SAND 79-0677C

PHYSICAL PROTECTION OF POWER REACTORS

John L. Darby
Sandia Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

Sandia Laboratories has applied a systematic approach to designing physical protection systems for nuclear facilities[1,2] to commercial light-water reactor power plants. A number of candidate physical protection systems were developed and evaluated.[3] This paper focuses on the design of access control subsystems at each of three plant layers: the protected area perimeter, building surfaces, and vital areas. Access control, as used here, refers to barriers, detectors, and entry control devices and procedures used to keep unauthorized personnel and contraband out of the plant, and to control authorized entry into vital areas within the plant.

PHYSICAL PROTECTION SYSTEM DESIGN

Concern over possible sabotage acts at power reactors has resulted in strengthened regulatory requirements for security.[4] The Office of Safeguards and Security (OSS) of the Department of Energy (DOE) is sponsoring a task at Sandia Laboratories to develop candidate physical protection systems for reactors. Various design and evaluation methodologies developed at Sandia under both DOE and Nuclear Regulatory Commission (NRC) sponsorship were applied to pressurized and boiling water reactors.

For design and evaluation, physical protection can be separated into three parts: access control, operations control, and response. Access control prevents unauthorized entry or the introduction of contraband (explosives and weapons) into the plant. Operations control prevents unauthorized manipulation of vital components that could sabotage the plant. Guards respond to detected threats. In general, both access control and operations control combine hardware components with procedures to thwart potential saboteurs. An entry portal which verifies personnel identity and checks for weapons, and where guards perform a search for explosives is an example of access control. Secure, remote start capability for a pump from the control room and remote control over the position of a valve are examples of operations control.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

A recent classified Sandia report describes this physical protection system design work for pressurized and boiling water reactors.[3] This study rigorously identified vital areas and vital components that must be protected, proposed and evaluated candidate physical protection systems, identified specific hardware components to satisfy performance requirements of a highly effective system, and estimated the cost of implementing this system into a commercial plant. The conclusions of the study are as follows:

1) A minimum set of vital areas and vital components at a given plant can be identified by developing and analyzing sabotage fault trees.[5]

2) The minimum number of vital areas and vital components that must be protected is not prohibitive to implementing physical protection.

3) State-of-the-art hardware can provide highly effective access control except for totally automated explosives detection . A number of alternative access control systems can be effective.

4) Development of operations control concepts which emphasize use of hardware for specific vital components is recommended. Extension of existing safety instrumentation to operations control may be possible.

5) The cost of implementing sophisticated access control in a commercial plant is not prohibitive when compared to current security costs.

As a result of this study, two areas are currently being pursued. An access control handbook for power reactors is being produced, and operations control concepts emphasizing hardware are being developed. Access control system design technology will be transferred to nuclear plant security organizations through the access control handbook. The handbook will present alternatives for access control and address current problems at operating plants. The operations control task is aimed at identifying hardware that could provide protection of vital components against unauthorized manipulation, as a possible alternative to across-the-board two-man rule or subcompartmentalization. Since the operations control work is in a preliminary state, this paper will focus on access control.

ACCESS CONTROL FOR POWER REACTORS

The physical protection system design study for power reactors identified the possible need for access control of

three plant layers: the protected area perimeter, building surfaces, and vital areas.[3] To assist power reactor utilities in designing access control subsystems at each layer, Sandia is producing an access control handbook for power reactors. This handbook will contain the following information:

1) The specific purpose and application of access control systems for power reactors,

2) General experiences of utility designers in implementing access control,

3) Candidate access control elements to be considered for reactors and factors affecting their implementation,

4) Access control subsystem alternatives for each of three plant layers,

5) Comparison of subsystem alternatives,

6) A design approach for implementing chosen subsystem alternatives.

Sandia/DOE has produced handbooks which characterize entry control, barrier, and intrusion detection elements.[6,7,8] A handbook for coordinating these elements using hardware, software, and procedures into a control center which communicates with the response force is being produced;[9] the Safeguards Control and Communications System (SCCS) collects data from the access control system and provides information on the status of plant security to the response force. These handbooks provide information pertinent to the selection, procurement, installation, testing, and maintenance of specific elements. The purpose of the access control handbook is to apply this expertise directly to power reactors to provide guidance in system design. Appropriate standards, NRC regulations, and operational experience are considered in this application.

The effectiveness of subsystem alternatives will not be rigorously evaluated in the access control handbook. Access control is only a part of an overall physical protection system and the relative effectiveness of physical protection system alternatives for power reactors has been evaluated previously.[3] The handbook will present a number of subsystem alternatives at each layer, identify advantages among alternatives, and assist a security system designer in implementing selected alternatives at his particular site. It is left to the handbook user to decide how much access control will satisfy his overall security needs.

An extensive site survey of power reactors was conducted to identify real problems that must be addressed when implementing access control in operating plants. The site survey included 18 operating and 31 planned reactor units. A general summary of problems encountered, lessons learned, and recommendations of the participating power plant companies, as a whole, will be in the handbook. The following information is indicative of results of the survey.

Plant security personnel emphasize that the purpose of access control is to provide security for the plant, but the system application cannot degrade the safety or reliability of a plant whose primary function is to produce electricity. Access control systems that are cumbersome, impede necessary operations, or require a high degree of maintenance are not acceptable to the nuclear power industry. Throughput is a major concern at operating plants, especially during shutdown when as many as 1000 people require access.

Most facilities encounter site-specific problems relating to terrain and environment whose effects on particular hardware components is uncertain. Access control must be applied to different size facilities ranging from single 200 MWe sites to four-reactor 5000 MWe sites. Smaller single-unit sites may have more severe manpower constraints than multifacility sites; however, sites with more than one unit must interface security at operating plants with those under construction. Some two-unit sites share common control rooms, radwaste buildings, emergency power buildings, intake structures, and protected areas, and security at an on-line unit is directly affected if the other unit is shut down for refueling, safety modifications, or maintenance.

The security hardware-personnel interface differs among sites. Large utilities which do their own architectural engineering and construction may exclusively utilize their employees within their security organization, while other utilities prefer to use contract security guards within their organization. The degree to which a security system is automated depends upon company philosophy. Some plants use watchtowers at the perimeters while others use fully automated intrusion detection and assessment systems. At some units, controlled doors into vital areas fail open upon loss of power while at others they fail closed; the safety and security interface depends upon plant procedures for ensuring necessary access during such emergencies.

A generic access control system, directly applicable to any site, does not exist for the reasons just discussed; however, specific steps can be followed which enable cost-effective access control to be systematically developed for a particular site. The design sequence for a user to

develop access control is tabulated in Table I. First, the user must have information on the kind of access control that he can implement in the near term at his plant. The access control handbook will indicate what role access control can play in an overall physical protection system. Then, the user must select the access control subsystems at each layer which fulfill his access control requirements. The handbook will provide a number of subsystem alternatives and supporting information for consideration in this selection. To design the chosen subsystems, the user must consider site specific effects. The access control handbook will identify those effects to be addressed, and with the additional use of the appropriate Sandia handbooks, the user can select appropriate components and/or procedures.[6,7,8] Once the subsystems have been designed, they must be integrated into an overall access control system. Factors pertinent to the control of the overall system and subsequent communication with the response force will be described in the access control handbook with detailed supporting information available in the control and communications handbook.[9] Finally, a check on how the overall system meets its original requirements should be performed, and the handbook will assist in this check.

Table II lists some candidate access control subsystems for each layer. Each subsystem is comprised of specific elements, (fences, intrusion detectors, and so forth), but some subsystems at a given layer have more elements than others. For example, subsystem 1b provides for personnel identification and contraband detection at the perimeter while subsystem 1a does not. It is up to the user to decide, based on supporting information, whether he wants these elements at the perimeter (1b), at the buildings (2b), or at both layers (1b and 2b). This decision depends upon how much access control he has decided upon.

Once the subsystems have been selected, the user must pick components and/or procedures to provide the elements of those subsystems. Table III tabulates the 10 elements that can comprise subsystems, and components and/or procedures that can provide those elements and factors affecting their implementation.

Two aspects should be considered when selecting components to meet a chosen subsystem design: desired performance and site-specific factors. For example, to provide intrusion detection at the perimeter better performance can be attained by using a combination of sensors -- such as micro-wave, E-field, and buried line -- over that achievable with any one sensor alone; however, environment affects which particular sensors are best suited to a given site, and without due consideration to such factors the optimum sensors may not be selected. The user

decides what performance he desires for an element then picks the components and/or procedures best able to provide that performance at his site.

This paper has outlined the DOE/Sandia power reactor physical protection program with emphasis on the power reactor access control handbook.

ACKNOWLEDGMENTS

The assistance of International Energy Associates Limited in developing the access control handbook is appreciated.

REFERENCES

1. Department of Energy, A Systematic Approach to the Conceptual Design of Physical Protection Systems for Nuclear Facilities, prepared by Sandia Laboratories, HCP/D0789-01, May 1978.

2. M. N. Cravens, A. E. Winblad, "Safeguards System design Methodology," INMM Proceedings, Vol. VI No. III, Fall 1977.

3. J. L. Darby, A Physical Protection System Concept Definition for Typical Pressurized and Boiling Water Reactors, SAND78-1394, Sandia Laboratories, to be published.

4. The Code of Federal Regulations, Title 10, Energy, Part 73, February 1977.

5. N. R. Ortiz, G. B. Varnado, Generic Sabotage Fault Trees for Nuclear Power Plants, SAND77-1805, Sandia Laboratories, to be published.

6. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, October 1977.

7. Entry-Control Systems Handbook, SAND77-1033, Sandia Laboratories, September 1977.

8. Barrier Technology Handbook, SAND77-0777, Sandia Laboratories, April 1978.

9. Safeguards Control and Communications System Handbook, SAND78-1785, Sandia Laboratories, to be published.

TABLE I

ACCESS CONTROL DESIGN SEQUENCE

Design Steps	Supporting Information in Access Control Handbook	Other Supporting Information
Determine Amount of Access Control Desired to Meet Plant Security Requirements	Description of Role Access Control Can Play in Physical Protection	Physical Protection System Design Studies Other Sandia Handbooks NRC Regulations and Requirements
Pick Access Control Subsystem at Each Layer	Access Control Subsystem Alternatives at Perimeter, Buildings, and Vital Areas	Appropriate Standards Operational Experience
Design Chosen Subsystems	Site Specific Considerations Component Selection Criteria	Other Sandia Handbooks Vendor Information Operational Experience
Integrate Subsystems Into Overall System	Control and Communication Factors Affecting Subsystem Integration Checks for Completeness in Meeting Desired System Requirements	Other Sandia Handbooks Operational Experience

TABLE II

CANDIDATE ACCESS CONTROL SUBSYSTEMS

Plant Layer	Candidate Access Control Subsystems
1. Perimeter	a) Fences, Vehicle Barrier, Vehicle Portal, Intrusion Detection, Intrusion Assessment
	b) Fences, Vehicle Barrier, Vehicle Portal, Metal Detection, Explosives Detection, Personnel Identification, Intrusion Detection, Intrusion Assessment
2. Buildings	a) Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection
	b) Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection, Metal Detection, Explosives Detection, Personnel Identification
3. Vital Areas	a) Personnel Identification, Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection
	b) Personnel Identification, Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection, Intrusion Assessment

TABLE III

Options for Providing Access Control Elements

Element	Component and/or Procedure to Provide Element	Factors Affecting Component and/or Procedure Implementation
1. Fence	One, two, or three chain-link fences 7 to 11 feet high with outriggers or barbed tape.	Soil characteristics and erosion affect surface preparation, fabric-bottom tiedown.
		Wind determines tension necessary to minimize fabric movement.
		Snow affects height selection.
2. Vehicle Barrier	Natural barriers, steel cables on fences, trapezoidal ditches, concrete barriers, railcar derailers	Terrain and plant layout
		Environmental effects on ditch maintenance
3. Personnel Identification	On-site security organization issuance of credential (photo ID, coded badge)	Throughput required
		Personnel turnover rate
	Credential verification (man or machine depending on credential)	Reliability of security organization
		Performance desired
	Positive personnel identification (hand geometry reader, fingerprint)	
	Memorized code number	
4. Metal Detection	Pat-down search	Employee relations
	Electromagnetic detectors	Throughput required
		Reduction of external influences on automatic detectors
5. Explosives Detection	Pat-down search	Employee relations
	Dogs	Throughput required
	Vapor collection detectors	Vapor collection detector sensitivity

TABLE III (Continued)

	Element	Component and/or Procedure to Provide Element	Factors Affecting Component and/or Procedure Implementation
6.	Vehicle Portal	Vehicle search	Throughput required
		Vehicle escort	Plant layout
7.	Walls, Floors, and Ceilings	Concrete with rebar	Existing safety and seismic required hardness
		Armor plate	Additional barriers surrounding area to be protected
8.	Doors and Locks	Doors of varying hardness	Mounting requirements
		Locks of varying sophistication	Key control procedures
		Key control	Lock change-out requirements
			Emergency egress considerations
9.	Intrusion Detection		
	- External	Watchtowers	Manpower limitations
		Sensors (microwave, E-field, buried cable, fence tamper)	Environment
			Perimeter layout
	- Internal, Unoccupied Areas	Sensors (door switches, infrared, ultrasonic, microwave, video motion detection)	Normal state of area (noise, vibration, size)
10.	Intrusion Assessment		
	- External	Watchtower and lights	Manpower limitations
		CCTV and lights	Camera lens capability
			Camera, lighting compatibility
			Environment
			Perimeter layout
	- Internal, Unoccupied Areas	CCTV	Normal state of area (size, layout)

A recent classified Sandia report describes this physical protection system design work for pressurized and boiling water reactors.[3] This study rigorously identified vital areas and vital components that must be protected, proposed and evaluated candidate physical protection systems, identified specific hardware components to satisfy performance requirements of a highly effective system, and estimated the cost of implementing this system into a commercial plant. The conclusions of the study are as follows:

1) A minimum set of vital areas and vital components at a given plant can be identified by developing and analyzing sabotage fault trees.[5]

2) The minimum number of vital areas and vital components that must be protected is not prohibitive to implementing physical protection.

3) State-of-the-art hardware can provide highly effective access control except for totally automated explosives detection . A number of alternative access control systems can be effective.

4) Development of operations control concepts which emphasize use of hardware for specific vital components is recommended. Extension of existing safety instrumentation to operations control may be possible.

5) The cost of implementing sophisticated access control in a commercial plant is not prohibitive when compared to current security costs.

As a result of this study, two areas are currently being pursued. An access control handbook for power reactors is being produced, and operations control concepts emphasizing hardware are being developed. Access control system design technology will be transferred to nuclear plant security organizations through the access control handbook. The handbook will present alternatives for access control and address current problems at operating plants. The operations control task is aimed at identifying hardware that could provide protection of vital components against unauthorized manipulation, as a possible alternative to across-the-board two-man rule or subcompartmentalization. Since the operations control work is in a preliminary state, this paper will focus on access control.

ACCESS CONTROL FOR POWER REACTORS

The physical protection system design study for power reactors identified the possible need for access control of

three plant layers: the protected area perimeter, building surfaces, and vital areas.[3] To assist power reactor utilities in designing access control subsystems at each layer, Sandia is producing an access control handbook for power reactors. This handbook will contain the following information:

1) The specific purpose and application of access control systems for power reactors,

2) General experiences of utility designers in implementing access control,

3) Candidate access control elements to be considered for reactors and factors affecting their implementation,

4) Access control subsystem alternatives for each of three plant layers,

5) Comparison of subsystem alternatives,

6) A design approach for implementing chosen subsystem alternatives.

Sandia/DOE has produced handbooks which characterize entry control, barrier, and intrusion detection elements.[6,7,8] A handbook for coordinating these elements using hardware, software, and procedures into a control center which communicates with the response force is being produced;[9] the Safeguards Control and Communications System (SCCS) collects data from the access control system and provides information on the status of plant security to the response force. These handbooks provide information pertinent to the selection, procurement, installation, testing, and maintenance of specific elements. The purpose of the access control handbook is to apply this expertise directly to power reactors to provide guidance in system design. Appropriate standards, NRC regulations, and operational experience are considered in this application.

The effectiveness of subsystem alternatives will not be rigorously evaluated in the access control handbook. Access control is only a part of an overall physical protection system and the relative effectiveness of physical protection system alternatives for power reactors has been evaluated previously.[3] The handbook will present a number of subsystem alternatives at each layer, identify advantages among alternatives, and assist a security system designer in implementing selected alternatives at his particular site. It is left to the handbook user to decide how much access control will satisfy his overall security needs.

An extensive site survey of power reactors was conducted to identify real problems that must be addressed when implementing access control in operating plants. The site survey included 18 operating and 31 planned reactor units. A general summary of problems encountered, lessons learned, and recommendations of the participating power plant companies, as a whole, will be in the handbook. The following information is indicative of results of the survey.

Plant security personnel emphasize that the purpose of access control is to provide security for the plant, but the system application cannot degrade the safety or reliability of a plant whose primary function is to produce electricity. Access control systems that are cumbersome, impede necessary operations, or require a high degree of maintenance are not acceptable to the nuclear power industry. Throughput is a major concern at operating plants, especially during shutdown when as many as 1000 people require access.

Most facilities encounter site-specific problems relating to terrain and environment whose effects on particular hardware components is uncertain. Access control must be applied to different size facilities ranging from single 200 MWe sites to four-reactor 5000 MWe sites. Smaller single-unit sites may have more severe manpower constraints than multifacility sites; however, sites with more than one unit must interface security at operating plants with those under construction. Some two-unit sites share common control rooms, radwaste buildings, emergency power buildings, intake structures, and protected areas, and security at an on-line unit is directly affected if the other unit is shut down for refueling, safety modifications, or maintenance.

The security hardware-personnel interface differs among sites. Large utilities which do their own architectural engineering and construction may exclusively utilize their employees within their security organization, while other utilities prefer to use contract security guards within their organization. The degree to which a security system is automated depends upon company philosophy. Some plants use watchtowers at the perimeters while others use fully automated intrusion detection and assessment systems. At some units, controlled doors into vital areas fail open upon loss of power while at others they fail closed; the safety and security interface depends upon plant procedures for ensuring necessary access during such emergencies.

A generic access control system, directly applicable to any site, does not exist for the reasons just discussed; however, specific steps can be followed which enable cost-effective access control to be systematically developed for a particular site. The design sequence for a user to

develop access control is tabulated in Table I. First, the user must have information on the kind of access control that he can implement in the near term at his plant. The access control handbook will indicate what role access control can play in an overall physical protection system. Then, the user must select the access control subsystems at each layer which fulfill his access control requirements. The handbook will provide a number of subsystem alternatives and supporting information for consideration in this selection. To design the chosen subsystems, the user must consider site specific effects. The access control handbook will identify those effects to be addressed, and with the additional use of the appropriate Sandia handbooks, the user can select appropriate components and/or procedures.[6,7,8] Once the subsystems have been designed, they must be integrated into an overall access control system. Factors pertinent to the control of the overall system and subsequent communication with the response force will be described in the access control handbook with detailed supporting information available in the control and communications handbook.[9] Finally, a check on how the overall system meets its original requirements should be performed, and the handbook will assist in this check.

Table II lists some candidate access control subsystems for each layer. Each subsystem is comprised of specific elements, (fences, intrusion detectors, and so forth), but some subsystems at a given layer have more elements than others. For example, subsystem 1b provides for personnel identification and contraband detection at the perimeter while subsystem 1a does not. It is up to the user to decide, based on supporting information, whether he wants these elements at the perimeter (1b), at the buildings (2b), or at both layers (1b and 2b). This decision depends upon how much access control he has decided upon.

Once the subsystems have been selected, the user must pick components and/or procedures to provide the elements of those subsystems. Table III tabulates the 10 elements that can comprise subsystems, and components and/or procedures that can provide those elements and factors affecting their implementation.

Two aspects should be considered when selecting components to meet a chosen subsystem design: desired performance and site-specific factors. For example, to provide intrusion detection at the perimeter better performance can be attained by using a combination of sensors -- such as micro-wave, E-field, and buried line -- over that achievable with any one sensor alone; however, environment affects which particular sensors are best suited to a given site, and without due consideration to such factors the optimum sensors may not be selected. The user

decides what performance he desires for an element then picks the components and/or procedures best able to provide that performance at his site.

This paper has outlined the DOE/Sandia power reactor physical protection program with emphasis on the power reactor access control handbook.

ACKNOWLEDGMENTS

The assistance of International Energy Associates Limited in developing the access control handbook is appreciated.

REFERENCES

1. Department of Energy, A Systematic Approach to the Conceptual Design of Physical Protection Systems for Nuclear Facilities, prepared by Sandia Laboratories, HCP/DO789-01, May 1978.

2. M. N. Cravens, A. E. Winblad, "Safeguards System design Methodology," INMM Proceedings, Vol. VI No. III, Fall 1977.

3. J. L. Darby, A Physical Protection System Concept Definition for Typical Pressurized and Boiling Water Reactors, SAND78-1394, Sandia Laboratories, to be published.

4. The Code of Federal Regulations, Title 10, Energy, Part 73, February 1977.

5. N. R. Ortiz, G. B. Varnado, Generic Sabotage Fault Trees for Nuclear Power Plants, SAND77-1805, Sandia Laboratories, to be published.

6. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, October 1977.

7. Entry-Control Systems Handbook, SAND77-1033, Sandia Laboratories, September 1977.

8. Barrier Technology Handbook, SAND77-0777, Sandia Laboratories, April 1978.

9. Safeguards Control and Communications System Handbook, SAND78-1785, Sandia Laboratories, to be published.

TABLE I

ACCESS CONTROL DESIGN SEQUENCE

Design Steps	Supporting Information in Access Control Handbook	Other Supporting Information
Determine Amount of Access Control Desired to Meet Plant Security Requirements	Description of Role Access Control Can Play in Physical Protection	Physical Protection System Design Studies Other Sandia Handbooks NRC Regulations and Requirements
Pick Access Control Subsystem at Each Layer	Access Control Subsystem Alternatives at Perimeter, Buildings, and Vital Areas	Appropriate Standards Operational Experience
Design Chosen Subsystems	Site Specific Considerations Component Selection Criteria	Other Sandia Handbooks Vendor Information Operational Experience
Integrate Subsystems Into Overall System	Control and Communication Factors Affecting Subsystem Integration Checks for Completeness in Meeting Desired System Requirements	Other Sandia Handbooks Operational Experience

TABLE II

CANDIDATE ACCESS CONTROL SUBSYSTEMS

Plant Layer	Candidate Access Control Subsystems
1. Perimeter	a) Fences, Vehicle Barrier, Vehicle Portal, Intrusion Detection, Intrusion Assessment
	b) Fences, Vehicle Barrier, Vehicle Portal, Metal Detection, Explosives Detection, Personnel Identification, Intrusion Detection, Intrusion Assessment
2. Buildings	a) Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection
	b) Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection, Metal Detection, Explosives Detection, Personnel Identification
3. Vital Areas	a) Personnel Identification, Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection
	b) Personnel Identification, Walls, Floors, Ceilings, Doors, Locks, Intrusion Detection, Intrusion Assessment

TABLE III

Options for Providing Access Control Elements

Element	Component and/or Procedure to Provide Element	Factors Affecting Component and/or Procedure Implementation
1. Fence	One, two, or three chain-link fences 7 to 11 feet high with outriggers or barbed tape.	Soil characteristics and erosion affect surface preparation, fabric-bottom tiedown.
		Wind determines tension necessary to minimize fabric movement.
		Snow affects height selection.
2. Vehicle Barrier	Natural barriers, steel cables on fences, trapezoidal ditches, concrete barriers, railcar derailers	Terrain and plant layout
		Environmental effects on ditch maintenance
3. Personnel Identification	On-site security organization issuance of credential (photo ID, coded badge)	Throughput required
		Personnel turnover rate
	Credential verification (man or machine depending on credential)	Reliability of security organization
		Performance desired
	Positive personnel identification (hand geometry reader, fingerprint)	
	Memorized code number	
4. Metal Detection	Pat-down search	Employee relations
	Electromagnetic detectors	Throughput required
		Reduction of external influences on automatic detectors
5. Explosives Detection	Pat-down search	Employee relations
	Dogs	Throughput required
	Vapor collection detectors	Vapor collection detector sensitivity

TABLE III (Continued)

	Element	Component and/or Procedure to Provide Element	Factors Affecting Component and/or Procedure Implementation
6.	Vehicle Portal	Vehicle search	Throughput required
		Vehicle escort	Plant layout
7.	Walls, Floors, and Ceilings	Concrete with rebar	Existing safety and seismic required hardness
		Armor plate	Additional barriers surrounding area to be protected
8.	Doors and Locks	Doors of varying hardness	Mounting requirements
		Locks of varying sophistication	Key control procedures
		Key control	Lock change-out requirements
			Emergency egress consideration
9.	Intrusion Detection		
	- External	Watchtowers	Manpower limitations
		Sensors (microwave, E-field, buried cable, fence tamper)	Environment
			Perimeter layout
	- Internal, Unoccupied Areas	Sensors (door switches, infrared, ultrasonic, microwave, video motion detection)	Normal state of area (noise, vibration, size)
10.	Intrusion Assessment		
	- External	Watchtower and lights	Manpower limitations
		CCTV and lights	Camera lens capability
			Camera, lighting compatibility
			Environment
			Perimeter layout
	- Internal, Unoccupied Areas	CCTV	Normal state of area (size, layout)