuclear University “MEPhI”, Moscow, (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards - A Common Basis for Judgement, Safety Reports Series No. 12, IAEA, Vienna (1998).

[3] BENNETT, C., MURPHEY, W., and SHERR, T., SOCIETAL RISK APPROACH TO SAFGUARDS DESIGN AND EVALUATION, ERDA-7, Energy Research and Development Administration, Washington, D.C., (1975).