SAND2020-0738C

RADIOLOGICAL MATERIAL SECURITY IN LARGE PANORAMIC IRRADIATORS: *Lessons Learned*

MARTIN SANDOVAL
Sandia National Laboratories
Albuquerque, NM USA
Email: mwsando@sandia.gov

MARK BAUMANN
Sandia National Laboratories
Albuquerque, NM USA

Abstract

Large Panoramic Irradiators (LPI) are widely used to sterilize medical supplies, food products, spices, cosmetics, and other consumable goods. LPIs typically use a large array of cobalt-60 (Co-60) sources to expose the products to gamma radiation. Co-60 is desirable to terrorist and criminal organizations that are interested in developing a radiological dispersal device (RDD) or radiological exposure device (RED). It is often believed that the LPI Co-60 provides an adequate level of self-protection because of the large radiation dose associated with the source array. This is not true in all scenarios and operational conditions. One typical LPI site with a one-source pool may contain millions of curies (Ci) of cobalt. Approximately 50 commercial irradiators are in operation in the United States and over 200 are in operation worldwide. The United States Department of Energy National Nuclear Security Administration's Office of Radiological Security (ORS) is collaborating with LPI facilities to protect Co-60 with the goal of preventing the unwanted removal and misuse of the source material.

This paper will focus on the efforts by ORS to protect LPI sites from a successful theft of Co-60 and will include key lessons learned. These efforts include improving the performance of detection and delay systems to provide local law enforcement the ability to respond to an attack on the facility in a timely manner to prevent the removal of the source material. The protection strategy is to develop continuous and balanced layers of security measures. This objective is achieved through security upgrades to access control, intrusion and detection systems, and delay features.

ORS is currently working with several LPI industrial partners to implement the protection strategy. ORS worked with LPI partners over several years to develop a mutually acceptable base-line design and implementation process. The design is based on facility assessments, system analysis, component testing, and prudent security practices. For each facility, ORS and partners consider the operational aspects of each facility to develop protection enhancements that minimize any impact to efficiency and effectiveness of the LPI production process.

1. INTRODUCTION

Large panoramic irradiators (LPI) are widely used to sterilize medical supplies, food products, spices, cosmetics, and other consumable goods. These Irradiators typically use a larger array of cobalt-60 (Co-60) sources to expose the products to gamma radiation. Co-60 is also sought after by terrorist and criminal organizations that are interested in developing a radiological dispersal device or radiological exposure device. The source pool of a typical LPI site may contain millions of curies of Co-60. It is often believed that the LPI Co-60 provides an adequate level of self-protection because of the large radiation dose associated with the source array. However, this is not true in all scenarios and operational conditions.

This document provides concepts for improving security at a typical LPI facility. The focus is on improving the performance of detection and delay systems to provide local law enforcement the ability to respond to an attack on the facility in a timely manner and prevent the removal of the source material. The protection strategy is to develop continuous and balanced layers of security measures. This objective is achieved through security upgrades to access

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

control, intrusion and detection systems, delay features, and adequate law enforcement response. Operational aspects of the facility are considered to minimize the impact on efficiency and production. Both engineered controls and procedural controls are presented for consideration, but in most cases the controls work together to enhance the security and minimize operational impact. Most of the enhancements work together as a system. For example, a proximity card reader is used in conjunction with an electronic lock and contact switch to unlock a door and shunt the intrusion alarm to allow authorized personnel access to a room.

The typical LPI security enhancements greatly increase the overall security posture of the facility. This work will present considerations and challenges associated with developing a security system for an LPI that is operational 24 hours per day, 7 days per week. Although response is a critical security system element, it will not be specifically addressed in this paper since its implementation varies widely by location. The following sections of this paper provides examples of potential security upgrades for an LPI type facility.

2. RADIOACTIVE SOURCES OF CONCERN

The goal of a terrorist organization in obtaining radiological material can be to develop a Radiological Dispersal Device (RDD) or Radiological Exposure Device (RED). These unconventional weapons could be used to disperse radiological material that would increase the levels of radiation in an area. The dispersal could be confined to a small area intended to expose a specific population or could be widespread intended to contaminate a large area, which would require an extensive clean-up effort before the area could be safely inhabited.

Although several radionuclide source materials are utilized at LPI and industrial facilities, studies have shown that the most common and the ones that pose the greatest potential security risk are cesium-137 and cobalt-60. Cobalt-60 is the most widely used source material in LPI operations. The activity level of these sources is an important aspect to consider. The International Atomic Energy Agency (IAEA) has established a threshold for the categorization of radioactive sources.

3. SECURITY OVERVIEW

Because of the potential to use the radioactive source material for an RDD or RED, the LPI facility should be properly protected to prevent the removal of the source material from the facility. The LPI security system should have a high probability of detecting an attempted attack on the source material and delay the removal of the source material while minimizing disruption of authorized access to the irradiator for legitimate purposes. An appropriate effort by a capable response force is critical to the overall security system effectiveness.

Threats to an LPI irradiator range from an opportunistic criminal to a sophisticated, organized terrorist organization. Government facilities and private enterprises have been the target of extremist groups who expressed their distain with government policy or a company product in violent ways. Terrorist organizations have carried out unconventional warfare on several facilities throughout the world. The numbers of participants and complexity of weapons can range from a single individual with limited tools to a well-funded terrorist organization with multiple attackers and sophisticated tools and weapons that include explosives. The more aggressive organizations will likely use an insider who has knowledge of the security system.

The protection concepts presented in this paper will focus on the theft of material through an overt attack by an outside organization with limited knowledge of the security system. Insider knowledge and sabotage-in-place are beyond the scope of the security system presented in this paper. Many security system elements that influence an overt attack will also have a positive security effect on a covert insider attack and a sabotage attack.

An effective LPI security system must include detection, delay, and response, and should strive to achieve balanced and layered protection. The following sections provides details of these concepts.

3.1. Detection – Delay – Response

3.1.1. Detection

Detection is the discovery of an adversary's action. This should be achieved early in the attack cycle. Detection is typically accomplished by stimulating a sensor, which generates an alarm that is reported to an alarm monitoring location. Effective detection also includes alarm assessment. Assessment is the process of determining whether an alarm activation is due to an adversary's action or is caused by an inadvertent action. A true alarm is the first indication that an attack is underway. People can perform the detection and assessment function, but studies have shown people are easily distracted and, over time, make poor detectors.

3.1.2. Delay

Delay is intended to slow the adversary along the path to the intended target or at the target itself. Examples of delay elements include barriers, locks, grates, *etc*. To be effective, delay elements must be placed after detection. Ideally an adversary would be detected and then they would be slowed advancing to the target. This gives responders (police) time to reach the facility and interrupt and stop an attack.

Placing delay before detection can be a waste of security resources. With no detection, a delay element, such as a grate or bars on a window, can be cut and removed without anyone noticing (particularly after hours). Such delay elements can deter unsophisticated adversaries but, in general, provide no impediment to determined persons.

Access control is sub-set of delay and detection. It is a security element that controls which persons have access to a room or space. An example is a locked door with only selected persons having a key. Ideally only those persons with a key can enter a room. Electronic access controls are systems that perform the same function as a key. Only persons with a proper badge or proper code are allowed access into a room. Generally, electronic systems are more secure than mechanical key locks since keys can be acquired by unauthorized persons. Electronic access control, while more complex, uses badges and codes [i.e., card reader and personal identification number (PIN)] as the 'key' to gain access. Also, biometric access control devices are available that use fingerprints or iris patterns to grant access to specific individuals. Limiting access to radioactive sources to authorized personnel can enhance overall security.

Access control systems can also be used to deactivate, or shunt, a detection element such as a contact switch on the door being entered.

3.1.3. Response

Response is the human element that is used to interrupt and stop an adversary's actions. This is usually performed by armed guards or police. Note that in all cases a good response requires an appropriate number of responders with appropriate weapons to stop an adversary. This subject will not be covered in the security system designs presented in this paper because of the special intricacies associated with jurisdictional authority and localized tactical procedures.

3.2. Continuous and Balanced Protection

Continuous and balanced protection refers to all elements of the security system being equally difficult to defeat with no gaps in coverage. Detection is consistent with no gaps in detection, and delay is the same no matter how an adversary enters an area. Balanced protection means there are no alternative means of entry that provide an adversary any advantage. Good security designs call for balanced protection.

It is rarely possible to get complete balanced protection due to specific site conditions. For example, consider a room that has three concrete walls, but the front wall is standard stud and wallboard construction with a single door. Obviously, the breaching delay for this room varies depending on which wall is breached. The stud wall would be much easier to break through, and the door is likely even easier to forced open. In such cases, additional physical

barriers could be added to the stud wall (example: metal mesh) and the door replaced with a solid core door. Also, sensors could be installed to detect breaching of the softer wall and the door. Since in this case there is not equivalent delay through all adversary paths, a successful security design would increase the detection and delay on the front wall and door. All three security elements need to be considered to achieve a balanced system.

3.3. Layers of Protection

Layers of protection (also referred to as protection-in-depth) is the use of multiple levels of continuous and balanced security elements in an adversary's path to a target or attack goal. For example, an adversary might have to tamper an access control system, then defeat a barrier, then avoid a sensor, and finally breach a delay device on the target before the objective can be accomplished. Each layer may not be equal, and the effectiveness may be quite different, but in general the layers should be more difficult to defeat or avoid closer to the target. Access through each layer should be granted only to individuals who have legitimate work-related activities in that specific area. The number of individuals who have access to the radioactive source should be limited to end users only. Others who have occasional need to access the source should be allowed access by authorized individuals and never be left by themselves at the target area. The security system should isolate the source from the other areas of the facility, and the security system of the facility should isolate it from the general public.

4. SECURITY OF LPI CONCEPTS AND LESSONS LEARNED

The security system design concepts for an LPI facility and source material can have unique elements or features to allow proper usage without significantly interfering with facility operations and product movement. The following sections describe security elements that should be considered in the development of an LPI specific design.

4.1 Intrusion Detection and Assessment

4.1.1. Intrusion Sensors

In addition to the BMS on the control room door, volumetric motion sensors should be positioned to detect a breach of the door surface, walls, windows, and ceiling in the control room. The motion sensor should be a high-security dual/tri technology (Passive Infra-Red (PIR) + Microwave + anti- masking). Duress button/switches should be located in the control room where site personnel are typical located and pressed in the event of an intrusion. The duress button/switch should be resistant to accidental triggering.

Lesson Learned: It is critical to apply layers of protection beyond the control room / source containment boundary entry points. Focussing on detection at the outer layers and more delay closer to the target area.

4.1.2. Source Containment Boundary and Product Carrier Entry Points

BMSs should be mounted on the source containment product entry doors. Pressure pads, independent of the safety system, should be positioned inside the source containment boundary entrances. Implementation of these security elements will be dependent on the configuration of the irradiator, source containment, and control room. In most cases the detection sensors within the source containment would only be activated when the source rack is in the down position or no personnel are present on site.

Lesson Learned: Every LPI facility has slight differences in configuration, particularly the product carrier types and source containment arrangement. The security system needs to accommodate the specific operational configuration of the specific facility.

4.1.3. Assessment Cameras

Assessment cameras should be located in the control room and outer source containment boundary area to assess the situation if an alarm is generated by any sensor (duress PIN, BMS, motion sensor, duress button, or pressure pad). The cameras should be in a fixed position and focused on a specific area associated with a sensor to quickly assess the alarm events. The camera should have built-in infrared illumination to allow viewing in the dark and should be able to detect loss of video and generate an alarm, also known as video presence detection.

Lesson Learned: Because of the radiation environment when the source is out of the pool in the source containment boundary area, assessment cameras should be located near the entry into the source containment boundary were the radiation levels are lower.

4.1.4. Radiation Detection

Radiation sensors, for detecting the removal of source material from the source containment, should be installed near the exit points of the source containment boundary. The radiation sensor in this scenario is not truly part of the intrusion detection system, because it not detecting an intrusion prior to an adversary's source removal tasks. In this configuration, the radiation sensor provides positive evidence that source material has been removed from the source containment area. Ideally the radiation sensor would be incorporated in an independent stand-alone security system that is capable of detecting, assessing, and reporting radiation alarms.

Lesson Learned: Similar to the assessment camera issue, the radiation sensor should be located outside the high radiation area to avoid false alarms from the background radiation.

4.2. Delay, Structural Elements, and Access Control

4.2.1. Control Room Door Access Control

A proximity card reader should be used to gain access to the control room. Two-factor proximity reader with Personal Identification Number (PIN) readers provide better security and should be used when possible. Authorized site personnel should be able to gain entry to the control room by presenting their badge to a proximity card reader. When access is granted, the door will unlock, and the door contact sensor will be shunted for a short period of time. If a two-factor access control system is used, a silent duress function can be triggered by entering a special code instead of the PIN. To exit the control room, site personnel should use the door handle to mechanically disengage the lock. The handle should have a built-in Request to Exit (REX) function. The REX will mask the door contact upon exit to prevent generating a door alarm. The door contact should be re-enabled upon door closure. Electronic strike locks are preferred over magnetic locks. An override key should be located on site in a secure location, preferably a high security safe. The key should be used for emergency purposes only. To complete the access control system on the control room door, a contact switch will be required to activate an alarm if the door is forced open or held open longer than a prescribed amount of time. The contact should be mounted on the secure side of the door and be a triple-biased Balanced Magnetic Switch (BMS).

Lessons Learned: The control room door is often accessible to all facility staff. It is imperative that access to the control room be limited to essential personnel only.

4.3.4. 4.2.2. Source Containment Boundary Access Control

Two-factor (Proximity card reader with PIN) should be used on the source containment boundary entry room door. Biometrics (fingerprint or facial recognition) and PIN readers provide better security and should be used when possible. This system should operate the same as the control room door with the addition of two-person controls. Two-person control requires two individuals enter their unique credentials into the access control system before access is granted through the source containment boundary entry door.

Lesson Learned: Biometric access controls have been resisted by some LPI facility personnel because of the perceived complications and additional time required to access a room. After installation and operation for a few weeks, the facility staff have accepted the biometric access controls. It does take a little additional time to access a room, but with practice and regular use it is minimized.

Two-person access controls can be difficult to implement because of personnel restrictions. One way to accommodate this to utilize a mobile app that will allow a second person to authorize access remotely.

4.2.3 Large Openings

Openings greater than 96 in^2 in the control room and source containment boundary should be covered with grates or expanded metal mesh.

Doors should be solid-core or steel-clad doors. Doors should have a mechanical door closer, security astragal (bolt pry protection), and security hinges to prevent hinge pins from being removed.

Lesson Learned: All nonessential large openings should be eliminated by covering with material similar to the surrounding surfaces to provide balanced protection.

4.2.4 Cages

A cage to house the source removal tools should be constructed. The cage should include a steel tube frame, solid steel bars on 6-inch centers attached to the frame and expanded metal mesh attached to the outside of steel bars. The frame should cover all sides except the floor. Doors should have a security astragal (bolt pry protection), and security hinges to prevent hinge pins from being removed. High security shrouded pad locks should be used to secure any doors.

Lesson Learned: A cost effective option to designing and manufacturing a cage is to use a commercial vault/safe. The size of the vault/safe needs to accommodate all critical source manipulation tool, if stored on site.

4.2.5. Alarm and Video Communications

Spaces that contain Information Technology (IT) related infrastructure directly supporting security enhancements should be protected by a means of single-factor automated access control, intrusion detection at the point(s) of entry, alarm panel tamper switches, and video assessment of the alarm points.

Lesson Learned: If practical, all IT infrastructure should be collocated and positioned in a space that is already protected.

4.2.6. Alarm Monitoring

Alarms should be monitored and assessed on-site 24-hours/day, 7-days a week. The alarm monitoring space should include single-factor access control and appropriate hardening of all walls and windows.

Lesson Learned: It is not always practical, or feasible, to perform alarm monitoring on-site. If this is the case, an off-site alarm monitoring company should be contracted to perform the alarm monitoring function. All responsible monitoring alarm dispatchers should pass a criminal background check.

5. SUMMARY

Basic security concepts that apply detection, delay, and response can be used at LPI facilities to effectively secure the irradiator. Some operational aspects may have to be adjusted to accommodate the security system, but nothing that will severely affect the process flow in the LPI facility. This paper provides security concepts to improve the security of an LPI facility and irradiator. Lessons learned are provided to address unique LPI security system applications.

ACKNOWLEDGEMENTS

This work was funded by the United States of America's Department of Energy, National Nuclear Security Administration, Office of Radiological Security.

This work was performed at Sandia National Laboratories. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525