



LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Physical Protection at Non-Reactor Facilities

M. O'Brien

October 12, 2012

India-U.S. Cooperation on global Security: A Workshop on
Technical Aspects of Civilian Nuclear Security
Bangalore, India
October 28, 2012 through November 1, 2012

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.

Physical Protection at Non-Reactor Facilities

Author: Michael O'Brien, Lawrence Livermore National Laboratory

Introduction

Protection of nuclear facilities has evolved over many decades. This evolution has been necessitated by advances in technologies as well as the need to adapt to a changing threat. The U.S. Department of Energy National Nuclear Security Administration (DOE-NNSA) maintains facilities of the highest consequence of risk due to the types of nuclear materials in storage or in use. These facilities require the highest level of security. This paper sets forth standard protection philosophies found in the U.S. and throughout the world. While the paper will use DOE-NNSA as a basis, a vast number of nuclear facilities world-wide use International Atomic Energy Agency Guide INFCIRC 225 rev5 as their principle guidance. While the protection philosophies are similar, one would expect the rigor of DOE-NNSA protection implementation to be at a higher level due to the types of nuclear materials its facilities possesses.

Protection Planning

Nuclear facility physical protection should be based on a defined threat. This threat and the characteristics of the threat are defined at the government level. The facility physical protection system would be expected to adequately address sabotage and theft attempts by adversaries defined in threat guidance and therefore requires development of appropriate protection strategies and proper implementation.

Threat

Threat guidance, generally referred to as a Defined Basis Threat (DBT), describes the number and attributes of adversaries. A common DBT would define a group of outsider (those with no authorized facility access) adversaries and one or more insider (those with authorized facility access) adversaries. In addition it might be expected that the outside group would collude with an insider. The capabilities of the adversaries would also be defined in terms of their knowledge, skills, weaponry, and equipment.

Protection Philosophy

Nuclear facilities should be designed to allow for *redundancy* and *defense in depth* in the protection system to avoid single point failure points and force the adversaries to defeat several protection elements in order to achieve their intended task. An example of this would be a secondary alarm station in lieu of only one central alarm station. In addition, complimentary sensors can be deployed in a way to increase the difficulty of an adversary defeating detection in lieu of deploying a single sensor technology. The facility layout may also be designed in a way to afford a *layered or graded protection* approach

Physical Protection at Non-Reactor Facilities

in which protection measures increase closer to target locations. This is common for entry control points whereas the level and type of access authentication and search measures may increase as one enters technical areas of a higher security level located within technical areas of a lower security level.

Protection Objectives

A protection system may encompass several principle objectives. These may include protection against:

- theft by outsider and/or insider adversaries,
- sabotage by outsider and/or insider adversaries, or
- cyber attacks

The combination of protection systems and protective force deployment must effectively mitigate each of these threats. This deployment may require the implementation of multiple strategies.

Protection Strategies

Strategies are specific to the type of threat.

- **Containment**- A containment strategy is used for protection against theft of nuclear material. This is achieved through use of appropriate detection, delay, assessment and response capabilities. Protective force assets should be able to respond in time to interdict, contain and neutralize an outsider adversary force before completion of an attempted theft attempt.
- **Denial** - A denial strategy is used for protection against theft of nuclear material. This is achieved through use of appropriate detection, delay, assessment and response capabilities. Protective force assets should be able to respond in time to interdict, and neutralize an outsider adversary force prior to the adversary forces arrival at the target location thus denying their access to the location and their attempted sabotage attempt.
- **Insider** – An insider strategy encompasses some appropriate combination of separation of duties, limited access, limited responsibilities, compartmentalization, two person rule procedures, material surveillance, material controls and accountancy measures, as well as safety procedures and systems in order to increase the likelihood of detecting

Physical Protection at Non-Reactor Facilities

an insider attempt of theft or sabotage. A human reliability program may be administered to further enhance an insider protection program.

- **Cyber**- A cyber strategy encompasses analysis of electronic networks and the identification of appropriate electronic measures to detect network penetration attempts.

Protection System Design

A proper protection system design effectively integrates people, procedures and equipment to meet the objectives of the system. The PPS design must facilitate protection elements working together to assure protection rather than treating each single element separately. For example ensuring that fences, sensors, delay systems, closed circuit television assessment systems, procedures, communication systems, and protective force personnel act as an integrated system meeting protection objectives. The primary PPS functions are to *detect, delay, assess, and respond* to adversary actions. These functions are outlined below:

Intrusion Detection

Intrusion detection may consist of an array of technologies designed to detect penetration by an adversary. Some examples include:

Exterior/interior sensor technologies such as microwave, active or passive infrared, vibration, magnetic field, and electric field

Delay Systems

Delay systems decrease the adversary rate of ascent toward the target allowing an adequate number of protective force personnel to respond in time to stop a malevolent act. Some examples include:

Fences, walls, doors, structural enhancements, vehicle barriers, smoke or fog visual obscurants, entanglement systems,

Assessment Systems

Assessment systems aid in the visual verification of adversary actions. Some examples include:

Closed circuit television cameras, lighting systems, and posted or patrolling protective force personnel

Physical Protection at Non-Reactor Facilities

Protective Force Response

Protective force personnel provide the response actions to interdict and neutralize adversaries. The response force is generally comprised of:

Tactically trained primary responders, tactically trained secondary responders, posted or patrolling protective force personnel who augment the engagement by primary and secondary responders

Protection Integration

To achieve an appropriate level of system effectiveness, the entire protection system must operate in a complementary and integrated manner. This does not mean that protection elements have to be physically integrated but rather work in synergy to achieve the overall protection objective. Three noteworthy points of integration include 1) nuclear material controls which allow material accountancy and physical protection to work in a complimentary fashion, 2) protection systems and protective force which form the main core of the protection system, and 3) command and control system integrating physical protection systems as a single command center operated by a protective force.

Nuclear Material Controls

Nuclear material controls may include material surveillance systems, material tie-downs, and entry control measures such as nuclear detection portal monitors, metal detectors, vault alarm sensors, and electronic access control

Protection Systems and Protective Force

Physical protection systems provide the means for the protective force to detect, delay, and assess adversary actions allowing the response force to tactically engage the adversaries in a timely manner. When needed in situations of shortcomings, compensatory measures for and integrated system can be either physical protection system elements or protective force personnel

Command and Control

Integration of physical protection systems into a single alarm control and display unit with assessment, entry control and communication capability allows protective force personnel the ability to effectively operate the entire system for daily operations and in emergency situations such as adversary malevolent acts.

Physical Protection at Non-Reactor Facilities

Protection System Evaluation

Protection systems should be in a constant state of evaluation. This assures the system effectiveness can be validated and any shortcomings addressed in a timely manner. This is best implemented through a performance assurance program.

Performance Assurance Program

A performance assurance program is a means to collect and store system data in a single location. A system testing plan should define the manner and frequency system components are tested for functionality as well as performance against design criteria.

System Performance Testing

All critical systems and their critical elements should be regularly performance tested. These tests can be at the system level or component level. Test results should be documented and archived for use by system administrators, performance assurance program administrators and vulnerability analysts.

Protective Force Testing

Protective force personnel should be subject periodic testing to validate tactics, procedural compliance, and response times. Test results should be documented and archived for use by performance assurance program administrators and vulnerability analysts.

MC&A Testing

MC&A systems and their critical elements should be regularly performance tested. These tests can be at the system level or component level. Test results should be documented and archived for use by system administrators, performance assurance program administrators and vulnerability analysts.

Vulnerability Analysis

Vulnerability analyses and the documented system effectiveness level should be validated on an annual basis as well as when a change in operations or facility configuration occurs.

Physical Protection at Non-Reactor Facilities

Conclusion

In summary, nuclear facilities require the highest level of security due to the high consequence to the public if a malevolent act were to occur. Proper protection planning, design, and implementation approaches are well documented and shared within the global security community.

Prepared by LLNL under Contract DE-AC52-07NA27344.