SAND-77-0846C

DESIGN OF AN ENGINEERED SAFEGUARDS SYSTEM FOR A MIXED-OXIDE FUEL FABRICATION FACILITY*

A. E. Winblad, R. P. McKnight
W. C. Fienning, B. R. Fenchel

Advanced Facilities Protection Division
Sandia Laboratories, Albuquerque, New Mexico

June 1977

Abstract

Several Engineered Safeguards System concepts and designs are described that provide increased protection against a wide spectrum of adversary threats. An adversary sequence diagram that outlines all possible adversary paths through the safeguards elements in a mixed-oxide fuel fabrication facility is shown. An example of a critical adversary path is given.

Introduction

Improved safeguards systems that can counter the postulated threats to nuclear facilities are now feasible through applications of current and improved technology to physical protection, materials measurement and accounting systems, and facility designs. Adequate protection of special nuclear material (SNM) and vital systems from adversary activity is accomplished, with acceptable operational impact, by coordinating safeguards functions with plant design and operations to produce an effective safeguards system called an Engineered Safeguards System (ESS). The ESS development for a mixed-oxide fuel fabrication facility (MOFFF) is a joint effort by Sandia and Los Alamos Scientific Laboratories, and is part of a broad program sponsored by the Division of Safeguards and Security of the Energy Research and Development Administration.

The baseline facility used for this study was modeled after the Westinghouse Corporation Recycle Fuels Plant at Anderson, South Carolina (Ref. 1) for which license application

*This work was supported by the U.S. Energy Research and Development Administration.

was made. This facility would produce mixed-oxide fuel rods for light-water nuclear reactors. Powdered oxides of plutonium and uranium are received periodically and stored for a limited time. After the oxides are blended, the powdered mixture is formed into pellets, which are sintered, ground to the proper size, and loaded into fuel rods. The rods are inspected and tested and then stored until time for fuel assembly and shipment. This study used the baseline facility with no essential changes in the plant process flows.

Design Concepts

A safeguards system has four basic objectives:

- deterrence of potential adversary actions,
- detection of unauthorized activities and discrepancies,
- delay of unauthorized activities until appropriate response can be made,
- response to unauthorized activities and discrepancies in an adequate and timely manner.

To meet these objectives, two interactive safeguards systems are employed, the physical protection system and the materials measurement and accounting system. The physical protection system controls people and operations. The materials measurement and accounting system provides information on the locations and quantities of SNM in the facility. This information can be used for process and quality control as well as for safeguards.

The physical protection system has two subsystems, zone operations control, and access control both of which can detect and delay unauthorized activity and provide direct physical control to ensure the protection of SNM. Zone operations control is concerned with the operational interfaces among people, vital equipment, and SNM. Working in conjunction with the access control subsystem, it enables and monitors authorized plant activities, allows only those persons with requisite authorization into proximity of SNM, and permits them to perform only authorized activities, thereby preventing unauthorized actions that could result in theft or sabotage. Through an interface with the materials measurement and accounting system, it is apprised of material balance discrepancies and can initiate appropriate physical protection countermeasures. Access control enables and monitors authorized movements of people and SNM across barriers and regulates unauthorized movement of people, SNM, and contraband.

All operations and access activities involving SNM or vital equipment are directed by control elements that enforce closed-loop control. A detailed and thorough access and operational control analysis of the facility is made to determine those closed-loop controls that are required to ensure adequate protection during plant activities. Both the access and operation control elements are implemented by using monitor and actuation elements at the activity site and information processing and decision logic in a central control system. The computer logic compares the measured information with a standard of authorized activity, and if a deviation is detected, appropriate action is prescribed. The standard is a description of the activity as a series of monitor signals corresponding to those steps that are necessary for safeguards, an authorization permitting the activity, and other information such as the identification of operators and material items. The acceptance criteria for the monitor signals are as broad as possible, consistent with safeguards, to draw a proper balance between flexibility and control. When a discrepancy is discovered, direct physical control measures are initiated to restore adequate protection.

Direct physical control involves a hierarchy of responses depending on the discrepancy detected between actions that are authorized and actions that are performed and on an assessment of the severity of the threat. For some discrepancies, the control function may be automated. Although temporary delays may occasionally be required to ensure proper safeguarding of SNM, adequate plant design to include buffer storage areas should minimize the impact. Serious discrepancies requiring more extensive disruption of operations or needing security force response would require decisions by safeguards coordination and plant operations.

The central responsibility for monitoring the safeguards system is assigned to the safeguards coordinator. The coordinator supervises operation of the safeguards systems and coordinates the flow of safeguards information among the safeguards systems, management, and plant operations.

To aid in controlling personnel, the facility is divided into zones. These zones are defined by combining contiguous material access or vital areas that have common protection requirements. Only personnel essential to operations within a zone are authorized to enter.

The materials measurement and accounting system gathers and processes information concerning SNM in the facility. It provides near real-time information to the physical protection system on both long-term diversion and short-term theft. The appropriate measurement equipment in each area and a computerized data processing system enable calculation of material balances at frequent intervals to permit rapid detection of discrepancies.

When it appears that material may be lost or stolen, the physical protection system can take appropriate actions--such as a sweep of the facility to locate cached material or more stringent searching of personnel and monitoring of vehicles. Detection of loss at the point where the theft actually occurs can facilitate identification of the suspects, increase deterrence, and increase the time for the security force to respond. The closing of the material balance provides a verification that the Engineered Safeguards System is performing its function of protection. The Los Alamos Scientific Laboratory is developing the materials measurement and accounting system for this representative facility.

Design Evaluation

A preliminary evaluation of the relative effectiveness of the ESS facilities was made using the analytical approach and computerized simulation models described in the Sandia Laboratories paper "Safeguards System Design Methodology" by M. N. Cravens and A. E. Winblad also presented at this conference.

The evaluation begins with an adversary sequence diagram. A diagram is shown in Figure 1 for a typical facility design. This diagram provides a geometrical representation of the complete physical protection system for the entire facility, with rectangles representing areas, and lines representing barriers and detection elements that the adversary may encounter in passing from one area to another. Access control and zone-operations control elements are located within the areas to provide the required overall detection and delay capability.

A single logic equation whose terms represent the detection and delay elements is derived directly from the adversary sequence diagram. This equation, a portion of which is shown in Table I, defines all possible adversary paths including stealth, deceit, and forcible modes of attack. The numbers in the logic equation refer to the areas in the adversary sequence diagram. The S prefix refers to stealth or deceit, and the F prefix refers to force. Terms are combined using the symbol "*" for "AND" and "+" for "OR," and by substitution of term identities. Fault-tree analysis provides estimates of detection probabilities and delay times that are assigned to each term, based on the particular facility design option and the methods of attack used by the adversary. As the adversary advances through the path, the probability of detection increases while the delay time remaining to complete the path decreases. A safeguards criterion is established requiring a specified cumulative probability of detection before the delay time remaining becomes too short for guard force response. Any path which fails to meet this criterion is termed a critical path. Through computer analysis of the logic

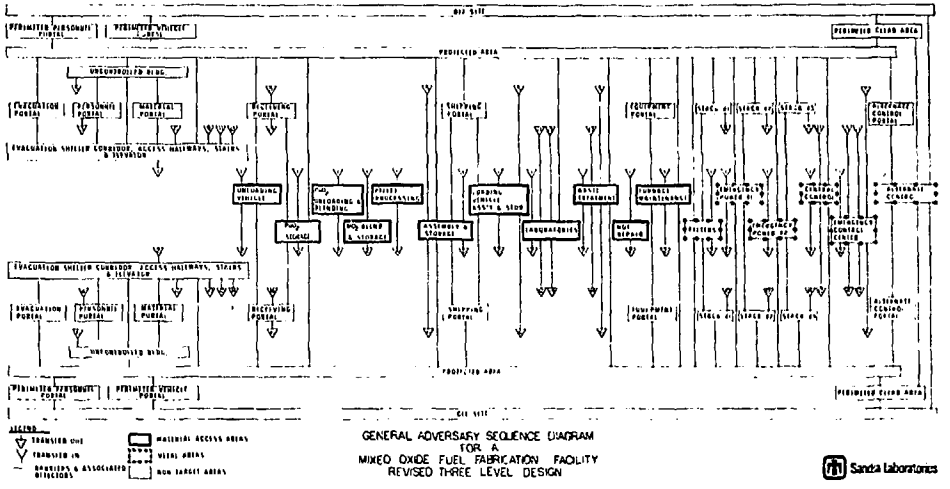

GENERAL ADVERSARY SEQUENCE DIAGRAM
FOR A
MIXED OXIDE FUEL FABRICATION FACILITY
REVISED THREE LEVEL DESIGN
Sandia Laboratories

FIGURE 1

TABLE I - PARTIAL BOOLEAN EQUATION FOR THE MOFFF ADVERSARY SEQUENCE DIAGRAM

STEALTH OR DECEIT TERMS

```
S100-=S000-0000-*S000-S100-.
S133-=S000-0000-*S000-S133-.
S166-=S000-0000-*S000-S166-.
S200-=S100-*S100-S200-+
      S133-*S133-S200-+
      S166-*S166-S200-.
S300-=S200-*S200-S300-.
S325-=S200-*S200-S325-.
S350-=S200-*S200-S350-.
S375-=S200-*S200-S375-.
S400-=S200-*S200-S400-.
S414-=S300-*S300-S414-.
S428-=S300-*S300-S428-.
S442-=S200-*S200-S442-+S300-*S300-S442-.
S456-=S200-*S200-S456-.
S470-=S200-*S200-S470-.
S484-=S200-*S200-S484-.
S500-=S200-*S200-S500-+S300-*S300-S500-+
      S325-*S325-S500-+S350-*S350-S500-+
      S375-*S375-S500-+S400-*S400-S500-+
      S414-*S414-S500-+
      S428-*S428-S500-+
      S442-*S442-S500-.
```

FORCE TERMS

```
F100-=S000-0000-*F000-F100-.
F133-=S000-0000-*F000-F133-.
F166-=S000-0000-*F000-F166-.
F200-=(S100-+F100-)*F100-F200-+
      (S133-+F133-)*F133-F200-+
      (S166-+F166-)*F166-F200-.
F300-=(S200-+F200-)*F200-F300-.
F325-=(S200-+F200-)*F200-F325-.
F350-=(S200-+F200-)*F200-F350-.
F375-=(S200-+F200-)*F200-F375-.
F400-=(S200-+F200-)*F200-F400-.
F414-=(S300-+F300-)*F300-F414-.
F428-=(S300-+F300-)*F300-F428-.
F442-=(S200-+F200-)*F200-F442-+(S300-+F300-)*F300-F442-.
F456-=(S200-+F200-)*F200-F456-.
F470-=(S200-+F200-)*F200-F470-.
F484-=(S200-+F200-)*F200-F484-.
F500-=(S200-+F200-)*F200-F500-+(S300-+F300-)*F300-F500-+
      (S325-+F325-)*F325-F500-+(S350-+F350-)*F350-F500-+
      (S375-+F375-)*F375-F500-+(S400-+F400-)*F400-F500-+
      (S414-+F414-)*F414-F500-+
      (S428-+F428-)*F428-F500-+
      (S442-+F442-)*F442-F500-.
```

equation, all critical paths can be located (Refs. 2 and 3). Through an iterative process, the critical paths for a particular ESS configuration can be eliminated by modifying the detection and delay elements or by changing guard responses and capabilities.

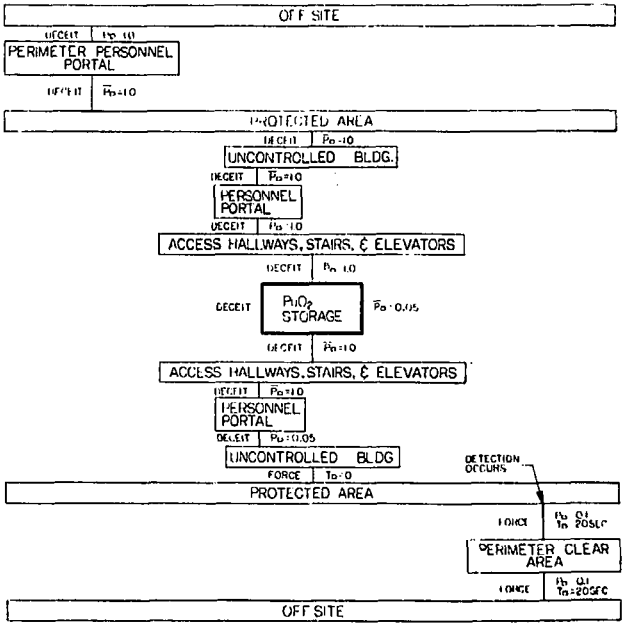
Figure 2 shows an example of a single critical path through the adversary sequence diagram of Figure 1. In this hypothetical example a single insider, such as the vault custodian, attempts theft of SNM from the plutonium storage area. This adversary has access to the plutonium vault, and in the baseline facility he can obtain a canister of plutonium with no probability of detection. Having thus obtained the SNM, he leaves the material access area, attempting to avoid or defeat monitoring by his co-workers and the SNM detection elements in the portal from the area. If these two elements are assumed to each have a detection failure rate of 0.05, then the probability that the adversary would not be detected before he leaves the building is 0.0025. In this example, detection occurs just prior to reaching the perimeter, and a 40-second delay remains for the adversary to forcibly penetrate the perimeter fences. If the safeguards criterion requires that the probability of non-detection is no greater than 0.001 and that the time delay after detection is at least 100 seconds, this is a critical path. This path might be made non-critical by incorporating a closed-loop control element in the storage area that would increase detection of unauthorized activities and delay acquisition of the stored material. For example, a heavy, monitored lid that requires a crane for removal could be placed over the storage cubicle. The crane could be centrally controlled so that material could not be moved without the appropriate authorization and monitoring.

After sufficient detection and delay level requirements have been established for the safeguards hardware portion of the ESS, the protection capabilities of the on-site and off-site response forces must be evaluated against a spectrum of threats. Guard deployment and adversary confrontation scenarios are examined using two dynamic simulation models, the Forcible Entry Safeguards Effectiveness Model (Ref. 4) and the Insider Safeguards Effectiveness Model (Ref. 5). The criterion for the relative effectiveness of the designs is the probability of preventing adversary theft or sabotage sequence completion.

Facility Descriptions

Several ESS configurations were produced using the design approach above and the following criteria:

- centralized closed-loop control of significant activities,
- near real-time measurement and accounting of nuclear material,



$\bar{P}_D$ — PROBABILITY OF ADVERSARY NOT BEING DETECTED

T_D BARRIER DELAY TIME.

PATH EVALUATION

PERFORMANCE MEASURE	DESIGNATED SAFEGUARD REQUIREMENT	CALCULATED PATH RESULTS
CUMULATIVE $\bar{P}_D$	$\leq$ 0.001	0.0025
MINIMUM TIME DELAY	$\geq$ 100 SEC	40 SEC.

CRITICAL PATH FOR A SINGLE INSIDER THEFT ATTEMPT ON THE THREE-LEVEL MOFFF

Sandia Laboratories

FIGURE 2

- continuous verification of safeguards system performance,
- maximum isolation of personnel from SNM and vital equipment,
- minimum operational impact,
- minimum reliance on guards.

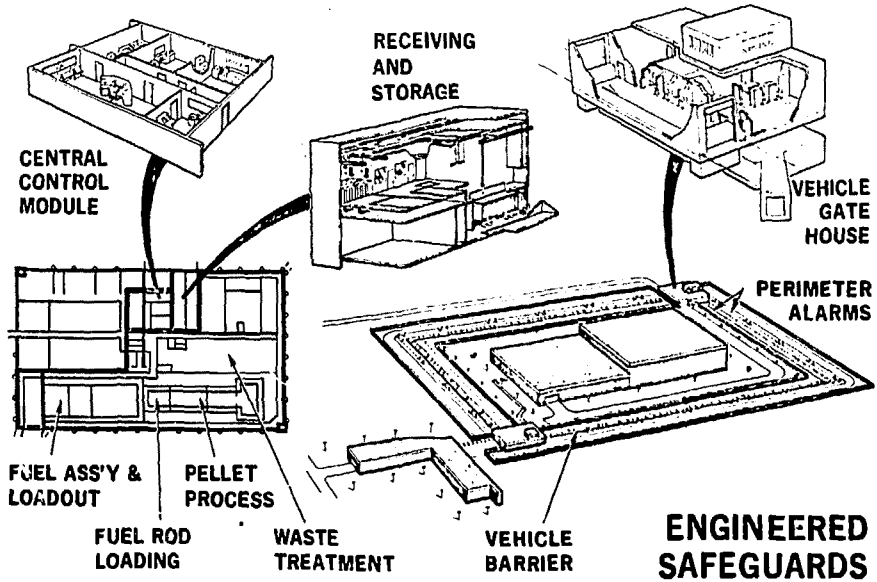
Figures 3, 4, and 5 illustrate some of the major features of an Engineered Safeguards System design that evaluation has shown to improve protection. The three-level, rectangular fabrication building sits in an unobstructed protected area surrounded by dual fences, a vehicle barrier, and intrusion detectors. Intrusion assessment is aided by perimeter lighting and closed circuit television cameras.

Two gatehouses, one for personnel and one for vehicles, are located at diagonally opposite corners of the protected area. Each has protected, defensive positions on the second floor with a vantage of the protected area for the on-site guards. Persons are admitted to the protected area only after passing through hardened, secure personnel portals with positive identification checks and detectors for contra- band such as metal, explosives, and SNM.

Within the plant, secure portals control access to areas containing SNM or vital support functions. These portals are similar to those in the gatehouses. However, with the reduced traffic here, the monitoring can be more stringent. Inside the material access area, centrally controlled doors requiring appropriate identification of personnel further limit passage.

The central control module, which is the operations center for all safeguards control, is a significant addition to the baseline plant. This module contains the security operations center, the zone operations control center, the safeguards coordination center, and the materials measurement and accounting center. It provides space, if desired, for a plant operations control center with its emergency control section. Security of this vital area and its associated equipment is essential for safeguards operations. The central control module is hardened against forcible attacks and has sufficient radiation shielding to permit operation during a criticality incident.

The security operations center is the focal point for all plant security. The guards stationed there are continually apprised of the total security situation by remote devices. An



Sandia Laboratories

FIGURE 3 - MIXED OXIDE FUEL FABRICATION FACILITY

alternate security operations center in one of the gatehouses has a redundant system and can assume all of the essential responsibilities of the primary center in an emergency.

Emergency evacuation systems that permit employees uncontrolled exit directly into the protected area are inadequate. For example, once in the protected area, scaling the perimeter fences or pick-up by helicopter can occur with such rapidity that timely guard response becomes marginal. For the three-level facility shown in Figure 4, this mode of escape can be prevented by the secure evacuation system concept. In this concept evacuation is controlled by channelling personnel through existing stairwells to the basement where an evacuation corridor leads to a secure evacuation shelter. After personnel have congregated in the shelter, their release through the shelter portal is supervised. Implementation of this concept will require design review by the Occupational Safety and Health Administration to assure that safety requirements are met.

The two-level, earth-cover design shown in Figure 5 provides increased penetration resistance to external attacks and additional containment of SNM in the event of a sabotage attempt involving explosives inside the plant. The earth-covered facility has access tunnels for shipping and receiving of material and for passage of personnel. Since the tunnel entrances are the only locations likely to be attacked, adversaries are channeled to locations where guards can provide maximal defensive response with minimal danger to themselves and others. Furthermore, the access tunnels facilitate the use of physical barriers and activated delays. In this design the evacuation corridors can be located in the ground-level berm as well as in the basement. The earth-covered design is in the conceptual stage and further effort is required to evaluate its utility, safety, and cost.

A preliminary evaluation of the ESS designs described above has been completed (Ref. 6). This analysis indicates that it is possible to provide large improvements in protection for special nuclear material against theft and sabotage attacks by adversaries, whether an insider, an outsider, or a combined threat.

NOTES:

1. FIGURES IN ◯ INDICATE ESTIMATED NUMBER OF PERSONNEL LEAVING AREA.
2. FIGURES IN □ INDICATE CUMULATIVE NUMBER OF PERSONNEL LEAVING AREA.

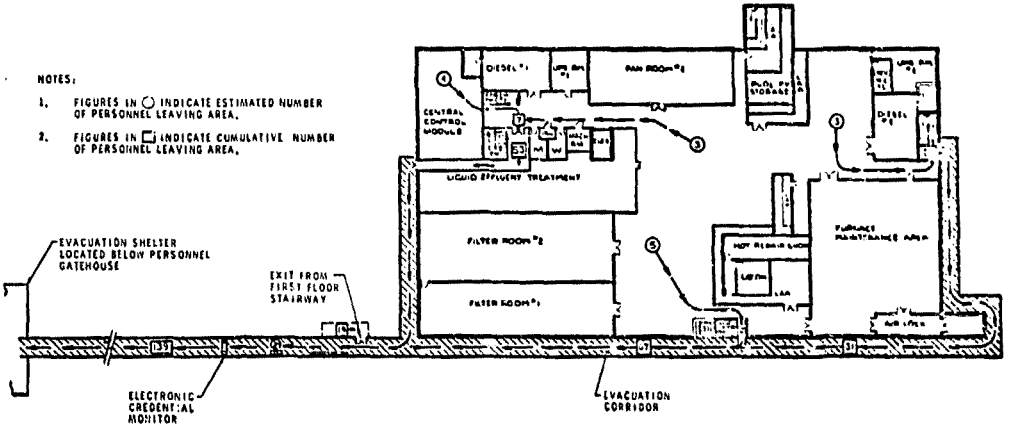


FIGURE 4 - BASEMENT PERSONNEL EVACUATION ROUTES FOR THE THREE-LEVEL FACILITY

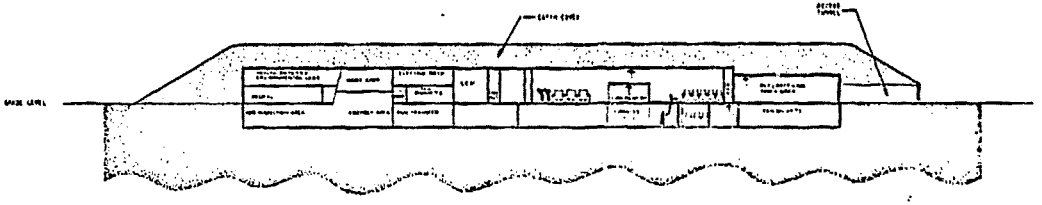


FIGURE 5 - TWO-LEVEL MOFFF WITH EARTH COVER

References

1. "Westinghouse License Application for the Recycle Fuels Plant at Anderson, S. C.," USAEC Docket No. 70-1432, July 1973.

2. Worrell, R. B., Using the Set Equation Transformation System in Fault Tree Analysis, SAND74-0240, Sandia Laboratories, NM, September 1974.

3. Worrell, R. B., Instructions for Using the SETS Program, SLA-73-0908A, Sandia Laboratories, NM, October 1974.

4. Chapman, L. D., A Model for Evaluating Alternative Fixed-Site Security Systems (U), SAND75-0512, Sandia Laboratories, NM, April 1976, Confidential.

5. Boozer, D. D., and D. Engi, Simulation of Personnel Control Systems Using the Insider Safeguards Effectiveness Model (ISEM) (U), SAND76-0682, Sandia Laboratories, NM, January 1977.

6. A. E. Winblad, et al, A Concept and Preliminary Definition of an Engineered Safeguards System for a Mixed-Oxide Fuel Fabrication Facility, SAND76-0528, Sandia Laboratories, NM, September 1976, Confidential.