5.0 Physical Security ITAAC

This set of ITAAC is tailored to the ABWR reactor design and Security Program requirements for STP 3 & 4. Table 5.0-1 addresses security requirements associated with the generic PS-ITAAC contained in NUREG-0800 14.3.12, “Physical Security Hardware.” Table 5.0-1 provides the Security ITAAC proposed for STP 3 & 4.

Table 5.0-1 Physical Security— Inspection, Test, Analysis, and Acceptance Criteria| (PS-ITAAC)[1]

Design Description	Inspections, Tests, Analysis	Acceptance Criteria
(1) Vital equipment shall be located only within a vital area. (2) Access to vital equipment requires passage through at least two physical barriers.	Inspections will be performed of the location of as-installed vital equipment.	(1) Vital equipment is located only within a vital area. (2) Access to the vital area has at least two physical barriers
Physical barriers for the protected area perimeter are not part of a vital area barrier.	An inspection of the protected area perimeter barrier will be performed.	Physical barriers at the perimeter of the protected area are separated from other barriers designated as a physical barrier.
Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area permit observation on either side of the barrier.	An inspection will be performed of the outdoor areas adjacent to the physical barrier at the perimeter of the protected area.	Isolation zones exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and are large enough to permit observation of the activities of people on either side of the barrier.
Intrusion detection system detects penetration or attempted penetration of the Protected Area (PA) Barrier.	Tests of the protected area (PA) intrusion detection system will be performed using simulated penetration.	The intrusion detection system detects the simulated penetration of the PA barrier and alarms annunciate in the CAS and SAS.
Exterior areas within the protected area are illuminated.	Tests will be performed of the illumination in the isolation zones of the PA and the external areas within the PA.	Illumination in isolation zones and exterior areas within the protected area is not less than 0.2 footcandle measured horizontally at ground level.
External walls, doors, ceiling and floors in the main control room, central alarm station, and the last access control function for access to the protected area are bullet resistant.	Inspections, analysis or a combination of inspections and analysis of the walls, doors, ceiling and floors will be performed for the main control room, central alarm station, and the last access control function for access to the protected area are bullet resistant.	The walls, doors, ceiling and floors have been constructed and analysis demonstrate the the main control room, central alarm station, and the last access control function for access to the protected area are bullet resistant.

Table 5.0-1 Physical Security— Inspection, Test, Analysis, and Acceptance Criteria| (PS-ITAAC)[1] (Continued)

Design Description	Inspections, Tests, Analysis	Acceptance Criteria
Vehicle barrier systems protect against use of a land vehicle.	Inspections, analysis or a combination of inspections and analysis of the systems will be performed for vehicle control measures, including vehicle barrier systems.	The vehicle control measures, including vehicle barrier systems, have been constructed and analysis demonstrate the Vehicle Barrier System is capable of protecting against the land vehicle bomb.
Personnel and vehicle control into the protected area at access points protect against the intrusion of firearms, explosives and incendiary devices.	A test of the personnel search and detection equipment and procedures will be performed at the PA boundry.	Search and detection equipment and procedures identify firearms, explosives and incendiary devices prior to entering the Protected Area.
A picture badge identification system exists.	A test of the numbered picture badge identification system will be performed using an unauthorized picture badge.	The picture badge identification system does not allow access to the person with the unauthorized picture badge.
Unoccupied vital areas are equipped with locks that can be locked and alarmed, and activated intrusion detection systems that annunciate in the Central and Secondary Alarm Stations upon intrusion into a vital area.	A combination of tests and inspections will be performed of access points to unoccupied vital areas by personnel who attempt to gain access to the unoccupied vital areas.	(1) Access pionts to unoccupied vital areas are equipped with locks. (2) The attempts to intrude in the unoccupied vital areas are detected and annunciated in both the CAS and SAS.
Alarm annunciation occurs in the central alarm station and in at least one other continuously manned station not necessarily onsite.	Tests of the installed detection annunication systems will be performed using simulated intrusion.	Upon simulated intrusion, alarms annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station.
Secondary security power supply system for alarm annunciator equipment and non-portable communications equipment is located within a vital area.	Inspections will be performed of the location secondary security power supply system and non-portable communication equipment.	Onsite secondary power supply systems for alarm annunciator equipment and non-portable communications equipment are located within a vital area.

Table 5.0-1 Physical Security— Inspection, Test, Analysis, and Acceptance Criteria| (PS-ITAAC)[1] (Continued)

Design Description	Inspections, Tests, Analysis	Acceptance Criteria
Alarm devices including transmission lines to annunciators are tamper indicating and self-checking. Alarm annunciation indicate the type of alarm and location.	A test will be performed of the alarm devices by tampering with the devices.	(1) Self-detection provision within the alarm devices detect the tampering. (2) The alarm annunication system identifies that tampering has occurred and the location of the tampering.
An onsite alarm annunciation system records the location, circuit, date, time and type of each alarm, false alarm, alarm check, and tamper indication .	Tests will be performed of the onsite alarm annunciation system using simulated intrusion and tampering.	The onsite alarm annunciation system records the simulated intrusion and tampering, including the type of alarm, location, alarm circuit, date, and time.
Emergency exits in each protected area and each vital area are alarmed.	A test is performed of each emergency exit in the protected area and vital area by opening the exit doors.	When the emergency exits are opened, an alarm is initiated.
(1) Alarm stations have conventional telephone service with law enforcement authorities. (2) Alarm stations have continuous communication capability with security personnel.	Tests will be performed of the communications systems in the alarm stations.	Through use of the communication systems in the the alarm stations: (1) security personnel communicate with law enforcement authorities and (2) security personnel communicate with security officers, watchmen, and armed response individuals in the field.

1 Physical Security Hardware—Equipment and/or features used for the physical security attributes of detection, assessment, delay, and response and to protect against the design basis threat of radiological sabotage as stated in 10 CFR 73.1(a). Examples of physical security system hardware include, but are not limited to, communication systems, assessment and alarm systems, locks, personnel access control, physical equipment barriers, and surveillance devices.