

DOMESTIC RADIOLOGICAL SOURCE TRANSPORTATION ASSESSMENT

Ken Martin
Oak Ridge National Laboratory
Oak Ridge, TN

Mike Skinner
Oak Ridge National Laboratory
Oak Ridge, TN

J.R. Martin
Oak Ridge National Laboratory
Oak Ridge, TN

ABSTRACT

An assessment will be conducted of the radiological source transports and provide a qualitative evaluation of the effectiveness of the transportation security approaches that are in place today. The assessment will evaluate detection, assessment, delay, and response. The transportation security effectiveness will be evaluated against a predetermined adversary threat with specific capabilities and attributes. The adversary set will include colluding insiders and outsiders. Insiders acting alone will be evaluated in a standalone assessment. The assessment will be based on laws and regulations that govern the transportation of radioactive sources. The assessment will establish a baseline through the review of applicable laws and regulations, interviews of key players in the transportation and end users of radiological sources, and consideration of the routes commonly used.

Based on the results of the baseline assessment, an upgrade case may be required. An upgrade case may be completed by layering on prudent cost-effective measures that will address vulnerabilities or weaknesses, should any be identified. The upgrades may be regulatory based, procedurally based, physical protection measures, response, training, cyber, and other related strategies to improve transport security to an improved and/or acceptable level of system effectiveness.

* Notice: This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (<http://energy.gov/downloads/doe-public-access-plan>).

INTRODUCTION

The security risk assessment technical standard developed by the US Department of Energy (DOE) provides a description of a departmentally approved physical protection system (PPS) security risk assessment (SRA) methodology. This process is a qualitative risk-based security assessment methodology to determine relative ratings representing risk to various DOE assets. The process incorporates an evaluation of threats, consequences of loss or damage, and protective system effectiveness. The SRA is designed for use in determining system effectiveness and relative risk when a formal vulnerability assessment is not required. This assessment will identify system effectiveness.

Although performance test data is preferred, in the absence of analysis or performance data, subject matter expert (SME) opinion, accompanied by a rationale, can be used to complete the analysis. As outlined in DOE Order 470.4B, *Safeguards and Security Program*, security planning should incorporate a risk-based approach to protecting department assets and activities, and this process is intended to be used to meet that requirement.

When departmental or national security requirements exist, an SRA can be used to understand PPS effectiveness and/or residual security risk to the assets. When departmental or national security requirements do not exist, an SRA can be used to understand PPS effectiveness and/or residual security risk to the assets and to aid in the determination of baseline protection requirements defined by the officially designated facility security authority.

METHODOLOGY USED TO ASSESS SYSTEM EFFECTIVENESS

The methodology used to assess system effectiveness is applied in a logical, sequenced fashion that considers the threat, target identification, adversary types, malevolent acts of concern, and consequences of a successful malevolent act.

There are several DOE-approved analytical tools used to assess protection of radiological material. The Vulnerability of Integrated Security Analysis (VISA) process is a qualitative vulnerability assessment tool used by DOE to evaluate safeguards and security systems against postulated design basis threats. It has also been applied to public and private sector analyses. The VISA process involves facilitated discussions between SMEs as well as recording of decisions made during those discussions. The product of a VISA analysis is a subjective matrix that identifies adjectival ratings for security system performance in areas of adversary detection, assessment, interruption, and neutralization. From this matrix, a numerical system-effectiveness score is determined that can be used to calculate proliferation risk.

The VISA method is a tabletop analysis technique used to analyze system effectiveness. It is step-dependent, meaning that developed scenarios, including the identified paths the adversaries take, are broken down into individual steps, evaluated as to the probabilities of detection, assessment, interruption, and neutralization (as assigned by the team), and then scored.

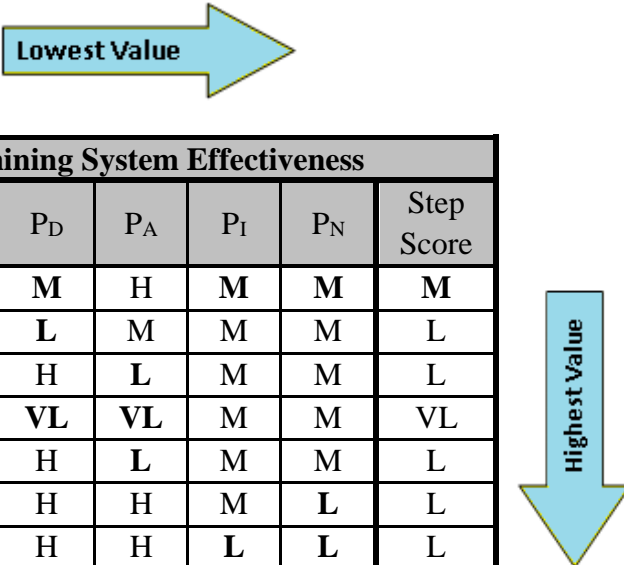
The VISA process is particularly useful in performing assessments of facilities about which little is known or to develop further information requirements about a facility before applying a quantitative analysis approach.

Other systems analysis methods, such as the Analytical System and Software for Evaluating Safeguards and Security (ASSESS) can be applied to the analytical process with similar results.

However, methods like ASSESS are not as interactive or as illustrative of security system effectiveness results as VISA. The VISA method provides a forum for group discussion not generally found in computer-assisted modeling; however, it is based on the knowledge and experience of multiple SMEs versus hard computer data.

Adjectival Ratings Used to Estimate the Probability of System Effectiveness

In establishing the probabilities of detection (P_D), assessment (P_A), interruption (P_I), neutralization (P_N), and system effectiveness (P_E), five adjectival ratings are assigned. These adjectival ratings are very low (VL), low (L), moderate (M), high (H), and very high (VH). Figure 1 illustrates a method used to determine system effectiveness.



Example Table for Determining System Effectiveness						
Step No.	Step Description	P_D	P_A	P_I	P_N	Step Score
1	Enter Site Perimeter	M	H	M	M	M
2	Enter Building	L	M	M	M	L
3	Enter Target Location	H	L	M	M	L
4	Acquire Material	VL	VL	M	M	VL
5	Exit Target Location	H	L	M	M	L
6	Exit Building	H	H	M	L	L
7	Exit Site Perimeter	H	H	L	L	L
System Effectiveness - P_E :						M

Figure 1. VISA Table Example

Probability of Detection (P_D). P_D is the ability to observe and report information about an area of responsibility by physical or mechanical means. Examples of detection are security personnel

observation, optics (day or night), and sensors (i.e., infrared or vibration). The P_D is step dependent.

Probability of Assessment (P_A). P_A is the ability to correctly determine and report that an illicit activity is occurring. Examples of assessment are security staff or closed-circuit television reporting to an alarm station. The P_A is step dependent.

Probability of Interruption (P_I). P_I is the ability of the security force to appropriately respond in time to engage an adversary. The P_I is timeline dependent.

Probability of Neutralization (P_N). P_N is the ability of the security force to deploy in sufficient force to stop the adversarial action. The P_N is scenario dependent.

System Effectiveness (P_E). P_E shows the effectiveness of the protection system and its components. Each layer or step is assigned a step score by taking the lowest element value (bold text in Figure 1) for that step. Once each step has been analyzed and the step score identified for each step, the highest step score (bold text in Figure 1) for the scenario is then identified as the system effectiveness value for that scenario.

Table 1 gives an example of how numerical values could be assigned to each adjectival rating. There are any number of variations for numerical values that could be assigned; however, those given in Table 1 demonstrate a typical example.

Table 1. Adjectival Values

Adjectival Rating	Numeric Range	Midpoint
Very Low	.01 to .2	.1
Low	.21 to .4	.3
Moderate	.41 to .6	.5
High	.61 to .8	.7
Very High	.81 to 1	.9

SCOPE OF A SECURITY RISK ASSESSMENT

The first step is to develop the scope of the assessment and identify the team members who will participate and support the analysis. The analysts will also develop the assessment parameters. In this case, they will identify where the radiological source transport process begins and ends.

They will determine how they will divide this process into logical portions for analysis purposes. When conducting an assessment of effectiveness of safeguards and security systems at a DOE facility, analysts normally evaluate the status of the PPS to identify differences in the facility state from a security and operational standpoint. For example, they might evaluate the day-shift PPS configuration as one state, and the second state would cover nights, weekends, and holidays

if all three were equivalent from a security and operational standpoint. Transportation is a little different. In that case, for instance, the analysts might set up three states of material configuration. The source movement from the facility to the shipping container could be identified as the first configuration, then look at the material in transit between the point of origin to its destination as a second configuration, and evaluate the shipment being stationary at a safe haven as the third and last configuration. From a security and operational standpoint, the three options are all different. Yet another variable is whether the material is moving from a manufacturer to the end user or whether the material is moving from the end user to a secure source storage facility. The shipping container may be carried into the hospital or university and the source packaged in the container at the end user location, or the source may be carried outside the end user location and packaged in the container in a predetermined secure staging area.

DATA COLLECTION

One of the most important portions of the system effectiveness analysis process is data collection. The analysts can be told how this material movement occurs, but the best way to gather that data is for the analysts to witness the process themselves. When operators are describing a process, they may only hit the highlights or assume a step is irrelevant to the analysis process and not pass it on to the analysts. Oftentimes it is routine to them because they have “lived it” many, many times, and they assume “everybody knows it” because it is routine.

Through site visits; document reviews; and interviews with shipment participants such as the drivers, operators, security personnel, material custodians, local law enforcement, and source removal vendors, the analysts will develop a baseline security configuration that they use to develop their base case analysis. In some cases, no matter how hard analysts try, though, there will be some data that they just cannot define. In this situation, they have to develop assumptions that assist them in defining the analysis parameters. Whenever possible, delay times should be based on actual times that are identified through performance testing. In some cases, due to cost and availability, it is not possible to do explosive breach performance testing, for example. In instances such as this, analysts may go to explosives experts who can take drawings of delay barriers and have them calculate the breach time to establish a realistic time for use in the timeline. In other cases, such as mechanical breaching using power tools to remove bolted barriers, performance testing can be repeated time and again to develop the best breaching methods.

Target Identification

Analysts have to identify and rank the targets as one aspect of data collection. They have to determine if they are evaluating the targets for theft and sabotage (dispersal/exposure). The security posture should be layered on a graded approach. The more valuable the target, the higher the security should be. A full-up nuclear weapon should not be protected in the same way as would Category IV special nuclear materials or vice versa. The same is true for radiological sources. A radiological source that poses no long-term effects to the environment or society should not be protected to the same level of security as a radiological source that poses grave danger to the environment and/or society. To apply graded security to radiological sources, analysts have to rank them. The sources have to be analyzed to determine what the dispersible dose would be for each one. They also have to be analyzed from an exposure standpoint.

Analysts could evaluate each source based on (1) its shipping container limits, (2) its category level, (3) the largest source being shipped, or (4) all three options. A country's design basis threat (DBT) may also provide limitations that could affect the dispersion analysis and apply limits on how much of an isotope can be dispersed at one time.

Threat Identification

As part of the data collection, analysts also have to determine the threat they are protecting against. Are they analyzing both insider and outsider adversary threats as well as colluding? In most cases, a DBT has been developed by a competent authority in collaboration with others based on a credible threat assessment. As outlined by the International Atomic Energy Agency and practiced by many countries worldwide, the DBT is based on a national threat assessment. The threat assessment should be based on a classified, multiagency intelligence community assessment of potential terrorist threats within their own country as well as worldwide. The DBT should outline the motivation, intent, strategies, and capabilities of the threat. Analysts need to know the size of the group, weapons, tools, skills, training, as well as funding and transportation. From an insider standpoint, they need to know their access, authority, and knowledge base. Insider threats present a unique problem for a PPS. Insiders could take advantage of their access rights, complemented by their authority and knowledge of a process, to bypass dedicated physical protection elements or other provisions such as operating measures and procedures. Further, as personnel with access in positions of trust, insiders can carry out "defeat" methods not available to outsiders when confronted with protection elements and access controls. Insiders have more opportunities to select the most vulnerable target and the best time to execute the malicious act. To identify the worst-case insiders, analysts must evaluate their access, authority, and knowledge.

TYPES OF INSIDER AND OUTSIDER THREATS

Below are a few examples of insider and outsider types, including explanations of the differences between an insider and an outsider. Analysts have to identify and define each threat type and break down the adversary type by motivation, intention, and capabilities.

Insider Threat

An insider can be anyone who has routine authorized access to the facility, including a visitor who has access to the facility. This is critical when defining the insider attributes such as access, authority, and knowledge. A visitor will not have the in-depth knowledge of the layout of the facility, where the targets are located on the site or in the building, access to floor plans, or other knowledge that would be critical to aiding an outside adversary team in developing an attack plan on a facility. If the insider is acting alone with no outside adversary support, he/she would have to have knowledge of the facility, the process, and the security to have a chance of being successful in accomplishing his/her mission. In general, there are three types of insiders: (1) passive, (2) active nonviolent, and (3) active violent. These insiders can act alone or in collusion with outsiders. The three insider types are defined as follows:

- **Passive Insider.** A passive insider will only provide information to an outside adversary group to assist in accomplishing its goal. The Passive insider does not participate in

any other way. The Passive insider acting alone is not considered a theft or sabotage threat.

- **Active Nonviolent Insider.** The active nonviolent insider is a person who is knowledgeable of the site operations and has authorized, unescorted access to critical parts of the site. The active nonviolent insider is covert and motivated by revenge, prospect of profit, or blackmail. Acting alone, this insider is active and nonviolent (not willing to kill or be killed) and requires anonymity and secrecy to complete the task(s). Being “active,” the insider may disable or ignore select PPS measures designed to detect or delay his/her actions. Because he/she is nonviolent, upon detection and assessment of unauthorized activity, the insider will surrender. The active nonviolent insider will commit acts of sabotage against equipment (e.g., turn off critical valves; drain oil from generators, engines, transformers, or other devices to disable or destroy equipment he/she will not use flammables or other incendiary devices to destroy assets).
- **Active Violent Insider.** The active violent insider differs from the active nonviolent insider only in that he/she does not require anonymity, will use force against personnel, and is willing to kill in order to complete the mission. The active violent insider will commit violent acts of sabotage and will use flammables and weapons to destroy assets without regard to the well-being of others.

The data in Table 2 allows an analyst to rank the threats posed by different insider types to determine who has the most access, authority, and knowledge.

Table 2. Insider Access, Authority, and Knowledge

		Operator	Operations Supervisor	Security	Control Room Tracking	Driver	Driver Supervisor	Receiver	Local Law Enforcement	Outside Oversight	Freight Forwarders
ACCESS	Hands-On Access in Loading	X						X			
	Hands-On Access in Transit					X					X
AUTHORITY	Tamper Indicating Devices	X									
	Authorizes Source Transfers		X								
	Writes Security Plan			X							
	Briefs Drivers on Security Plan			X							
	Identifies Routes & Alternates			X							
	Tracks Shipment				X						
	Measurement Verification										
	Packs Shipping Container	X									
	Receives Shipping Container							X			
	Directs People w/ Hands-On Access		X				X				
KNOWLEDGE	Routes and Alternate Routes			X	X	X			X	X	
	Operational Activities	X	X	X							
	Tamper Indicating Devices	X	X	X							
	Shipment Schedule			X	X	X	X		X	X	X
	Access to Security Plan			X	X	X					X
	Shipment Configuration	X	X	X		X		X			X

Note: This is only an example. There may be numerous insiders and many different attributes.

Outsider Threat

Terrorists and criminals are the most common examples of outsider threat types. Analysts would not expect criminals that are conducting an attack for monetary gain to be as well organized, trained, or equipped from a weapon and explosives standpoint or as large in number as an international terrorist group. The type of outsider threat will be defined based on intelligence regarding a local threat as well as intelligence from state and international standpoints. The DBT should be the minimum level that an agency protects against. If through a local or regional threat it is determined that the adversary attributes are higher, the agency or facility should document this threat as justification to raise the threat level for a particular adversary or threat. Outsider adversary groups differ in their motives, capabilities, and size. It should be assumed for any outsider threat that the outsiders have received site-specific information from an insider. Four examples of outsider threat types are (1) international terrorist, (2) domestic terrorist, (3) criminal, and (4) activist. The definition of each follows:

- ***International Terrorist.*** The international terrorist may have full knowledge about the facility that he/she is attacking, including knowledge regarding response procedures (gained from an insider through collusion). He/she may be armed with handguns, rifles, automatic weapons, and light antitank weapons. He/she may be equipped with hand and power tools, bulk explosives, bridging equipment, incapacitating agents, and ground transportation vehicles. It should be assumed that this attacker is dedicated and well-trained in military tactics and skills and is willing to die and/or to kill to be successful. He/she would consider attacking during normal working hours to take advantage of removed delay elements (such as doors left open or tie-downs removed) and intrusion detection sensors being in the “access” mode (turned off). This attacker would also consider attacking during the transportation of nuclear materials between various protected areas and could be capable of diversionary tactics.
- ***Domestic Terrorist.*** The domestic terrorist’s primary motivation is to make a political statement and/or retaliate against the government. He/she will have full knowledge about the facility that he/she is attacking, including information regarding response procedures (through information provided by the insider). This attacker may be armed with handguns, rifles, automatic weapons, and commercially available explosives. He/she may be equipped with hand and power tools, bulk explosives, bridging equipment, and ground transportation vehicles. It should be assumed that this person is dedicated and well-trained in military tactics and skills and is willing to die and/or kill to be successful. He/she would consider attacking during normal working hours if it was to his/her advantage.
- ***Criminals.*** The criminal’s motive is theft for financial gain, and he/she will target high-economic-value assets. He/she will have full knowledge of the facility (through information provided by the insider). He/she may be armed with handguns, rifles, and automatic weapons. This attacker may be equipped with hand tools, power tools, and ground transportation vehicles. It should be assumed that he/she is dedicated and trained in tactics. He/she will avoid confrontation but revert to violence to keep from being captured. This attacker would consider attacking during normal working hours if it was to his/her advantage.

- **Activist.** The activist's motive/goal is to make a political statement through protest and civil disobedience. He/she will target facilities with political or environmental significance to acquire local and/or national attention. He/she may have hand tools, flammables, chains, and clubs. It should be assumed that this attacker is dedicated and willing to cause damage to assets located on site to gain attention; however, he/she is unwilling to kill or die for his/her cause.

SCENARIO DEVELOPMENT

After identifying and ranking the targets and defining the threat, analysts have to develop scenarios. The data that has been collected, along with the DBT, is used to develop realistic insider and outsider scenarios taking into account the insider's capability to mask or ignore security and/or operational systems, the route to be taken, state restrictions/laws, and regulatory limitations to include local or regional threats along a specific route.

BASE CASE ANALYSIS

Based on the material type, the PPS configuration, and threat that has been identified, analysts will then conduct an assessment of the baseline configuration and provide a qualitative evaluation of the effectiveness of the transportation security approaches that are in place. This is accomplished by evaluation of the detection, assessment, delay, and response associated with the material being assessed. The transportation security effectiveness is evaluated against a predetermined adversary threat with specific adversary capabilities and attributes. The adversary set includes colluding insiders and outsiders. Insiders acting alone are evaluated in a standalone assessment of the identified worst-case insiders. The assessment is based on laws and regulations that govern the transportation of radioactive sources. The assessment establishes a baseline through the review of applicable laws and regulations, interviews with key players in the transportation and end users of radiological sources, and consideration of the routes commonly used.

UPGRADE CASE ANALYSIS

Based on the results of the baseline assessment, an upgrade case may be needed. If an upgrade case is needed, it will be completed by layering on prudent cost-effective measures that address vulnerabilities or associated weaknesses identified in the base case analysis. The upgrades may be based on regulations, procedures, physical protection measures, response capabilities, training, cyber, and other related strategies to improve transport security to an acceptable level of system effectiveness.

CONCLUSION

The results of the base case analysis will only be as good as the data gathered. In order to have graded security, targets must be ranked based on consequence. Using the DBT ensures a balance across an agency and supports cost benefit versus consequence.

REFERENCES

- US Department of Energy Order, DOE O 470.4B, *Safeguards and Security Program*, 2011
- US Department of Energy Order, DOE O 470.3C, *(U) Design Basis Threat (DBT)*, 2016

**Proceedings of the 19th International Symposium on the
Packaging and Transportation of Radioactive Materials**

PATRAM 2019

August 4-9, 2019, New Orleans, LA, USA

IAEA Nuclear Security Series No.8 Implementing Guide, *Preventive and Protective Measures
Against the Insider Threat*, International Atomic Energy Agency, Vienna, 2012

IAEA Nuclear Security Series No.10 Implementing Guide, *Development, Use and Maintenance
of the Design Basis Threat*, International Atomic Energy Agency, Vienna, 2012