



U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

14.3.12 PHYSICAL SECURITY HARDWARE – INSPECTIONS, TESTS, ANALYSES, AND ACCEPTANCE CRITERIA

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of physical security hardware

Secondary - None

I. AREAS OF REVIEW

This section of the Standard Review Plan (SRP) specifically addresses inspections, tests, analyses, and acceptance criteria related to physical security hardware (PS-ITAAC). Physical security hardware characteristics include, but are not limited to, communication systems, assessment and alarm systems, locks, personnel access control, physical equipment barriers, and surveillance devices. ITAAC information is contained in the final safety analysis report (FSAR) of a combined license (COL) application or Tier 1 information from the design control document (DCD) of a design certification (DC) application.

Revision 1 – May 2010

USNRC STANDARD REVIEW PLAN

This Standard Review Plan (SRP), NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The SRP sections are numbered in accordance with corresponding sections in Regulatory Guide (RG) 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of RG 1.70 have a corresponding review plan section. The SRP sections applicable to a COL application for a new light-water reactor (LWR) are based on RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by e-mail to NRR_SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, or by fax to (301) 415-2289; or by e-mail to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/>, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at <http://www.nrc.gov/reading-rm/adams.html>, under Accession No. ML100970568.

The staff of the U.S. Nuclear Regulatory Commission (NRC) will review PS-ITAAC for the facility's physical security system for consistency with Appendix A of the SRP Section 14.3.12. PS-ITAAC specifically addresses equipment and/or features used for the physical security attributes of detection, assessment, delay, and response to protect against the design-basis threat (DBT) of radiological sabotage as stated in Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.1(a).

The specific areas of review are as follows:

1. For a DC application:
 - A. The NRC staff reviews any proposed PS-ITAAC to determine whether they are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the DC has been built and will operate in conformity with the DC, the Atomic Energy Act (AEA), and the NRC regulations.
 - B. The NRC staff reviews the information submitted to ensure that compliance with the requirements is verifiable through PS-ITAAC. The NRC staff also reviews the methods that are to be used for verification of the requirements.
2. For a COL application:
 - A. The NRC staff reviews the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the COL, the AEA, and the NRC regulations.
 - B. If the application references a standard DC, the staff verifies that the ITAAC contained in the certified design apply to those portions of the facility design that are approved in the DC.

3. COL Action Items and Certification Requirements and Restrictions

For a DC application, the staff review must address COL action items and requirements and restrictions (e.g., interface requirements and site parameters).

For a COL application referencing a DC, a COL applicant must address COL action items (referred to as COL license information in certain DCs) included in the referenced DC. Additionally, a COL applicant must address requirements and restrictions (e.g., interface requirements and site parameters) included in the referenced DC.

Review Interfaces

The following SRP sections interface with this section by providing physical security review guidance for COL and DC reviews:

1. SRP Section 13.6.1, "Physical Security—Combined License Review Responsibilities"
2. SRP Section 13.6.2, "Physical Security—Design Certification"
3. SRP Section 13.6.3, "Physical Security—Early Site Permit"

The specific acceptance criteria and review procedures are contained in the referenced SRP sections.

II. ACCEPTANCE CRITERIA

Requirements

Acceptance criteria are based on meeting the relevant requirements described below.

Commission Regulations:

1. 10 CFR 73.1, as it relates to the prescribed requirements for the establishment and maintenance of a physical protection system and to protect against the DBT of radiological sabotage.
2. 10 CFR 52.79(a)(35)(i), which requires each applicant for an operating license (OL) for a utilization facility that will be subject to the requirements of 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," to include a physical security plan.
3. 10 CFR 52.79(a)(36)(i), which requires each applicant for a license to operate a utilization facility that will be subject to 10 CFR 73.55, to include a licensee safeguards contingency plan in accordance with the criteria set forth in Section II of Appendix C, "Nuclear Power Plant Safeguards Contingency Plans," to 10 CFR Part 73. The "implementing procedures" required in Section II of Appendix C to 10 CFR Part 73 do not have to be submitted to the Commission for approval.
4. 10 CFR 52.79(a)(36)(ii), which requires each applicant for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a training and qualification plan in accordance with the criteria set forth in Appendix B VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," to 10 CFR Part 73, "Physical Protection of Plants and Materials."
5. 10 CFR 52.79(a)(36)(iii), which requires each applicant for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a and a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."
6. 10 CFR 52.47(b)(1), which requires that a DC application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the DC has been built and will operate in conformity with the DC, the provisions of the AEA, and the NRC's regulations.
7. 10 CFR 52.80(a), which requires that a COL application contain the proposed inspections, tests, and analyses, including those applicable to emergency planning, that the licensee shall perform, and the acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the COL, the provisions of the AEA, and the NRC's

regulations.

8. 10 CFR 73.55, as it relates to the requirements for the design of a program to provide physical protection against radiological sabotage for licensed activities in nuclear power reactors.
9. 10 CFR 73.70(e), as it relates to documentation of all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security related equipment used pursuant to the requirements of 10 CFR Part 73.

SRP Acceptance Criteria:

Specific SRP acceptance criteria are described in this SRP section. The SRP is not a substitute for NRC regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide acceptable methods of compliance with the NRC regulations.

1. Appendix A to this SRP section provides an acceptable set of generic PS-ITAAC that an applicant may use to develop application-specific PS-ITAAC, tailored to specific physical security hardware.
2. Additional plant-specific PS-ITAAC (i.e., other than those listed in Appendix A) may be proposed and will be examined to determine acceptability on a case-by-case basis.

Technical Rationale

The technical rationale for application of these acceptance criteria is discussed in the following paragraphs:

1. 10 CFR 52.79(a)(35)(i), which requires each applicant for an operating license (OL) for a utilization facility that will be subject to the requirements of 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," to include a physical security plan.
2. 10 CFR 52.79(a)(36)(i), which requires each applicant for a license to operate a utilization facility that will be subject to 10 CFR 73.55, to include a licensee safeguards contingency plan in accordance with the criteria set forth in Section II of Appendix C, "Nuclear Power Plant Safeguards Contingency Plans," to 10 CFR Part 73. The "implementing procedures" required in Section II of Appendix C to 10 CFR Part 73 do not have to be submitted to the Commission for approval.
3. 10 CFR 52.79(a)(36)(ii), which requires each applicant for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a training and qualification plan in accordance with the criteria set forth in Appendix B VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," to 10 CFR Part 73, "Physical Protection of Plants and Materials."
4. 10 CFR 52.79(a)(36)(iii), which requires each applicant for a license to operate a

utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a and a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."

5. 10 CFR 73.55, establishes the detailed requirements for development and implementation of a physical security plan. The physical security plan describes the administrative, physical, and operational measures that provide protection of the facility, and any associated special nuclear material, from both internal and external threats. Compliance with 10 CFR 73.55 provides high assurance that the plant is protected against radiological sabotage.
6. 10 CFR 73.70(e), establishes the requirements for the documentation of all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security related equipment used pursuant to the requirements of 10 CFR Part 73.

III. REVIEW PROCEDURES

The reviewer will select material from the PS-ITAAC listed in Appendix A, as may be appropriate for a particular case.

These review procedures are based on the identified SRP acceptance criteria. For deviations from these specific acceptance criteria, the NRC staff will review the applicant's evaluation of how the proposed alternatives to the SRP criteria provide an acceptable method of complying with the relevant NRC criteria identified in Appendix A.

1. For review of a DC application, the reviewer will follow the above procedures to verify that any elements of the physical protection program included in the design, including requirements and restrictions (e.g., interface requirements and site parameters), described in the FSAR meets the acceptance criteria. DCs have referred to the FSAR as the DCD. The reviewer should also consider the appropriateness of identified COL action items; however, to ensure that these COL action items are addressed during a COL application, they should be added to the DC FSAR.
2. For review of a COL application, the scope of the review depends on whether the COL applicant references a DC, an early site permit, or other NRC approvals (e.g., manufacturing license, site suitability report, or topical report) and the scope of the information submitted in connection with such a previous approval.
3. Implementation of ITAAC will be inspected in accordance with NRC Inspection Manual Chapter (IMC) 2503, "Construction Inspection Program: Inspections of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Related Work," and, specifically for physical security, the PS-ITAAC Inspection Procedure 65001.17, "Inspection of ITAAC Security-Related Structures, Systems and Components."

IV. EVALUATION FINDINGS

The reviewer verifies that the applicant has provided sufficient information and that the review and calculations (if applicable) support conclusions of the following type to be included in the staff's safety evaluation report (SER). The reviewer also states the basis for those conclusions.

1. The reviewer verifies that sufficient information has been provided to satisfy the criteria of SRP Section 14.3.12 and concludes that Tier 1 is acceptable. For a DC application, this is done only to the extent the DC application describes SSCs as part of the physical protection system. A finding similar to that in the “Evaluation Findings” section of SRP Section 14.3.12 should be provided in a separate section of the SER.
2. For DC and COL reviews, the findings will also summarize the staff’s evaluation of requirements and restrictions (e.g., interface requirements and site parameters) and COL action items relevant to this SRP section.

V. IMPLEMENTATION

The staff will use this SRP section in performing safety evaluations of DC applications and license applications submitted by applicants pursuant to 10 CFR Part 52, “Licenses, Certification, and Approvals for Nuclear Power Plants.”

Except when the applicant proposes an acceptable alternative method for complying with specified portions of the Commission’s regulations, the staff will use the method described herein to evaluate conformance with Commission regulations.

VI. REFERENCES

1. 10 CFR 8.5, “Interpretation by the General Counsel of § 73.55 of this Chapter; Illumination and Physical Search Requirements.”
2. 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.”
3. 10 CFR 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage.”
4. Regulatory Guide (RG) 1.70, “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition).”
5. RG 1.206, “Combined License Applications for Nuclear Power Plants (LWR Edition).”
6. RG 4.7, “General Site Suitability Criteria for Nuclear Power Stations.”
7. RG 5.7, “Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas.”
8. RG 5.12, “General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials.”
9. RG 5.44, “Perimeter Intrusion Alarm Systems.”
10. RG 5.65, “Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls.”
11. RG 5.68, “Protection against Malevolent use of Vehicles at Nuclear Power Plants.”

12. RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program That Meets 10 CFR 73.55 Requirements."
13. RG 5.76, "Physical Protection Programs at Nuclear Power Reactors."
14. NUREG-0800, SRP, Section 9.5.2, "Communications Systems."
15. NRC IMC-2503, "Construction Inspection Program: Inspections of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Related Work."
16. Inspection Procedure 65001.17, "Inspection of ITAAC-Related Security Structures, Systems and Components."
17. NRC Regulatory Issue Summary 2008-05, "Lessons Learned to Improve Inspections, Tests, Analyses, and Acceptance Criteria Submittal," February 27, 2008.
18. Nuclear Energy Institute Letter, December 19, 2009, "Security ITAAC Related to New Plant Construction," ADAMS Accession No. ML090630433.
19. NRC Letter, March 26, 2009, "PS-ITAAC Related to New Plant Construction," ADAMS Accession No. ML090630299.
20. Underwriters Laboratories Standard 752, "The Standard of Safety for Bullet-Resisting Equipment,"
21. National Institute of Justice, U.S. Department of Justice, NIJ Standard-0108.01, "Ballistic Resistant Protective Materials," Washington, DC.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the SRP are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52 and were approved by the Office of Management and Budget, approval number 3150-0011 and 3150-0151.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

PS-ITAAC #1 Vital Area and Vital Area Barrier Requirements:

Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.55(e)(9)(i). “Vital equipment must be located only within vital areas, which must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers, except as otherwise approved by the Commission and identified in the security plans.”

10 CFR 73.55 (e)(9)(iv). “More than one vital area may be located within a single protected area.”

10 CFR 73.55(e)(9)(v). “At a minimum, the following shall be considered vital areas: (A) The reactor control room; (B) The spent fuel pool; (C) The central alarm station; and (D) The secondary alarm station in accordance with § 73.55(i)(4)(iii).”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|--|---|
| 1(a). Vital equipment will be located only within a vital area. | 1(a). All vital equipment locations will be inspected. | 1(a). Vital equipment is located only within a vital area. |
| 1(b). Access to vital equipment will require passage through at least two physical barriers. | 1(b). All vital equipment physical barriers will be inspected. | 1(b). Vital equipment is located within a protected area such that access to the vital equipment requires passage through at least two physical barriers. |

PS-ITAAC #2 Protected Area Barrier Requirements:

10 CFR 73.55(e)(3)(i). “Physical barriers must be designed and constructed to (A) Protect against the design-basis threat of radiological sabotage; (B) Account for site-specific conditions; and (C) Perform their required function in support of the licensee’s physical protection program.”

10 CFR 73.55(e)(3)(ii). “Physical barriers must provide deterrence or delay or support access control.”

10 CFR 73.55(e)(8)(i). “The protected area perimeter must be protected by physical barriers that are designed and constructed to (A) Limit access into the protected area to only those personnel, vehicles, and materials required to perform official duties; (B) Channel personnel, vehicles, and materials to designated access control portals; and (C) Be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the Physical Security Plan.”

10 CFR 73.55(e)(8)(ii). “Penetrations through the protected area barrier must be secured and monitored in a manner that prevents or delays, and detects the exploitation of any penetration.”

10 CFR 73.55(i)(5)(iii). “Unattended openings that intersect a security boundary such as underground pathways must be protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|---|
| 2(a). Physical barriers for the protected area perimeter will not be part of vital area barriers | 2(a). The protected area perimeter barriers will be inspected. | 2(a). Physical barriers at the perimeter of the protected area are separated from any other barrier designated as a vital area barrier. |
| 2(b). Penetrations through the protected area barrier will be secured and monitored. | 2(b). All penetrations through the protected area barrier will be inspected. | 2(b). All penetrations and openings through the protected area barrier are secured and monitored by intrusion detection equipment. |
| 2(c). Unattended openings that intersect a security boundary, such as underground pathways, will be protected by a physical barrier and monitored by intrusion detection equipment or provided surveillance at a frequency sufficient to detect exploitation. | 2(c). All unattended openings within the protected area barriers will be inspected. | 2(c). All unattended openings (such as underground pathways) that intersect a security boundary (such as the protected area barrier), are protected by a physical barrier and monitored by intrusion detection equipment or provided surveillance at a frequency sufficient to detect exploitation. |

PS-ITAAC #3 Isolation Zone Requirements:

10 CFR 73.55(e)(7)(i). “An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be (A) Designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier; (B) Monitored with intrusion detection equipment designed to satisfy the requirements of § 73.55(i) and be capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier; and (C) Monitored with assessment equipment designed to satisfy the requirements of § 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.”

10 CFR 73.55(e)(8)(iv). “Where building walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary provided that the detection and, assessment requirements of this section are met, appropriate barriers are installed, and the area is described in the security plans.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|--|--|
| 3(a). Isolation zones will exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and will be designed of sufficient size to permit observation and assessment on either side of the barrier. | 3(a). The outdoor areas adjacent to the protected area perimeter barrier will be inspected. | 3(a). The isolation zones exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and are of sufficient size to permit observation and assessment of activities on either side of the barrier in the event of its penetration or attempted penetration. |
| 3(b). Isolation zones will be monitored with intrusion detection and assessment equipment that is designed to provide detection and assessment of activities within the isolation zone. | 3(b). The intrusion detection equipment for monitoring the isolation zones will be inspected. | 3(b). Isolation zones are monitored by intrusion detection and assessment equipment capable of providing detection and assessment of activities within the isolation zone. |
| 3(c). Areas where permanent buildings do not allow sufficient observation distance between the intrusion detection system and the protected area barrier (e.g., the building walls are immediately adjacent to, or are an integral part of the protected area barrier) will be monitored with intrusion detection and assessment equipment that is designed to detect the attempted or actual penetration of the protected area perimeter barrier before completed penetration of the barrier and assessment of detected activities. | 3(c). Inspections of areas of the protected area perimeter barrier that do not have isolation zones will be performed. | 3(c). Areas where permanent buildings do not allow sufficient observation distance between the intrusion detection system and the protected area barrier (e.g., the building walls are immediately adjacent to, or an integral part of, the protected area barrier) are monitored with intrusion detection and assessment equipment that detects attempted or actual penetration of the protected area perimeter barrier before completed penetration of the barrier and assessment of detected activities |

PS-ITAAC #4 Protected Area Perimeter Intrusion Detection and Assessment Systems Requirements:

10 CFR 73.55(e)(7)(i). “An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be: (A) Designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier; (B) Monitored with intrusion detection equipment designed to satisfy the requirements of § 73.55(i) and be capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier; and (C) Monitored with assessment equipment designed to satisfy the requirements of § 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.”

10 CFR 73.55(i)(1). “The licensee shall establish and maintain intrusion detection and assessment systems that satisfy the design requirements of § 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the licensee’s protective strategy.”

10 CFR 73.55(i)(2). “Intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations,…”

10 CFR 73.55(i)(3)(vii). The systems shall “Ensure intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.”

10 CFR 73.55(e)(3)(i). “Physical barriers must be designed and constructed to: (A) Protect against the design basis threat of radiological sabotage; (B) Account for site-specific conditions; and (C) Perform their required function in support of the licensee physical protection program.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|--|--|
| 4(a). The perimeter intrusion detection system will be designed to detect penetration or attempted penetration of the protected area perimeter barrier before completed penetration of the barrier, and for subsequent alarms to annunciate concurrently in at least two continuously manned onsite alarm stations (central and secondary alarm stations). | 4(a). Tests, inspections, or a combination of tests and inspections of the intrusion detection system will be performed. | 4(a). The intrusion detection system can detect penetration or attempted penetration of the protected area perimeter barrier before completed penetration of the barrier, and subsequent alarms annunciate concurrently in at least two continuously manned onsite alarms stations (central and secondary alarm stations). |
| 4(b). The perimeter assessment equipment will be designed to provide video image recording with real-time and playback capability that can provide assessment of detected activities before and after each alarm annunciation at the protected area perimeter barrier. | 4(b). Tests, inspections, or a combination of tests and inspections of the video assessment equipment will be performed. | 4(b). The perimeter assessment equipment is capable of real-time and playback video image recording that provides assessment of detected activities before and after each alarm annunciation at the protected area perimeter barrier. |

| | | |
|--|---|---|
| <p>4(c). The intrusion detection and assessment equipment at the protected area perimeter will be designed to remain operable from an uninterruptible power supply in the event of the loss of normal power.</p> | <p>4(c). Tests, inspections, or a combination of tests and inspections of the uninterruptible power supply will be performed.</p> | <p>4(c). All Intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.</p> |
|--|---|---|

PS-ITAAC #5 Illumination Requirements:

10 CFR 73.55(i)(6)(ii). “The licensee shall provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the protected area. Alternatively, the licensee may augment the facility illumination system by means of low-light technology to meet the requirements of this section or otherwise implement the protective strategy.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|--|
| 5. Isolation zones and exterior areas within the protected area will be provided with illumination to permit assessment in the isolation zones and observation of activities within exterior areas of the protected area. | 5. The illumination in isolation zones and exterior areas within the protected area will be tested or inspected as appropriate. | 5. Illumination in isolation zones and exterior areas within the protected area is 0.2 foot candles measured horizontally at ground level or alternatively augmented, sufficient to permit assessment and observation. |

PS-ITAAC #6 Bullet-Resisting Barriers Requirements:

10 CFR 73.55(e)(5). “Bullet Resisting Physical Barriers. The reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed, must be bullet-resisting.”

10 CFR 73.55(i)(4)(iii). “Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station contained in this section. Both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of this section can be performed in both alarm stations.”

Note: 10 CFR 73.55(a)(6) states, “Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, that do not reference a standard design certification or reference a standard design certification issued after May 26, 2009 shall meet the requirement of § 73.55(i)(4)(iii).”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|--|--|
| <p>6. The external walls, doors, ceiling, and floors in the main control room, central alarm station, secondary alarm station, and the last access control function for access to the protected area will be bullet resistant, to at least Underwriters Laboratories Ballistic Standard 752, “The Standard of Safety for Bullet-Resisting Equipment,” Level 4, or National Institute of Justice Standard 0108.01, “Ballistic Resistant Protective Materials,” Type III.</p> | <p>6. Type test, analysis, or a combination of type test and analysis of the external walls, doors, ceiling, and floors in the main control room, central alarm station, secondary alarm station, and the last access control function for access to the protected area will be performed.</p> | <p>6. A report exists and concludes that the walls, doors, ceilings, and floors in the main control room, central alarm station, secondary alarm station, and the last access control function for access to the protected area are bullet resistant to at least Underwriters Laboratories Ballistic Standard 752, Level 4, or National Institute of Justice Standard 0108.01, Type III.</p> |

PS-ITAAC #7 Vehicle Control Measures Requirements:

10 CFR 73.55(e)(10). "Vehicle control measures. Consistent with the physical protection program design requirements of § 73.55(b), and in accordance with the site-specific analysis, the licensee shall establish and maintain vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage vehicle bomb assault."

10 CFR 73.55(e)(10)(i). "Land vehicles. Licensees shall: (A) Design, construct, install, and maintain a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems necessary to prevent significant core damage and spent fuel sabotage against the effects of the design basis threat of radiological sabotage land vehicle bomb assault. (B) Periodically check the operation of active vehicle barriers and provide a secondary power source, or a means of mechanical or manual operation in the event of a power failure, to ensure that the active barrier can be placed in the denial position to prevent unauthorized vehicle access beyond the required standoff distance. (C) Provide periodic surveillance and observation of vehicle barriers and barrier systems adequate to detect indications of tampering and degradation or to otherwise ensure that each vehicle barrier and barrier system is able to satisfy the intended function. (D) Where a site has rail access to the protected area, install a train derailer, remove a section of track, or restrict access to railroad sidings and provide periodic surveillance of these measures."

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|--|
| 7. The vehicle barrier system will be designed, installed, and located at the necessary standoff distance to protect against the design-basis threat vehicle bombs. | 7. Type test, inspections, analysis or a combination of type tests, inspections, and analysis will be performed for the vehicle barrier system. | 7. A validated report reviewed in accordance with NUREG/CR-6190 exists and concludes that the vehicle barrier system will protect against the design-basis threat vehicle bombs based on the standoff distance for the system. |

PS-ITAAC #8 Personnel, Vehicle, and Material Access Control Portals and Search Equipment Requirements:

10 CFR 73.55(h)(2)(iv) and (v). “Owner controlled area searches. (iv) Vehicle searches must be accomplished through the use of equipment capable of detecting firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage, or through visual and physical searches, or both, to ensure that all items are identified before granting access. (v) Vehicle access control points must be equipped with video surveillance equipment that is monitored by an individual capable of initiating a response.”

10 CFR 73.55(h)(3)(i). “Protected area searches. Licensees shall search all personnel, vehicles and materials requesting access to protected areas. (i) The search for firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage shall be accomplished through the use of equipment capable of detecting these items, or through visual and physical searches, or both, to ensure that all items are clearly identified before granting access to protected areas....”

10 CFR 73.55(g)(1)(i)(A) and (B). “*Access controls.* (1) Consistent with the function of each barrier or barrier system, the licensee shall control personnel, vehicle, and material access, as applicable, at each access control point in accordance with the physical protection program design requirements of § 73.55(b). (i) To accomplish this, the licensee shall: (A) Locate access control portals outside of, or concurrent with, the physical barrier system through which it controls access. (B) Equip access control portals with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|--|
| 8(a). Access control points will be established and designed to control personnel and vehicle access into the protected area. | 8(a). Tests, inspections, or a combination of tests and inspections of installed systems and equipment will be performed. | 8(a). Access control points exist for the protected area and are configured to control access and are equipped with locking devices, intrusion detection equipment and surveillance equipment consistent with the intended function. |
| 8(b). Access control points will be established and designed with equipment for the detection of firearms, explosives, incendiary devices or other items which could be used to commit radiological sabotage at the protected area personnel access points. | 8(b). Tests, inspections, or a combination of tests and inspections of installed systems and equipment will be performed. | 8(b). Detection equipment exists and is capable of detecting firearms, explosives, incendiary devices or other items which could be used to commit radiological sabotage at the protected area personnel access control points. |

PS-ITAAC #9 Picture Badge Identification System Requirements:

10 CFR 73.55(g)(6)(ii). "The licensee shall implement a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas."

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|---|---|
| 9. An access control system with a numbered photo identification badge system will be installed and designed for use by individuals who are authorized access to protected areas and vital areas without escort. | 9. The access control system and the numbered photo identification badge system will be tested. | 9. The access authorization system with a numbered photo identification badge system is installed and provides authorized access to protected and vital areas only to those individuals with unescorted access authorization. |

PS-ITAAC #10 **Vital Areas Access Control Requirements:**

10 CFR 73.55(e)(9)(iii). “Unoccupied vital areas must be locked and alarmed.”

10 CFR 73.55(i)(2). “Intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations....”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|---|
| 10. Unoccupied vital areas will be designed with locking devices and intrusion detection devices that annunciate in the central and secondary alarm stations. | 10. Tests, inspections, or a combination of tests and inspections of unoccupied vital area intrusion detection equipment and locking devices will be performed. | 10. Unoccupied vital areas are locked and alarmed and intrusion is detected and annunciated in both the central and secondary alarm stations. |

PS-ITAAC #11**Alarm Station Requirements:**

10 CFR 73.55(i)(2). “Intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations....”

10 CFR 73.55(i)(4)(i). “Both alarm stations required by paragraph (i)(2) of this section must be designed and equipped to ensure that a single act, in accordance with the design basis threat of radiological sabotage defined in § 73.1(a)(1), cannot disable both alarm stations. The licensee shall ensure the survivability of at least one alarm station to maintain the ability to perform the following functions: (A) Detect and assess alarms; (B) Initiate and coordinate an adequate response to an alarm; (C) Summon offsite assistance; and (D) Provide command and control.”

10 CFR 73.55(i)(4)(ii)(A) and (F) . “Licensees shall: (A) Locate the central alarm station inside a protected area. The interior of the central alarm station must not be visible from the perimeter of the protected area...(F) Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station.”

10 CFR 73.55(i)(4)(iii). “Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station contained in this section. Both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of this section can be performed in both alarm stations.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|---|--|
| 11(a). Intrusion detection equipment and video assessment equipment will annunciate and be displayed concurrently in at least two continuously manned onsite alarms stations (central and secondary alarm stations). | 11(a). Tests, inspections, or a combination of tests and inspections of intrusion detection equipment and video assessment equipment will be performed. | 11(a). Intrusion detection equipment and video assessment equipment annunciate and display concurrently in at least two continuously manned onsite alarm stations (central and secondary alarm stations). |
| 11(b). Central and secondary alarm stations will be located inside the protected area and will be designed so that the interiors of both alarm stations are not visible from the perimeter of the protected area. | 11(b). The central and secondary alarm station locations will be inspected. | 11(b). Central and secondary alarm stations are located inside the protected area, and the interiors of both alarm stations are not visible from the perimeter of the protected area. |
| 11(c). The alarm system will not allow the status of a detection point, locking mechanism or access control device to be changed without the knowledge and concurrence of the alarm station | 11(c). Tests, inspections, or a combination of tests and inspections of intrusion detection equipment and access control equipment will be performed. | 11(c). The alarm system will not allow the status of a detection point, locking mechanism or access control device to be changed without the knowledge and concurrence of the alarm station operator in the other alarm station. |

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|--|--|
| <p>operator in the other alarm station.</p> <p>11(d). Central and secondary alarm stations will be designed, equipped and constructed such that no single act, in accordance with the design-basis threat of radiological sabotage, can simultaneously remove the ability of both the central and secondary alarm stations to (1) detect and assess alarms, (2) initiate and coordinate an adequate response to alarms, (3) summon offsite assistance, and (4) provide effective command and control.</p> | <p>11(d). Tests, inspections, or a combination of tests and inspections of the central and secondary alarm stations will be performed.</p> | <p>11(d). Central and secondary alarm stations are designed, equipped, and constructed such that no single act, in accordance with the design-basis threat of radiological sabotage, can simultaneously remove the ability of both the central and secondary alarm stations to (1) detect and assess alarms, (2) initiate and coordinate an adequate response to alarms, (3) summon offsite assistance, and (4) provide effective command and control.</p> |
| <p>11(e). Both the central and secondary alarm stations will be constructed, located, protected, and equipped to the standards for the central alarm station (alarm stations need not be identical in design but shall be equal and redundant, capable of performing all functions required of alarm stations).</p> | <p>11(e). Tests, inspections, or a combination of tests and inspections of the central and secondary alarm stations will be performed.</p> | <p>11(e). The central and secondary alarm stations are located, constructed, protected, and equipped to the standards of the central alarm station and are functionally redundant. (Stations need not be identical in design.)</p> |

PS-ITAAC #12**Secondary Power Supplies for Alarm Annunciation and Communication Equipment Requirements:**

10 CFR 73.55(e)(9)(vi). "At a minimum, the following shall be located within a vital area: (A) The secondary power supply systems for alarm annunciation equipment; and (B) The secondary power supply systems for non-portable communications equipment."

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|---|--|
| 12. The secondary security power supply system for alarm annunciator equipment and nonportable communications equipment will be located within a vital area. | 12. The secondary security power supply system will be inspected. | 12. The secondary security power system for alarm annunciator equipment and nonportable communications equipment is located within a vital area. |

PS-ITAAC #13 Intrusion Detection Systems Console Display Requirements:

10 CFR 73.55(i)(3)(i)–(vi). “The licensee’s intrusion detection and assessment systems must be designed to:

- (i) Provide visual and audible annunciation of the alarm.
- (ii) Provide a visual display from which assessment of the detected activity can be made.
- (iii) Ensure that annunciation of an alarm indicates the type and location of the alarm.
- (iv) Ensure that alarm devices to include transmission lines to annunciators are tamper indicating and self-checking.
- (v) Provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply.
- (vi) Support the initiation of a timely response in accordance with the security plans, licensee protective strategy, and associated implementing procedures.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|--|---|
| 13(a). Security alarm devices, including transmission lines to annunciators, will be tamper-indicating and self-checking (e.g., an automatic indication is provided when failure of the alarm system or a component occurs or when on standby power), and alarm annunciation indicates the type of alarm (e.g., intrusion alarms, emergency exit alarm) and location. | 13(a). All security alarm devices and transmission lines will be tested. | 13(a). Security alarm devices including transmission lines to annunciators are tamper-indicating and self-checking; an automatic indication is provided when failure of the alarm system or a component occurs or when the system is on standby power; the alarm annunciation indicates the type of alarm and location. |
| 13(b). Intrusion detection and assessment systems will be designed to provide visual display and audible annunciation of alarms in both the central and secondary alarm stations. | 13(b). Intrusion detection and assessment systems will be tested. | 13(b). The intrusion detection systems provide a visual display and audible annunciation of all alarms concurrently in at least two continuously manned onsite alarms stations (central and secondary alarm stations). |

PS-ITAAC #14 Intrusion Detection Systems Recording Requirements:

10 CFR 73.55(i)(4)(ii)(h). “Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm.”

10 CFR 73.70(f). “A record at each onsite alarm annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other security incident shall be recorded. The license[e] shall retain each record for three years after the record is made.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|--|
| 14. Intrusion detection systems recording equipment will record onsite security alarm annunciation including the location of the alarm, false alarm, alarm check, and tamper indication and the type of alarm, location, alarm circuit, date, and time. | 14. The intrusion detection systems recording equipment will be tested. | 14. Intrusion detection systems recording equipment is capable of recording each onsite security alarm annunciation including the location of the alarm, false alarm, alarm check, and tamper indication and the type of alarm, location, alarm circuit, date, and time. |

PS-ITAAC #15 **Vital Area Emergency Exits Requirements:**

10 CFR 73.55(e)(8)(iii). “All emergency exits in the protected area must be alarmed and secured by locking devices that allow prompt egress during an emergency and satisfy the requirements of this section for access control into the protected area.”

10 CFR 73.55(e)(9)(ii). “The licensee shall protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements of this section.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|--|--|--|
| 15. Emergency exits through the protected area perimeter and vital area boundaries will be alarmed with intrusion detection devices and secured by locking devices that allow prompt egress during an emergency. | 15. Tests, inspections, or a combination of tests and inspections of emergency exits through the protected area perimeter and vital area boundaries will be performed. | 15. Emergency exits through the protected area perimeter and vital area boundaries are alarmed with intrusion detection devices and secured by locking devices that allow prompt egress during an emergency. |

PS-ITAAC #16**Communication Requirements:**

10 CFR 73.55(j)(3). “All on-duty security force personnel shall be capable of maintaining continuous communication with an individual in each alarm station, and vehicle escorts shall maintain continuous communication with security personnel. All personnel escorts shall maintain timely communication with the security personnel.”

10 CFR 73.55(j)(4). “The following continuous communication capabilities must terminate in both alarm stations required by this section:
 (i) Radio or microwave transmitted two-way voice communication, either directly or through an intermediary, in addition to conventional telephone service between local law enforcement authorities and the site, and (ii) A system for communication with the control room.”

10 CFR 73.55(j)(5). “Non-portable communications equipment must remain operable from independent power sources in the event of the loss of normal power.”

| Design Commitment | Inspections, Tests, Analysis | Acceptance Criteria |
|---|---|--|
| 16(a). The central and secondary alarm stations will have conventional (land line) telephone service with the control room and local law enforcement authorities. | 16(a). Tests, inspections, or a combination of tests and inspections of the central and secondary alarm stations’ conventional (land line) telephone service will be performed. | 16(a). The central and secondary alarm stations are equipped with conventional (land line) telephone service with the control room and local law enforcement authorities. |
| 16(b). The central and secondary alarm stations will be capable of continuous communication with on-duty security force personnel. | 16(b). Tests, inspections, or a combination of tests and inspections of the central and secondary alarm stations’ continuous communication capabilities will be performed. | 16(b). The central and secondary alarm stations are capable of continuous communication with on-duty watchmen, armed security officers, armed responders, or other security personnel who have responsibilities within the physical protection program and during contingency response events. |
| 16(c). Nonportable communications equipment in the central and secondary alarm stations will remain operable from an independent power source in the event of loss of normal power. | 16(c). Tests, inspections, or a combination of tests and inspections of the nonportable communications equipment will be performed. | 16(c). All nonportable communication devices (including conventional telephone systems) in the central and secondary alarm stations are wired to an independent power supply that enables those systems to remain operable (without disruption) during the loss of normal power. |

SRP Section 14.3.12
Description of Changes

This Revision 1 to SRP Section 14.3.12, dated April 2010, updates the initial issuance of this section, dated March 2007, to reflect the changes of the recently issued 10 CFR Part 73, Power Reactor Security Requirements (published in the *Federal Register* on March 27, 2009 (74 FR 13926)).

The technical changes in accordance with the new 10 CFR Part 73 Rule are incorporated in each section of this revision (Revision 1, dated April 2010) of the SRP as applicable.