LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-CONF-418137

Insider Threat Identification and Mitigation (ITIM) Training Workshops for Abrupt and Protracted Theft

M. O'Brien, P. Gibbs, R. Larsen, T. Edmunds and N. Peterson

October 14, 2009

4th Russian International Conference on Nuclear Material Protection, Control and Accounting
Obninsk, RUSSIA
October 19-23, 2009

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Insider Threat Identification and Mitigation (ITIM) Training Workshops for Abrupt and Protracted Theft

Michael O'Brien, Lawrence Livermore National Laboratory; Phillip Gibbs, Gregg Services; Robert Larsen, Los Alamos National Laboratory; Tom Edmunds, Lawrence Livermore National Laboratory; Nancy Peterson, Department of Energy-National Nuclear Security Administration;

Abstract

As part of its international cooperation activities, the Department of Energy's National Nuclear Security Administration, Office of International Material Protection and Cooperation, Office of Material Consolidation and Civilian Sites, has developed training workshop materials in the area of insider threat identification and mitigation. The workshop used a hypothetical facility as a basis for analysis. The workshop was two weeks in duration and required detailed scenario development and analysis of abrupt and protracted theft scenarios. Topics covered included: administrative and technical measures against an Insider; Limited Error of Inventory Difference processes to detect Insider activity; vulnerability assessment techniques for assessing Insider Threats. The workshop was a significant step in addressing the challenges of potential insider threats facing nuclear facilities world-wide. The workshop material is adaptable for use in any country and most nuclear facilities.

This paper provides an overview of the methodologies presented to analyze and mitigate the threat of an insider attempting an abrupt theft and those involved as an insider attempting protracted thefts.

Background

Recognizing the global concern regarding the protection of nuclear materials against evolving terrorist threats, the Department of Energy's National Nuclear Security Administration (NNSA), Office of International Material Protection and Cooperation, Office of Material Consolidation and Civilian Sites and the China Atomic Energy Agency (CAEA) agreed to conduct training workshops focusing on the insider threat. After a successful one week workshop in 2008, it was decided to expand the workshop by placing more focus on protracted theft and by adding more practical exercises. The NNSA provided a team of experts to develop the advanced course material and coordinate it with the China Institute of Atomic Energy (CIAE). The team developed additional lecture and exercise material resulting in an expansion of the previous one week workshop into a two week workshop. The Chinese identified personnel from their nuclear facilities to receive the training and hosted the workshop in Beijing, China. This effort resulted in an advancement of the type of topics typically covered in various vulnerability analysis (VA) training courses. The new workshop material takes into account the difficulty of identifying and mitigating protracted theft and provides additional instruction and exercises for development of a broad range of protracted theft scenarios and mitigation measures.

In Russia, Rosatom Regulation No. 167, "Methodological Recommendations for Categorizing Objects of Physical Protection and Nuclear Sites," 10 May 2001, provides regulatory direction on analyzing protracted theft and diversion of nuclear material by insiders. However, it is unlikely that training material, specifically training material for detailed protracted theft analysis, exists in training courses currently available in Russian training centers. The ITIM Workshop material could be adapted for immediate workshop instruction for Russian nuclear sites and ultimately for use in Russian training centers.

ITIM Workshop

The advanced ITIM workshop was held February 16-27, 2009, in Beijing, China and was attended by 26 personnel from various Chinese nuclear facilities. Approximately half of the participants had a materials control and accountability background while the other half had physical protection backgrounds. Prior to the workshop, each student received a Primer documenting material control and accountability basics and a Primer documenting physical protection basics. This allowed participants to gain some familiarity with concepts and terminology for areas not specifically associated with their particular technical background. The workshop utilized a classroom setting within a Chinese nuclear facility. This allowed for some exercises to be conducted outside the classroom in a more realistic environment. The ITIM workshop consists of 20 modules:

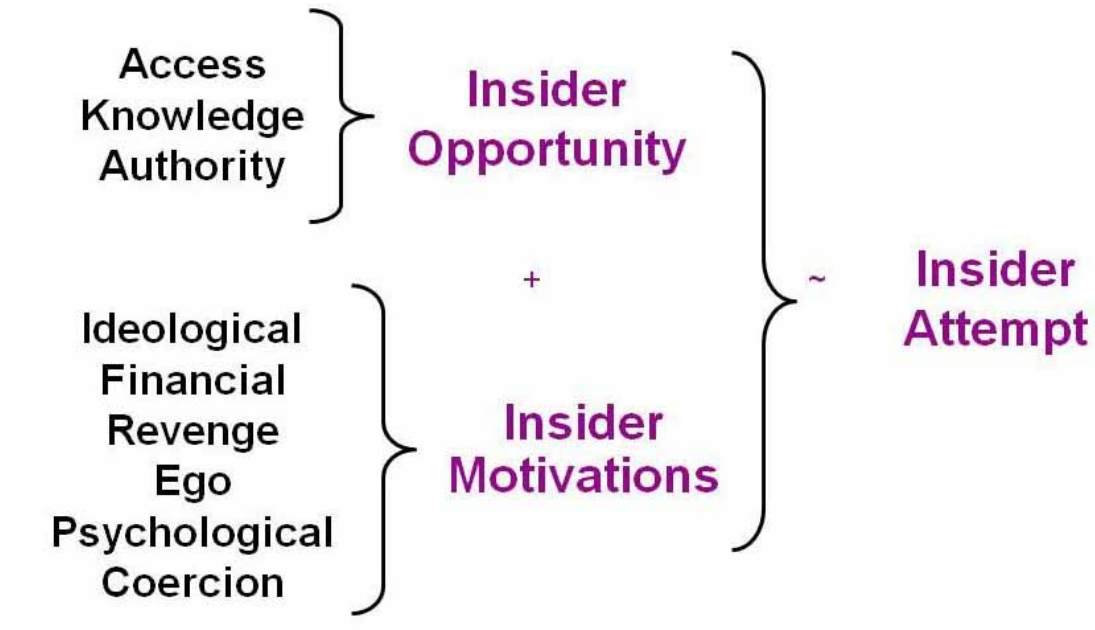
1) Insider Overview
2) Facility Overview
3) Personnel Measures
4) Administrative Measures
5) Technical Measures
6) Detection, Assessment, Recovery, and Prosecution
7) Video & Discussion
8) Quantifying MC&A
9) Item Inventory and Attribute Sampling
10) Bulk Processes
11) Material Balance Evaluation
12) Establishing Control Limits
13) Target Analysis
14) Insider Characterization
15) Case Studies
16) Insider Analysis
17) Abrupt Theft Analysis
18) Protracted Theft Analysis
19) Upgrades Analysis
20) Maintaining System Effectiveness

In addition to material presented in the lectures, the workshop also includes 12 practical exercises and numerous group discussions. At the beginning of the workshop, the participants are divided into four sub-groups. This allows each group to work as a team

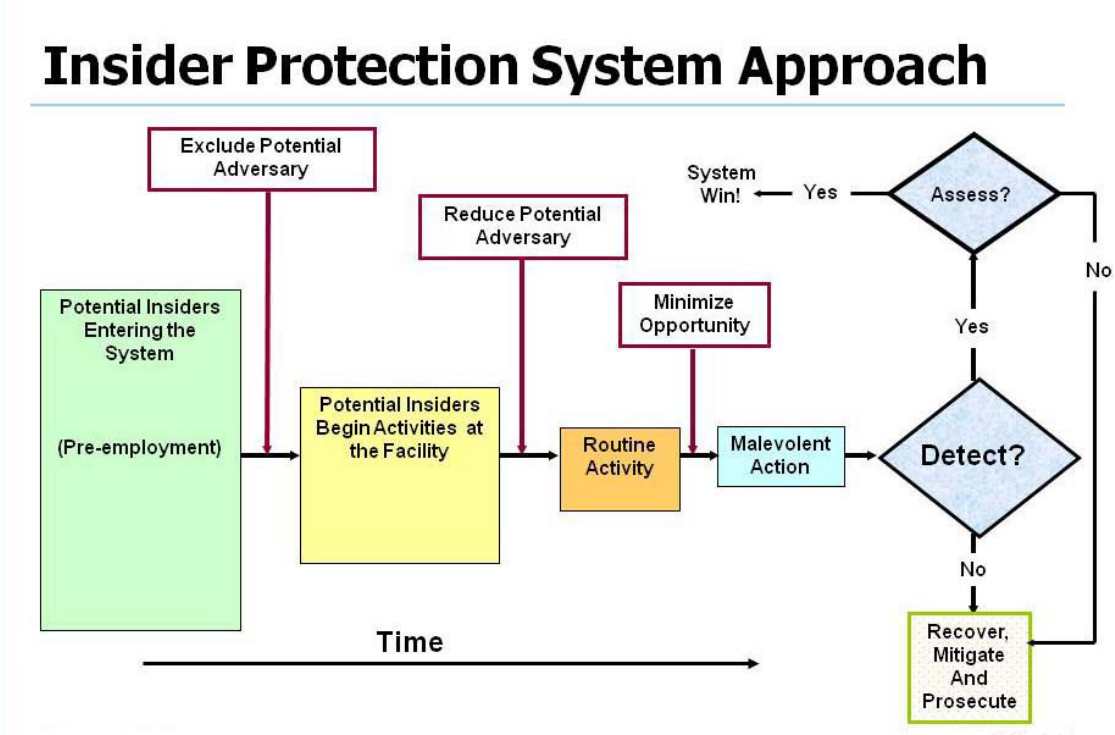
throughout the workshop. For the 2009 workshop, each team included personnel with MC&A backgrounds and personnel with physical protection backgrounds. This is the optimum pairing, as one intent of the workshop is to instruct personnel on how to work effectively within a vulnerability assessment team using various subject matter experts (SME's) . Each team selected a spokesperson to present their team's exercise results to the other teams. A summary of each workshop module is provided below.

Insider Overview

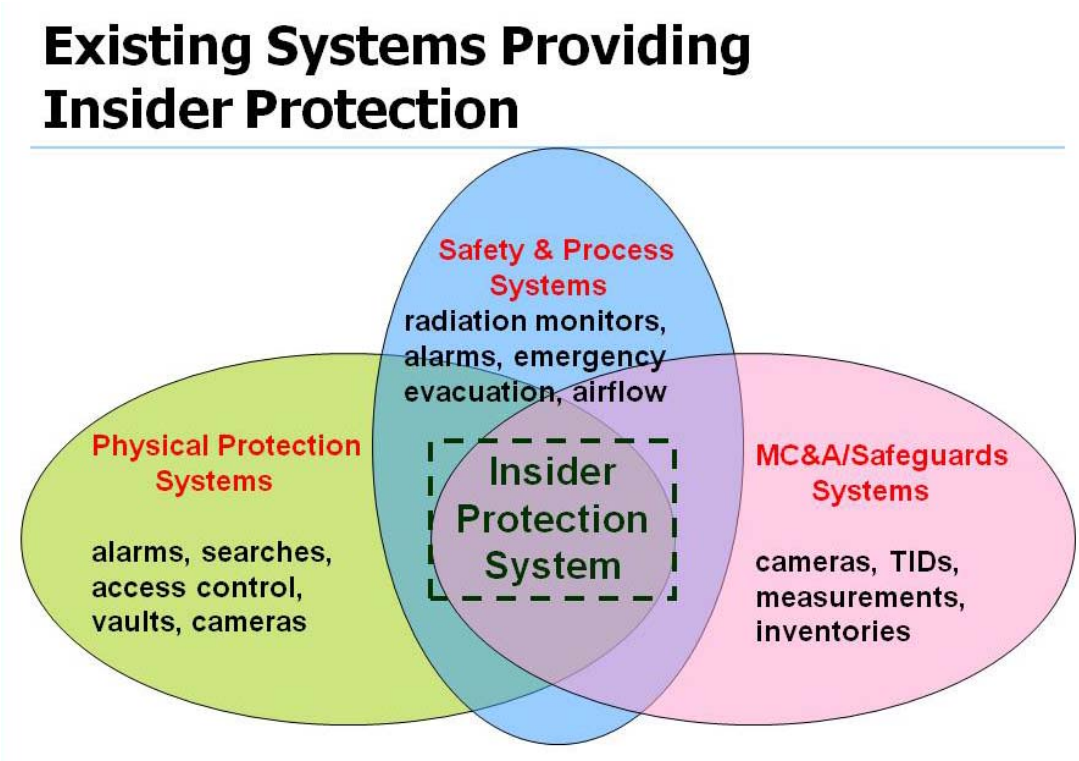
The insider overview module describes the threat that the insider poses to a nuclear facility. A description of the types of insiders, e.g. passive, active, violent, and non-violent, and their various motivations are provided. When coupled with opportunity based on their access to material, knowledge of the insider protection system and the authority they may possess, the combination may result in an insider attempt.



A systematic approach provides the ability to mitigate the insider. The approach is described, applied and reinforced throughout the workshop. The approach, shown below, allows for continued screening of employees in order to reduce the potential insider adversary population. This is further enhanced through a check and balance system of sound operational procedures, e.g. separation of duties, periodic inventories, proper measurements of waste material, two person rules and administrative checks. Collectively, these types of "best practices" can help detect the insider if a malevolent act were to occur. Detection, followed by assessment mitigates the insider from acquiring a goal quantity of nuclear material. For a protracted theft, initial smaller thefts may go undetected but, over time, detection and assessment should eventually occur. The role of various types of safeguards and their value is emphasized throughout the workshop.

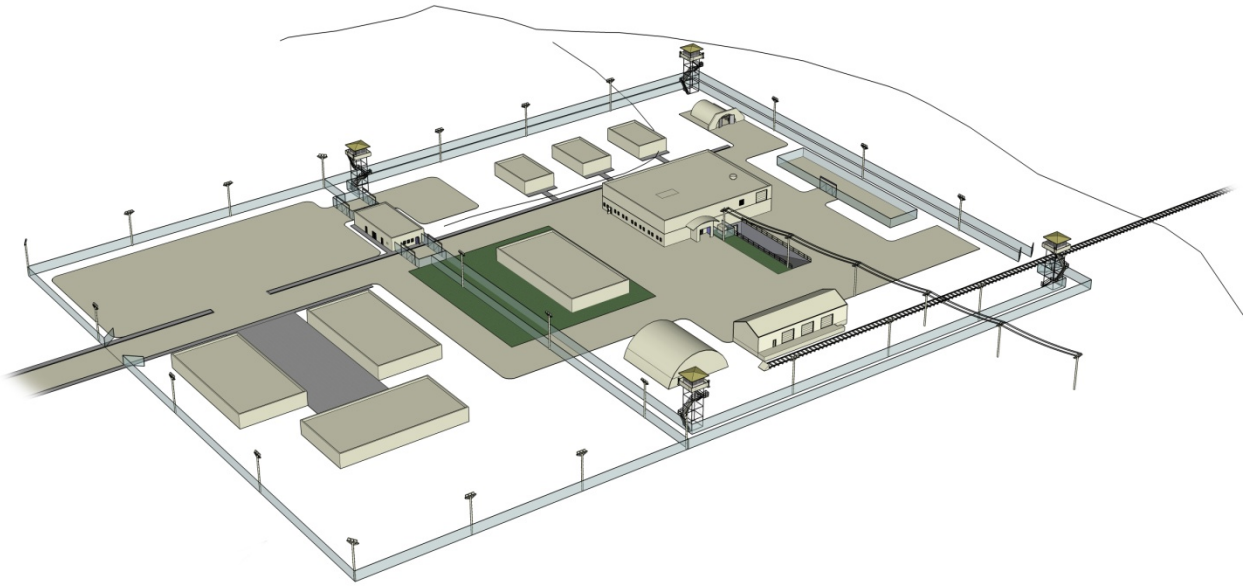


The overview module also describes how the different aspects of an insider protection system work in synergy:



Hypothetical Facility Overview

The facility overview module introduces the workshop participants to the workshop's hypothetical facility and provides instruction on how to conduct a facility characterization in order to collect the necessary data for analyzing the insider threat. The hypothetical facility used in the workshop represents a uranium research plant. As a role play exercise, instructors act as facility personnel and brief the VA teams separately on the facility's mission, site operations and local threat conditions, security measures, and material control and accountability operations. Each VA team has an opportunity to question the site representatives after their respective briefings. The VA teams then are expected to use their recorded site characterization data later when modeling the insider.

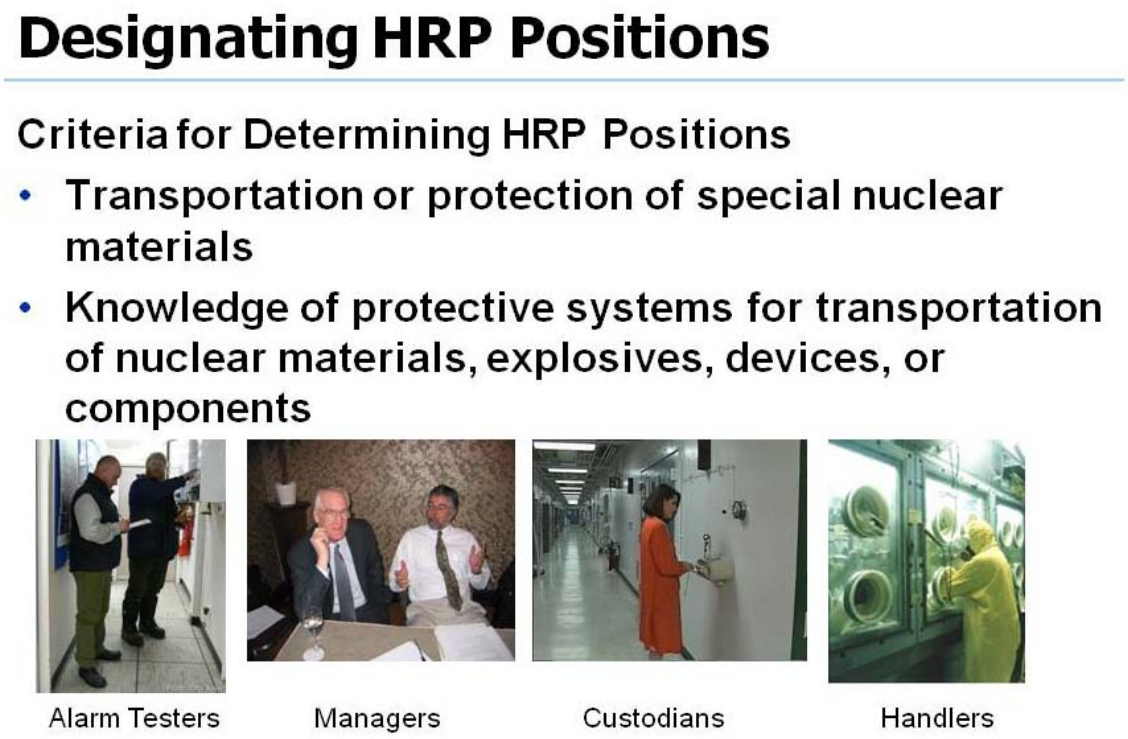


In addition, workshop participants are provided a copy of the hypothetical facility file for reference. The material contained in the file includes building diagrams, descriptions of processes, material characteristics, personnel duties, protective force, and security systems. The hypothetical facility plays an important part in the overall workshop. Participants later learn how to understand the material flow of the respective facility operations. This allows each team to understand the inherent strengths and vulnerabilities associated with this facility. Participants learn how various safeguards strengthen the insider protection system and how the lack of other needed safeguards weaken the system. In addition to facility specific information, the participants also learn about the local threat conditions and how various types of local conditions, e.g. criminal groups, thefts, and employee morale can increase the likelihood of an insider theft attempt.

Personnel, Administrative, and Technical Measures

The personnel, administrative and technical measures modules describe best practices, facility designs, and various systems associated with operations at a nuclear facility. Particular emphasis is placed on safeguards that have become "best practices" and what value they bring to the overall system. Some, but not all, of the measures described exist in the hypothetical facility. This allows participants to begin thinking about which safeguards may be candidates for upgrades at the hypothetical facility to help mitigate insider scenarios.

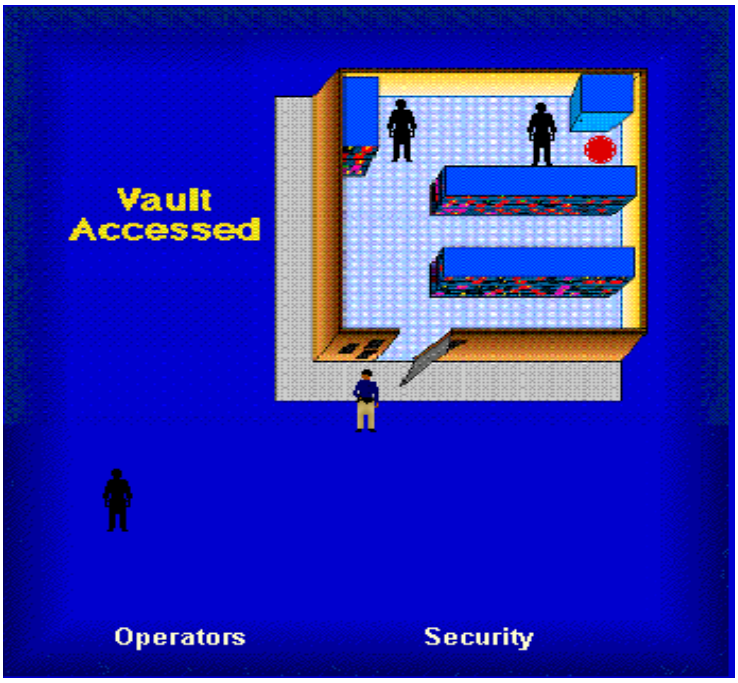
As mentioned in the first module, personnel screening begins during the hiring process and continues into the selection of personnel for critical positions. Prosecution of malevolent acts is an important personnel deterrent measure. An important measure pertaining to persons in critical positions is a Human Reliability Program (HRP). This program generally consists of some form of psychological testing, drug testing, financial reviews, supervisor and co-worker observation.



Workshop participants also learn how effective personnel measures are supported by a strong security culture, training, and an awareness program.

Administrative measures such as daily administrative checks, use of tamper indicating devices, etc. are often inexpensive upgrades and can have a significant impact on mitigating the insider. The two person rule is discussed in detail and a

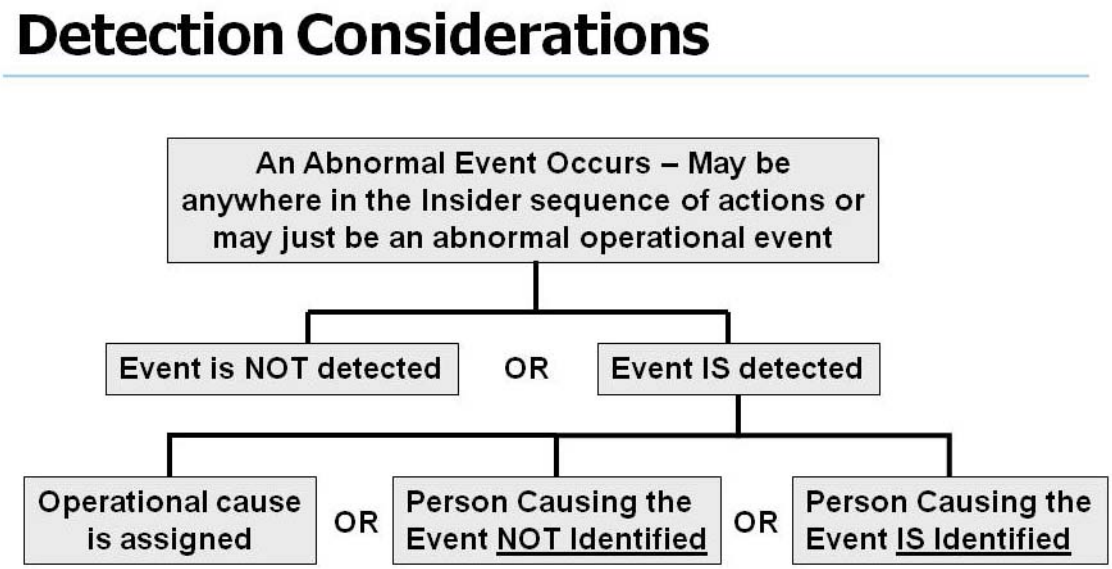
group exercise is provided to test the workshop participants understanding of its proper application.



The technical measures module describes various systems which work collectively to mitigate the insider and provide the insider protection system described in the first module. An example of complimentary systems is a personnel portal operation which should include a radiation monitor, x-ray machine, metal detector, safety systems, and a member of the protective force. The module concludes with a practical exercise of identifying technical measures in a nuclear facility.

Detection, Assessment, Recovery, and Prosecution

The detection, assessment, recovery, and prosecution module focuses on safeguard measures which afford detection and how assessment is generally achieved after detection occurs. The detection element is defined as any component of a facility's MPC&A system which can generate an alarm indicating an abnormal condition or event involving the control, or possible loss of SNM. Depending on the safeguard, the detection could be prompt (timely) or delayed.



The assessment element is defined as the determination, either through direct observation or an electronic system, of the cause of an alarm. "Assessment" is the act of correctly assessing the detected insider action as an unauthorized action.

Example Assessment Elements

- **Protective Force**
- **Two Person Rule**
- **Surveillance Systems**
- **Administrative Checks**
- **Transfer Verification**
- **Inventory difference resolution**

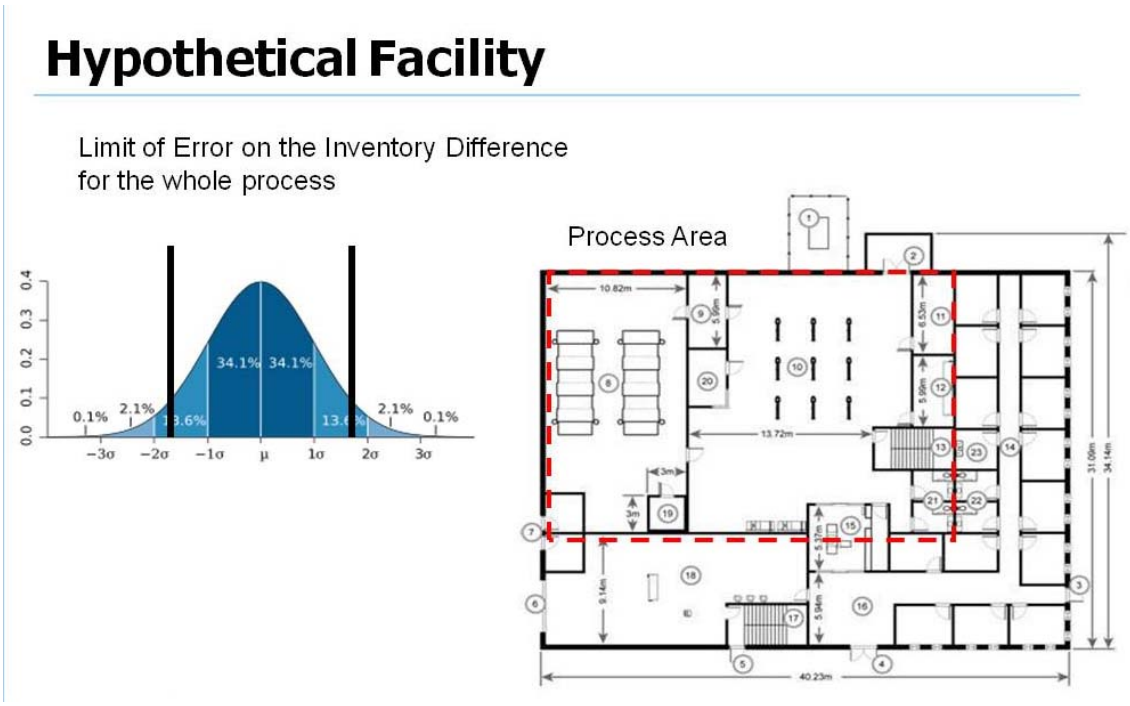
The workshop does not focus on protective force response after assessment, as assessment against an insider is assumed to end the insider sequence of actions unless the insider is violent. At the end of the module a group exercise is conducted in which participants review a video and identify detection and assessment elements.

Quantifying MC&A

After the presentation of personnel, administrative, and technical measures and practices associated with the hypothetical facility, a module is presented on quantifying performance of material control and accounting systems. The module is then followed by several associated modules; Item Inventory and Attribute Sampling, Bulk Processes, Material Balance Evaluation, and Establishing Control Limits. A description is provided on determining detection probabilities of items and how the process is dependent on numerous factors, e.g. how the item is inspected, the number of defects, number of items inspected, and the frequency of inspections. Examples of timely detection and delayed detection are provided followed by an exercise in defining probabilities.

The workshop participants are also shown how to determine the probability with which the Safeguards systems can detect a diversion of material due to insider activity using statistical process controls. A group exercise is conducted after the presentation.

Examples of material processes from the hypothetical facility are used in the workshop to help participants understand how an adversary might exploit the system leading to protracted theft.



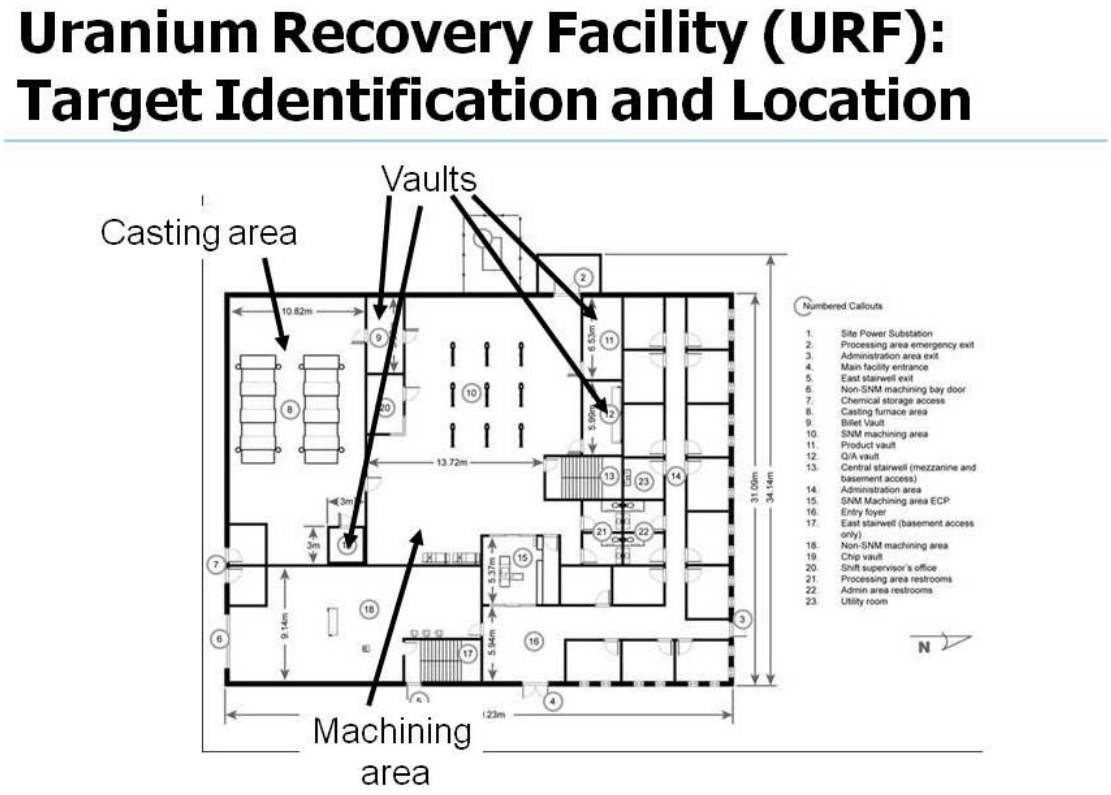
Using the hypothetical facility in the exercises allows the workshop participants to better understand the material flows, processes, and associated safeguard measures, which participants will need in developing insider scenarios.

Target and Insider Characterization, and Case Studies

With all the relevant background instruction completed, the workshop then focuses on building the insider analysis by characterizing the target material and the insiders who may try to exploit the system. Information from the hypothetical facility is again used for the practical exercise in applying the methodology.

A discussion of determining if there is a material roll-up concern and aspects of material diversion and protracted theft are included in the target characterization module. Emphasis is placed on protracted theft because small quantities are easier to remove undetected but the strategy requires multiple theft attempts and has a longer time line than abrupt theft. Probability of detection, does increase as the number of attempts increase. Similar attributes exist for a protracted diversion scenario where material is diverted within a facility; however, theft of diverted material still requires an attempt or attempts to remove the material undetected from a material access area.

Workshop participants then review and document the nuclear materials contained within the hypothetical facility as potential theft targets.



The workshop uses many large scale facility diagrams as aids to assist participants in developing their insider analysis.

The workshop participants are instructed on how to define the potential insiders who work at the hypothetical facility. Insiders are initially grouped based on access, authority, and knowledge. Ranking determinations are then made for each attribute and each insider in relation to each target. Rankings of High, Medium, or Low are used.

Example of H,M,L Applied to Threat Group Table for the Bunker

Position (Number)	Routine Access	Routine Authority / Responsibility	Knowledge
Plant Manager (1) (Plant Manager Org.)	Protected Area, All Inner Areas (usually escorted) L	Overall direction. Not authorized to direct detailed facility operations M	General knowledge of plant operations, lacks detailed understanding of facility M
Shift Supervisor (3 total with 1 per shift) (Shift Supervisor Org.)	Protected Area, All Inner Areas L	Detailed direction of all facility activities. Direction obeyed without question in most situations H	Extensive, detailed knowledge about all aspects of facility design, layout, and operation.
Machining operator (6 total with nominal 4 per day shift) (Operations Support Org.)	Protected Area, All Inner Areas L	Detailed direction of all machining activities. Under direction of shift supervisor. L	Extensive, detailed knowledge about all activities in the machining area. M
Health Physics Technicians (4 total with nominal 3 per day shift) (Health Physics Org.)	Protected Area, all Inner Areas and occasional escorted access to Storage M	Monitor radiological conditions. Not permitted to work on plant equipment. L	Specialized knowledge related to their duties. Narrow knowledge of facility systems. M
Operations Support (6 total with nominal 4 per day shift) (Operations Support Org.)	Protected Area, All Inner Areas and occasional escorted access to Storage M	Perform specific operations tasks under direction of machining and casting operators L	Specialized knowledge related to their duties. Narrow knowledge of complete facility systems. M

After characterizing the insiders of the hypothetical facility, a module describing actual case studies of insider thefts is presented. The presentation is followed by an exercise in which workshop participants identify the exploited system weaknesses. The theft scenarios are then discussed in the individual cases.

Insider Analysis

After much preparation in regards to gaining an understanding of the physical and operational characteristics of the hypothetical facility, definition of the material theft target, and the capabilities of the potential insiders, the workshop participants then learn how to conduct the insider analysis. The insider analysis instruction is done in four modules.

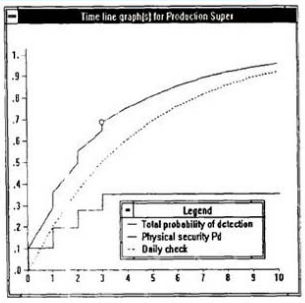
The first module provides an overview of the standard table top (*e.g.,* Vulnerability Integrated Security Analysis (VISA) approach used by SME's. This module provides a foundation for the participants to understand the fundamentals of the analytical process. Participants learn how to define pathways and the safeguard elements associated with each path in order to develop credible scenarios. Participants develop the sequence of actions, their task times, and associated strategies that an insider could use to defeat the safeguard elements and succeed in a theft. The participants then are presented with the methodology to conduct an insider analysis.

The second module focuses on abrupt theft analysis. This allows workshop participants to use the information obtained in the first module to analyze the facility's insider protection system's ability to mitigate a single theft attempt by an insider of a goal quantity of nuclear material. Workshop participants work within their respective teams and to identify their worst case scenario, then they present their results to the other teams. Each team is given a different target to analyze. The team presentations allow for an open peer review process and feedback from the instructors.

The third module focuses on protracted theft. Instruction is provided on how to model numerous theft attempts of smaller quantities of material. The same analytical process is repeated by the individual teams, with each team again presenting their results to the other groups.

Protracted Theft Scenario Analysis Incorporates PP, MC And MA Factors

- Acquisition and exit events
  - Use abrupt theft techniques
- Material accounting system
  - Compute cumulative probability of detection during protracted theft timeline
- Overall probability of detection for scenario is:



$$P_d = 1 - (1-P_{da})^n \times (1-P_d(t))^i \times (1-P_{de})^m$$

Avoid detection during n acquisitions	Avoid detection during i balance periods	Avoid detection during m exits

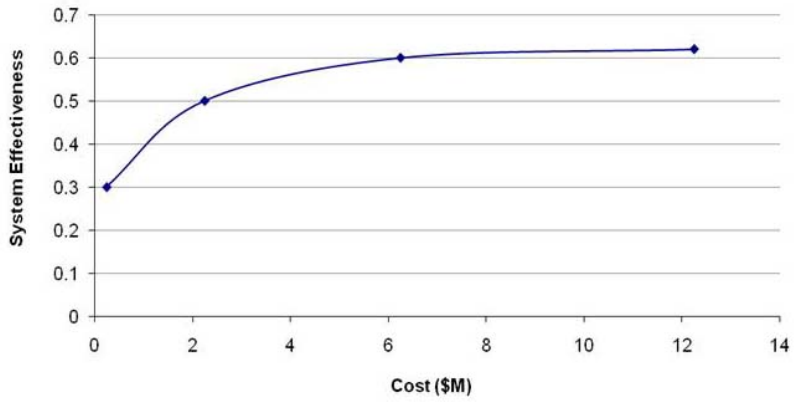
- Perform for each adversary, location and scenario

The fourth module provides instruction on the upgrades analysis process. The presentation emphasizes the various factors considered when identifying potential upgrades, *e.g.* initial and long term cost, maintenance, sustainability, and, in the case of procedural upgrades, if they can be implemented. Examples are provided on the process of analyzing the effect of individual upgrades as well as the effect of grouping several upgrades into a cost-effective upgrades package. The costs of the upgrades are weighed against the relative risk reduction achieved by the upgrades.

A cost benefit analysis model is presented.

Cost Benefit Ratios

Safeguards package	Cost ($M)	Effectiveness (increased Pd)	Effectiveness/cost	Cumulative cost	Cumulative benefit
Vault upgrades	0.25	0.3	1.2	0.25	0.3
Emergency exit	2	0.2	0.1	2.25	0.5
Vehicle portals	4	0.1	0.025	6.25	0.6
Fenceline	6	0.02	0.003333333	12.25	0.62

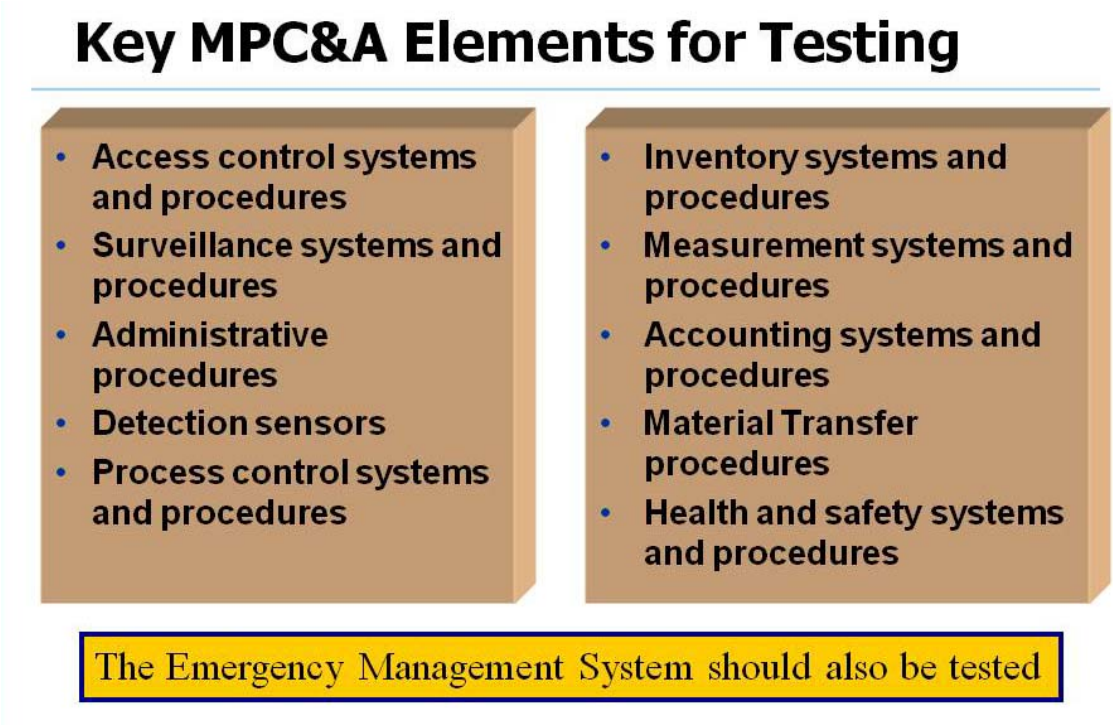


For the final practical exercise, each team must then identify additional safeguards that could be applied to reduce the risk of their worst case scenario. The teams then conduct a final analysis with the postulated safeguards and present their results to the other groups. Large facility diagrams are used for the presentations. Each team spokesperson provides a rational for choosing the specific upgrades.

After all the individual team presentations have been given, a group discussion occurs to compare and contrast the various scenarios and value of the chosen upgrades.

Maintaining System Effectiveness

The final module of the workshop describes necessary elements of a performance assurance program to assure an acceptable level of risk is maintained. Workshop participants gain an understanding of the importance of performance testing by facility personnel and the potential threat of insiders conducting their own performance testing when developing theft scenarios.



Following the module a final group discussion is conducted as a review of the entire workshop. This allows participants to receive any necessary clarifications on the workshop material.

Conclusion

The ITIM Workshop has been very successful thus far. The workshop material continues to be updated to allow for instruction to assist in mitigating current threats. Using a hypothetical facility for the workshop allows for detailed analysis in a non-sensitive environment. Special thanks to the China's CAEA and CIAE for working so enthusiastically with NNSA to advance the state of the art in this important area.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.