

CHAPTER 26

ELECTRONIC SECURITY

26-1. Electronic security methodology

Electronic security is an intrusion detection system (IDS) installed to adequately protect valuable assets against adversaries who pose a threat to these assets. Electronic security systems (ESS) are used to alert responsible personnel, such as security guards, to intrusions at protected facilities. In some cases, the system may cause actuation of physical barriers to prohibit intruders access.

a. Physical barriers. At most facilities, three barriers are utilized to form lines of defense to physically protect valuable assets. Perimeter barriers are normally found at the edge of the protected property and are considered to be the first line of defense. This may be a fence, wall, or a natural barrier, such as a river, lake, cliff, ravine, or other terrain that is difficult to traverse. The second line of defense is building exterior walls and roof. Interior building rooms, safes, and vaults make up the third line of defense. These physical barriers are mentioned because they establish areas where intrusion detection may be warranted. Depending on the type, configuration, location, and other conditions of the protected area, applicable ESSs are selected from several different types. At property lines and large building walls, intrusion detectors covering large areas are required as opposed to a room within a building or a vault. Also, exterior applications require weatherproof enclosures and are sometimes subjected to a wide temperature range.

b. Detection systems. There are many types of electronic security systems in use at military installations. All require frequent tests and checks, in some instances as often as once a day. The emphasis is on operational tests to ensure the continued functionality of the designed system, rather than on routine maintenance of component parts. Before the advent of low-cost computer multiplexed hardware, security systems were simple hardwired alarm systems, providing a minimum level of intrusion detection. Today, the system may be a fully redundant computer-based system interfaced with a redundant looped time-division-multiplexed communication network for gathering alarm data from sensors and for sending commands to release locked doors under the card-access control subsystem. The remote multiplexer may be microprocessor-based units, capable of data collection, communication with the host computer, and performing limited-access control functions. The security system provides location information as well as delay time for the guards. By successive detections, the security force can track the intruder and relay location information via portable radio communications equipment to the responding guards. In turn, the guards can constantly inform the security force on the progress of their work or the need for additional assistance. The cameras, using various means of target intensification, can “see” better than the human eye. Guard patrols are also used to detect unusual activity. Perimeter detection is accomplished by the application of electronic detection systems.

26-2. Types of electronic security

Electronic security systems can be placed into two categories – perimeter detection and interior detection.

a. Perimeter detection. Perimeter detection is that used to prevent entry into a restricted area and the devices are usually located to protect the exterior premises.

(1) Microwave detection links are devices mounted on posts inside the fence. Transmitters radiate amplitude modulated X-band energy, and receivers detect and process the received energy. Thus, an invisible energy envelope is produced that will detect an intruder.

(2) Infrared detection links are devices that are post-like and mounted inside the fence. Transmitters radiate multiple beams of modulated infrared energy, and the receivers detect and process the energy. Penetration of the invisible infrared shield will alarm the system.

(3) E-field links are transmitter wires and receiver wires are strung horizontally from mounting posts located inside the fence or mounted on the fence. A radio-frequency energy field is generated around the wires. The intrusion of a person into the invisible field will “short” energy, creating an alarm.

(4) Buried sensor links are devices sensing seismic pressure, [or electromagnetic (EM)disturbances for a combination of these] are buried inside the fence, and alarm upon the intrusion of someone into the field of detection.

(5) Other systems are available that can be used in combination with the previously mentioned systems. The probability of detection by these outdoor devices depends on their application. Perimeter detection equipment must be applied with consideration of the environmental limitations of the device’s technology.

b. Interior detection. If the intruder penetrates the perimeter detection, the protected area has been breached. The interior detection then must be in place to prevent further entry into controlled or protected buildings.

(1) Visual or closed-circuit television surveillance may detect the intruder.

(2) Entry into a building is provided by the application of a balanced magnetic switch on doors and openings. This device uses an internal bias magnet to balance a delicate reed switch in the field of the external magnet attached to the door. Should the door be opened, even a fraction of an inch, or should another magnet be introduced in an attempt to defeat it, the switch will change state and alarm.

(3) Other devices for detection of an intruder may be applied inside the building, including microwave and infrared motion detection, photoelectric or laser beams, seismic, sound detection, passive infrared, and other devices.