Addressing the Insider Threat Through the Use of a Real Time Personnel and Material Tracking System

Amado A. Trujillo

Division 5245-Sandia National Laboratories*
Albuquerque, New Mexico 87185-5800

SAND--89-1409C

DE89 013258

ABSTRACT

Past experience in addressing the insider threat has led to the development of general principles for mitigating the insider threat while minimizing adverse impacts on site operations. Among the general principles developed was the requirement for real time tracking of personnel and material. A real time system for personnel and material tracking will aid in mitigating the insider threat by providing critical information regarding the movement and location of personnel and material. In addition, this system can provide an early detection mechanism for potential insider actions. This paper describes the development, operation, and performance of a technology-based system which utilizes radio frequency transmitters to achieve the real time tracking of personnel and material. The major elements of this system are a personnel tracking credential which cannot be removed from an authorized individual without an alarm being sounded, and a material control device which is utilized to control and monitor access to material. These elements form an insider protection system through the use of software which establishes the "rules" under which the system will operate. The performance of this system has been evaluated under both laboratory and operational settings in order to: 1) demonstrate the system's ability to successfully control access to material and areas by personnel, and 2) provide information regarding the status of materials in transit and storage.

INTRODUCTION

There exists a requirement in the nuclear industry to protect against the "Insider" threat. The insider is defined as any individual who has authorized access to facility protected areas. As a result, the insider has the potential for accessing all areas, equipment, material, and information at a nuclear facility. The traditional application of barriers, sensors, and alarms to protect material are much less effective for the insider than for the outside adversary.

*This work was supported by the U.S. Department of Energy under Contract DE-AC04-76DP00789.

Sandia National Laboratories (SNL) is involved in a number of programs whose purpose is to investigate the insider threat and develop technology which can be used to mitigate this threat. These programs have resulted in the development of insider general principles. Two of the most important principles for mitigating this threat involve the real time tracking of personnel and the real time tracking of material.

Based on these two principles, a conceptual design which would allow implementation of the principles at an actual site was developed. Because the system would be used in an operational setting, it was important that the design of the system incorporate features which would result in minimum impact on site operations.

A description of the system, as well as the results of evaluations of elements of the Personnel and Material Tracking System (PMTS) in a number of operational settings, are presented in the following sections.

PERSONNEL TRACKING

One element of an insider protection system is real time tracking of personnel within a facility[1]. A promising concept for personnel tracking consists of an unobtrusive credential which is worn by the employee and is continuously interrogated to provide real time information regarding the employees' access authorization and location. The use of a credential is appealing since employees at nuclear facilities already employ a credential for the purposes of either identification (badge) or safety (dosimeter).

Johnson Engineering Corporation; Boulder, CO; developed a real time personnel tracking system under a contract awarded by SNL. The tracking

---

system was designed to accomplish three major tasks: 1) track the movement and location of personnel within the facility, 2) protect against procedural violations such as removing or exchanging credentials used for identification, and 3) monitor any violations of two-person rules in sensitive areas and during material transfers. The system was developed for use in nuclear facilities or other high security areas.

The credential utilizes a proximity credential, manufactured by Eureka Systems, Inc., of Englewood Cliffs, NJ, to identify and track personnel. Protection of the credential is achieved through the use of an RF transmitter which is included in the credential package. The protection function is implemented using a fiber optic loop which doubles as a neckband. The length of the fiber optic loop is set so the loop cannot be removed without disconnecting the connector or cutting the fiber optic loop. Tampering or removal, by disconnecting or cutting the loop, interrupts an optical pulse train which leads to the transmission of an RF alarm signal.

The computer software has been designed to update the tracking environment as personnel move between the various detection locations and areas. Violations are reported for unauthorized movements, procedure violations, or tamper conditions. In addition, a detailed system log is generated showing all movements and violations as they are detected.

The personnel tracking system software is designed to be easily configured to any site's physical layout or organization. Graph and set theory are used to achieve this degree of functionality.

MATERIAL TRACKING

Material tracking was achieved through the use of proximity tags and the Wireless Alarm Transmission of Container Handling (WATCH) system[2]. The proximity tags functioned in the same manner as was utilized for personnel tracking except no tamper protection for the tag was provided.

Sandia developed the WATCH system which monitors movement of discrete items, critical controls, or critical components. Item monitoring is intended to provide an early indication that a theft, diversion, or sabotage incident has been initiated by an insider. The items which could be monitored include cans of raw materials, finished weapon components, fuel assemblies, critical process controls, etc. The WATCH system provides both a routine state of health message as well as an immediate alarm if the undesired movement occurs. WATCH systems are being evaluated for container movement monitoring in both manual and automated vaults. The vault application not only detects insider-perpetrated incidents but also assists in providing continual surveillance of the material. The WATCH system consists of a number of remote, wireless sensor points that communicate with a central receiver/controller unit. These sensor points are designed to detect movement through the use of a sensor-transducer, such as a mercury switch or a bubble level. Authorized movements of items to which the WATCH sensors are attached are accomplished through the use of bar-code readers and specialized software which imposes very specific rules regarding the proper movement or transfer of these items.

OPERATIONAL TESTING OF PERSONNEL AND MATERIAL TRACKING SYSTEM

During the development of the PMTS agreements were reached with staff of Mason and Hanger-Silas Mason Co., Inc., the contractor who operates the Pantex Plant for the United States Department of Energy (DOE) to conduct an evaluation of the PMTS at the Pantex Plant under actual operational conditions. Installation of the complete system at the Pantex Plant took place in March 1988. Approximately six weeks of testing of the system was conducted at the Pantex Plant. More complete details of the testing program can be found in Reference 1. During the testing period, some difficulties were encountered with some of the equipment used in the system. However, once these difficulties were corrected, the system functioned as designed. Based on the results of this testing, upgrades involving many of the concepts involved in the PMTS have been undertaken at the Pantex Plant.

It should be noted that this program was intended to gather specific information regarding the concept of personnel and material tracking in an operational setting using state-of-the-art equipment. Since this was primarily a proof-of-principle test, a minimum effort was made at miniaturizing the credential. Most of the effort was involved in developing the capability of tracking personnel

using the credential and ensuring no one could remove the credential after it was attached to an individual without generating an alarm.

DEMONSTRATION TESTING OF PERSONNEL AND MATERIAL TRACKING SYSTEM

Based on the results from the operational testing of the system at the Pantex Plant, improvements in the system were undertaken. These improvements involved reduced size and increased performance of the personnel tracking credential, new antenna configurations which allow tracking and enforcement of two person and material control/movement rules at workstations, improved operational effectiveness, improved tracking software, and greatly enhanced visual representations of personnel and material movement and alarms.

Discussions with Rockwell International staff at the Rocky Flats Plant; Golden, CO; regarding the possibility of evaluating the improved system at their site were undertaken. Agreement was reached that a demonstration system would be set up which simulated the operations of an area at one of their facilities. Based on the results of the demonstration and funding availability, a decision would then be made regarding the installation and evaluation of the improved system at the Rocky Flats Plant. A contract was placed with Johnson Engineering Corporation to set up the demonstration facility which simulated the Rocky Flats facility, develop the software which represented the operational "rules" of the Rocky Flats facility, and conduct the demonstration program.

The objectives of the demonstration were to provide evaluation of the improved PMTS regarding door alarms, several levels of access authorization, control of material at workstations, and enforcement of procedures involving the movement and control of both personnel and material within the demonstration area. The demonstration area, shown in Figure 1, represents a room containing a double door (Location 1), a single door (Location 4), workstation A (Location 2), workstation B (Location 3), and a corridor containing six antenna positions (Locations 5 through 10). In addition, the demonstration had an entry/exit area and material transfer car which are not shown but are described in the sections which describe the operation of the demonstration PMTS.

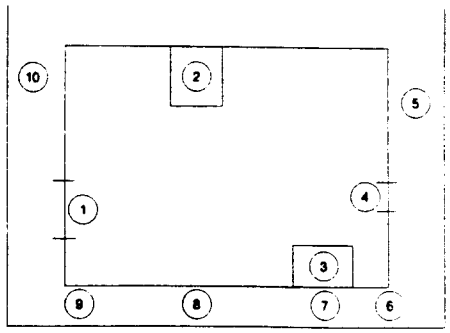

Figure 1 Demonstration Area

ELEMENTS OF DEMONSTRATION SYSTEM

The demonstration system consisted of a number of discrete elements which are described in this section.

Door Sensors - Door sensors were placed at each of the room doors - Locations 1 and 4. These sensors were balanced magnetic switch (BMS) sensors which were connected to WATCH transmitters. Whenever personnel opened a door, an alarm would be transmitted by the BMS/WATCH system. If the personnel were wearing an authorized credential, the alarm would be masked and not transmitted by the system software. If the personnel were wearing an unauthorized credential or not wearing any credential, the alarm would be transmitted by the system software and an appropriate response would be initiated.

Antenna Locations - The proximity tags are read at the discrete antenna locations within the demonstration area. Each of the door locations, Locations 1 and 4, has an antenna located on either side of the door to provide information regarding the direction of personnel travel either into or out of the room. Each of the workstations, Locations 2 and 3, has overhead antennas which read any proximity tag located in the area immediately around and on the workstation surface. The antennas located in the corridor, Locations 5 through 10, provide information regarding the movement of the transfer cart and material. A single antenna was located at the entry/exit location which was utilized during the personnel enrollment process. Two types of proximity tags were used in the demonstration - Eureka was previously mentioned as the tag used in the personnel tracking credential. The other tags were manufactured by Indala, Corporation; San Jose, CA; and

were used to track the material when it was moved in the transfer cart.

Bar Code Readers - Bar code readers were located at each of the workstations, Locations 2 and 3. The WATCH units controlling material movement at each of the workstations were activated and deactivated by means of the bar code readers. They were also used to enter material movement destinations. Bar code reads made at the various locations were transmitted to the computer via RF modems connected to the bar code system.

Positive Identity Verifier (PIV) - A PIV was utilized at the entry/exit location to perform a biometric verification which was compared with a badge read to ensure the proper credential was issued to the proper person and thereby result in proper personnel enrollment in the system.

Material Control Sensors - Three sensors were used to control material movement. The first was at workstation 2. At this location, the material was controlled by utilizing a four-legged platform which straddled the material and had a movement sensor WATCH on it. Personnel could work on the material by reaching between the legs. If they wanted to move the material from the workstation, they had to first move the platform which would alarm the WATCH movement sensor if the proper rules were not followed. The second sensor was located at workstation 3 and consisted of a contact switch which was connected to a WATCH transmitter. The material was placed on a fixture in a way which activated the switch when it was present. If the material was removed without observing the proper rules, an alarm was generated. The third material control sensor was associated with the material transfer cart. The cart is used to move material from one location to another. The material is placed into a box on the transfer cart for transport. A contact switch connected to a WATCH transmitter is located in a position such that it is activated when the lid is opened. If the box is opened and the proper rules are not observed, an alarm is generated.

DEMONSTRATION SYSTEM RULES

The demonstration PMTS was designed to enforce rules and procedures which represent the operation of the Rocky Flats facility being simulated.

Access Categories - The entry/exit area represents the area where credentials are issued and personnel are properly authorized to enter and move through the demonstration area. There were three categories of access utilized in the demonstration.

Category 1 - This individual can travel into any area, workstation, or part of the corridor alone.

Category 2 - This individual can travel into any area or part of the corridor alone. This individual can only be alone at a workstation for a limited time before an alarm is transmitted. If he is joined by another Category 1 or Category 2 individual or leaves the workstation before the time limit is exceeded, no alarm is transmitted.

Category 3 - This individual can travel into any area or part of the corridor alone. If this individual approaches a workstation, an immediate alarm is sounded.

Personnel Movement - Personnel credentials are issued at the entry/exit location and personnel/credential matching is achieved through the use of the PIV/credential read system. Once the individual has been properly registered in the system, he can move through the demonstration area and will be identified and tracked each time his credential passes an antenna location. Alarms are only generated if the individual attempts to access areas which are not authorized by his category of access or if he violates the two-person rule.

Material Movement - There are a number of rules associated with the transfer of material. Material can be transferred from one workstation to another or from either workstation to a location outside the room. In order to make an authorized movement from a workstation, there must be two authorized personnel at the workstation location. One of the individuals reads the bar code on the WATCH unit which controls the material in order to deactivate the WATCH alarm and allow material movement. The material is then moved into the box on the transfer cart; the box lid is closed; and the WATCH on the cart is read, activating the WATCH controlling the lid movement. The bar code indicating the cart destination is then read and a software clock is

started that will alarm the system if the material is not deposited at that destination in the time specified by the software. In addition, if the cart is moving outside the room into the corridor, the cart cannot move to antenna locations 5 or 10 or an alarm will sound. The system rules specify that the cart can only travel in a direction which takes it along the corridor where antenna locations 6 through 9 are located.

DEMONSTRATION SYSTEM EVALUATION

An improved demonstration PMTS has been evaluated. The demonstration system functioned as designed. The system demonstrated the capability for 1) enforcing rules and procedures controlling the movement of personnel and material, 2) controlling access to material and areas, 3) minimizing operational personnel actions, and 4) improved tracking and material movement visualization.

Another application of the material tracking and control elements of the PMTS is described in another paper being presented at this meeting.[3] This application is a cooperative program between Argonne National Laboratories-West (ANL-W); Idaho Falls, Idaho; Los Alamos National Laboratory (LANL), and SNL. This program involves the SNL WATCH unit for material control and tracking, a Los Alamos provided material accounting (PC-DYMAC) system, both operating at the ANL-W facility.

An additional application of this system is to the monitoring of personnel during emergency evacuations. While this is a safety, rather than a security, application, the system can provide this additional capability.

Discussions are continuing with a number of facilities regarding the installation of all or portions of the demonstration system for operational evaluation.

REFERENCES

1. Trujillo, A. A., C. E. Hoover, B. A. Garcia. (June 1988). Evaluation of a Real-Time Personnel and Material Tracking System. Proceedings of the 29th Annual INMM Meeting, pp. 783-788.

2. Sanderson, S. N. (July 1987). WATCH-A Low Cost, Secure-Item Monitoring System. Proceedings of the 28th Annual INMM Meeting, pp. 310-315.

3. Roybal, J. A., B. A. Garcia. (July 1989). Development and Integration of a Material Monitoring/Tracking System at ANL-W. 30th Annual INMM Meeting.