SAND2012-6364C

Special Nuclear Material and Critical Infrastructure Security Modeling and Simulation of Physical Protection Systems

Dean Dominguez, Mancel Jordan Parks, Adam D. Williams, and Susan Washburn
International Nuclear Security Engineering
Sandia National Laboratories
Albuquerque, NM USA 87185
{ddoming, mjparks, adwilli, swashbu} @sandia.gov

***Abstract*— Over the last decade, the world has faced a rapidly expanding and dynamic threat environment. As demonstrated by the 9/11 and 26/11 terrorist attacks, adversary capabilities have evolved to include advanced tactics and increased militancy. For the Department of Energy's National Nuclear Security Administration (DOE/NNSA), and other organizations responsible for protecting facilities housing special nuclear materials, this fragile mix of global uncertainty makes nuclear weapon security an important challenge. Sandia, using scientific and mathematic methodologies, is considered one of the world leaders in the design and implementation of physical protection systems (PPS) and VA methodology, in order to reduce the risk to both domestic and international high consequence facilities. Using the Presagis commercial software suite – primarily Scenario Toolkit and Generation Environment (STAGE), a complex simulation engine – the authors have developed a single analyst, Monte Carlo derived, agent decision-based, and event-driven interactive tool to help meet this need. Evaluating risk reduction for critical infrastructure against increasingly complex adversaries requires high fidelity VA modeling tools. Advanced adversary capabilities require modeling complex scenario variables, including multiple attack vectors and dynamically selected targets of opportunity. Large threat profiles with complex character behavior are needed for increasing adversary militancy. Coupled with Sandia methodology, the strength of the tool stems from the decision logic structure and built-in artificial intelligence components. STAGE allows for an inclusive command and control VA model that uses all traditional elements of a PPS (detection, communication, assessment, delay, command and control, response, interdiction, attrition, and neutralization). This paper will briefly describe the effect that the current threat environment has had on the VA process and then outline the role of STAGE in VA modeling and new threat reduction methodology. This paper also provides an update to the development of the STAGE tool, as well as a description of future plans to advance VA methodology and integrate STAGE simulation analysis with an existing physical site (the Integrated Security Facility at Sandia – a former Category I facility).**

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. **SAND 2012-6364C**

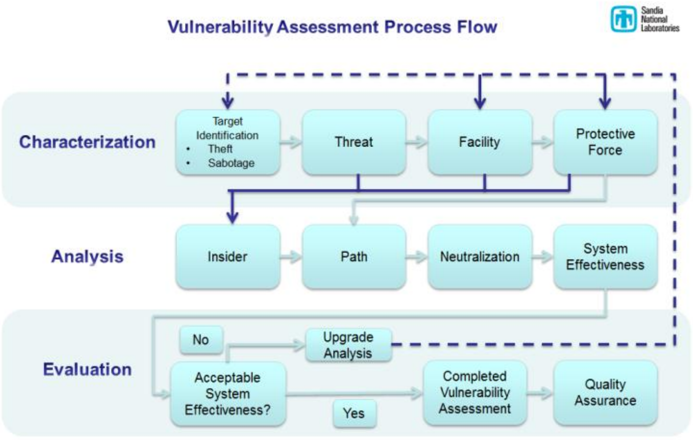


Figure 1. Vulnerability Assessment Process Flow

I. BACKGROUND

The National Nuclear Security Administration (NNSA) has a well-established vulnerability assessment (VA) methodology to evaluate the physical security requirements for nuclear weapons and Category I quantities of special nuclear material (SNM). NNSA engages complex wide to standardize the processes and implement a comprehensive and consistent characterization of the threat and protection system, including all resultant mitigation strategies.

The VA methodology is a series of components that includes the use of many analytical tools and processes utilized by subject matter experts (SME). As the process evolves, the series of components build upon each other feeding information from one component to the next. As such, this evidence gathering continues to add more fidelity to each respective component. The use of analytical tools is further enhanced with high fidelity data. Sandia, as an agent for NNSA, provides technical expertise to the complex in various capacities to satisfy the methodology outlined in Figure 1.

This tool-based approach satisfies each component and directly supports the performance-based methodology that characterizes the VA process as a whole. For example, the Protective Force (PF) Characterization component includes response time performance tests; subsequently, these response force times (RFT) are then implemented in force on force

(FoF) exercises as well as computer simulations (both part of the Analysis phase). Figure 2 outlines the analytical tool approach to solving the neutralization (PN) component of the VA process.

Simulation has been used for physical security since the late 1980s, when the Air Force began using Lawrence Livermore National Laboratory's (LLNL's) Security Exercise Evaluation System (SEES) as a force on force modeling tool. By 1996, DOE had adopted the Joint Tactical Simulation (JTS) as an approved VA tool basing the results of the Air Force's verification, validation, and accreditation project of JTS. At this point, most DOE sites had installed their own systems, and DOE HQ had a system in Germantown. Later, LLNL released the Joint Conflict and tactical Simulation (JCATS) and this was adopted by the DOE. The emphasis of simulation was and always has been to focus on the aspects of combat that are difficult to recreate or replicate in field exercises, and then be able to replicate these scenarios so that multiple observations on the same scenario could be collected.

The cumulative data gathered during FoF exercises and limited scope performance tests (LSPT's), such as the ability to execute the security incident response plan (SIRP), response force times, command, control, communications, the ability to demonstrate tactical efficiency (shoot and move), and the ability to effectively use weapon systems and vehicles, etc. are carefully analyzed to ensure they support key assumptions used in computer models and the resultant PN value.

Sandia as a leader in the industry for physical security-related modeling and simulation is active in the development of analysis tools, performance testing for databases, high fidelity geographic information systems (GIS) integration, state of the art 3D modeling, analytical methodologies, validation/verification, and integration with technical experts in respective engineering fields. The performance-based approach to systems engineering for physical protection systems (PPS) includes the integration of detection, delay, and response. This integration is the foundation of security system effectiveness. Working with SMEs in each field, Sandia has developed and maintained modeling and simulation methods that address the Neutralization component of the VA process.

As the years have progressed, modeling and simulation has also evolved. Growing interest in single analyst toolkits has followed the trend of budget cuts, the need to maintain performance, the need for high fidelity computer modeling, the need to model specific response/attack plans, and the need to increase the amount of data available to the Security Analyst. These needs have furthered a trend in the industry to develop high fidelity toolkits that integrate human decision making through the use of artificial intelligence (AI), decision making, path planning, and the execution of all potential contingencies in a scenario. Additionally, adversary tactics have shifted, changing the landscape of VA methodologies and threat definitions. Terrorism shifted the threat spectrum significantly in the first decade of the 21st century, following smaller attacks on the World Trade Center in 1993, and the Paris Metro attacks of 1995. The attacks of 9/11 (2001) in New York, Pelindaba (2007), and more recently 25/11(2008) in Mumbai, India, have demonstrated the influence of terrorist training and capabilities on the threat spectrum. Briefly, significant changes to the threat spectrum include insider knowledge of facilities, advanced military tactics, and coordinated multi-vector attacks intended to multiply forces and stress a facility's security response capability.

Sandia – with guidance and support from NNSA/NA-25 – led an effort to find a commercially available tool that would support the complex nature of Sandia's methodologies, as well as be available to international partners. This international partnership continues to develop, with program emphasis on shared technology and expert methodologies. The evaluation process for a Commercially available Off-the-Shelf (COTS) modeling and simulation toolkit considered a range of requirements; including but not limited to, exportability, meeting industry standards, adaptability to Sandia methodologies, AI components, analytical capabilities, and ability to model the complexities of an Sandia Vulnerability Assessment.

Presagis International, an industry leader in modeling and simulation, authors of the computer combat model Scenario Toolkit and Generation Environment (STAGE), have partnered with Sandia to provide a COTS solution to VA. From initial discussions with Presagis, Sandia's evaluation and subsequent capability development for STAGE was based on the ability to adapt the tool to ground combat applications. Presagis, as part of their business plan, offers the code for the software to the end user, to allow the user to modify components as needed. This flexibility has enabled Sandia to fill the analysis gaps that the tool may not have initially contained.

In addition to supporting Sandia's international modeling and simulation needs, STAGE's key design features also support efforts that extend beyond traditional VA needs. The analytical flexibility of the tool allows for outsider adversary evaluation, insider and process evaluation, training, and conceptual design of facilities and procedures. Utilizing STAGE, the project team is able to leverage the Integrated Security Facility (ISF) at Sandia to provide a mock special nuclear material (SNM) facility with a fully functioning physical protection system (PPS) for training, demonstration, testing, and evaluation. The ISF is a location to develop exportable technologies and integrate both commercial and custom technologies for security and safeguards systems around the world. Coupled together, STAGE and the ISF provide Sandia and their international partners a capability to better understand the full spectrum of VA functions, components, and best practices.

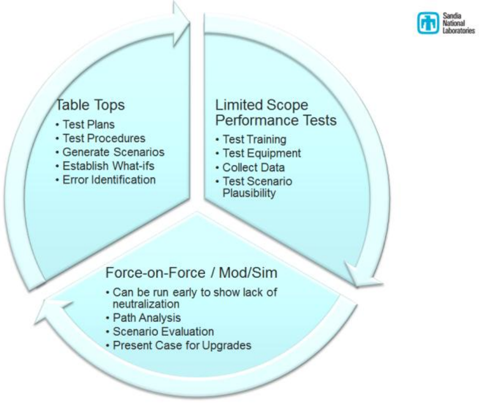


Figure 2. Tools for Neutralization Solutions

II. STAGE – DEVELOPMENT OF APPLICATION & CAPABILITIES

The STAGE software interface utilizes five editors when developing scenarios:

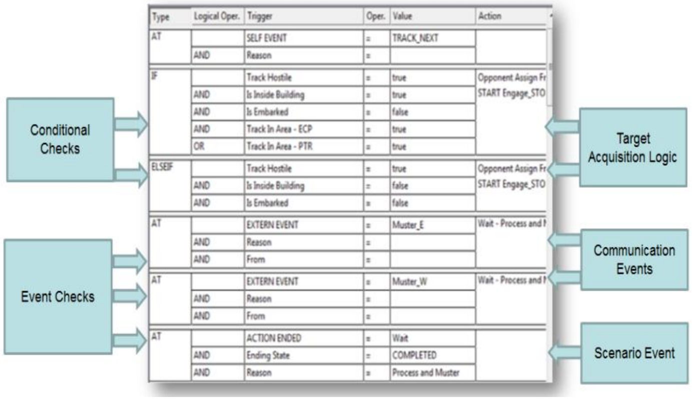
- The first editor is the database editor, a library which contains all of the critical performance data that feeds into the system. This editor allows the user to define all of the various computational sensors, weapon effects, combat speeds, load outs, armaments, and other various fidelity variables. As with most tools (commercial or government), the database ships with default data that does not tie to performance testing. The onus remains on the user to populate the database with respective site data. Over the years, DOE has and continues to perform testing on critical physical protection components that feed into the vulnerability process. These values provide the data foundation for the STAGE software.
- The second editor is the mission editor. The mission editor will be discussed more below, but provides the character AI in the model.
- The third editor is the script editor, which historically served as the behavior editor for STAGE. Utilizing the script editor, the user could have entities in the simulation automatically react to the environment. This editor is often described as the legacy behavior model, but has proven to be a powerful supplement to the mission editor. As the script editor and the mission editor can run concurrently, the script editor is used to provide the weapons effects behavior. This logic runs independent of navigation logic, and has the entities in game decide when/how/where/why to shoot based on different logic criteria. This is beneficial when determining rules of engagement for each respective side. For example, an adversary entity may have two different weapons. One weapon may be for long range effectiveness and one weapon may be for short range effectiveness (such as a sidearm). There may also be different weapon preferences depending on whether an entity is shooting a vehicle or a human. Priorities may be based on how the scenario is progressing. At some point in the scenario it may no longer advantageous to shoot vehicles. The script editor allows the user to define the logic that takes into account moving/stationary conditions, human/vehicle differentiation, weapon target preference, scenario target priority, and also keep track of ammo. The ammo tracker is effective when rationing ammo; as the ammo count lowers, an entity can switch from a higher burst count to single shots.
- The fourth and fifth editors are the scenario editor and run time editor. These editors are the environment for setting up and running the scenarios, providing graphical displays (2D/3D), and showing the numerical data. Once all of the data is input in the first three data editors (database, mission, script), it is then assigned and organized in the scenario editor, then run in the run time environment editor.

All of the editors work together to create a modeling and simulation tool capable of simulating ground combat at a fidelity capable of reflecting DOE methodologies and principals.

One of the strongest aspects of STAGE is its logic based behavioral model (executed in the mission editor). This model consists of an if/then structure which, while fairly simple, is incredibly powerful. It contains both conditional checks and event based logic. Hundreds of behaviors and conditions are prebuilt in the model and can be implemented to create desired entity behaviors. The model's extreme flexibility provides the user with the ability to model a wide variety of behaviors. Behavioral choices range from basic behaviors such as navigation/locomotion, detection/sensing, and weapon deployment/operation to more complex behaviors such as communication, mission switching/adaptation, and defeat of physical protection barriers.

STAGE ships with an AI software package known as AI.implant. AI.implant is a commercially successful behavior modeling tool used in both the gaming and combat simulation industries. Its applications range from crowd modeling to traffic flow and even emergency response procedures. AI.implant integrates as additional features in the logic based behavior model, and functions as the STAGE scenario is running to provide basic levels of intelligence for entities. This capability allows the user to focus more on of the complex behaviors of the scenario and less on plotting the exact course of entities. Including vehicle behavior as well, as the user can utilize road networks to have vehicles behave in a manner conducive to site procedure. Reactions formed in the mission editor also dynamic, meaning that entities are constantly aware of their changing environments and can compensate to avoid new obstacles. These capabilities allow entities within STAGE to dynamically plan paths, recognize and avoid obstacles or harsh terrain, and stay on defined pathways such as roads or sidewalks. The ability to react with intelligent behaviors at the entity level is another example of the overall flexibility that STAGE has in modeling complex scenarios.

Perhaps the most flexible capability that STAGE employs is the mission editor and its behavior capabilities.



Type	Logical Oper.	Trigger	Oper.	Value	Action
AT		SELF EVENT	=	TRACK_NEXT	
	AND	Reason	=		
IF		Track Hostile	=	true	Opponent Assign Fr
	AND	Is Inside Building	=	true	START Engage_STO
	AND	Is Embarked	=	false	
	AND	Track In Area - ECP	=	true	
	OR	Track In Area - PTR	=	true	
ELSEIF		Track Hostile	=	true	Opponent Assign Fr
	AND	Is Inside Building	=	false	START Engage_STO
	AND	Is Embarked	=	false	
AT		EXTERN EVENT	=	Muster_E	Wait - Process and M
	AND	Reason	=		
	AND	From	=		
AT		EXTERN EVENT	=	Muster_W	Wait - Process and M
	AND	Reason	=		
	AND	From	=		
AT		ACTION ENDED	=	Wait	
	AND	Ending State	=	COMPLETED	
	AND	Reason	=	Process and Muster	

Figure 3. Logic based behavioral model

III. STAGE -- IMPLEMENTATION

Integrating the capabilities of STAGE with the VA methodologies used in DOE has proven to be an effective partnership between industry and Sandia's international work. Utilizing the principals of DOE Vulnerability Analysis methods, STAGE has supported Sandia's international and domestic analysis needs for various applications. These applications include analysis, training, demonstration, evaluation, and conceptual design.

Analysis: The genesis of STAGE for the International Nuclear Security Engineering group at Sandia was primarily physical security modeling and simulation for two unique programs; the Global-Critical Energy Infrastructure Protection (G-CEIP) program and the Material Protection Control and Accounting (MPC&A) program. Both programs have unique and diverse mission spaces that rely on a tool capable of meeting each respective program need. For example, the G-CEIP program deals primarily with critical infrastructure sites that have many high value assets that often have interdependencies. Defeat of a high value asset may only require partial destruction and, when coupled with another asset being incrementally damaged, could create a non-desirable effect. Additionally, at a city-sized critical infrastructure site, a threat may not be interested in only one target location but choose to have a list of primary assets to attack, and deviate their plan based on their unit strength. As their unit strength continues to decline, the adversary team is able to take stock of their strength and base their mission directives based on that information. As an adversary team, completing a primary critical event would require full team strength, a secondary critical event would require half team strength, and down the line of possible permutations. Conversely, a traditional nuclear site may require less complexity of adversary strategy, but may require more complex adversary insertion vectors. A physical protection system becomes much more stressed when dealing with multi vector attacks or more concerning diversionary attacks. The behavioral model in STAGE offers the flexibility to adapt a response posture based on the location and direction of an attack. This flexibility allows a site to evaluate the nuances of security response plans regardless of attack vector. The next section will discuss this further, but the applications of MC&A process flow is a current development area in STAGE. The ability to model material flow, material loss, and subsequently material theft can then be integrated with a site physical protection system.

Training: The International Nuclear Security Engineering group at Sandia has re-commissioned a former Category I special nuclear material facility. The Integrated Security Facility (ISF) at Sandia used to house nuclear material for the DOE/NNSA. In 2009, the Global Security Program at Sandia funded a re-fresh of critical technology components, and to date has updated numerous facilities, sensors, cameras, and security features into a mock facility. The ISF now operates training workshops, exercises, demonstrations, and testing for commercial technologies. Leveraging the capabilities of the ISF, STAGE is able to provide a training capability for physical protection. Students are able to design protection systems utilizing the ISF and implement/test their designs in STAGE. As their design fails/succeeds, the students are able to tweak components until they find the right balance of detection, delay, and response.

Demonstration: Much like training, the demonstration of best practices through modeling and simulation has proven to be a powerful capability when presenting to international partners. Successful integration of all components of a physical protection system does not always become apparent until the system is tested as a whole. Simulation provides the ability to test individual and integrated components efficiently and economically while deciding as a site is deciding how to implement upgrades, decide configuration, and implement best practices.

Evaluation and Conceptual Design: The concepts of evaluation and conception design are similar to sensitivity analysis in that additional variables are added to a physical protection system, but it also could be more of a stand-alone evaluation. As building/site designs are constructed, modeling their integration into the protection system can include many layers of complexity with regard to security. Questions during conceptual design include, for example, how does the building change the security posture and how does the design affect the response? Evaluating the new changes built into the existing facility can be achieved in simulation. A field exercise would be limited with such analysis as the notional facility has yet to be constructed.

IV. CONCLUSION AND NEXT STEPS

The strength and flexibility of STAGE are very beneficial to physical security. The traditional means of using simulation in DOE/NNSA has always been for neutralization analysis (combat analysis). Given a path, given scenarios of concern, how does the physical protection system hold up against a given threat? How does a system respond to the stressors and complexities of combat? This threat dynamic has become as complex a variable as anything else tested. STAGE helps the analysts and the trainers model these complexities.

Road maps for STAGE look to build on this success and continue into the next realm of security analysis. In addition to modeling the neutralization piece of System Effectiveness (PE), STAGE will fully integrate all components of a physical protection system. This will take into account path analysis variables (PD) and provide a single conclusive look at a system. This does not necessarily mean STAGE will find most vulnerable paths, but given a path(s) PD, values can be integrated to find a final PE value.

Also, the research that has been done on material processing is very promising. Various computational models exist that track the flow of material in an MC&A system. Integrating these models into physical protection system software that shows the flow as part of a bigger system remains the goal. Exploratory scenarios have been modeled to show insider activity with regard to material flow. As the insider is able to divert material, the software tracks discrepancies in the process flow. This activity is then reported to the main protection system. Preliminary results show the ability to integrate the two models and further work continues.

The STAGE program is only a small piece of a much larger, multi-faceted program at Sandia Labs in support of nonproliferation global security training. Part of the mission of the Nonproliferation and Cooperative Threat Reduction

Program is to develop exportable technologies and integrate commercial and custom technologies into security and safeguard systems around the world. This mission is leveraged with the Integrated Security Facility (ISF) currently being utilized at Sandia. The ISF is being used as a testing/evaluation/demonstration area that can be fully implemented in the STAGE software to provide physical security solutions in a setting that has historically served the nuclear weapon mission in DOE/NNSA.

In addition to being an industry tool available for our international partners, STAGE is also currently being used in military applications for flight combat and simulation training and analysis. The Department of Defense (DOD) programs at Sandia Labs are also currently using STAGE as a single analyst tool to complement their site security analysis, as well as other agencies within the sector that protect strategic assets around the world.

ACKNOWLEDGMENT

Special thanks to NNSA/NA-25. Special thanks to Dominic Martinez manager of International Nuclear Security Engineering, and Bill Rhodes manager of International Security Programs.

REFERENCES

[1] M.L Garcia, Vulnerability Assessment of Physical Protection Systems. Burlington, MA: Butterworth Heinemann is an imprint of Elsevier, 2006.

[2] F.A. Duran, D. Dominguez, M.J. Parks, and R.M. Ward, “Modeling and Simulation of Insider Adversary Scenarios” *Proceedings of the 53rd Annual Meeting of the Institute of Nuclear Materials Management,* Institute of Nuclear Materials Management, Orlando FL.