Topic 6
Security Systems

Introduction and Issues

- Security is a fundamental human requirement. It is a natural instinct to preserve ourselves, our loved ones and our property from any intrusion or any danger.
- This lecture looks at the security factors affecting the design of the building, its interior layouts and surroundings.
- We will look at related aspects of types of security breaches planning, detection devices and alarm systems.

In reality, all parts of a building can be penetrated, even those made of steel and reinforced concrete. All buildings, no matter how small, should provide some level of security.

- Security systems can be divided into two major types, passive systems and active systems.
- Passive systems do not include any dedicated hardware for security, but is based mainly on spatial planning and organization, management and building fabric and construction.
- Active security systems employ dedicated hardware that actively detects and controls security breaches and conditions. Active systems include detection and alarm systems.

Security Planning

- Even though there is no full-proof security systems, the objective of security planning is to delay, confuse and control intruders throughout the building's lifetime.
- The first aspect of security planning is to determine the level of risk from intrusion that the building is susceptible to and to strategise accordingly.

There are 5 levels of security

Level 1

- Security against vandals and opportunists. For example targeted public amenities, confidential information.

Level 2

- Security against intruders and interlopers, unwanted and unwelcome visitors with dubious intentions.

Level 3

- Security against burglars and burglaries of household items, important information.

Level 4

- Security against planned and deliberate crimes. Security for high value items such as jewelry, valuable paintings, cash etc.

Level 5

- Security against acts of terrorism and espionage e.g. industrial and political

Types of Intrusions

Intrusions and security breaches become increasingly more complex day by day in terms of techniques and targets.

These can be classified into the following:

- Voyeurism, vandalism and unplanned thefts. Taking advantage and opportunities of insecure locations.
- Spying and espionage as well as planned robberies. The intruder determines the target and the methods. This includes deceptions and embezzlements. Can occur from without or within an organization. Counter measures on top of physical aspects include tightening of management systems.
- Sabotage. Intended destruction of property or industrial/business processes. Arson, explosions, etc.
- Assault. Usually towards an important target, core of an organization. Effective active and passive systems are necessary, including the use of security personnel.

Vandalism and Design Solutions

- Vandalism results in the destruction of public property in public places. Significant social studies have been conducted and theories applied but the problem is difficult to control. Mitigation procedures can nonetheless be taken.

Why does vandalism occur?

- Vandalism is usually associated with crimes or misdemeanors carried out by juveniles under 15 years of age. Between the ages of 10 and 15, vandalism is considered as a game. As the child grows older, interests change and the sense of responsibility and possession increases. Acts of vandalism are also conducted by adults especially where there is social decay. Targets of vandalism include property that is seen as public and without direct ownership. In such cases, it is important to inculcate the sense of belonging and community among the surrounding people.
- Examples of targets: Playgrounds, walkways, lifts, public furniture and toilets.
- Types of vandalism: destruction, graffiti and misuse.

What triggers vandalism?

- Factors which trigger vandalism include:
- Untended property
- Property that is already damaged, e.g. Dirty walls and broken windows
- Continuous deterioration of the above leading to social distress and low quality surroundings and discomfort resulting in slum areas.

How to avoid vandalism?

Defensible Space

- Apply the concepts of defensible space where the spirit of ownership and belonging is inculcated, and where public and public access spaces are observable by segments of the community.
- Reduce the number of public spaces and encourage social surveillance. Surveillance by individuals and/or groups of individuals that have a stake or commitment towards a particular space.
- Places that appear without owners are often targeted.

Defensive Concepts

- Ensure that public amenities are made of sterner materials that are difficult to damage.

Management Concept.

- Ensure damaged property or items are repaired quickly before the situation deteriorates.
- Public Awareness Campaigns.

Security Planning

Security planning consists of

- Physical Planning
  - made up of passive security systems combined with active security system.
  - includes hardware as well as what is already physically in place.
- Management Planning
  - includes the policies in place within the organizations and the work culture.

Physical Planning

- Use of physical barriers as a line of defense around an area, space or building.
- There are three stages of physical Planning for security:

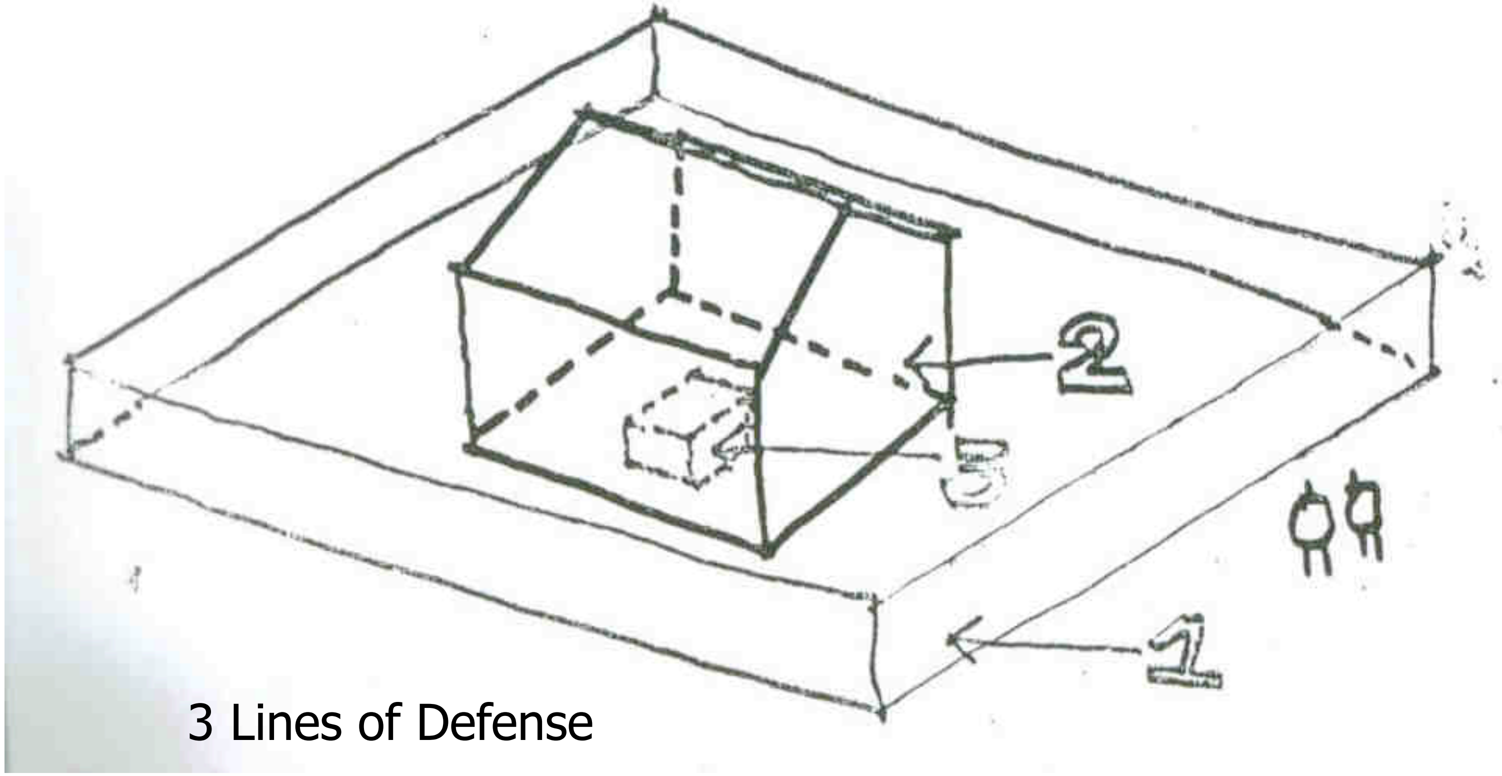

Fig 6.1 Three Lines of Defense

Physical Planning

First Line of defense

- Normally occurring around the perimeter along the site boundary.
- It can be either man-made (gates, fences etc.) or natural (rivers, lakes, cliffs etc)
- Serves to delay or temporarily obstruct intended intruders. Serves as a deterrent and discourages random acts of security breach.
- Elements that need consideration are ingress and egress, emergencies and control.

- Can be combined with active security systems
- When the barriers are located over a wide area, a clear zone can be created over which visual surveillance can occur, between the 1st and 2nd line of defense.
- If there is considerable landscaping, it is advisable to include active systems. Thorny plants add to the security aspect.
- A security tower system can be utilized. Its effectiveness depends on its location and height. Its isolated location may result in a reduction in alertness of the security personnel.

2nd Line of Defense

This is a 3-dimensional mechanism which is more important than the 1st line of defense as there are several potential weak points. Elements that need particular attention are:

- **Doors** – hinges and locks need particular consideration depending on the buildings risk factors.

- **Windows** – the weakest point considering glass is often used. For high risk buildings that do not have security grilles, sensor alarm systems should be used.

- **Emergency doors** – If not planned properly, this is the most vulnerable point of intruder entry. Direct one way exit that is unlocked should be connected to security sensors. These exits should be located in exposed areas that are not hidden from general views.

- Roofs –

3rd line of Defense

- A 3-dimensional system that if designed properly can prevent transgressors from acquiring valuables.
- Examples are safes, strong rooms, panic-rooms.
- Risk levels will determine the type of security required.
- Valuables should only be handled and guarded by specific personnel only.
- An effective barrier is a room within a building that is isolated from other areas.
- Its location is often in the central parts of a building without windows or direct exit points.
- Entry points are minimized and controlled. Avoid common walls with other buildings.

Internal Circulation and Security Management

- Properly planned buildings limit areas that need to be protected, reduce entrances and provide no unobserved lines of approach.
- Costs of providing alarms, security guards and protection are reduced and more secure buildings result.
- Internal circulation of a building can present many security problems especially at entrances.
- Each unsupervised entrance is a risk day and night and 24 hour supervision with holidays and relief can bear significant cost.

3 types of intruders for buildings in use are:

- Unauthorised persons
- Authorised persons who commit transgressions
- Visitors with official business who take advantage

- Only proper security management systems can prevent 2 and 3 above.
- Architects must allow for security planning to enable the organization to plan its management of security especially for high risk buildings.

Target Risks

- Every building has high risk targets, example: cash registers, safes, strong rooms etc.
- Concentric zones according to the level of security risks can be utilized to raise the awareness of the levels of security for staff and visitors.

Active Intrusion Detection Systems

- To understand the design of intrusion detection systems, it is necessary first to understand the characteristics of the commonly available intrusion detectors (sensors) on which these systems are based.
- Once an intrusion alarm has been given by a sensor, the signal must be processed and appropriate action taken. This may include sounding loud alarms, turning on lights, sending signals to proprietary or private surveillance services or police etc.

Elements in an active Intrusion Detection System include:

- Detection devices or Sensors
- Control Equipment – switches, relays, reset buttons
- Signaling link – wired connection to alarm bells or surveillance service providers or police.
- Wired connection to power source – mains or battery.
- Power source

Mechanical Motion Detectors

- This can be used where window foil or fixed contacts are impractical.
- This device is a spring mounted contact suspended inside a second contact surface.
- Any appreciable motion of the surface on which the device is placed causes the contacts to connect temporarily, turning in an alarm.
- These devices are very sensitive and can be activated by sonic booms, wind, and even a heavy truck passing by. For this reason such units are provided with sensitive adjustment.

Photo Electric Devices

- These devices operate on the simple principle of beam interruption. When the beam is received, a contact in the receiver is closed.
- Interruption in the beam causes the contact to open setting of the alarm.
- Older devices use visible light beam which is effective indoors, but outdoor dust, insects, birds etc. show the location of the beam. Birds and small animals set it off. Dispersion of light also limits the throw of the devices outside.
- Modern units use lasers and infra-red (IR) beams, which are less easily detected and can be arranged to differentiate between intruders and other disturbances.
- When a laser beam is used, the signal can be picked up, amplified and transmitted a different direction, thus establishing a perimeter security fence from a single source.

- The ability to focus on a particular area is utilized to cover areas both horizontally and vertically.
- As the PIR detectors are not sensitive to motion but are to heat it is usable where motion is unavoidable.
- The principle disadvantage of PIR detectors is that rapid temperature changes caused by direct insolation, a cold breeze, a heater turning on etc can cause the alarm to trigger.
- PIR detectors can be used as motion detectors by using a multi-beam (zone) unit.
- Motion is detected as changes in IR radiation of adjacent zones or in the radiation of a zone or in the radiation of a zone with respect to the background, both of which characterize motion.

- However because Doppler effect depends on relative motion between the source and the moving body, an intruder moving laterally may go undetected if sensitivity has been reduced to avoid false alarms.
- Therefore units should be located so that the path of an intruder is as nearly as possible directly toward or away from the detector.
- Ultrasonic units are cheaper than microwave units but can be disturbed by strong air turbulence and very loud noises.
- Microwave units are undisturbed by air or noise but because they penetrate solids they can be affected by motion outside the protected area.

Acoustic Detectors

- These units alarm when the noise level exceeds a preset maximum.
- Alternatively they can be arranged to respond to a particular range of frequencies corresponding to the noise of breaking glass, forced entry or whatever is desired.
- Although applied principally in security systems, they can also be used as occupancy sensors for switching of lighting.

Multiple Detectors

- As with fire detectors, a balance must be struck between the sensitivity of detectors and the nuisance of false alarms as increasing the former increases the latter as well.
- One very effective method is to use multiple detectors with different technologies that verify each other. Units are available that combine PIR and ultrasonic detectors in a single housing.
- It does not transmit an alarm until both detectors indicate intrusion. This dual technique is applicable for area and perimeter protection as well as portal surveillance.

Residential Intrusion Alarm Systems

- Residences usually utilize door and window magnetic switches as well as PIR and /or motion detectors.
- A manual switch at the end of a long cord is also provided so that a resident may set off the alarm at will if an intruder is heard.
- If the system employs the same audible signal devices as the fire system, the sound should be distinctive so that the nature of the alarm could be discerned aurally.
- Intrusion alarm systems can be continually supervised by connections with central stations of companies whose business is such supervision and that respond directly to an alarm call or notify local police of any illegal entry.

Multiple Dwelling Entry and Security Systems

- Apartment houses and other large residences combine the functions of the familiar lobby-to-apartment communication system.
- The most basic system is a series of pushbuttons in the lobby and an intercom speaker or telephone with which to communicate with residents.
- At the other end the tenant has a speaker microphone plus a lobby door opener button.
- This system can also be arranged to utilize the tenant’s regular telephone.

- When the number of tenants is very large, an alphabetical roster is added to the apartment button panel to avoid the nuisance of scanning all the apartment names when the sought party's apartment number is not known.

- For even larger numbers, an alphabetical tenant register plus a button phone is used. Closed circuit t.v. system is frequently added to the lobby system enabling the tenant to also see the caller.

- Such a system increases the electrical contract cost for an average apartment house 5% to 7%.

- Call buttons within apartments can be used to perform any alarm functions required to deal with an intruder who manages to bypass the lobby security check.

- In geriatric housing designs, these buttons also serve to unlock the apartment door to allow helpers to enter if summoned by lights and alarms.

- In luxury apartment buildings, apartment doors can be monitored from a central security desk and any unscheduled door movement subjected to immediate investigation.

- These systems are custom designed to meet the requirements of the owner.

Hotels and Motels Security Systems

- A security problem applicable to all facilities , including residential, involves limiting entry in unsupervised areas to authorized persons (i.e. unsupervised access control)
- The problems of keys and locks is well known, despite advances in that field.
- More sophisticated means include magnetic cards and electronic combination locks which, because of the ease of code change, are particularly useful for residential facilities that cater for transients.

- The emergency call system is also appropriate for all housing installations especially for the elderly and handicapped.
- The purpose of the system is to alert outsiders to an emergency situation inside a closed apartment. The alarm system is a way to call for help in times of illness or other distress.
- Most often these systems prescribe a call initiation button in each bedroom and bathroom that registers an audible (alarm) and visible (annunciated) signal at a location that is monitored locally or remotely 24 hours a day.
- Additional signals are required in the floor corridor and at the apartment, to alert the immediate neighbours.

Hotels and Motels Security Systems

- Because of the transient population of these facilities and the need to provide maximum service and security for guests during their stay, the principal problem in addition to room access security is hotel equipment security (i.e. prevention of *shrinkage*).

Room Access Security.

- The ineffectiveness of key-locks in preventing undesired entry even in private homes is well known in hotels. The key is little more than a psychological barrier.
- As a result most modern hotels have installed electronic room locks whose opening device code is changed with every new guest.
- These locks may be of the coded push-button type whose coding is changeable from a central lock security console; a magnetically or punch-hole coded card type (figure6.9); or a programmable coded lock and coded key type (figure 6.10).
- All of these systems have relative advantages and disadvantages, depending on the number of rooms, whether the installation is new construction or retrofit, and the average length of the guest stay.

Equipment Security.

- The need to provide expected services requires that guest rooms be equipped with a television and possibly other electronic a.v. devices, meeting rooms with t.v.s, computers and LCD projectors; and that these and other devices be made available for guests use as part of the room fee or on a rental basis.

- One system that's also applicable in schools, offices and industrial buildings senses the disconnection of the equipment from its power connection (wall plugs) and transmits an alarm over the power lines to an annunciator at a selected control location.

- This has the advantage of alarming immediately of equipment removal permitting appropriate retrieval action to be taken in time.

School Security Systems

- Although intrusion alarm and security systems are not historically normal school requirements, the situation has unfortunately changed.

- Sensing devices on windows and doors can be arranged both to trip local alarms and via auxiliary circuits, to notify police headquarters.

- Often vandals can be frightened off by having the alarm system actuate a protective lighting system that illuminates a building exterior and any building interior required, such as record rooms.

- A perimeter alarm detection system of the types described earlier can be installed in particularly vandal prone areas to assist in preventing entry to school premises after hours.

- One model of door opener alarms requires a continuous pressure on the door opening bar of 10 to 20 seconds before the door opens, with the door being immediately activated upon the application of pressure.

- This arrangement (used only where fire codes permit) allows sufficient time for the facility's staff to investigate the attempted exit before the door opens and is applicable only where exit control is the overriding consideration.

- Stair and exit door locks can be arranged to be centrally released from the fire control centre.

- Alternatively the clock is wall mounted and the guard carries with him a key.

- A computerized version of this system is available that simplifies station check-in, automatically checks in guard visit data, and provides a hard-copy data.

- Guard tour systems are also available that permits constant supervision and are particularly active when there are more than one guard on duty.

- Such systems show on a panel the location and progress of the watchman by means of lights that glow when the device at each location is operated.

- Because part of the effectiveness of these systems lies in the timing of the tour, a system can be arranged to sound an alarm if a particular station is not operated within a specific time period.

- Telephone jacks along the route allow the guard to communicate with the supervising office or other point without interrupting the scheduled tour.

- For protection of areas containing highly valuable items, an intrusion alarm system can be employed.

Industrial Buildings Security Systems

- The design and engineering of personnel access control systems is a specialty that has burgeoned since the 1980s and is now an independent profession.
- The large variety of identification technologies plus the control and supervisory functions of computers, has greatly enhanced the access control capabilities of even a relatively small system.

- The traditional access control question was always “who is permitted to pass through a specific portal?”

- The means by which the identification is made that answers this question varies with the importance of access control at that portal.

- Thus entrance to a large, multipurpose space used by many people must be rapid and must avoid the delay caused by a physical barrier.

- The means commonly used is one or more guards who visually and in a relatively cursory fashion inspect a badge with an ID photo.

- When a physical access barrier is involved, passage is slow, depending only partly on the identification process.
- Even with the most rapid electronic identification, a door or portal closure must be physically released and operated, which can be very time consuming. In the particular instance shown in figure 30.23, the identification process is very time consuming as well as it involves human intervention.
- Unattended physical barriers can be released by a multitude of identification technologies depending on their level of importance. At the lower end of the security scale are barriers that require some knowledge and/or inspect an object presented by the user such as a magnetic, bar-coded or proximity reader card (figure 30.24). Because locks can be controlled electronically and programmed remotely, they can be programmed to give access at certain times only, to specific groups of cards or individual cards only, or to prevent access to specific cards (e.g. cards reported lost) or for any other reason. The element of time controlled access is relatively new; it integrates relatively well with intrusion security systems because portals can be easily coordinated with changing work schedules. Thus a person can be barred form entering an area in which he is not concerned with at that time of day (figure 30.25)

- Because locks can be controlled electronically and programmed remotely, they can be programmed to give access at certain times only, to specific groups of cards or individual cards only, or to prevent access to specific cards (e.g. cards reported lost) or for any other reason.
- The element of time controlled access is relatively new; it integrates relatively well with intrusion security systems because portals can be easily coordinated with changing work schedules.
- Thus a person can be barred form entering an area in which he is not concerned with at that time of day (figure 6.16)

- In view of the many methods of available access control technologies, access control is used to limit access to other aspects such as to copy machines, fax machines, phone lines and other office facilities frequently used by employees for other than purely business purposes.