MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 4.3: Activity - Perimeter Security System Design for a Hypothetical Industrial Facility: Manufacturing Plant

This design focuses on a manufacturing plant, emphasizing robust physical security and detection of unauthorized access.

I. Area Definition: The perimeter encompasses the entire manufacturing plant site, including buildings, storage areas, and any surrounding land. Specific high-risk areas, such as loading docks and access roads, require extra attention.

II. Fencing Type:

Main Perimeter Fence: A combination of 8-foot high chain-link fence with barbed wire at the top will provide a visual deterrent and physical barrier. The fence should be securely anchored to prevent easy removal or climbing.

High-Security Areas: For particularly sensitive areas (e.g., chemical storage, high-value equipment), consider a higher fence (10-12 feet), potentially with additional security features like razor wire or concertina wire.

Gated Access Points: Multiple gates with secure locking mechanisms will manage access to and from the site.

III. Sensor Selection:

Perimeter Intrusion Detection System (PIDS): A combination of technologies is recommended for redundancy and comprehensive coverage.

Fiber Optic Sensors: Ideal for detecting vibrations along the fence line, offering high accuracy and minimal false alarms. These are especially useful in areas where other sensor types might be prone to interference (e.g., heavy machinery vibration).

Microwave Sensors: For wide-area coverage, especially in areas with difficult terrain or vegetation. They detect movement across a beam but can be susceptible to weather conditions.

Infrared Beam Sensors: These detect interruptions in infrared beams across access points. They are relatively inexpensive but can be easily compromised if lines of sight are obstructed or manipulated.
Ground-Based Vibration Sensors: Useful in detecting attempts to tunnel or bypass the fence underground.

IV. Access Control Points:

Gated Entrances: Secure gates with keypads, card readers, or biometric access control systems will manage entry and exit. These should be integrated with a central access control system.

Guard Stations: Strategically located guard stations near high-traffic areas will allow for visual monitoring, access control verification, and immediate response to incidents. These should be equipped with communication systems and emergency call buttons.

Controlled Access Roads: Access roads should have gates, speed bumps, and potentially bollards to control vehicle access and prevent unauthorized entry.

V. Integration with Other Security Measures:

Video Surveillance: High-definition IP cameras will supplement PIDS by providing visual confirmation of alarms and recording events. Cameras should be strategically placed to cover all vulnerable areas, including blind spots. Analytics such as motion detection and facial recognition will enhance the system's capabilities.

Lighting: Adequate lighting will deter intruders and assist surveillance cameras. Motion-activated lighting can be used to increase visibility in specific areas.

Alarm System: The PIDS, access control system, and video surveillance system should be integrated into a central alarm system. Alerts should be transmitted to a monitoring station or security personnel.

Security Personnel: Regular patrols and security personnel presence will provide an additional layer of deterrence and immediate response capability. Response protocols and procedures should be clearly defined.

VI. System Architecture: The system should be designed with redundancy and fail-safe mechanisms to ensure continuous operation. This includes backup power supplies, network redundancy, and failover systems for critical components.

This design offers a multi-layered approach to perimeter security, balancing cost-effectiveness with robust protection. The specific technologies and configurations should be tailored to the plant's size, layout, security risks, and budget. Regular maintenance and testing are essential for the system's ongoing effectiveness.