SAND2012-4677C

# NEW APPROACH FOR ANALYZING THE INSIDER THREAT

Ruth A. Duggan and Carol J.B. Scharmer
Sandia National Laboratories[1]
P.O. Box 5800, MS-1361, Albuquerque, NM 87185-1361

## ABSTRACT

In Revision 5 of INFCIRC/225, there is greater emphasis on addressing the insider threat, but little guidance on how to do so. In 2010, the World Institute for Nuclear Security (WINS) released a best practices document on internal threats and INMM has hosted two workshops on the subject. Tools have been developed to analyze the facility using adversary sequence diagrams developed for the external threat and modifying the process to account for insider access and authority as well as any administrative procedures used to address the insider threat. While the current analysis process is very systematic in nature, some find it very cumbersome with little benefit. A different, more direct approach may yield alternatives that could enhance not only physical protection, but also personnel security, material control and accounting, and information security processes for better overall nuclear security. This paper presents such an alternative systematic approach that is threat neutral, but consequence-based. This process takes into account different viewpoints to cover traditional aspects of physical protection and the additional aspects of nuclear security. A benefit of this approach is being able to analyze cyber-based attacks and combination physical/cyber-based attacks. This approach also provides a basis for cost-benefit analysis.

## INTRODUCTION

According to Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), the insider is defined as "*One or more individuals with authorized access to nuclear facilities, or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so.*" The attributes typically used to characterize an insider are access, knowledge, and authority.

**Access -** Access refers to authorized access to work areas, process systems, and protection systems. This includes normal access, temporary (escorted access), emergency access (by emergency response personnel), and no access. Required access/entry control must be identified early in the design of the intrusion detection and entry control systems. This is part of the site specific Concept of Security Operations as defined in the Site's Security Plan.

**Knowledge** - Knowledge or skills refers to what the insider knows about the systems. An individual is authorized to access systems or areas based on work assignments that are based on knowledge or skills. The analysis must assume that all individuals with access have sufficient knowledge to accomplish the task. For example, one cannot

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000, SAND2012-XXXX.

assume the janitor does not know how to operate the reactor. The insider is assumed to have knowledge of the facility layout, location of targets, process and material handling procedures, emergency procedures and protection procedures. Procedures are for regular, temporary and emergency activities.

**Authority** - Authority can be over people, procedures (tasks), process equipment or protection equipment and over the material itself. Authority includes having authorized access (completing the loop) to work areas near or at the target of concern.

## ASSUMPTIONS

The following assumptions are made for the proposed insider evaluation methodology:

- Targets include material, vital equipment, physical protection equipment and systems, process control systems, where material is handled and moved. Targets also include passageways and material loading areas associated with transportation of material. Collusion targets that an insider might attack to support an external adversary should also be included in the analysis.
- Attack methods may be physical attack or cyber-based attack of information systems targeted toward theft of nuclear materials or sabotage resulting in radiological release. Physical attacks include attacks in areas where material is used and stored, vital areas identified for protection against radiological release, and transport between or within buildings and any other transport within the facility. Cyber-based attacks include attacks against process control systems, physical protection systems and systems that contain mission critical information including material accountancy and control data.
- Temporary unescorted access is the same as authorized access.
- Since insider protection features depend heavily on administrative procedures, the features are not able to be statistically performance tested. The protection features are best performance tested by limited-scope performance tests. Therefore, this evaluation process is not intended to generate a quantitative value to use for a probability of detection ($P_{D)}$ or probability of interruption ($P_I$).

## PATH ANALYSIS

A facility model depicts the facility in terms of adjacent physical areas and protection layers defined in terms of path elements. The model identifies all targets, whether direct, indirect or cyber at the appropriate physical area or protection layer path element. For external threat system analysis using adversary sequence diagrams, the physical layers and each protection element are assigned probabilities of detection and delay times based on a design basis threat scenario (approach and tactics) against a particular target. If the same tool is applied for insider threat analysis, probabilities of detection of zero and no delay time are assigned for the path elements for which the insider has normal access. Where the insider does not have normal access, the analysis should treat the insider the same as an external adversary. Whenever and insider no longer has access, he/she can only proceed using techniques that an outsider would use or with collusion of another insider. It should be noted that the insider potentially has a “familiarity advantage” that distraction techniques might favor.

However, in strong security cultures, distraction techniques should be addressed in training.

Therefore, when a facility model is reviewed for paths unique to the insider, only the path elements associated with entry control remain and access need be analyzed. For each successive physical layer, fewer and fewer insiders should have access to the target. As could be predicted, those insiders with direct access to material or sensitive information pose the greatest challenge for protection. Since the protection elements models are primarily technical, this method does not take into account procedures or administrative processes (policies) that may be used for protection against the insider such as the two-man rule for which there are many variations.

The proposed process takes advantage of the evaluation techniques and tools already in use but simplifies the analysis by eliminating insider actions which are the same as outsider actions.

## PROPOSED EVALUATION PROCESS

The proposed evaluation process consists of 5 basic steps:

1. Determine access authorization groups
2. Identify each target and associated attack path/tactics for the insider in a complete facility model.
3. Evaluate the use of technical protection measures relevant to attack path/tactics.
4. Evaluate the use of administrative protective measures relevant to path/attack tactics.
5. Apply technical and administrative protection features consistently across the facility

These five steps are described in greater detail below.

### Step 1 – Determine Access Authorization Groups

It is necessary to understand who has physical and cyber access to what at a site. This is most often controlled at a site by the use of electronic access control database(s) and key control databases. These databases can be used to associate access groups with the doors or information systems that can be accessed by that group. Minimizing the number of groups should only be done when access and protections measures are the same and it minimizes the number of persons with access to any given protection layer. Additionally, a higher access level should be applied to areas where access control lists are managed.

### Step 2 – Identify each target and associated attack path/tactics for the insider in a complete facility model

Develop a (or obtain an existing) Facility/Target Model that includes all physical areas as well as insider targets. Then “eliminate” path elements that could only be defeated using the same methods as an outsider such as through a concrete wall. Protection for the outsider elements are considered in the design against the outsider and need not be

repeated under the insider analysis. A path element cannot be eliminated if an insider might obtain temporary or emergency access.

An example of an insider target might be the Central Alarm Station (CAS) since it houses critical portions of the protection system. The location of the CAS must be included in the Facility Model as a target for insider analysis. Another example of an insider target that should be identified on the facility model is the field panels housing the communication components for the intrusion detection system.

**Step 3 - Evaluate the use of technical protection measures relevant to attack path/tactics.**
All identified targets must consider the technical protection measures before considering administrative protection measures, such as procedures. As in the safety systems, the use of technology or hardware is applied first, then administrative processes (physical barriers before administrative procedures). Therefore this step evaluates technical protection measures.

Beginning with each target and working outward, analyze all path elements (excluding those eliminated in Step 1) for the insider with authorized access to determine the access level, contraband detection and surveillance systems to apply at that element. For example, the required level of access to the process control room, the CAS and to the field panels will be identified. Note that similar targets, such as field panels, will thus be evaluated simultaneously. Once the protection features for one field panel is identified, the protection features for all other field panels must be the same.

The access level may be credential, credential plus personal identification number (PIN), credential plus biometric or even credential, PIN and biometric.

The evaluation will also assist in the identification of optimum locations of protection features. Several access layers provide defense in depth. Cost savings may be realized when appropriate access through a physical layer is applied for all targets within the layer. For example, in some cases contraband detection may be located at a boundary common to several buildings containing nuclear materials.

**Step 4 – Evaluate the use of administrative protective measures relevant to path/attack tactics.**
Beginning with each target and working outward, analyze all path elements (excluding those eliminated in Step 1) for the insider with authorized access to determine the administrative procedures applied as protection measures. Three types of administrative procedures must be evaluated. First, the procedure that permits the authorized access, such as initial and periodic management evaluation of access areas required for assigned job responsibilities. Second, procedures that prevent a single individual to have access to or approval to use or transport a target (or modify or transmit in the case of cyber), such as the two-person rule, password privilege assignment, and notification of anticipated protection system changes, work authorizations, or inspections. And third, review procedures for material control and

accountancy (or cyber-based procedures) to determine if protection features are inherent in such procedures. For example, chain of custody documentation for material including isotopic measurements may be provided during material movements. Through this analysis, opportunities for insiders to perpetrate malicious acts undetected are considered and addressed.

**Step 5 – Apply technical and administrative protection features consistently across the facility**

Once all identified targets have been evaluated individually or as a common group. The technical and administrative protection features identified in Steps 3 and 4 should be reviewed and evaluated for consistent application for similar types of targets across the facility. This step is beneficial for developing standards and establishing the conduct of security operations for the site. For example, field panels and intrusion detection network equipment may be identified as requiring the same administrative protection methods.

## CONCLUSION

The primary protection philosophy for the proposed evaluation process is to protect against a single individual who may have authorized access near or at the target. Most entry control systems are designed to limit the number of authorized individuals with direct access. Contraband systems are designed to detect theft of material by the insider. The majority of protection measures designed for insiders are procedural or administrative. Examples include the two-person rule, escort procedures, and vehicle/package searches. Combinations of these measures serve as "multiple complementary sensors". For example, optimum 2-person implementation would require two persons to access where material is handled (independent key codes or keys) and require both persons to participate in the operation, each with different responsibilities, each checking the other's work/action. Such procedures are often implemented for better safety. Thus, for each case when material is being handled for use, storage, or transport, the use of technology as detection or delay and modification of procedures to also improve detection or delay must be considered so that opportunities for unobserved insider malicious acts are minimized.

This evaluation process provides a mechanism to identify areas of weakness that require specific protection against the insider and for evaluating physical and administrative protection options for those areas. The results of the evaluation effectively become the basis for the physical protection system design and operation, specifically for authorized access through physical layers.

Because this process does not generate a $P_D$ or $P_I$, the metric for determining the effectiveness of the protection system against the insider is now based on the robustness of the combined technical and administrative protection features that limit insider threat opportunities. The insider threat must be analyzed throughout the facility for the specific insider threat adversary actions required for theft, sabotage, or compromise of information. As indicated by the variety of insider targets included in

the Facility Model, specific adversary actions may include compromise of the physical protection system itself in order to complete the theft or sabotage. Therefore, for the insider the metric cannot be based on just the robustness of potential detection at specific locations.

Additionally, the concept of Security by Design includes the principle that physical protection be considered through all phases of the project life cycle and the PPS design requirements included in the conceptual design phase of the project. Therefore, by implementing the insider process during the conceptual design and updating the analysis as the detailed design evolves, the PPS design will inherently address the insider threat.