THE VULNERABILITY ASSESSMENT PROCESS APPLIED TO RADIOACTIVE WASTE TRANSPORTATION

J. G. Phillips
Y-12 National Security Complex
P.O. Box 2009, Oak Ridge, TN 37831-8287

ABSTRACT

Developing comprehensive Vulnerability Assessments (VA) of the protection elements afforded Category I and II nuclear materials during transport has long been a requirement. The VA methodology and computer simulation and modeling techniques are the same tools used for shipment scenarios, fixed sites, and materials under the normal states of process or storage. After identifying the need for a VA, current computer modeling and simulation techniques and a sound VA process should be applied to radioactive waste shipments. The modeling of protection elements in relation to the shipment process can be equated to a search for imperfections in which each concentric level of protection is placed into a computer model. The computer simulation provides the active portion of the analysis by reflecting the capabilities of prevention or mitigation of a malevolent act within a certain range of probability. World events have dictated the need for these questions to be answered. To expand the VA process to shipments of radioactive waste, determining the threats against the types of materials in transit would be first in a series of fault-tree-type decisions. Developing these answers and using computer technologies provides the method of analysis needed to ensure the safe transport of nuclear waste products.

INTRODUCTION

The methodologies for conducting VAs are well validated in the Department of Energy (DOE) system of Safeguards and Security—both for the evaluation of fixed sites and transportation activities. Providing the assurances of safe and secure shipments of radioactive waste is a primary concern of DOE and the Nuclear Regulatory Commission (NRC). However, rather than the DOE orders and manuals holding shippers of DOE nuclear waste materials to a standard, the shipper also complies with the regulations set forth by the NRC and those imposed by individual states. Providing assurances that radioactive waste shipments are conducted in a safe and secure manner is of utmost importance to involved shippers and the government agencies providing oversight. Therefore, the search for security-related vulnerabilities and determining the effects of a malevolent act against a shipment requires physical security analysis, dose-rate calculations, plume modeling, and computer-generated simulations, providing accurate representation of the shipments’ security posture.

Sabotage of Radioactive Waste Shipments

When evaluating the VA process and shipment security, only sabotage threats against waste shipments can be deemed credible because of the attractiveness and category of materials in transport. The Vulnerability of Integrated Security Analysis (VISA)a tabletop methodology for evaluating the shipment process is widely used within the DOE complex for site intra-area shipments that require analysis, but it can easily be adapted to domestic radioactive waste movements (Reference 1). In addition to the VISA tabletop methodology, a method is needed to determine the results of a sabotage attack on a shipment and to determine if a terrorist group can be defeated before executing a malevolent act. Having an integrated system for conducting a transportation VA is essential to provide assurances that acceptable levels of system effectiveness are attained for each type of shipment.

The VISA methodology, or an acceptable variation thereof, will provide the basis for analysis by deciding worst-case scenarios, evaluations of terrorist task times, and police response times. A determination of adversary neutralization probabilities is commonly portrayed within DOE by use of the Joint Conflict and Tactical Simulation (JCATS)[b] program (Reference 2). The JCATS program also is used in other simulations of transportation activities within DOE. In addition to the analysis associated with the adequacy of physical security measures is the evaluation of radiological releases into the atmosphere caused by a malevolent act. One accepted program with the DOE Complex is the Hotspot Gaussian Plume model that provides accurate and timely short-term exposure data for the kind of releases expected during a terrorist attack[c].

Combining these three methods of evaluation can provide reasonable assurance and documented analysis of the viability of shipment protection elements. Ensuring that the analysis can be cost-effective is achieved through the bounding of like targets. This enables the analyst to combine targets by radioisotopes, curie-activity levels, and demographics of transport routes and conduct one bounding analysis rather than conducting numerous, time-consuming evaluations of individual material shipments.

The Physical Security VA Process

The physical security vulnerability assessment process is, in essence, a search for weaknesses in a facility or process. As weaknesses or vulnerabilities are identified, security upgrades are identified to mitigate the weak points in the system. As this process is applied to the transportation of nuclear or radioactive waste, the parameters of the evaluations must be set to apply appropriate and cost-effective security measures in the protection of target material.

As targets of interest change between fixed sites to transportation scenarios, the basis for the VA remains the same. There are essentially six steps that may be applied to the VA process, based on accepted DOE methodologies (Fig. 1). The primary and most commonly used methodology, which has the broadest application across the spectrum of targets, is VISA. This process can be readily applied to the transportation process and can provide quantitative risk- and system-effectiveness ratings for given shipments.

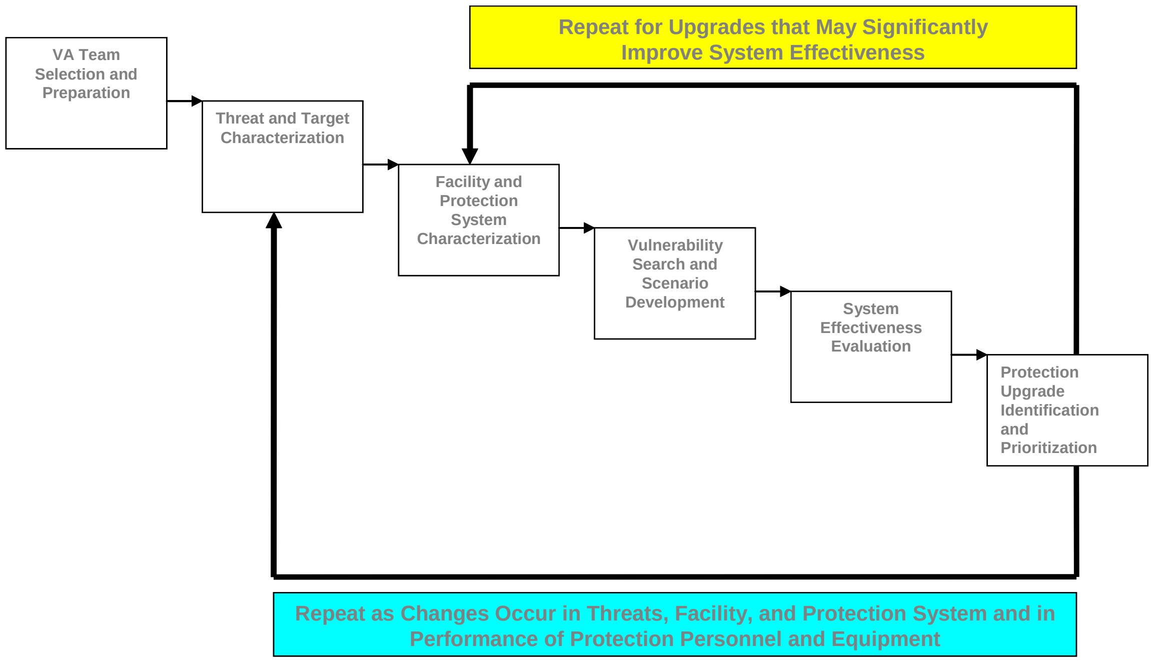

Fig. 1. VISA methodology flow chart

VA Process for Transportation Scenarios

Forming the VA Team – The VA Team is made up of personnel who have extensive and wide-ranging expertise in security and transportation operations. Usually, the VA Team leader has had experience in conducting vulnerability assessments. Other team members have knowledge of shipment security, protective force and police operations, waste management shipment procedures, and DOE and NRC transportation regulations and orders.

Threat and Target Characterization – During this phase of the Transportation VA, the threat is evaluated based on the type and description of acts and information pertaining to the number, tactics, and motivation of the adversaries. The target(s) are characterized based on the type of radioactive material, shipment routes and locations, and the type of threat or act against the target. During the threat analysis, several sources of information are considered: the U.S. Government-formed Design Basis Threat, local threat assessments, and an evaluation of historical threats may be used. The type of adversary is evaluated based on motivation, numbers, capabilities, tactics, equipment, and extent of insider information regarding facility and target operations. All targets for a given type of shipment should be identified and prioritized based on susceptibility to sabotage and the demographics affected. During this target characterization, the target or material is evaluated based on the attractiveness as a sabotage target, including the shipment routes and areas that would be affected during a malevolent act.

Transportation and Protection System Characterization – The next phase of the VA is to characterize, or fully describe, the type of shipment and the security and escort protection measures in place. This activity provides the "base case" for the VA. To fully identify the attributes of the shipment process, the VA Team must evaluate the routes and population areas involved in the shipment. Transportation procedures should be reviewed with attention to safe havens, environmental responses, and other similar transportation operations. Identification of the security afforded a shipment will provide the basis for the initial or base-case analysis in the VA. Security evaluation should consider the overall protection strategy, access control to the vehicle and contents, security tracking systems and reliability, police procedures, secondary response force procedures and response times, and human reliability programs.

Vulnerability Search and Scenario Development – Based on the previous activities during the preparation phases of the VA process, adequate information pertaining to the transport, police operations, and critical target locations should be primary concerns of the VA Team. Because the team is familiar with the shipment and its operations, the search for vulnerabilities, and the development of scenarios will be conducted in a team setting. The team must consider the type of attack that will be evaluated and the type of adversary based on credible scenarios. The expert judgment of the VA Team and computer analysis should be used to identify vulnerabilities in the transportation system.

The VA Team will consider the scenario and the vulnerabilities of the shipment during the same phase and not view the process as dependent on conducting the search for vulnerabilities a required step before scenario development. Again, based on expert judgment and computer analysis, the VA Team will postulate the worst-case attack scenario against the shipment material in the worst location as simulate the greatest number of causalities.

System Effectiveness Evaluation – System Effectiveness Evaluation is the analysis phase of the VA process. The VA Team will evaluate the shipment's security posture against an identified threat. During this process, the team will evaluate four major areas associated with the facility's protection elements: Probability of Detection, Probability of Assessment, Probability of Interruption, and Probability of Neutralization. Correct evaluation of these four areas will provide the VA Team with a system-effectiveness rating, which will ultimately provide a manager with a risk rating for each analyzed target.

Protection Upgrade Identification – As vulnerabilities are identified during the evaluation of the shipment process, mitigating or compensatory protection measures are recommended to improve the shipment system effectiveness against a malevolent event. As system effectiveness improves, the risk to the shipment, the public, and the environment is lowered. For example, if a shipment is determined to be vulnerable to an attack while traveling through a highly populated area, additional police responders and added surveillance could be added to mitigate that vulnerability.

Consequence of Loss

The consequence of loss, or consequence value, is a factor in determining the level of risk associated with an explosive release of radioactive material. In general, DOE currently relies on a system-effectiveness method of quantitative ratings regarding the risk associated with a certain target, however, some agencies use a risk-based equation. Regardless of the method of risk rating, the capability to determine the extent of a radiological release will drive the extent of safeguards applied to an individual shipment or a category of shipments. Not every radioactive waste shipment would require analysis. Those shipments of highly radioactive substances deemed attractive targets for sabotage, should be evaluated not only regarding the release at the possible site of attack, but it should also include an assessment of the psychological impacts of smaller releases resulting from a malevolent event.

Computer Simulation Programs

In the late 1970s, the Lawrence Livermore National Laboratory provided a combat simulation program to the Department of Defense to meet simulation and combat analysis needs and to make both logistical and neutralization/loss predictions associated with armed conflict. The early predecessors to the JCATS system laid the groundwork for simulation technologies of today. These state-of-the-art combat simulation systems that have been used in operations in Panama, Somalia, Bosnia, Operation Desert Storm, and, most certainly, in the current war in Iraq.

In 2002 the JCATS program was introduced to the Y-12 National Security Complex, performing probability of neutralization evaluations in the Site Safeguards and Security Plan (SSSP) process. This program replaced the Joint Tactical Simulation (JTS), which was introduced during the early and mid 1990s at various DOE facilities (Reference 4). JCATS is a computer-assisted simulation system developed to exercise commanders and their staff in the command and control of combined arms operations in urban terrain environments. JCATS is currently in use by DOE and the National Nuclear Security Administration (NNSA) as a tool for validation of vulnerability assessments within the Complex.

The JCATS combat system represents teams of personnel as ground and air mobile platforms equipped with direct and indirect fire capabilities. The program can readily simulate terrorist attacks on shipments of radioactive materials. Some of the key functions of the JCATS system are to provide individually controlled combat activities in and around detailed buildings, terrain, and urban areas as well as movement of vehicles and small tactical units, including mounting and dismounting vehicles. Buildings and building interiors can be modeled, portraying exact floor plans for numerous floors. The doors and windows are defined to accurately reflect the kind of construction and the delay each feature may pose to specific breeching tools. Individual soldiers or police officers can be directed into buildings and can engage adversaries as dictated by the scenario being evaluated. JCATS uses event data, such as sensor acquisitions, direct-fire engagements, and movement orders that allow near-real-time analysis of simulation, field exercise data and scenario, and response-force neutralization validation (Reference 4). An analyst can examine this information to help develop realistic, detailed operational plans (Fig. 2).

Other than neutralization probability and responder analysis, the advantage to transportation scenarios is the capability to simulate lethal plume models by obtaining data through radiological release software and then simulating casualties to first responders and law enforcement through the JCATS model. The lethal effects reflected in the internal Gaussian Plume model can significantly alter the outcome of neutralization probabilities through the attrition of law enforcement defenders and secondary responders. Available weather and atmospheric data can be entered into the system to provide analysis of worst-case scenarios.

Actual weapon capabilities are found within the JCATS simulation models and accurately portray the capabilities of certain weapons. The Probability of Hit/Probability of Kill (PH/PK) tables provide detailed information regarding the kind of weapon and ammunition needed to stop a vehicle. The information contained in the current JCATS program is reliable enough to provide probability data accurate enough that DOE can base risk ratings on the results of simulations.

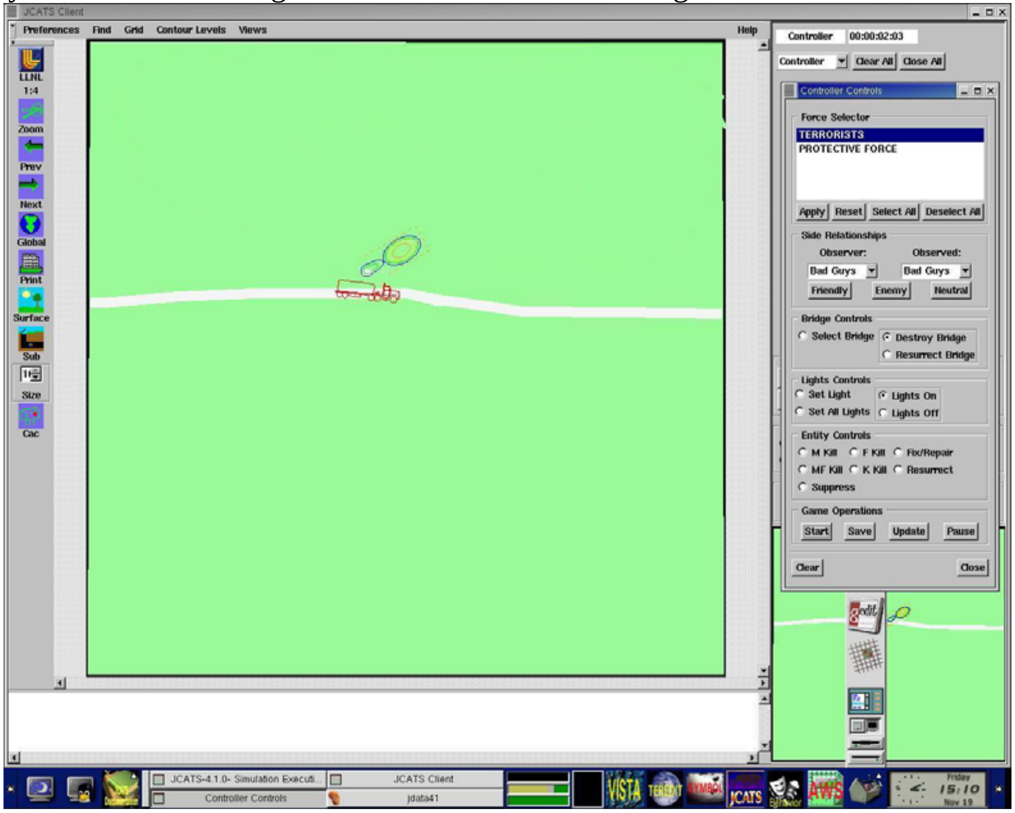

Fig. 2. Screen depiction of JCATS simulation

Hotspot Gaussian Plume Model

The Hotspot health physics codes were developed to provide personnel in the field with a quick, reliable method to evaluate radiological releases and the associated effects on humans. The Hotspot codes are designed for evaluations of short-term release durations but would not be the most useful program available for complicated terrain features and weather data. The four major programs within the Hotspot code are the plume, explosion, fuel fire, and the area-contamination events (Fig. 3).

The main interest for the VA analyst lies within the area of explosive releases. During the VA process, environmental accidents are not considered. The Hotspot codes are capable of providing reasonably accurate, timely information about an explosive release of a radioactive material, which provides valuable data regarding the consequence of loss of a shipment.

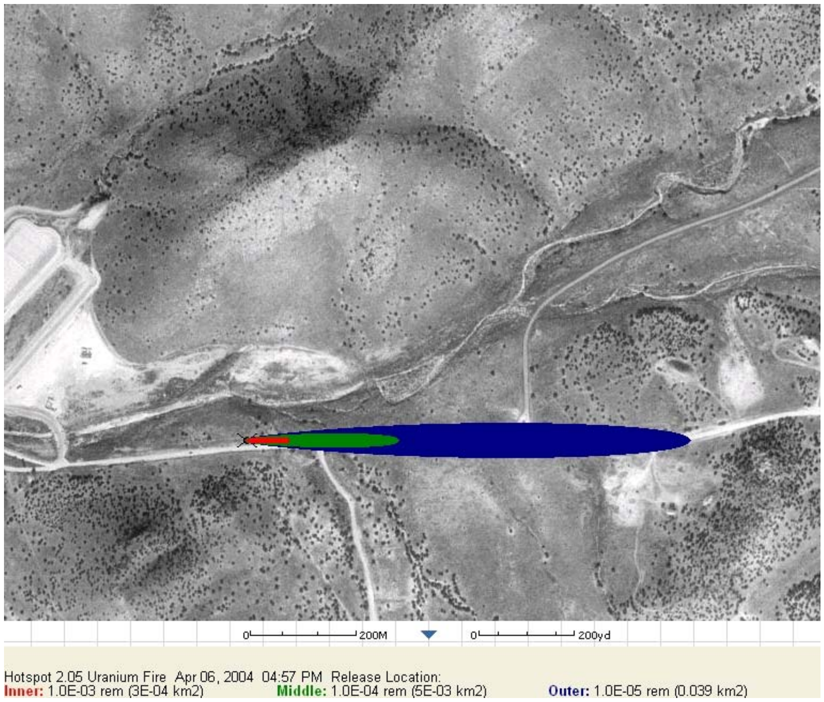

Fig. 3. Hotspot Gaussian Plume

New Simulation Programs

Simulation programs within the DOE arena provide tools to assist in the analytical process. While these tools have progressed to containing highly reliable sets of data, the depiction of the analysis continues to provide a less-than-desirable picture of the analysis and subsequent results. The JCATS system, which provides the analysis in real-time, is set up in a two-dimensional (2-D) format. Having the correct computational science of the analysis is a requirement that cannot be compromised. However, a simulation that is aesthetically pleasing to the viewer and can be developed to incorporate the physical attributes of buildings, vehicles, and terrain with the properties that provide accurate representation of the actual environment, would be considered a breakthrough technology.

The ADEPT program is a 3-D interactive simulation model that replicates terrain, facility characteristics, weapon attributes, police, and terrorist groups to create a real-time user-interactive platform (Fig. 4). ADEPT was developed by a commercial company and continues to be upgraded. DOE has provided preliminary funding for the further evaluation of the ADEPT program. This product of the gaming industry holds promise of being a tool that can first be used as an interactive training tool, and, through subsequent improvements and testing, may be used as a tool in the analysis phase of the VA process.

Fig. 4. ADEPT – screen view (building/terrain/vehicle)

ADEPT uses the basic concepts of the commercial gaming industry. It incorporates 3-D imagery but will eventually allow analysis of real-world information to be displayed during operational, industrial, and tactical emergency situations to allow entities to respond and take appropriate measures to mitigate the incident stimulus. Currently, the ADEPT program is being evaluated at the Y-12 National Security Complex (along with other DOE site participation) to develop the system as a training platform for protective force personnel and then as an analytical program to be used in the VA process[d].

Partnerships between Government and Industry

Further development of analytical tools for use in the VA process is expected in the coming years. Agreements between government agencies, such as the U.S. Air Force Research Laboratory and DOE, will enhance the capabilities of both agencies to develop computer-simulation and modeling programs beneficial in improving the quality of analysis and lowering cost. DOE also is cognizant of the contribution of commercial and small businesses in developing programs that are useful in the VA analytical process. Many of the current programs being considered for future use within DOE are the products of commercial off-the-shelf software that, with some modification, can easily fit the needs in the VA process. Some of these new programs have been developed through agreements, such as the Small Business Innovation Research program, and agreements reached through the commercialization of products also should be promoted.

CONCLUSION

The need for a comprehensive and quantitative vulnerability analysis of radioactive waste shipments has become even more important because of recent world events. As the threat of terrorism increases for domestic cross-country shipments, the need is great to provide better assessment and computer-simulation models for analysis. The application of a vulnerability assessment methodology is essential to ensure accurate risk- and system-effectiveness ratings that provide a true representation to those responsible for these shipments. By applying the three parts of the transportation analysis (the VA Process, model of radioactive releases, and the response and neutralization computer simulation), the responsible contractor or agency can assign a risk rating to individual shipments or types of shipments. Risk is an inherent part of the shipment process, however; the acceptance of risk must be based on adequate, accurate information (Reference 5).

Using computer modeling and simulations in the VA process is not new in the DOE arena. As technologies continue improve in the commercial sector, applying these new programs and methods of computer-generated models for the analysis of transportation scenarios within the government agencies will require testing and validation. The aesthetically pleasing depiction of a transportation scenario cannot exist without the science to back up and support the analysis. DOE is currently looking toward small and corporate businesses for state-of-the-art computer programs that will assist in all aspects of nuclear safeguards and security. As we move toward replacing antiquated computer simulation and modeling programs within the government, we must ensure the quality and reliability of these new technologies.

REFERENCES

1. "*Vulnerability Analysis Process for Protection Against Design-Bases Threats*," L. Harris Jr. and L. Goldman, SAIC, San Diego, California.
2. "*JCATS System Managers Guide*," 2003, T. Peck, Lawrence Livermore National Laboratory.
3. "*JTS System Managers Guide*," January 1997, T. Peck, Lawrence Livermore National Laboratory.
4. S&TR January/February 2000, "*Simulating Warfare Is No Video Game*," A. Heller.
5. "Nuclear Waste Transportation Security and Safety Issues," October 1997, Robert Halstead, Transportation Consultant, J. Ballard, Grand Valley State University, Grand Rapids, Michigan.

FOOTNOTES

[a] **VISA** – *Vulnerability of Integrated Security Analysis*; resulted from a 1976 nationwide competition to develop a standard VA method to be used at U.S.–licensed nuclear facilities. The VISA method was first presented at the 1977 Institute of Nuclear Materials Management (INMM) annual meeting by SAIC. This VA methodology was applied to high-risk government facilities. Through the years, the method was refined, and the six-step process again was presented to the INMM annual meeting in 1992.

[b] **JCATS** – *Joint Conflict and Tactical Simulation*; is a computer-assisted simulation system developed to exercise commanders and their staff in the command and control of combined arms operations in urban terrain environments. JCATS is currently in use by the U.S. Department of Energy and the National Nuclear Security Administration (NNSA) as a tool for validation of vulnerability assessments within the DOE Complex.

---

[c] Other codes typically used within the government arena include, but are not limited to, Radiological Assessment System for Consequence Analysis (RASCAL) and Atmospheric Release Advisory Capability (ARAC).

[d] The development of the ADEPT program as an analytical tool for the VA process is an initiative that will require extensive study and evaluation. ADEPT could provide a very realistic depiction of the adversary neutralization process if its databases could be brought up to the current level found in JCATS and if the engine and algorithms can be improved to process the extraordinary amount of information required in DOE-scenario evaluation.