Appendix E
Physical Protection Systems

Introduction and Summary

Typical fixed-site targets of terrorists are private corporations' assets (e.g., buildings, pipelines, electric pylons), vehicles (planes are a current favorite), bridges, monuments, and diplomatic buildings.

Since a terrorist can seldom be identified before the act, the first line of defense against terrorists is usually proactive physical protection of the target (a barrier between the terrorist and the target). Depending on the degree of protection needed, the physical protection may range from a simple wall or fence, such as a boundary marker, to a sophisticated physical protection system (PPS). A physical protection system is a collection of system elements, combined to achieve protection according to a plan. The classical physical protection system incorporates two substantial surrounding fences with a clear zone between and includes many high-tech sensors and interconnecting communications.

Physical protection systems at different sites are seldom identical because of the differences in facilities, targets, and threats. The basic design for physical protection systems is quite well established but considerable engineering and design tailoring is usually required for each site.

The four basic functions of a modern physical protection system are:

- **entry control,**
- **. detection of the intrusion,**
- **. delay of the intruder, and**
- **• response to the intrusive action.**

All of these elements must be present in any effective physical protection system to the degree necessary to meet the threat expected. The last three functions must be performed in sequence and within a period of time that is less than that required for the adversary (i.e., terrorist) to overcome the physical protection system and commit the act (e.g., property destruction, kidnaping and hostage taking, personal injury, or murder).

The components of a physical protection system will be discussed in more detail below. Elements to be presented include description, applications, technology, operational limitations, existing deficiencies, development status and activity, costs, and expected new capabilities.

Threat assessment is usually the first step in any physical protection system design, followed by site assessment, physical design, construction, operation, and functional assessment. The system elements must be balanced so as not to create weak links. For example, an adversary is not likely to take time to burn a crawl hole in a steel door if the hinges can be easily dismantled. Several useful computer programs are available to aid in assessment of specific site security plans and in the design of a protection system (e.g., SAVI, ASSESS, and SENLAX are a few available at Sandia National Laboratories).

A physical protection system can also provide deterrence because it may be viewed by the terrorist as a formidable object requiring many tools and people to penetrate and thus may result in a delay in his plans, or better, a decision on his part not to act at all. Deterrence, however, is difficult to measure and cannot be depended on.

Brief Assessment of Current Physical Protection Technologies

Except for explosives detection, the technologies and hardware for entry control into a protected area are available and are reasonably adequate for screening personnel and packages.

The common and widely used coded photo badge technology is mature but, by itself, provides minimum security.

A variety of high-security identity verifiers based on personal biometric features are now available and functionally adequate for personnel screening. They are more reliable than using guards to screen entrants, especially for large populations and are operationally less expensive, but they do not present the deterrent and response value of guards.

The technology for metal detectors is mature; they are available and substantially adequate for most weapon screening except for a few selected handguns.

The familiar x-ray package search machine is widely used but some kinds of explosive devices are difficult to detect. Nuclear radiation-based detection systems are still bulky, expensive, and slow. The sensitivity can be set to detect a small mass of explosives if the corresponding false alarm rate can be tolerated.[1]

A perimeter system of a large physical protection system typically consists of two 8-foot chain link fences spaced about 30 feet apart with the area between graded

[1] See the first report in this series, U.S. Congress, Office of Technology Assessment, ***Technology Against Terrorism: The Federal Effort***, OTA-ISC-481 (Washington DC: U.S. Government Printing Office, July 1991), p. 10.

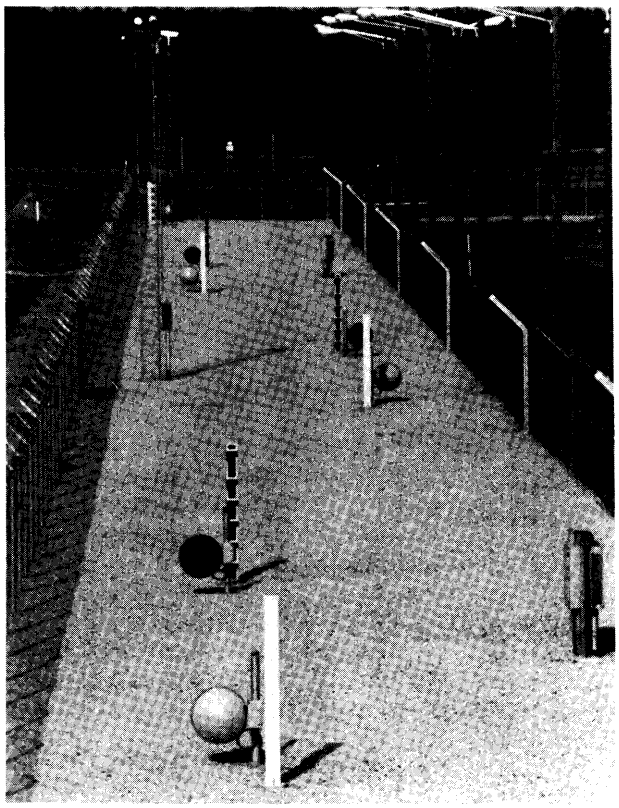


Photo credit: Sandia National Laboratories, 1990.

View of intrusion detection and assessment system.

and covered with rock. A disturbance detector (perhaps a seismic or a taut-wire sensor) is attached to the outer fence and one or two overlapping intrusion detectors, such as an electric field sensor and a beam type sensor are located between the fences. An array of surveillance TVs with matched lighting is typically also installed in this ''clear zone," (see figure E-l). All sensors are then connected to a common alarm, assessment, and control center. The cost of such a perimeter system is typically about $1,000 per foot.

Tests have shown that some barriers that appear to be impenetrable can be breached quite rapidly by determined terrorists who are trained and well equipped.

Although some improvements are being made in the more conventional structural barriers in terms of materials, designs, and construction, more visible technical advances have been achieved in the unusual quick-deployment barriers. These more exotic dispensable-on-command barriers are less developed, but first-generation versions are available for tactical and special defensive applications.

A risk in the use of quick deployment barriers, however, is that in addition to containing or slowing down the terrorists, they may also create a difficult escape path for the evacuees and the response force.

Reliable intrusion sensors are readily available from several suppliers. They are used extensively as single units and in multiple-unit networks in detection systems of all sizes. Internal-intrusion detectors, usually involving the use of a different set of sensors from those deployed along external perimeters, are usually mounted on the walls, windows, or doors of a building. Intrusion detectors are often used in overlapping arrays for mutual protection and reliability.

Closed circuit television (CCTV) is usually used for the initial assessment of an alarm. TV in a large system is usually cost-efficient since one person can monitor several areas at the same time from one central location.

Based on the principle of detection, delay, and response, Sandia Laboratories has developed, under the sponsorship of the U.S. Army RD&E center at Fort Belvoir, a medium-size, flexible physical protection system named SAFER that is quickly deployable on command. It was developed primarily to protect field sites and high-value military assets deployed in antiguerilla or countemarcotics operations. The system hardware is procured and stored in kit form and costs about $360,000 per kit. Each kit consists of infrared sensors, both passive and active, seismic sensors, an assessment platform with low-light TV, and a public-address-system speaker. A video display console is included. The system also includes a razor-tape concertina type of wire barrier, hand-held radios, electromagnetic fence-disturbance sensors, and night-vision binoculars. The kit may be retrieved for redeployment. Several have been procured and stocked and more are scheduled for procurement in 1991.

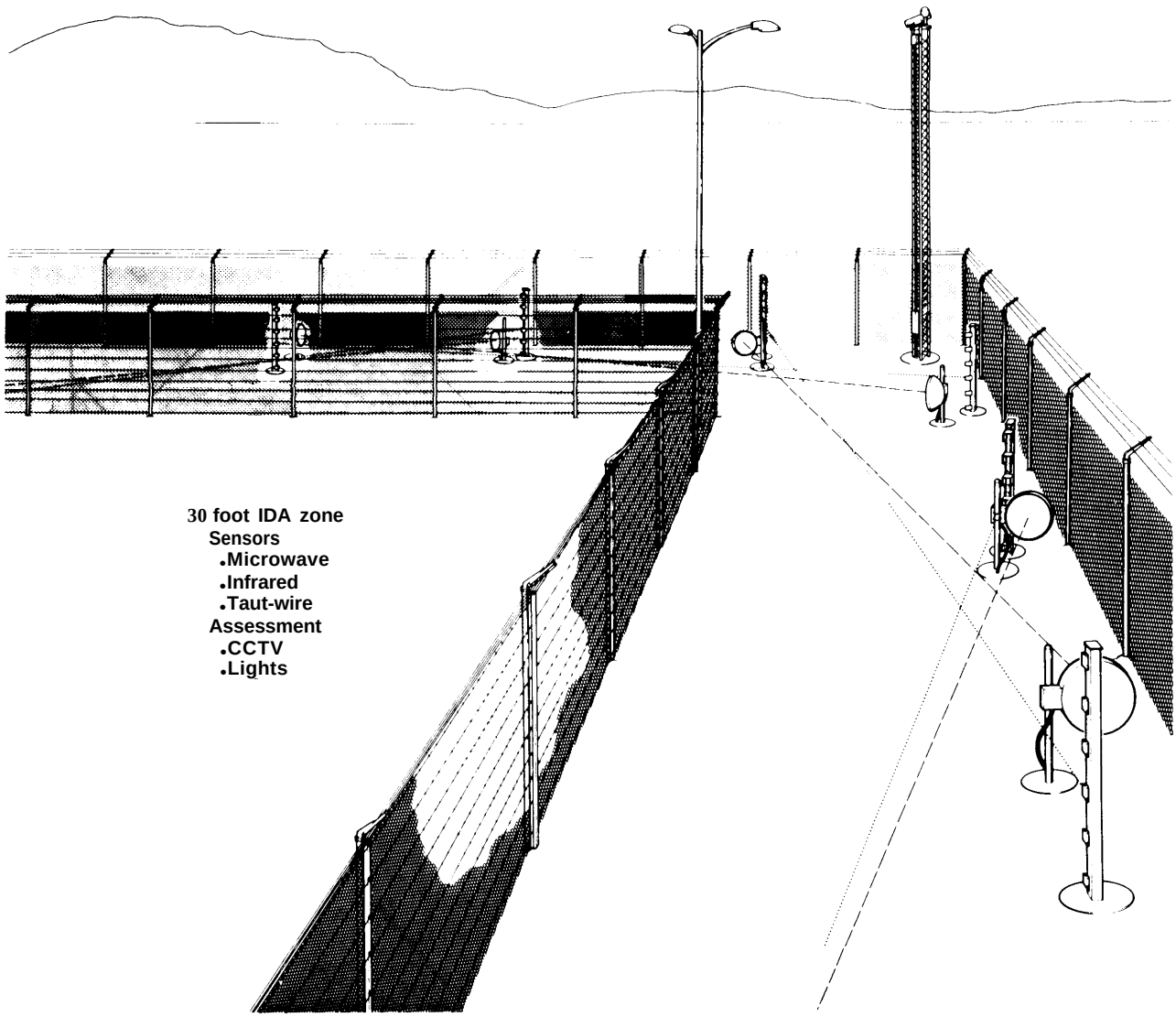
Entry Control

Entry control refers to the admission of authorized personnel to and the blocking of unauthorized personnel from a physically protected area; it includes screening personnel and material.

After a perimeter barrier is established around any protected area it must be provided with an entrance and exit corridor for the movement of personnel, material, and equipment for operation and maintenance. This entry control corridor must include a screening and separation enforcement system. Such systems range from totally manual to fully automatic and may be used for screening on the way out of as well as on the way into the area.

To prevent theft, sabotage, hostage taking, or other terrorist acts, it is necessary to search for concealed contraband, not only on persons but also in packages and vehicles passing through entry control. The items usually looked for are weapons, explosives, drugs, strategic and precious materials, special tools and parts, and hazardous

Figure E-l—Intrusion Detection and Assessment System



SOURCE: Sandia National Laboratories, 1990.

materials. Hand-searching, with or without hand-held sensors, is usually too slow or socially objectionable for a population of more than a few.

Personnel Screening, Manual

In a fully manual screening system inspection is done by a guard or security inspector on an individual basis.[2] At a facility where there are many authorized persons and the guard force is large, this system becomes ineffective and impractical without at least some minimal aid, such as the familiar photo badge, which is frequently coded for machine reading. The use of the photo badge requires that the screening guard make only a comparison between the person's face and the photo for admittance. This system assumes that the badge is authentic and is being presented by the authorized user. In the interest of cost and at additional risk, this comparison is sometimes accomplished remotely using closed circuit TV. Heavy dependence on the photo badge can be a security risk for several reasons: 1) photo badges can be counterfeited, 2) an impostor's face can be made up to match the photo on a stolen, borrowed, or found badge, 3) the guard's inatten-

[2]An example of such a system is at OTA, 600 Pennsylvania Avenue SE, Washington, DC.

tiveness due to boredom, distraction, preoccupation, etc., can make his activities ineffectual. However, as a first line of personnel screening the guard-plus-photo-badge system is often adequate and such systems are well developed and widely used. Photo badges cost from about $1 to $10 depending on the amount and kind of encoding used.

The cost of a full-time (three-shift) guard position is about $185,000 per year. Therefore, in the interest of cost saving, to say nothing of security quality, a reduction in the size of the guard force at entry control locations by using a machine-aided or fully automatic screening system may be attractive. A machine-aided system, for example, using a coded photo badge and a badge reader and leaving only the final approval for each entry attempt to the guard, may speed entry, improve security, and, in the long run, reduce screening costs. A much greater economic advantage may be gained from the use of an automatic screening system.

Personnel Screening, Automated

An automated entry control system, usually with only guard overview, can make use of personnel identity verification devices for screening. Such devices make a close assessment of a personal biometric feature, such as a hand profile, a fingerprint, a voice pattern, a retinal pattern, or the way a signature is written, then automatically compares that verification sample with a previously stored reference sample of the same biometric feature. These devices have existed in development form for a decade and are now available from several manufacturers who can supply not only hardware and software but also the necessary spare parts and technical assistance for installation, operation, and maintenance. Indeed the supply of a variety of functionally adequate identity verifiers is now available to fill the requirements of the security industry. The capital cost of a typical personnel identity verifier ranges from about $1,000 to $5,000 per verifier, which is generally small compared to the total cost of an operational entry control system. The total cost of using verifiers must also include not only machine procurement, but also installation, maintenance, user instruction, user enrollment, and many times the design, procurement, and installation of a management-system network.

The number of verifiers required in an entry control system depends on the speed of the verifier, the number of personnel to be screened, the number of portals, and the patience of the waiting users. Verified performance tests show that about 3 to 7 seconds are required for the verification of a claimed identity. A false acceptance of an unauthorized person and a false reject of an authorized person can occasionally occur, but broadly speaking, the frequency is less than 1 percent. These error rates are interrelated, however, and are dependent on machine adjustment. This kind of accuracy is acceptable for most well-designed entry control systems. More accuracy and speed and less cost is desired, of course, and those goals are the object of current development efforts.

The use of an identity verifier, now commercially available, in place of a guard is usually cost-effective but can also be justified because of fewer errors and better reliability. The deterrence associated with guard presence may be lost if the guard position is totally eliminated in favor of a verifier. However, some security personnel are generally required to oversee the screening operation, help visitors, provide occasional help for the handicapped, care for equipment breakdowns, prevent vandalism, and be available to challenge a suspected impostor.

Successful operation of the verifiers requires cooperation on the part of the user and a minimal amount of operator skill. A personnel screening machine, such as a facial-recognition device that could be used nonintrusively to scan a succession of people at a port of entry or at an airport security screening portal, would be extremely useful to search for certain wanted persons. For example, a known terrorist, who had previously been registered into the recognition system from a photograph could be covertly identified with such a system. With the recent advent of neural networks and other powerful algorithms,

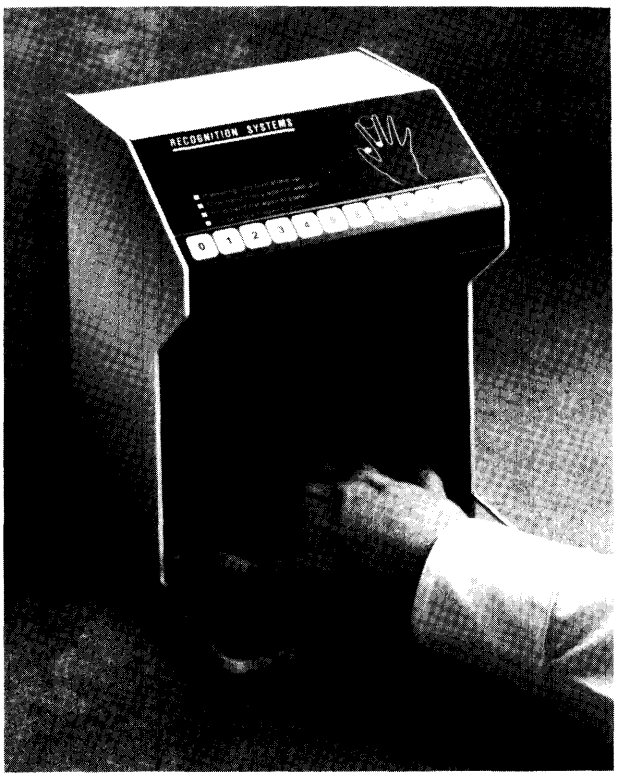


Photo credit: Sandia National Laboratories, 1990.

Hand profile identity verifier.

Photo credit: Sandia National Laboratories, 1990.

Fingerprint identity verifier.

several facial-recognition systems have been developed to a prototype state. Two developers are David Sarnoff Research Center in Princeton, NJ, and International Imaging Systems in Milpitas, CA. No device is yet commercially available.

Entrance barriers in an entry control corridor, including intrusion-resistant doors and turnstiles with associated latching hardware that can be operated remotely, have been in use for years. However, the technology required to insure that only one person, the person whose authority has just been verified, passes through a single door when it is released, is not yet commercially available. The two-door-portal assembly is an operationally adequate device for this entry control task, but it is bulky (3 to 5 feet square), slow (about 20 seconds per entry sequence), expensive ($20,000 to $60,000 per portal), and not widely available. The development of a much simpler, faster, and less expensive doorway monitor is needed.

Weapons Detection

Terrorist activities frequently involve the use of weapons and tools, usually made of metal. Therefore, an entry control system must also screen for unauthorized metal objects that may be carried on a person. The hand-held scanning metal detectors are the most sensitive but their use is slow and manpower intensive and

therefore not practical for screening large populations at a reasonable rate.

The basic portal metal detector has changed little in a decade. It senses a change in an electromagnetic field pattern when a metal object is moved into the active area of the portal. The pattern is sensed after a short electromagnetic field pulse is applied by the portal electronics.[3] The sensitivity of a weapon detector is effected by the weapon's shape, size and orientation, the kind of metal used, the size of the carrier, velocity and direction through the portal, and by other objects in and near the sensing magnetic field. Recent improvements, primarily centered around sensing only during various "time windows" after the interrogating pulse, have provided more sensitivity and more stable operation than previous models were able to attain. The metal detector is limited by its inability to distinguish between a weapon and a piece of innocent metal of the same or smaller size. It may be reasonable to expect that continued development will produce a metal detector that will find these weapons among other pocket clutter but it is unlikely that it will ever be able to find the emerging totally nonmetal gun, in the absence of metallic tags emplaced by the weapon manufacturer.

A software program is being developed for metal detector operation that will provide high sensitivity, regardless of the kind of metal (e.g., iron, copper, zinc, stainless steel, or aluminum) being passed through the portal. There is also some continuing effort toward the development of a very low-power microwave imaging device that will be able to search for high-density objects under clothing (see app. C).

The (regulatory) magnetic field intensity limitation of 1 gauss for metal detectors is restrictive and imposes limits on sensitivity and accuracy. However, in spite of its limitations the use of metal detectors at airports has apparently been effective in greatly reducing the number of weapons carried onto aircraft, as evidenced by the reduction of skyjackings in recent years. The cost of a portal-type weapon detector is about $6,000.

Explosives Detection

Explosives detection has been discussed in detail in the first OTA report of this study and in chapter 4 of this report and so will be discussed only briefly here.[4] An explosives detector is necessary in an entry control system because explosives are not only commonly used by terrorists for forceful entry but also for sabotage and injury within a protected area. Explosives detection is complicated by the variety of carriers to be searched such as personnel and their clothing, briefcases, packages, tool boxes, instruments, and other places where explosives can be hidden for smuggling. The basic methods used for bomb detection are explosives-material analysis (vapor and solid) and object identification with the aid of x rays and hand searching. Important features of a good searching system are high sensitivity, high resolution, high scanning rates, low false alarms, and safety.

Explosives Carried by Personnel

The material-analysis techniques being developed for explosives detection are based on well-known physical and chemical properties of explosives. Currently available explosive-vapor detectors, which use the only automated technique now acceptable for searching people, cannot detect all types of explosives that might be used by a terrorist. Several hand-held detectors based on explosive-vapor collection, concentration, and analysis are commercially available. The use of these devices, however, is manpower intensive and slow. Further, the devices are not sensitive to all types of explosives. However, technical developments in this area have become rapid and new, radically improved devices are now available.[5]

Package Search

For packages, a conveyor-belt search system, as seen in airports for baggage inspection, is frequently used. This scanning system, using x-rays, is limited to generating video images of concealed objects (of various densities) which, if suspicious, must be further assessed by inspectors. This technique relies heavily on the operator. Much attention is now being given to alertness enhancement techniques (part of human factors applications-see ch. 5) such as frequent rotation of inspection personnel and a reward program for the detection of planted test objects. Various x-ray inspection aids, such as color and image enhancement, zoom control, and density highlights are available.

Modern x-ray inspection systems, such as those found at airports, are designed to insure radiation safety. First, the x-ray dose per package scan is very low compared to medical and dental sources. Radiation shields effectively limit radiation levels anywhere immediately external to the search machine to less than 0.0005 Roentgens per hour, which is much less than the maximum allowable set by the Bureau of Radiological Health and Safety. By comparison, cosmic radiation at 35,000 feet is 0.0001 Roentgens per hour or more, so a passenger will receive far more radiation from a high-altitude flight than from x-ray screening of his luggage prior to boarding. These

[3] See app. C for more detailed discussion on metal and weapons detectors.

[4] U.S. Congress, Office of Technology Assessment, op. cit., footnote 1, chs. 4-5.

[5] Ibid., chs. 4-5 and app. C.

radiation levels are not damaging to pharmaceuticals, computers, magnetic tape, food, or and almost all other substances.[6]

Dual-energy x-ray inspection, as the name implies, makes use of two x-ray beams of different energies. This system, besides obtaining item profiles, can also provide information about an object, such as atomic number, when the images of the two beams are compared. By exposing objects to two or more x-ray beams from different directions, three dimensional information can also be obtained (this technique is called tomography). By employing computer processing the maximum image information can be obtained for better item identification. Dual-energy computerized tomography is well developed for the medical industry but is expensive. The radiation backscatter variation of x-ray imaging from materials of different density is also useful in identifying scanned materials. Minimal success has thus far been gained in the development of a computerized system using using neural networks for object recognition from the x-ray image. A fully automated x-ray system, without the human discriminating link, is not yet available, although one firm, AS&E of Cambridge, MA, claims to be close to marketing such a system.

Neutrons of normal thermal energy can also be used to screen packages for explosives materials. The procedure involves exposing the package and its contents to a very low dose of neutrons which interact with nitrogen to generate characteristic secondary radiation, which is detected. Such a machine was developed by Science Application International Corp. and sponsored by the FAA Several of these very large baggage search machines were then built at a cost of something over a million dollars each.[7] The use of high-energy neutrons in a similar system is being considered by other developers. The use of other types of radiation for package searching is an interesting and promising technology but further development is yet required to provide a practical time-efficient machine for the detection of explosives at airports.

Searching for explosives in vehicles such as cars and trucks is usually done by hand searching and sometimes with the aid of hand-held vapor detectors or with wipe patches that are later analyzed for traces of explosives.

Dogs are still used to determine the presence of contraband. Their sniffing time span is quite limited (about 20 minutes per session) and they are strongly dependent on interaction with a specific handler, thus making their availability and use relatively costly (see app. B).

Development activities in the area of explosive detectors has, in the last few years, improved sensitivity and reduced operating times by factors of 10 and 100. However, so far the urgently needed fast, sensitive, and accurate explosives detector for personnel and packages searches has not arrived. A practical and reliable detector for the more commonly used bomb explosives is urgently needed.

Reference 1 in the bibliography to this appendix contains additional information about entry control technology.

Intrusion Detection

Detection is the discovery of an intrusive action at any point in the protection system. Detection is usually reported by an intrusion sensor and announced through the alarm communication subsystem. The intrusion alarm must then be followed by an assessment; if appropriate, the response force will then be notified.

The detection of an intrusion or an attempted intrusion into a protected area is one of the four basic functions of a physical protection system. It is important to make this detection as soon as possible after the start of the intrusive action to provide the maximum time for assessment and response. Maximum delay usually means detection as far from the target as possible.

Exterior Sensors

Several fence-disturbance sensors have been developed to detect attempts at fence scaling or cutting. Personnel and vehicles used for forceful entry by ramming the fence can usually be detected by the same exterior sensors.

A fence disturbance caused by climbing can be detected by special sensors fastened to the fence. The heart of one such sensor consists of a magnet-and-coil arrangement; another utilizes piezoelectric crystals. These measure slight disturbances in the geometry of the fence caused by the intruder. Another relatively unsophisticated sensor utilizes a taut wire, usually barbed wire, stretched along the inside of the perimeter fence. Whenever the wire is stretched, cut, or misaligned by an intruder an alarm is generated by a contact closure. The Israelis are generally given credit for most of the development of the taut-wire sensor. Most of the fence-disturbance sensors are subject to defeat if the intruder avoids touching the fence.

More sophisticated detection sensors have also been developed, tested, and successfully used and are commercially marketed. A microwave intrusion sensor consists of a microwave transmitter and a receiver at opposite ends of a straight section of perimeter boundary. The received

[6] In the interest of safety and for further guidance there exists an ASTM specification, designated F-792.82, entitled Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas.

[7] U.S. Congress, Office of Technology Assessment, Op. cit., footnote 1, chs. 1, 4.

Photo credit: Sandia National Laboratories, 1990.

A taut wire fence sensor.

signal is the sum of the directly transmitted signal and the signals reflected from the ground and other objects in the intervening distance. When any object, for example an intruder, moves into the stable monitored field, the microwave signal received is altered, generating an alarm. These sensors are subject to defeat by a knowledgeable intruder. This deficiency can be overcome by overlap with another sensor such as a radar or infrared sensor. Microwave sensors, like other ray-type sensors, operate across a line-of-sight, so surface grading in the clear zone between the transmitter and the receiver may be required to eliminate a blind ground depression that could create a crawl space under the microwave beam. The height and alignment of the antennas and the distance between them are important factors. Adverse environmental conditions including heavy rain, water puddles, very deep or blowing snow, windblown dust and debris, fog, vegetation, birds, and wild animals can cause nuisance alarms or malfunctions. Deep snow can obscure a careful crawling intruder. Microwave sensors are available from several suppliers.

Infrared (IR) sensors, both active and passive, are also frequently used for intruder detection. The active infrared sensor generates an alarm when the IR light beam from a transmitter, similar in many respects to that used in the common remote TV-channel changer, is broken. The transmitter and receiver are located at each end of the detection zone. Multiple infrared beams are often used, especially at gates and doors, to create a web of rays that make the system more impenetrable. Passive infrared sensors operate on the fact that all animals emit IR energy, the amount and wavelength being dependent on their body temperatures. A passive IR sensor sends an alarm when it detects a change in the incoming IR energy from its field of view, as would be generated by an intruding person. The probability of not detecting an intruder and of getting a nuisance alarm is influenced by the speed of the object, by the ambient temperature, and other environmental conditions.

A video motion detector monitors the electronic signals from a video camera and detects changes in any designated part of the video scene as would occur when an object moves within the field of view. Sometimes only a portion of the total field of view is monitored for motion. Objects other than a person, such as animals and birds, blowing debris, and snow moving through the field of view, can cause nuisance alarms. The size of the moving object or its speed (consider a flying bird) can sometimes be used to distinguish a person from other alarm objects.

In addition to the beam type sensor described above there are several other devices now commercially available for intrusion detection at a perimeter. One known as the E-field detector sounds an alarm upon the disturbance of an established electric field near a conductor. It senses changes in capacitance between the sensor elements such as wires on a fence or between fence wires and the ground. The dielectric constant of human flesh is about 100 times that of air, so as an intruder approaches an E-field fence, the capacitance changes and a resulting alarm is issued, even when the person is not yet directly between the wires. Changing weather conditions, such as humidity, cause a change in circuit characteristics, but frequently the

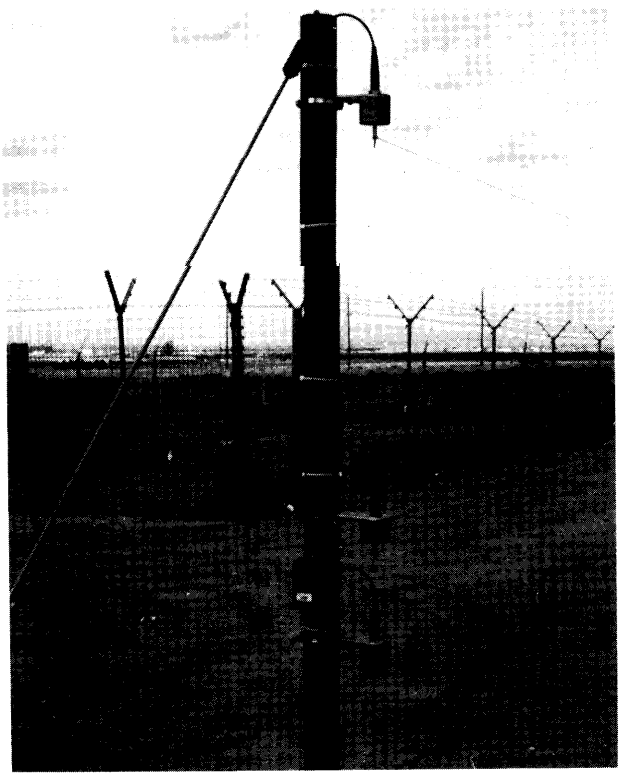
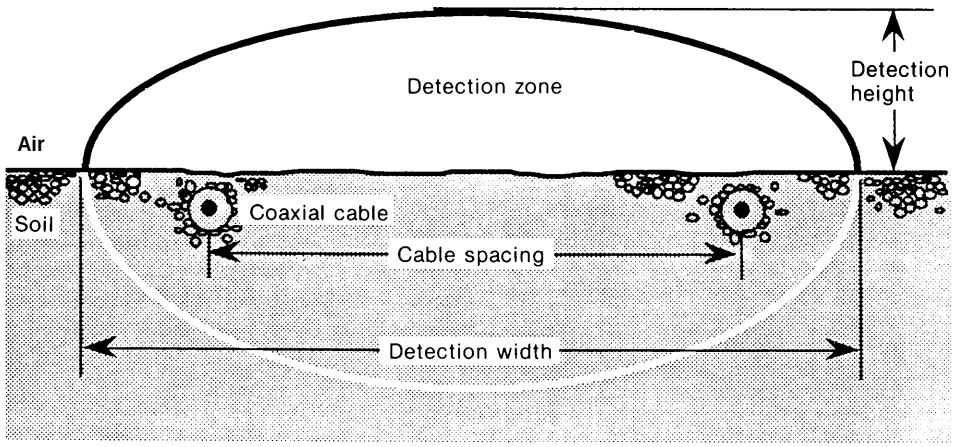


Photo credit: Sandia National Laboratories, 1990.

E-Field fence.

Figure E-2—Coaxial Cable Sensor



SOURCE: Sandia National Laboratories, 1990.

rate and size of the change can be analyzed to determine whether the change is likely to have been caused by an intruder. Unlike the beam from active sensors, the terrain along the monitored path can be crooked and irregular, providing an advantage for this type of detector. The E-field sensor is not sensitive to wind unless it carries with it snow or rain. However, the E-field sensor fence must be kept clear of moving vegetation.

Buried line **sensors are designed for intrusion detection. These sensors are usually buried in the ground for stability and protection but some are marginally suitable for stabilized temporary deployment above ground, for example around a parked aircraft or a building to be temporarily secured. Some lines are sensitive to seismic or magnetic disturbances, or both, that are transmitted through the ground to the sensing elements.**

The seismic line sensor employs transducers, which sense pressure waves from an intruder's footstep or vehicle. Piezoelectric crystals and strain gauges respond to stresses in the sensor cable due to any disturbance of the material around it. The balanced-pressure seismic sensor determines the pressure change between the two parallel segments of the buried flexible tubes caused by the added weight of a passing intruder. Another seismic-sensitive buried line responds to changes in the cable's magnetic core due to stress.

A **buried line magnetic sensor generates an electrical signal that triggers an alarm when an intruder carries or drives an object containing a magnetic material across the line. In the geophone line sensor a coil of wire is moved through a freed magnetic field by any seismic disturbance, thereby triggering an alarm.**

Disturbances that contribute to nuisance alarms are generated by animals, hail, blowing debris, nearby train **or** truck traffic, and **some** industrial noises. Nuisance alarms in magnetic sensors can also be generated by lightning or nearby unshielded power lines.

Another type of sensor consists of two coaxial cables buried in the ground about 6 inches deep and parallel **to** each other (see figure E-2). These cables are of **a conventional coaxial design except that the outer conductor is ported (made with many** closely spaced small holes through the shield). **When** electrical energy is injected **into one** cable, **some radiates out** through the cable shield and **is** coupled through the ground and the **air above the** ground **into** the nearby **receiver cable through similar small ports. When an intruder comes near one of the cables the change in coupling is** sensed and **an alarm is** generated. The sensing **zone** extends **out** about 3 feet from the cables and is effective under the cables too, so **it can** detect tunneling **as well as** aboveground activity. Surface **water from** any source, however, **is a major cause of nuisance alarms, and animals and tall plants in the vicinity of the cables can also contribute to false alarms.**

See reference 2 in the bibliography of this appendix for more detailed information about exterior intrusion detection.

Interior Sensors

A different group of sensors is available for detecting intrusion into a building that houses a protected target. Some of the intrusion sensors used at the external perimeter can also be used internally.

The widely applied balanced magnetic switch is used for indicating whether a door is open or closed and is an extension of the conventional magnetic switch used on doors and windows in home protection systems. A defeat technique is **to** place **an** overriding steel plate **(or** magnet) on the switch **to** keep the switch closed regardless of door

position. In the balanced magnetic switch system the act of adding the steel plate or the defeat magnet creates an alarm.

Sonic and vibration sensors listen and feel for intrusion indicators, such as breaking wood or glass at walls and windows, For monitoring areas like rooms during uninhabited times motion detectors are often used. Active devices for this purpose include the use of sound waves of various frequencies and beams of microwave radiation or infrared light. A very practical nonemitting (passive) infrared sensor is available that detects heat emitted from a warm object, such as a human body. An intrusion sensor that can be used very close to a target is a capacitance blanket that can be conveniently draped over a suitable target and will alarm if touched or even approached closely by an intruder.

Interior sensors are not without their vulnerabilities, which can be exploited by a knowledgeable intruder. This provides motivation for research into the operational characteristics of a sensor system prior to application. Altering power or signal lines to kill the sensor or mask its output or even interject false information is another countermeasure. Where the risk warrants, a device that monitors the line for tampering can be added.

Since commercial power sources and distribution lines are frequently vulnerable to failure due to generating equipment malfunction, storms, etc., uninterruptible electrical supplies with limited life are widely available. The size and capacity of such power supplies cover a wide range from a few cubic inches of batteries with backup energy for a few minutes to a multikilowatt diesel-electric powerplant that can be located and protected within the physical protection system.

Special design thought must be given to the routing and protection of power and signal cables to prevent exposure to adversarial attack and to protect them from ground erosion. Further, to minimize nuisance alarms, the routing of signal cables should be done so as to avoid inductive coupling with other circuits

Alarm Assessment

Alarm assessment is the next step in the security system after a sensor has detected and reported an alarm of any kind. By definition, a false alarm is caused by the malfunction of a sensor or a subsystem such as an intermittent electrical circuit or a power outage or a stray magnetic pulse (perhaps from lightning). A nuisance alarm is generated by a disturbance similar to that caused by a real intrusion but not actually generated by intruding personnel (e.g., blowing debris or animal activity). These invalid alarms, indicating intrusion activity when in fact there is none, are not only undesirable but, if frequent, are intolerable. Nuisance alarms may be eventually ignored or, worse, the offending sensor may be deliberately shut off by the irritated assessment personnel, leaving a hole in the detection system. This problem emphasizes the importance of reliability in physical protection systems. The validity of alarms in an in-depth system can frequently be determined by the simultaneous reporting of an alarm from an overlapping sensor, perhaps of a different type, detecting the same event in the same vicinity.

Closed **circuit** television is usually used for initial **assessment of an alarm. TV is usually cost-efficient in a large system since one person can monitor several areas at the same time from one central location. In addition, the TV can be ideally located and thus have a better field of view, especially with custom lighting. Personnel safety is also enhanced by the use of CCTV.**

An extensive variety of surveillance cameras is available, including the older electron tubes type and the **newer solid-state cameras each with pros and cons concerning illumination required, field of view and magnification, repositioning capabilities, power consumption, sensitivity, resolution, reliability, environmental resistance, maintenance, and cost. Additional hardware required to extend the capabilities of surveillance TV systems is available including special lenses, signal synchronizers, switches, transmission equipment, and video displays. The assessment ability of a surveillance camera is very dependent upon its mounting location and the illumination provided. The TV monitors at the central alarm and communication center are frequently operated in the standby or blank mode until an alarm is generated. They then may automatically be turned on for viewing, perhaps on a preplanned priority basis, and at the same time maps and views of the associated facility and other visual aids may be automatically brought into view to aid assessment. Another frequently used high-tech device is the alarm-triggered video recorder which can be used to provide immediate play-back of the alarm event. Recording on magnetic disc or tape or on optical disc, can be done continuously but is usually done intermittently in the interest of conserving recording media and recorder life. The TV equipment discussed above for surveillance and alarm assessment is practical, well developed, commercially available, reasonably priced, and widely used. Many suppliers are available to provide installation and maintenance information and service. Installation and maintenance is sometimes expensive, especially for retrofits.**

See references 3 and 4 in the bibliography of this appendix for supporting and additional information about intrusion **assessment and about alarm communications.**

Response Force Communication

Communication is a vital function in a physical protection system. The system most commonly used to maintain effective control and coordination of the protective force and response personnel is the popular, small, hand-held, battery-powered FAA voice radio. These radios have a range of about 1 to 3 miles, which is marginally adequate in some applications. Dead spots in the operating area are frequently experienced. The use of elevated repeaters can effectively reduce this problem. The ease with which an adversary can eavesdrop on unscrambled messages is a concern. Furthermore, deceptive messages can be injected into a radio conversation to distract and confuse the security force personnel. Message scrambling or encryption can be used to avoid this drawback. However, as a system becomes more secure, it also becomes more complex and costly and the messages become more noisy and less intelligible. Jamming, or flooding the radio transmission with noise by the adversary to make the conversation unintelligible, is also a potential vulnerability. Techniques, such as programmed frequency hopping, can be used to combat this problem. Other message-transmission media such as phone lines, intercom networks, public-address systems, and even hand signals can frequently be used as alternatives to or in conjunction with radios. See reference 5 for more detailed information about protecting security communications.

Delay Barriers

Most conventional **security** barriers **at** industrial facili**ties are** designed **to** deter **or** prevent occasional **acts of thievery or** vandalism. In the case of determined terrorist activity, however, the traditional fences, building walls, doors, locks, etc., will not prevent intrusion but each may contribute some delay. Barriers around a protected area simply slow down the adversarial penetration into the controlled area. Delay after intrusion detection contributes to the time needed for response-force notification, deployment, and action. Each additional second required by the adversary after detection provides that much more time for the security response force to interrupt the terrorist action. It should be emphasized that if the adversarial action is not detected early in the penetration attempt, barriers will be much less effective.

Tests have shown that some barriers which appear to be impenetrable can be breached quite rapidly by determined terrorists who are trained and well equipped. In keeping with the theme of protection-in-depth, the use of several different kinds of barriers may demand of the adversary more penetration equipment, a larger team, more transportation equipment, and more penetration time. If the imperviousness of a barrier (or the perception thereof) is sufficient to deter or prevent the attack, it has accomplished its purpose.

Large protected **sites** occasionally include **natural** barriers such **as rugged coastlines,** high cliffs, **mountains, or** long, clear **distances. Most** barriers, however, **must be constructed and installed.**

Perimeter Barriers

Perimeter barriers form the outermost elements of most physical protection systems. The most common type of outer perimeter is the chain-link fence. Security fences are usually about 8 feet tall and have extension arms angled upward at the top with several strands of barbed wire and are sometimes also topped with a roll of concertina (entanglement barbed wire). If appropriate, the lower edge of the fence can be buried deep enough to discourage shallow tunneling. Although chain-link fences may serve as a deterrent to the casual intruder, most industrial perimeter fences can be scaled or penetrated with handtools very quickly and they do not delay determined adversaries for more than a few seconds. Common handtools (manual and power), thermal cutting tools, explosives, and ram vehicles are the favorites for penetrating barriers. However, if one or several rolls of barbed wire or razor tape are placed on or near a perimeter fence, penetration can be made more difficult in some cases and more time consuming. Several configurations of barbed wire and razor tape, usually in rolls, have been developed and tested for delay efficiency. Some razor tapes have built-in sensors to detect cutting, thus making penetration without detection more difficult.

Much characteristic information regarding perimeter barriers of all types, including the approximate times to defeat have been determined from penetration tests. This sensitive information regarding effectiveness about many kinds of imposing barriers can be found in reference 6 in this appendix's bibliography and can be used for design and operational purposes.

Several lethal barriers, such as electrified fences and fields of explosive mines, have been considered as perimeter barriers, but many problems are involved in the installation, maintenance, safety, and legality of lethal barriers and they are seldom used except for high-risk military installations.

Vehicle Barriers

Personnel barriers are usually ineffective against even small vehicles such as cars and pickup trucks, so specially designed vehicle barriers must be erected where the threat of ramming is sufficiently high. There are many kinds of vehicle barriers to choose from, such as earthen ditches and banks and other fixed barriers (e.g., filled steel tubes), movable heavy concrete (e.g., ''Jersey bounce blocks' or heavy earth-filled concrete planters), and convertible barriers like the pop-up wedge. Loaded trucks and rail cars are sometimes used for quickly obtainable temporary barriers. Large, half-buried tires make reasonably effec-

tive barriers for some applications. An alternate to ramming a barrier is bridging it. Bridging may be especially applicable for excavated, earthen, and other low-level barriers. A motorcycle may be used by the adversary especially if the intrusion and escape equipment can be carried on such a vehicle and if the other onsite vehicle restrictions are designed against only larger vehicles.

The concrete Jersey bounce and conventional highway guardrail cost about $40 per foot installed. Half-buried, large tires cost about $5 per foot installed.

Barriers On Buildings

Doors and windows are logical points of attack. Attack methods for these portals include the use of manual and power handtools, oxygen-fed burn bars, explosives, and ramming vehicles. Attack-resistant windows and doors, doorframes, hinges, and locks are available for secure buildings at increased cost. A full-height turnstile is the functional equivalent of a security door and is generally subject to the same kinds of attacks. Other openings such as ventilation ducts, large water pipes, and other utility ports are also vulnerable points and must be considered.

Walls of buildings, vaults, and other structure are usually considered to be more resistant to penetration and less attractive as targets for forced entry than are doors, windows, air vents, and other conventional openings.

Because of their structural reputation and rugged appearance, concrete walls are almost universally believed to be formidable barriers. However, in conventional construction, the kind and shape of the concrete and the size and spacing of reinforcing bars are located for structural requirements and not to prevent penetration. Testing has shown that standard reinforced concrete walls are vulnerable to rapid penetration.

Explosives are especially effective against concrete walls. The shock waves produced by an explosion propagate through the concrete and result in fragmentation and spalling. The fragments are forced out, leaving a relatively clean hole except for the rebar, which often requires more time to remove than the concrete. The use of precast T-section walls or roofs generally provides little delay because of the lack of rebar. A technology for security walls, not usually used for conventional construction, includes the use of special aggregate ingredients such as steel wires or balls of ceramic or lead to provide more resistance to penetration by using cutting and burning tools or explosives. The use of a stand-off wall, located a few inches ahead of the main protection wall, requires added time for its removal or requires the use of a much larger or a second explosive charge. These supplementary features add cost to the protective structure.

One advantage of concrete barriers, even if penetration time is less than might be expected, is the sophistication and weight of tools that must be carried by the adversary.

Vaults

A vault is considered hereto be a strong repository the size of a small room, usually within a larger building. It is constructed to secure its content from unauthorized persons and is usually not a workplace. With the right equipment, the time required to penetrate an 8-inch reinforced-concrete vault wall and a half-inch steel door is only a few minutes. Earthen overburden when appropriate, can add appreciable time and adversary exposure to the breaching process, depending on its thickness and the removal equipment used. New facilities requiring heavy physical protection might appropriately be totally buried. Although subterranean construction is not frequently used, the technology and basic design considerations have been well established. The comparative cost range per square foot of several wall materials in place is about $15 for 1 inch of steel, $8 for 10 inches of conventional concrete, $40 for expanded metal/concrete (the kind frequently used in safe-deposit vaults), and $0.50 for 30 inches of soil overburden often used on the top of large vaults.

Dispensable Barriers

Barriers may be passive, like walls and fences, or active and quickly dispensed into place. Dispensable barriers and deterrents are designed to add physical encumbrances and to interfere with an adversary's personal sensory and motor processes. Such barriers include rapidly dispensable rigid foams, sticky foams, aqueous foams, sticky sprays, slippery sprays, sand columns, noise, lights, smoke, and rubble piles. Most of these materials can be stored in a compact form in an out-of-the-way place and dispensed quickly when sufficient threat warrants. This dispensable denial technology augments the usual protective structures. If such items are used, the adversary must conduct his breaching activities, which now may be more taxing or hazardous, while in personal protective gear further reducing his speed and endurance.

Obscurant materials include smoke of various kinds and aqueous foams. Techniques for generating obscuring and irritating smokes are quite well known from military literature.

Psychological stresses, such as flashing lights at various frequencies and intensities, are believed to be of little deterrent value. Likewise, the use of sound at very high and very low frequencies is not considered to be an effective adversarial deterrent. However, high-intensity audible sound, besides being very uncomfortable to the unprotected ear, makes audible communication between adversary team members very difficult, adding more time to the barrier breakthrough task. The cost of such a noise

generator is quite minimal. A very high-intensity continuous light (above 1 million candle power) has been determined by Navy security organizations to be effective in temporarily blinding an adversary and thus causing delay.

Polyurethane is a popular rigid foam that can be expanded to 30 times its stored volume. It can be used on short notice to block a passageway or sometimes directly to encapsulate a protected item. Many formulations of polyurethane foams for this purpose are commercially available and cost about $50 per cubic meter of foamed volume. The dispensing equipment costs about $5,000 to $10,000. There are hazards to a person caught in the foaming process such as entombment, exposure to 130 'C temperature, and possible chemical toxicity.

Sticky foam has an expansion ratio of about 30 to 1 for the frost few hours. It effectively entangles the adversary and fouls his equipment. When appropriate, it may even be applied to the target. The foam costs about $50 per cubic meter dispensed. Similarly, sticky spray, with little expansion, is intended to be applied on command with entangling effects similar to sticky foam. These sticky materials are very effective mechanical impediments. However, as one might imagine, the clean up operation after dispensing the sticky stuff is laborious and expensive.

Slippery materials greatly reduce normal friction on smooth walkways and equipment, making the terrorists' progress slower and more hazardous. The material is applied in dry powder form but when sprayed with water becomes an "instant banana peel."

An airborne obscurant can render the adversary "blind" and slow his progress by making it difficult for him to recognize targets, tools, team members, and entanglements. Several smokes and smoke generators are now commercially available. Smoke generators cost from about $25 for a single military smokepot to a more exotic and much faster system for about $10,000.

Aqueous foam is generated by spraying a detergent-like surfactant solution onto a screen while blowing air through the screen, resulting in a material expansion factor of from 100 to 1,000. A dispenser that makes about 100 cubic meters of soapsuds-like foam per minute costs about $2,000. This foam is also a fire suppressant and can absorb significant energy from an explosion, which may be of some interest. About the only hazard to personnel is becoming sufficiently covered so that the person can no longer breathe.

Sensory irritants, such as tear gas, respiratory irritants, and some pain-producing agents, quickly produce an incapacitating effect once in contact with the skin, eyes, and nose. Distress symptoms soon disappear when exposed to fresh air. The large margin between incapacitation and lethality makes some substances, such as "CS" and "CR," agents of choice.

The social acceptance of dispensable deterrents and the related legal aspects must be considered in determining their applications.

Physical protection systems range in size from one building with a few protection features to a multi-acre site with the full array of entry control, detection, assessment, delay, and response systems and the appropriate security and operating personnel.

Response Force

The last element of a physical protection system is the response force, made up of trained security personnel, and the necessary equipment, such as weapons, body protection, transportation, communication, etc. Clearly, a physical protection system without a response force would be of little use in many applications (although for some situations, the eventual response force may be local law enforcement personnel not actively involved in the site security plan). An intrusion alarm would get little response and any barrier, however formidable, would be eventually surmountable with no opposition. The purpose of the response force is to intercept and neutralize the intruding adversary.

A part or all of the response force may be located on-site or off-site. The response force maybe made up of local or State police, military force, a dedicated response team, or some combination thereof, which mayor may not include regular security system operating personnel. Because of the variety of response-force compositions, it is difficult to generalize about specific procedures and tasks that the force may be expected to perform but the final objective is clearly to prevent the adversary from accomplishing his objective.

Accurate and timely communications with the response force must contain as much information as possible about the adversary force size, actions, tools, weapons, location, direction, etc., and instruction for response-force deployment. Aside from the personal safety of the individuals, it is clear that the response force must survive intact and so must be trained in tactics for the safety of its personnel. Training includes instruction about the facility's corridors for cover and concealment and to avoid ambush. A computer-based technique known as surrogate travel is available to aid in deployment and tactical movement. Tactical practice is necessary for response-force proficiency and will provide realistic estimates of response times and tactical plan validity.

A group of firearms that project laser beams has been developed. When used with jackets and helmets that detect the laser light, response training may be devised with little risk to the trainees. These devices for shooting

"laser bullets' are commercially available in the form of handguns, rifles, submachine guns, and other weapons.

To ensure adversary neutralization in the most time-effective manner, a balance is necessary among the several response-force constituents, including the number of force personnel, planning, training and practice, and the available equipment. Members of the response force must have rapid access to the needed weapons, vehicles, radios, and personal protection equipment (i.e., body armor, helmet, protective clothing, and sometimes gas masks and contained breathing equipment), all consistent with the environment and the expected conflict. The equipment required for the response force is strongly dependent on the other characteristics of the physical protection system.

Construction Technologies and Strategies

Above, a number of technologies have been presented that help protect fixed sites against unauthorized entry. These fell into three broad categories: perimeter barriers, sensors and alarms, and access control. In addition to these fields, there is the important area of architecture and engineering applied to buildings that may become targets of attacks. The primary threat discussed below is bombing, perhaps the most common and certainly the most deadly tactic used by terrorists against U.S. diplomatic installations and military installations.

Obviously, it is far easier to implement protective measures by incorporating them into the design of a facility *before* **it is built, rather than to retrofit fixes after the fact. However, there exist options for reducing vulnerability to attack with explosives even in the latter case. Most of the technical aspects that follow are not "high tech," but, rather, are in the domain of classic civil engineering and architecture. What follows is a brief survey of a developing field.**

Bombs may be introduced into a site by brute force (e.g., a vehicle bomb), by throwing or launching, or by stealth (e.g., inside mail). The first tactic is the most difficult to defend against, since a very large quantity of high explosive (several tonnes) may be used. If this threat is successfully opposed, lesser tactics, such as throwing a bomb over a wall, can be dealt with relatively easily. To put the matter in perspective, the amount of explosive needed to destroy an aircraft is on the order of hundreds or thousands of grams; a tonne is a million grams. Car and truck bombs, made of up to a tonne or two of dynamite or plastic explosive, have been commonly used across the world, from Beirut (against the U.S. Marine Barracks and against diplomatic buildings), to Belfast, to Bogota, Colombia. They are able to cause the collapse of multistory buildings made of reinforced concrete, even when the bomb is located tens of meters from the target.

The design response to such a threat incorporates several elements. The first relies on enforcing a standoff distance around the potential target.[8] The standoff distance will depend on the size of the threat and on the inherent resistance of the building to overpressure. Only carefully screened vehicles would be allowed within this distance from the target. For some purposes, a 150-foot (about 45-meter) distance is used. Clearly, for retrofitting existing buildings, it is usually impossible to satisfy this requirement. However, the requirement can often be met when starting from scratch, that is, before site acquisition and design are completed for a new building.

Another layer of defense against vehicular bombs is the use of barriers and of layout and landscaping. The strength of the barriers is determined from the speed and the weight of the postulated threat vehicles. The energy that needs to be "absorbed" in order to stop a vehicle attempting to traverse a barrier is proportional to its weight (strictly speaking, to its mass) and to the square of its Speed.[9] Some types of barriers have been mentioned in the previous section (e.g., the Jersey Bounce blocks); there are others, ranging from large reinforced "flower pots' to concrete-filled cylinders, pyramids, cubes, tires, and 55-gallon drums. Stopping power for each in terms of vehicle speed and mass can be calculated and tested. Some barriers are active, rather than passive; normally not deployed, they can be rapidly activated in case of alarm. A familiar version is the drum type, which, when dormant, is flat, allowing easy passage. When activated, a plate, supported by a heavy cylinder, rapidly rotates upward from the ground to block a vehicle. In addition, one might place ditches or earthen berms in strategic places around a target building. The ditches would cause trucks to tip down if they attempt **to cross; any** blast would then be partially broken **by the ditch. Berms also function to break the path of the blast wave through the air.**

In order to reduce the speed to which vehicles may accelerate, barriers and obstacles may be laid out along access roads. Right angle turns, S-curves, traffic circles, movable barriers, are all options to this end. Maximum speed at turns are determinable from the turn radius; likewise, the maximum speed achievable between barriers (from a dead start) can be easily determined in planning traffic layouts.

In designing a building that maybe a target, both the layout and the strength of individual elements must be calculated. Those areas containing critical facilities

[8] **This discussion of protection against bombing attacks against fixed site facilities relies largely on** information from U.S. **Army Corps of** Engineers, *Security Engineering Manual (Official* Use Only), **Protective Design Center, Missouri River Division-Omaha** District (Omaha, NE: U.S. Army Corps of Engineers, January 1990).

[9] **The kinetic energy of a** moving object is one-half the product of its mass and **its speed squared.**

should be placed towards the interior of the structure. Corridors and less essential rooms may be placed as buffers around the more critical areas. Windows in exterior walls provide a clear vulnerability; it is preferable to place windows around an interior courtyard.

Exterior walls should be designed to resist blast effects, given the standoff distance and the quantity of explosive taken to be the credible threat. For engineering design, tables have been calculated showing, e.g., the protection levels afforded against a 1,000 pound high explosive by reinforced concrete walls of various thicknesses, as a function of the standoff distance. Similar analyses are available for blast resistance in doors and windows. Roofs should be designed of reinforced concrete with a maximum span of 1.5 times the supporting wall spans. The thickness of roof slabs can be determined from similar tables that provide the blast resistance as a function of thickness and stand-off distance. Additional safety measures to take include using shatterproof lenses on light fixtures and bracing suspended fixtures, ductwork and plumbing.

The structural framing system should be able to resist forces and torques applied when the building suffers the blast load. Exterior exposed columns must be hardened to withstand blast effects. The framing structure should be designed to avoid a concatenation of failures, in case of failure of an element. This criterion must be incorporated to avoid catastrophic collapse of the entire building under blast load.

The above discussion can be amplified by tables from reference 1. Technical experts present, in addition, abroad set of design features to avoid, such as long spans, prestressed load-bearing cables, masonry buildings, and bar joists. Implementation of the blast-resistant features provides protection similar to hardening buildings against earthquakes.

Appendix E Bibliography:

1. **"Entry-Control Systems Technology Transfer Manual," SAND87-1927 (Albuquerque, NM: Sandia National Laboratories, May 1989).**
2. **"Exterior Intrusion Detection Systems Technology Transfer Manual," SAND89-1923.UC-515 (Albuquerque, NM: Sandia National Laboratories, May 1990).**
3. **"Video Assessment Technology Transfer Manual," SAND89-1924.UC-515 (Albuquerque, NM: Sandia National Laboratories, October 1989).**
4. **"Alarm Communications and Display Technology Transfer Manual, " SAND90-0729.UC-515 (Albuquerque, NM: Sandia National Laboratories, November 1990).**
5. **"Protecting Security Communications Technology Transfer Manual," SAND90-0397.UC-515 (Albuquerque, NM: Sandia National Laboratories, March 1990).**
6. **"Access Delay Technology Transfer Manual," classified UCNI, SAND87-1926/l .UC-5 15 (Albuquerque, NM: Sandia National Laboratories, September 1989).**

All the above documents may be obtained from Director, Office of Safeguards and Security, U.S. Department of Energy, on a need-to-know basis.