SAND2016-10881C

Vulnerability Assessment Approach for Radiological Materials

Paper #338

IAEA Security Conference, Dec, 2016

Purpose of Paper

This paper will provide an approach to conducting a security vulnerability assessment for facilities possessing or using radioactive materials. The approach employs a less rigorous manner to apply performance-based techniques to assess security effectiveness than employed for nuclear material. As such, the approach may be more practical for regulators and operators of radioactive material. The approach addresses the objectives outlined in IAEA NSS#11 for Category 1, 2, & 3 sources.

Background:

A vulnerability assessment is a method for evaluating protective security systems. It employs a performance-based approach to identify vulnerabilities and to assess overall robustness of the physical security system. It is used to confirm that the performance of the integrated security measures effectively meets the regulatory security requirements. It does this by identifying gaps or weaknesses in the security system that could be exploited by the adversary characteristics described using a threat assessment. However, the approach developed for nuclear materials that is generally employed throughout the security community requires a high degree of sophistication of the security analyst in order to provide meaningful results.

Vulnerability assessments conducted for nuclear facilities employ a probabilistic, performance based approach in which the probability that an adversary is detected in a timely manner is determined for several hypothesized worst-case adversary scenarios. The quantified timely detection probability of these worst-case scenarios, when combined with the response force/law enforcement neutralization effectiveness, is conservatively used to represent the overall probability of system effectiveness for the security system. The benefit of the VA method is that it provides insight into how well the physical protection system performs if an attack occurred, thus allowing for identification of possible vulnerabilities and any security system weaknesses to be corrected. This method requires:

1. Characterization of the expected quantified data for all security measures, including:
    a. probability of alarming for all sensors,
    b. the lowest quantified delay time that can be depended upon for all barriers, and
    c. the slowest expected quantified response time for response forces.

Collection of quantified data on effectiveness sensors can be expensive and complex, requiring dedicated test laboratories and competent staff. Comprehensive barrier testing can be very expensive and hazardous; however, this data can perhaps be found through national law enforcement or fire department organizations that must conduct breaching. Dependable response times for law enforcement travel times can very difficult to ascertain, as there are so many uncertainties in the response time—primarily due to situational uncertainties and possible other competing priorities during the event.

2. A detailed scenario analysis to identify several worst case scenarios to evaluate.

   The development and identification of worst-case scenarios, despite efforts to simplify this effort through computer models, is still somewhat of an art. As such, it can be difficult to acquire or develop a competent artist. The effort involves:

   a. compiling all credible adversary attack scenarios, considering the capabilities of the defined adversary;
   b. isolating those scenarios that will be pose the most difficulty for the security system to detect, delay and respond, i.e. the worst-case scenarios;
   c. idenifying the security measures that would be encountered by the adversary along the scenario path; and
   d. comparing the ability of each of these security measures to detect or delay the adversary actions in the scenarios.

   In addition, the impact of any insider to reduce security measure detection or delay must be considered.

3. The skill to compile, along a single scenario timeline, the sequential detection possibilities and compare these to the response force deployment to determine the cumulative timely detection probability.

These requirements are difficult for many security experts, including radiological facility operators and regulators. This is due to:

1. the scarcity of experienced physical security experts in the regulatory or radiological operator environment to identify worst case scenarios, or to determine expected likely timely detection for these; and
2. the absence of quantified test data on sensor detection capability, barrier delay times, and expected response times of law enforcement (and inability to conduct meaningful tests to generate such data)..

The expertise needed for conducting vulnerability assessments cannot be easily nor quickly acquired through training alone, but is slowly acquired by conducting such assessments under the tutelage of experienced security experts. As such, this lack of experience is not easily overcome.

Generating data for security measures and response is difficult to develop, and cannot be generally shared because it tends to be equipment, installation and situation specific; and because the data can be sensitive.

In fact, even in the nuclear operational and regulatory environment, it might be difficult to find experienced security expertise, and adequate quantified data to identify the worst case scenarios and estimate effectiveness of timely detection and neutralization..

Objective of the Approach Outlined in this Paper

The objective of the proposed vulnerability assessment approach outlined in this document is to provide a tool that provides insight into security vulnerabilities and the overall security system effectiveness without requiring as high a degree of security sophistication and analysis rigor as is needed for the current VA approach. The motivation for developing such an approach was to provide an assessment tool for use by radioactive material regulators and operators who lack the quantified data and the level of security experience and analysis sophistication typically found in the nuclear community. In this sense, the rigor of the analysis approach outlined here is appropriately graded to correspond to the reduced consequences of radioactive material with respect to nuclear materials.

Need for a Specialized Approach

In order to confidently provide assurance that the public and environment is properly protected for the hazards of radioactive materials, regulators and operators need to be able to ensure that the consequences of a malicious intentional event involving radioactive materials would not result in undue risks. To confidently do this, the performance of the security system in the face of an adversary attack must be assessed.

IAEA NSS#11 recommends that a vulnerability assessment be conducted to perform this assessment.

The Vulnerability Assessment Approach for Radioactive Materials and Radiological Facilities

This approach is not a scenario-based analysis, nor is it a quantified, probabilistic approach.

Rather, the approach permits identification any security gaps, and provides a performance-based assessment of security effectiveness by assessing the application general security principles in the security system, including:

- Detection before delay.
  Any security system response is initiated by detection of unauthorized actions by the adversary. Once this occurs, the adversary is delayed while the response deploys. Any delay prior to detection does not contribute to timely response, and therefore is not useful to security system success.
- Balanced security along a layer
  Security systems are established along continuous layers enveloping targets. Security measures along these layers should be balanced in order to prevent any obvious path weakness.
- Defense in depth
  To complicate the adversary task, and to prevent a single point failure, depth of security measures is recommended. This is primarily accomplished by enveloping a target in multiple concentric layers of security.

This assessment of the security principles is accomplished by conducting the following steps:

1. Identifying/defining the layers of security. Effective security is defined along a continuous boundary that envelops the area or asset to be protected. The boundary is typically composed of walls, fences, doors, windows, ceilings and floors. Several such concentric layers of security may be employed to surround an asset. Any gap along the layer (detection, delay or access control) is a potential vulnerability in the protection system that could be exposed by an adversary.

   In the example below (Figure 1), the layers that completely envelope the target (star) are the outer building wall, including three doors and seven windows; the radiation therapy reception wall, including one door and one window; or the radiation device room wall, including one door. The decision on which layers(s) should be utilized as security layers is influenced by many considerations, including:
   - operational concerns of defining access control points and detection zones;
   - the robustness and balance of the existing barriers making up the layer (compared to the needed delay time given the expected response time); and
   - the length of the layer (and therefore the cost to alarm or strengthen barriers.

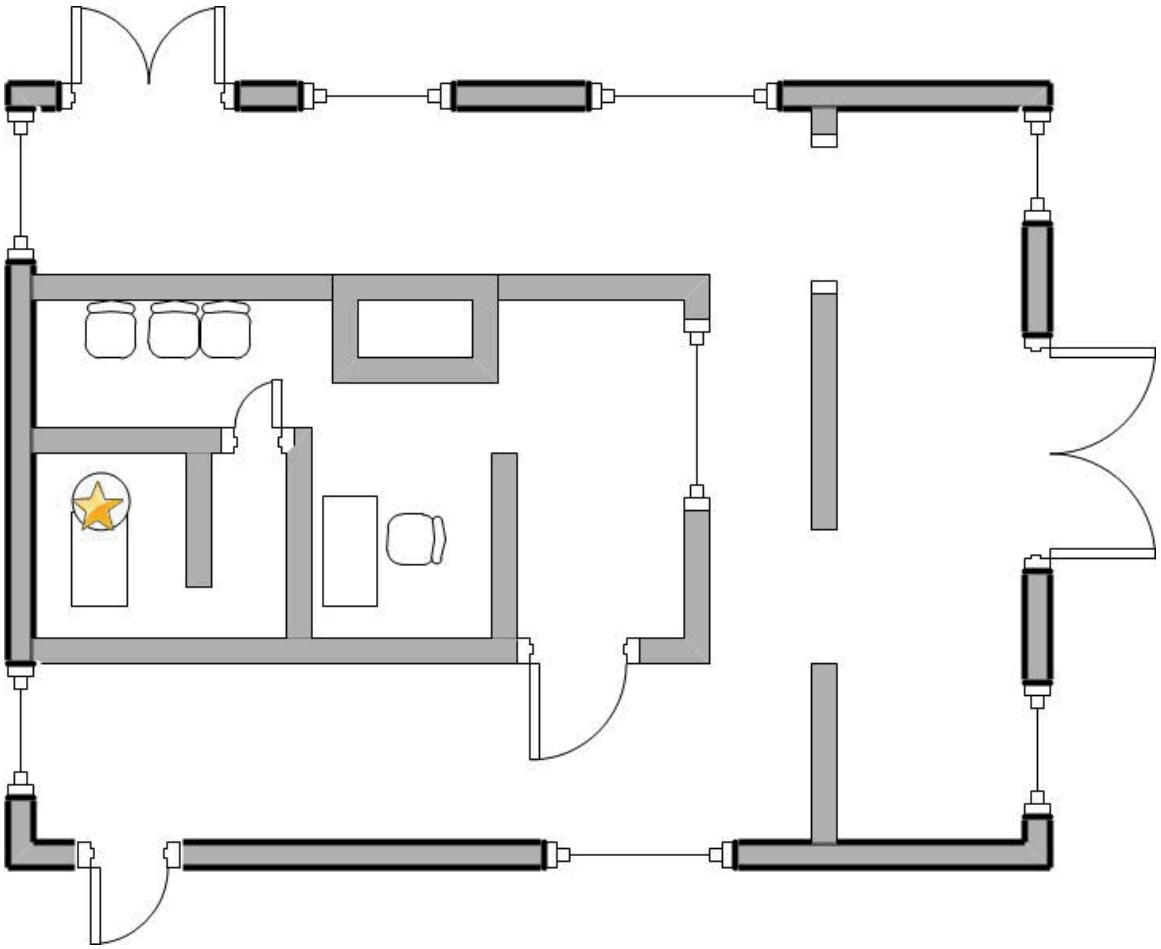

Figure 1. Radiation Therapy example building with possible security layers

2. Identifying/defining the detection, delay and access control applied along each layer to ensure that any unauthorized penetration is detected and delayed. This involves a walk-down of the layer to define the type of barriers, the method of intrusion detection, and the manner of controlling access. Any part of the boundary that is not covered by intrusion detection (sensors or procedures) represents a potential gap in security detection that could be exploited by an adversary (and is therefore a vulnerability).
3. Assessing if the layer detection and delay is properly defined to ensure that adversary intrusion detection precedes any adversary delay measures. The primary objective of the outer layer of security is to provide detection of the adversary. Assessing when on this layer detection occurs (before the layer barrier is defeated, during the defeat, or after the barrier defeat). This assessment will provide insight into whether the barriers installed will contribute to adversary delay or not. If the detection only occurs after the layer barrier is defeated, then the detection must be followed by the delay in a subsequent layer.
4. Assessing the balance of barriers and detection on each layer. This involves an intuitive examination of the layer boundary, detection equipment/procedures, and access equipment/procedures to identify locations where one of the contiguous barriers/detection methods/access control methods might be significantly weaker to unauthorized penetration than the others. This imbalance represents a likely adversary path, and a potential

vulnerability. Guidance will be provided for identifying imbalance and examples will be provided for possible compensatory measures.

5. Assessing the effectiveness of intrusion detection and access control on the layer. Verifying the schedule of sensor arming (are the sensors sending alarms?), guard patrol frequency, door alarms or lock engagement, and guard staffing will help quickly identify time-sensitive gaps in intrusion detection and access control. In addition, the type of intrusion detection measures installed or employed should be assessed for effectiveness. A list of typical sensor technologies and guard surveillance approaches will be provided with expected effectiveness if they are properly installed and maintained, or properly trained. Simple procedures will be provided to permit quick and easy tests of the sensors and guard procedures. Poor-functioning intrusion detection, or dis-armed sensors represent a potential path for an adversary.
6. Assessing the effectiveness of insider protection measures. Checking trustworthiness requirements and records, access authorizations, and surveillance requirements to verify that insiders are adequately deterred and detected. Verifying that access controls and authorities do not permit a single person to covertly remove material without a means of detection. Verifying that no person with intimate access to the material is exempted by trustworthiness checks, and verifying that surveillance or other measures are employed to prevent a single person from covertly removing radioactive materials. Further, verifying that measures are in place to detect attempts by insider to weaken protection system (detection, access, or alarm monitoring). This involves a check of access procedures to verify that areas are compartmentalized and that tamper alarms are in place.
7. Ensure that alarms and video are monitored 24/7, and that the monitoring facility is developed to minimize the chances that an assault could prevent communication of alarms to response forces.
8. Ensure that response force (law enforcement) is able to respond prior to malicious act completion. This is addressed through a facility-level tabletop exercise for category 1 sources. The tabletop involves facility and law enforcement personnel.

Benefits of Approach

Radiological facility and regulatory personnel can employ this approach for design and evaluation without requiring the development of quantified data, nor requiring extensive training and experience in the security discipline. The approach provides:

1. Confidence that the detection measures installed will provide adequate intrusion detection of the DBT-like adversary.
2. Confidence that there are adequate numbers of barrier layers, and that no gaps exist in each concentric layer.
3. Confidence that insiders are adequately addressed.
4. Confidence that there are adequate and redundant communications between the site and the response forces, and conducting tests to this end.
5. Confidence that the security measures in place will permit an effective and timely response by conducting a tabletop exercise on a periodic basis.

Summary

A practical approach is described to enable operators and regulators of facilities using or storing radioactive materials to conduct a security vulnerability assessment. The approach does not use quantified data, nor formal path analysis, and is therefore not as rigorous an assessment as that undertaken for nuclear facilities; however, the approach enables these operators and regulators gain insight into performance issues and overall effectiveness of the system without the complexity and data requirements of the traditional approach.