Security Design and Systems

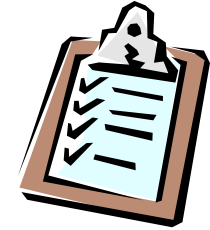*Ir. Dr. Sam C. M. Hui*
Visiting Assistant Professor
Department of Mechanical Engineering
The University of Hong Kong
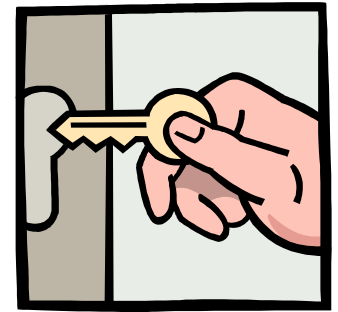E-mail: cmhui@hku.hk

Feb 2017

Contents

- Basic Concepts
- Physical Security
- Risk Assessment
- Security Planning
- Crime Prevention
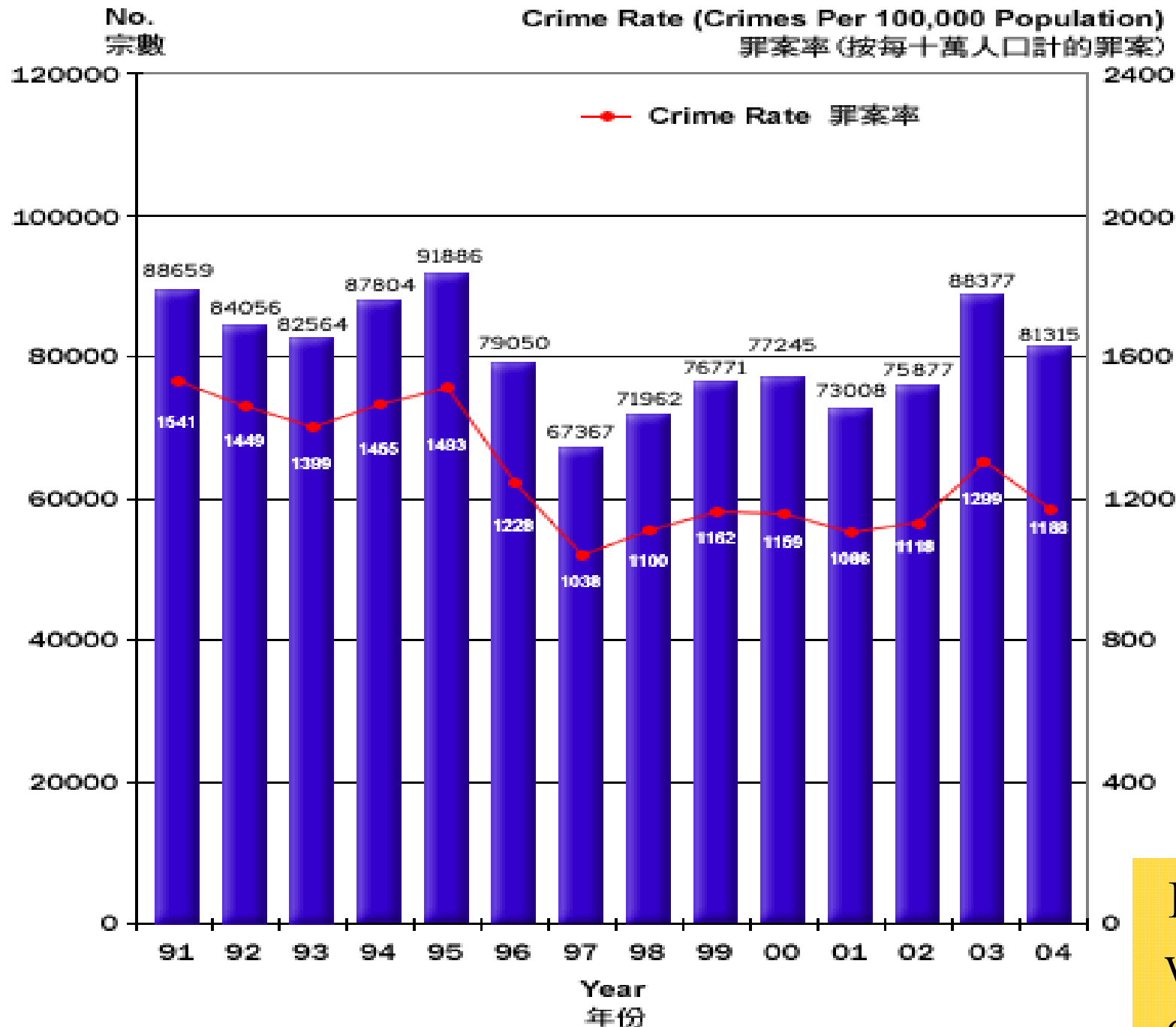- Security Systems

Basic Concepts

- Common terms
  - Security design/engineering
  - Crime prevention
  - Loss prevention
  - Crisis/Emergency management
- Relationship with insurance claims
  - Affect insurance premium costs
- Applications: residential, commercial and industrial security systems
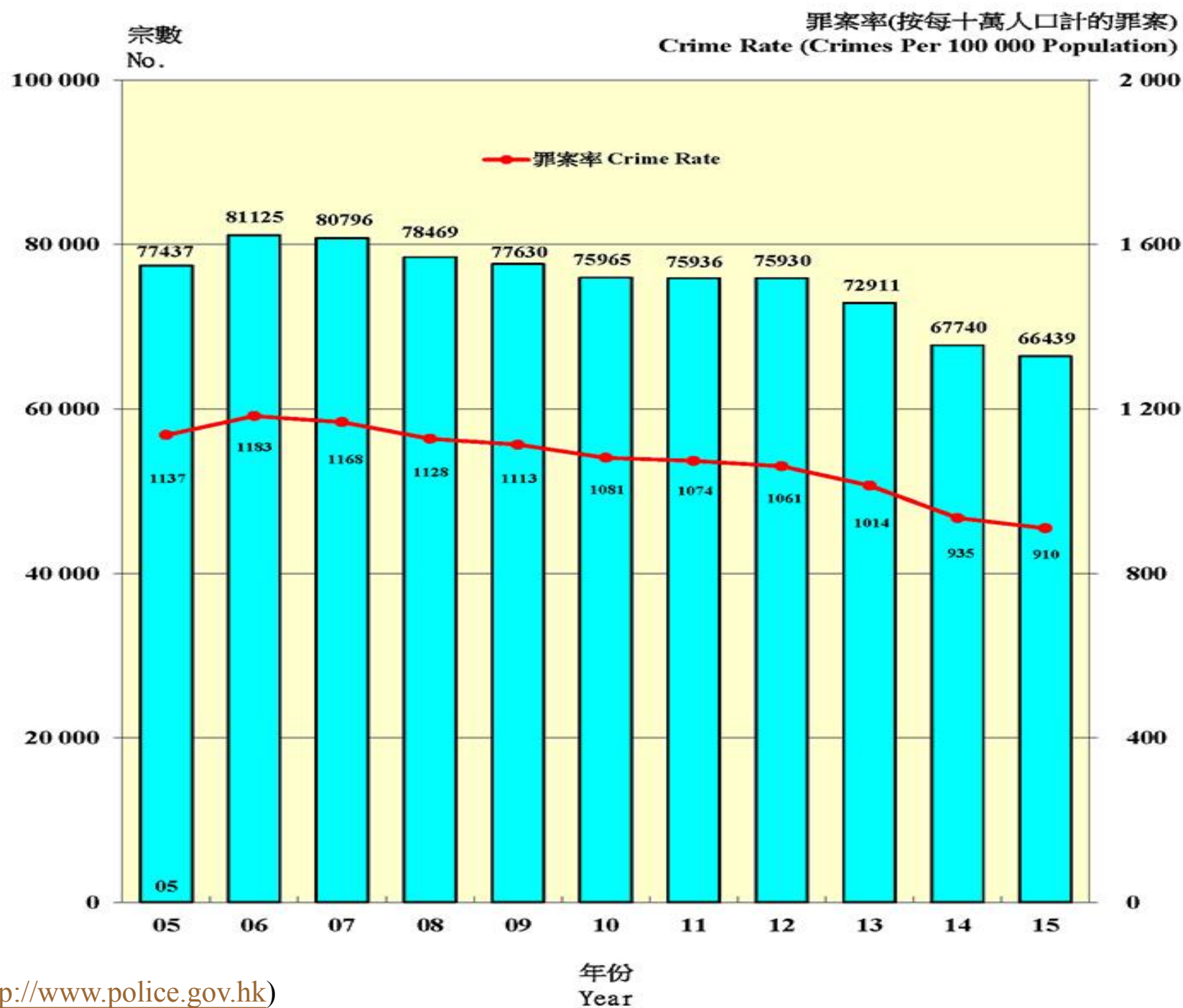
Overall Crime, 1991 - 2004
1991年至2004年的整體罪案

No.
宗數

Crime Rate (Crimes Per 100,000 Population)
罪案率 (按每十萬人口計的罪案)

— Crime Rate 罪案率

Year	宗數	罪案率
91	88659	1541
92	84056	1449
93	82564	1399
94	87804	1455
95	91886	1493
96	79050	1228
97	67367	1038
98	71962	1100
99	76771	1162
00	77245	1169
01	73008	1086
02	75877	1118
03	88377	1299
04	81315	1188

Year
年份

Crime in Hong Kong

Do you know why there is a drop in 1997?

(Source: http://www.police.gov.hk)

二零零五年至二零一五年的總體罪案
OVERALL CRIME, 2005 - 2015

(Source: http://www.police.gov.hk)

Basic Concepts
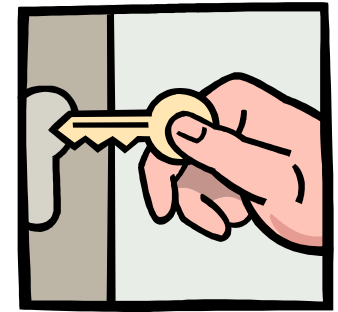
- Security engineering
  - Development of detailed engineering plans and designs for security features, controls and systems

- Physical security
  - Deter attackers from accessing a facility, resource, or information stored on physical media
  - Guidance on how to design structures to resist various hostile acts

- Nowadays, also *information security** (protect computer, information and data)

Example of a highly secured premise in Hong Kong

Security control centre

CCTV

Access control

Blocks & fencing

(Source: Hong Kong Note Printing Limited http://www.hknpl.com.hk/)

Integrated security in a typical building management solution

Telesecurity

Access Card

Biometrics

Asset Management

Fence defense

X-Ray Checking

CCTV

Metal Detector

Bollard

Road Blocker

LPR System

Sliding Gate
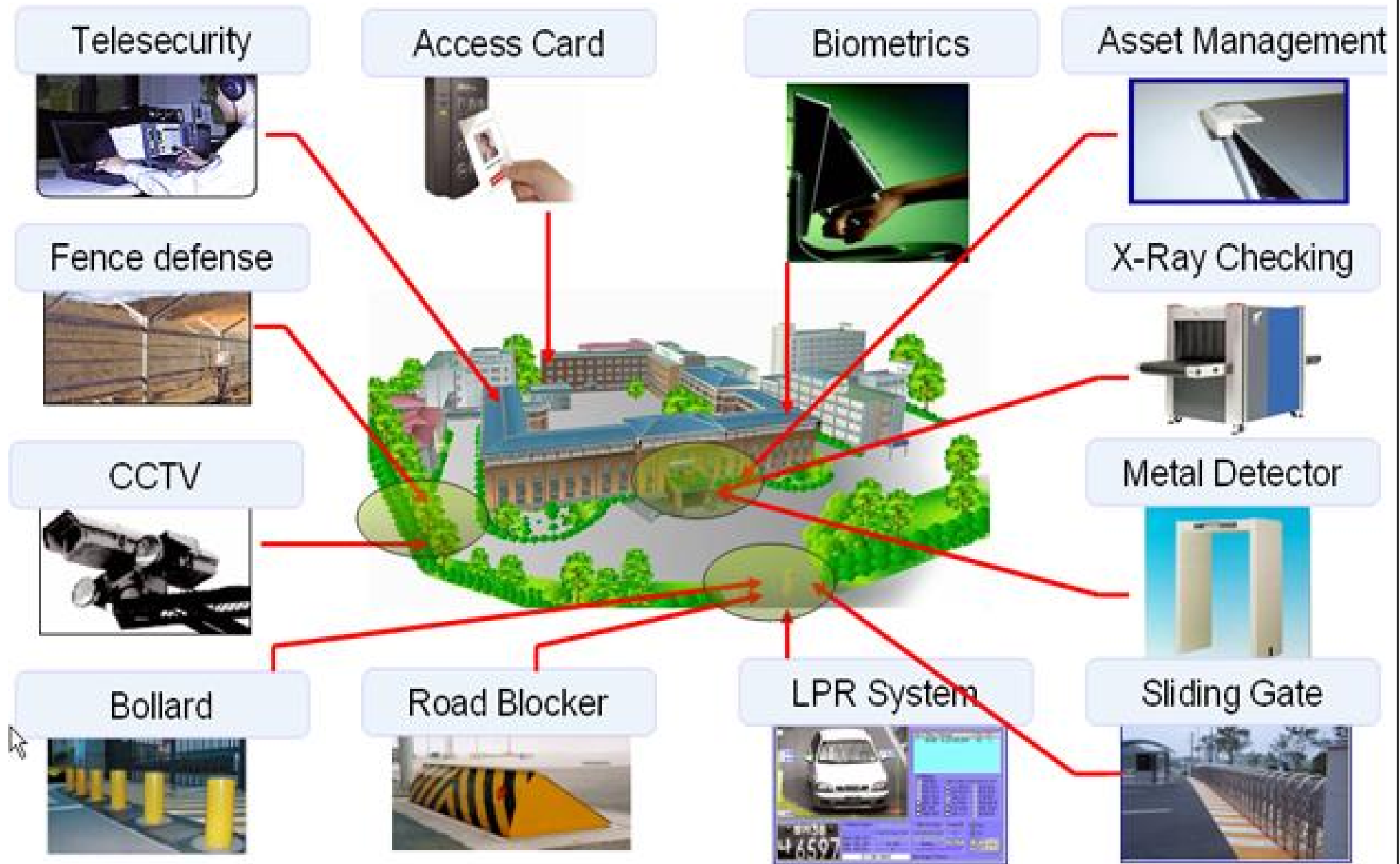
Basic Concepts
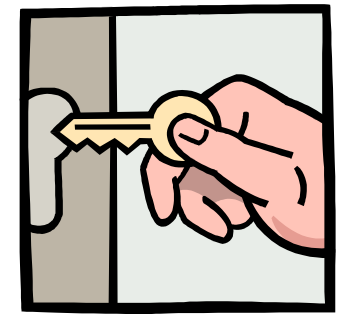
- Why security and alarm systems?

  - Decrease the chances of a burglary (if a burglar is aware a house has a system, he she might move on to another home)

  - Decrease the number of items stolen and the extent of damage done

- Objectives of security design

  - [Crime prevention](): aim to minimise, in and around the building, risks of theft, criminal damage, vandalism, personal attack and sabotage, both during the construction of the building and throughout its life

  - *Deter–detect–alarm–delay–respond*

Basic Concepts
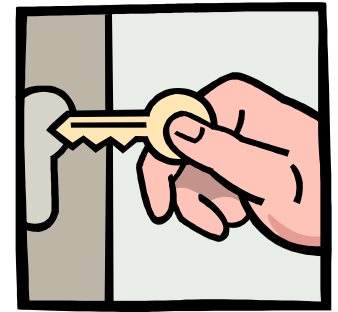
- Security measures are intended to: (The 4D)
  - **Deter** the criminal from attacking
  - **Detect** him or her if he or she does attack so that a police (or other) response may be initiated
  - **Delay** him or her so that he or she may be apprehended before achieving the objective
  - **Deny** him or her access to particular targets
- A combination of *physical*, *electronic* and *procedural* security measures can be used

Process and major issues of security design
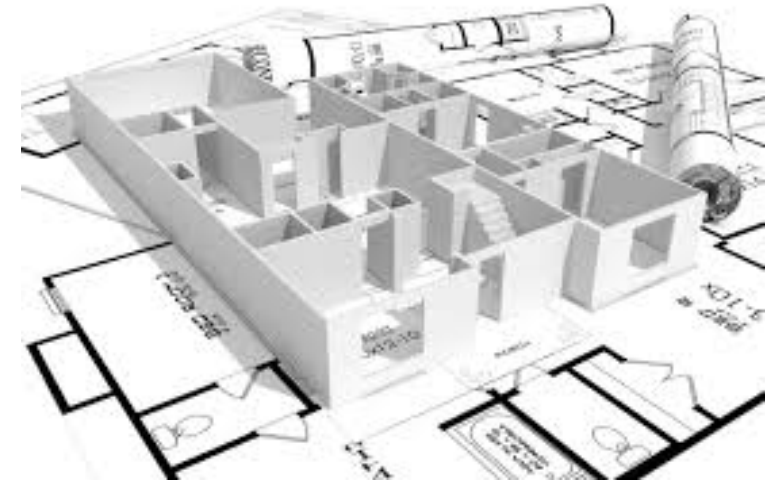
1. Evaluate the risk

2. Physical protection

3. Detection

4. Alarms

5. Response

6. Maintenance & review

Basic Concepts
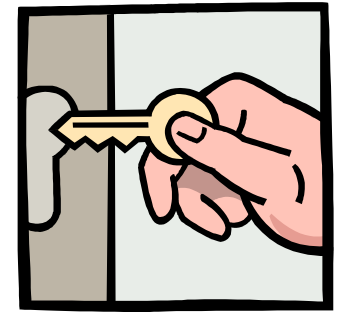
- Major issues of security design
  - 1. Evaluate the risk
    - Assess all possible risks e.g. damage by fire, water, vandalism, burglary (and terrorism), and the inconvenience suffered as a result
    - Estimate the required level of investment in security measures by evaluating the risk of <u>burglary</u>
    - Take into account the property value, degree of effort required to perpetrate the theft, the ease of subsequent conversion of misappropriated goods into cash, etc.

Basic Concepts
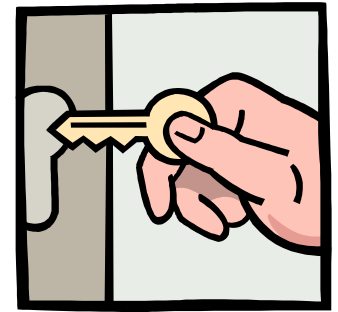
- Major issues of security design (cont'd)
  - 2. Physical protection
    - Form of fencing or building elements (e.g. walls, partitions, doors, windows, barriers, screens, bolts, locks, safes, and so on) which discourage and delay unauthorised entry
  - 3. Detection
    - Consider the assessed risk, the time needed to penetrate any physical protection and the speed of response necessary to prevent the successful completion of the criminal act

Basic Concepts
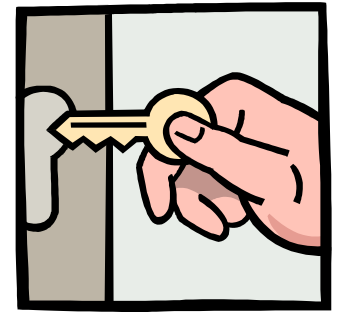
- Major issues of security design (cont'd)
  - 4. Alarms
    - Should disturb the perpetrator and/or inform the personnel responsible for security (e.g. the police or a private security service) that an unauthorised act is either imminent or taking place
      - Device & operational arrangement: manual, automatic, audible, visual, local, remote, broadcast or discrete
  - 5. Response
    - The response to an alarm is the action to be taken by the personnel responsible for security

Basic Concepts
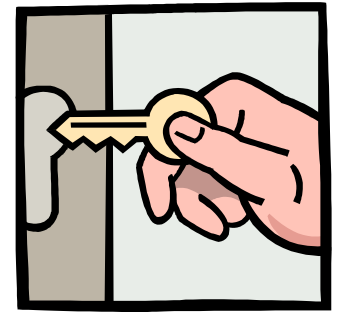
- Major issues of security design (cont'd)
  - 6. Maintenance and review
    - Frequent testing & competent maintenance minimise the possibility of system failure
    - Periodic reviews to determine the changes, if any, to the building's structure, usage, personnel, or to the items being protected

Physical Security

- Definition: (from U.S. Army Field Manual 3-19.30)
  - "It is defined as that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft."
- Physical measures used to protect people and property

(* See also: Physical Security Basics http://www.shieldjournal.com/physical-security-basics/)

Concentric circles of protection

Perimeter Fence

Exterior Door

Office Door

Locked Cabinet

(Source: Concentric Circles of Protection http://silvaconsultants.com/concentric-circles-of-protection.html)
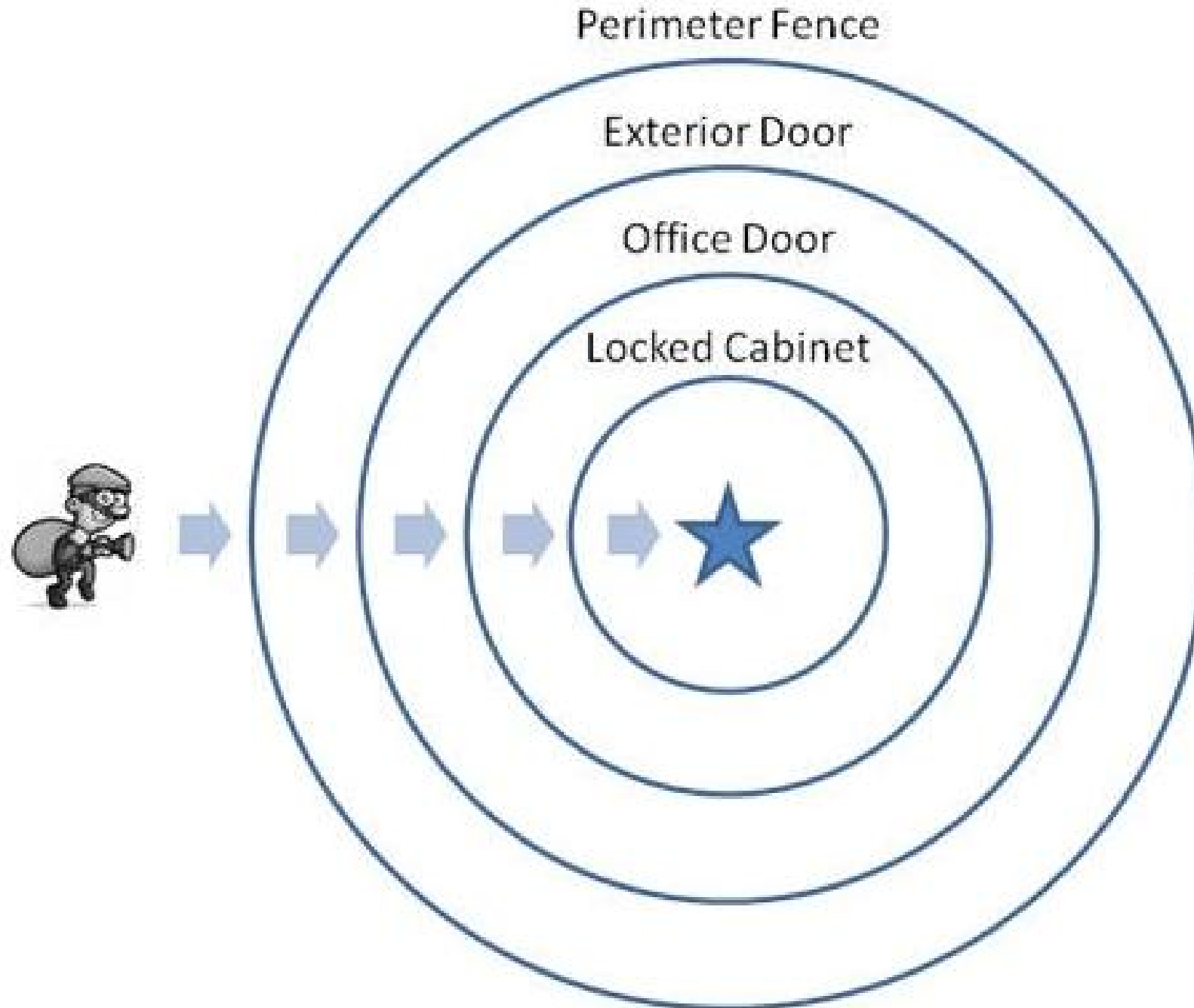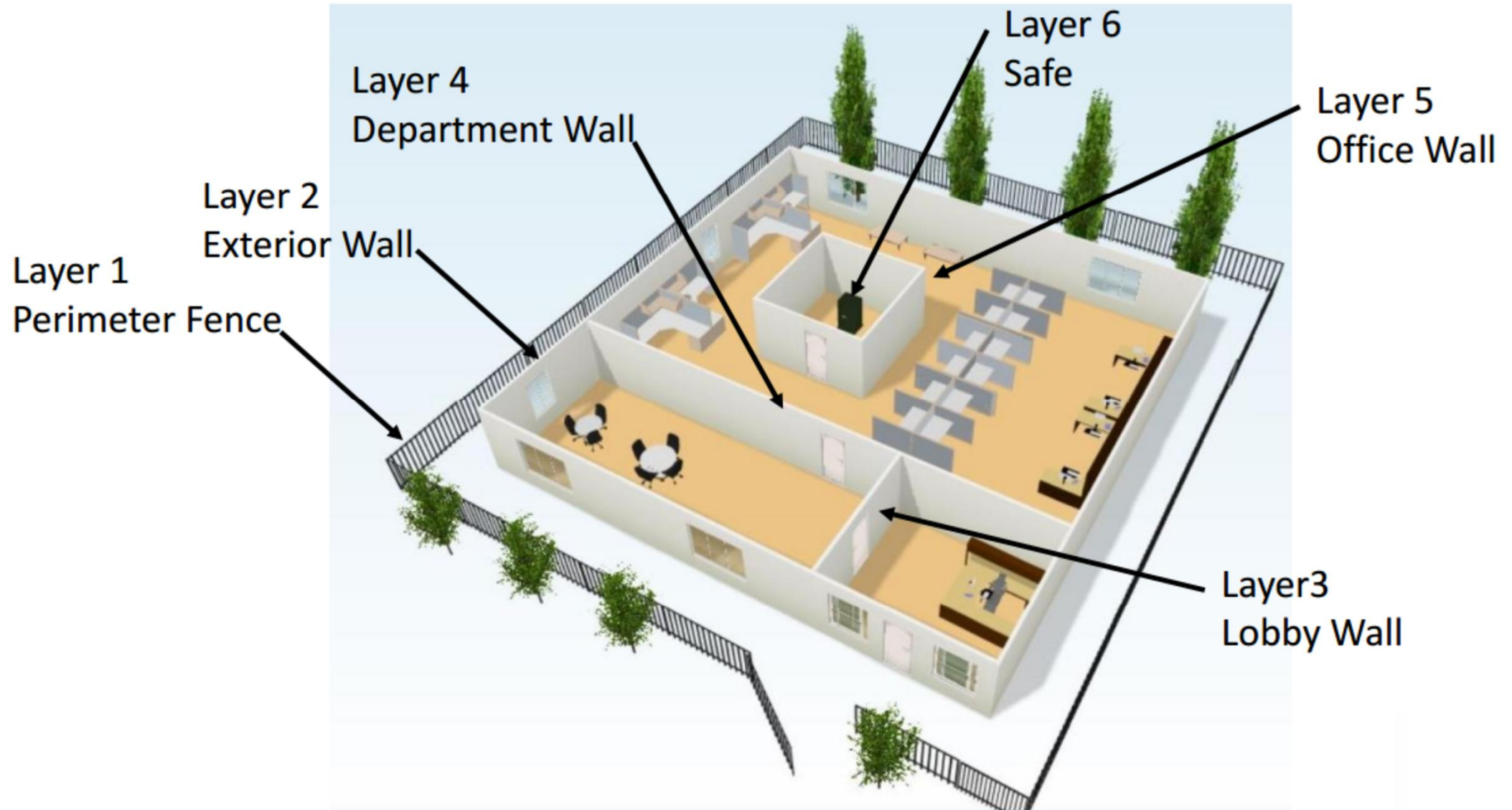
Layers of security

Having multiple layers eliminates total reliance on any single layer and provides redundancy.

Defense in depth and fundamental elements of physical security

Grounds - Set up a perimeter with a fence

Building - Cameras and security guards

Office - Door lock

Safe box - Combination

Asset to protect

4D
- Deter
- Detect
- Delay
- Defend

- Barriers (physical or psychological)
  e.g. fences and signs
- Alarm systems (sensors & alert)
- Access control
- Security force

(Source: Physical Security Basics http://www.shieldjournal.com/physical-security-basics/)

Physical Security

- Considerations of physical security
  - Understand a typical threat and the usual risks to people and property
  - Understand the incentives created both by the threat and the countermeasures
  - Understand risk and threat analysis methodology and the benefits of an empirical study of the physical security of a facility

Physical Security

- Considerations of physical security (cont'd)
    - How to apply the methodology to buildings, critical infrastructure, ports, public transport and other facilities/compounds
    - Overview of common physical and technological methods of protection and understand their roles in deterrence, detection and mitigation
    - Determine and prioritize security needs and align them with the perceived threats and the available budget $$

Physical Security

- Elements of physical security
  - Explosion protection & obstacles, to frustrate trivial attackers and delay serious ones
  - Alarms, security lighting, security guard patrols or closed-circuit television cameras, to make it likely that attacks will be noticed
  - Security response, to repel, catch or frustrate attackers when an attack is detected
- Need to know *how criminals think*

Physical Security

- Four layers of physical security
  - 1. Environmental design (to deter threats)
  - 2. Mechanical and electronic access control (e.g. locks and access cards)
  - 3. Intrusion detection (monitors for attacks)
  - 4. Video monitoring (for incident verification and historical analysis)
- The goal is to convince potential attackers that the likely costs of attack exceed the value of making the attack

Physical Security

- Key concerns of security design
    - Must be fully *co-ordinated*, at all stages of building design
    - Design of physical protection
        - Building design (e.g. landscaping, building inter-relationships, access)
        - Physical security components (e.g. doors and windows)
    - Design of security devices
        - Detection, alarms, and security lighting
    - Also, all personnel shall follow security procedure

Physical Security

- <u>Remember</u>: security systems do not 100% prevent thieves from breaking into buildings

- A good security plan should include:
  - Strong window, door, and lock products
  - Good security habits and lifestyles (e.g. always lock doors at night or when the house is vacant)
  - Natural surveillance, e.g. neighbourhood watches

- Conflicts between <u>security and fire safety</u>
  - Security requires lock-up; safety requires open

Door system components

Wood Frame Wall Structure

Masonry Wall Structure

Hinge

Lock

Bolt

Strike Plate

Door Frame

Typical warded locks and pin tumbler lock

Warded Rim Door Lock Set (with Latch)

Warded Mortise Door Lock Set (with Latch)

Warded Rim Post Key Wardrobe Lock

Warded Luggage Lock

Springs

Drivers (Upper Tumblers)

Key Pins (Lower Tumblers)

Pin Chamber

Cylinder Shell or Housing

Cylinder Plug

Cabinet or Drawer Warded Rim Lock

Warded Padlock

(Source: National Crime Prevention Institute, 2001. *Understanding Crime Prevention*, 2nd ed., Butterworth-Heinemann, Boston.)

Physical Security

- Floor plan and hierarchy of zones
  - Detailed floor plan to identify the following:
    - All exterior/perimeter access points to the facility, including doors and windows (ground level)
    - All interior/access control points within your facility
    - All locations where protected/classified material/information/assets will be viewed, processed, produced, or stored
    - All restricted areas
    - Location of storage cabinets & temporary holding areas
    - Location of any intrusion alarm components (motion sensors, keypad, door contacts, CCTV, etc.)
    - Location of servers, information technology systems, and peripherals

Organization of zones for physical security

Example of arrangement of zones for physical security

(Source: Canadian Conservation Institute http://www.cci-icc.gc.ca/)

Risk Assessment

- Risk assessment is a process for identifying:
  - Assets of an organization to protect
  - Threats to them
  - Assets criticality
  - Consequences if an asset would be lost or damaged
  - Existing vulnerabilities
  - Probabilities of attacks

Risk Assessment

- 4 categories of assets:
  - <u>People</u> (employees, customers, contractors, visitors)
  - <u>Property</u> (buildings, equipments, supplies, cash)
  - <u>Information</u> (secret formula, software, records)
  - <u>Reputation</u>
- Criticality is the measure of an asset's importance to the mission of the business
- Consequence -- the impact of loss or damage

Identify possible loss events and determine the likelihood

- Arson
- Assault
- Burglary
- Disturbances/Disorderly Conduct
- External Theft
- Internal Theft
- Robbery
- Sabotage

- Theft of Employee Personal Property
- Theft of Information
- Disclosure of Trade Secrets
- Trespassers
- Vandalism
- Graffiti
- Workplace Violence
- Product Tampering

Likelihood of event:

Very Likely = Greater than 90% chance of occurrence

Likely = Between 50% and 90% chance of occurrence

Moderately Likely = Between 10% and 50% chance of occurrence

Unlikely = Between 3% and 10% chance of occurrence

Very Unlikely = Less than 3% chance of occurrence

Determine consequences of events

Not Serious = No injuries, no downtime, $0 to $5,000 financial loss.

Not Too Serious = Minor injuries, less than 1 day of downtime. $5,000 to $50,000 financial loss.

Serious = Serious injuries, 1 to 7 days of downtime. $50,000 to $500,000 financial loss.

Very Serious = Loss of life or severe injuries, 7 to 30 days downtime. $500,000 to $1,000,000 financial loss.

Catastrophic = Loss of multiple lives or multiple severe injuries, significant or total destruction of facility, greater than $1,000,000 financial loss.

Risk Assessment

- 5 categories of threat actors :
  - Petty criminals – vandals, pickpockets, drunks
  - Violent criminals – deranged person, rapists, disgruntled employee
  - Economic criminals – transnational Mafia 黑手黨, organized crime, skilled thieves
  - Subversives – spies, hackers, N.G.O. activists
  - Terrorists – intelligence service, religious fanatics, guerrilla, amateurs

Impact of 9/11 on security design & requirements

(Source: http://www.skyscrappers.com)

Example of business impact levels

Business impact	Description
Low	Could be expected to harm government agency operations, commercial entities or members of the public
Medium	Could be expected to cause limited damage to national security, government agency operations, commercial entities or members of the public
High	Could be expected to damage government agency operations, commercial entities or members of the public
Very high	Could be expected to damage national security
Extreme	Could be expected to seriously damage national security
Catastrophic	Could be expected to cause exceptionally grave damage to national security

Risk assessment using a risk matrix

Consequences

Probability	Very low	Low	Moderate	Major	Critical

Risk scale

- Very High
- High
- Medium
- Low
- Very Low

Risk Matrix

At the end of this process we *express the risks* we face and *prioritize* them. Finally, we *recommend countermeasures* to reduce those risks.

(Source: How To Do A Risk Assessment http://www.shieldjournal.com/how-to-do-a-risk-assessment/)

Risk Assessment

- A vulnerability analysis should:
  - Define attack scenarios and their likely result
  - Evaluate the effectiveness of the security measures
  - Identify vulnerabilities (flaws)
- Estimate attack probability
  - The likelihood that a threat actor will select and then attack an asset
  - Use the statistics published by the local authorities or analyzing the assets attractiveness

Risk Assessment

- Security risk equation:
    - $R = P_A * (1 - P_E) * C$
    - where:
        - R = risk associated with adversary attack
        - P_A = likelihood of attack
        - P_E = probability that the security system is effective against the attack
        - $(1 - P_E)$ = system ineffectiveness
        - C = consequence of the loss from the attack
- Security risk is difficult to quantify. Why?

Risk Assessment

- Risk-based approach to planning security
    - Identify and prioritize your security risks
    - Determine the best types of security measures to mitigate those risks
    - Focus on high-priority risks first
    - Deal with lower-priority risks as resources allow
- Every security measure should be in response to one or more specific security risks

Focus on high-priority risks first (example of ranking on risk matrix)

Possible Loss Event	Likelihood	Consequence	Rank
Arson	VU	VS	M
Assault	U	VS	M
Burglary)	VL	S	H
Disturbances/Disorderly Conduct	U	S	M
External Theft	L	NTS	M
Internal Theft	VL	NTS	M
Robbery	VU	VS	M
Sabotage)	VU	C	M
Theft of Employee Personal Property	VL	NS	M
Theft of Information	L	VS	H
Disclosure of Trade Secrets	U	VS	M
Trespassers	ML	NS	L
Vandalism	U	NS	L
Workplace Violence	VU	S	L
Product Tampering	VU	VS	M

(Source: http://silvaconsultants.com/ifma-2014-security-presentation.html)

Determine appropriate measures to mitigate each security risk (examples)

Security Risk	Security Measures
Burglary	High-security locks Door frame strengthening Security window film Intrusion alarm system Security patrols
Theft of Information	Background checks Employee training Restricted access areas High-security file cabinets Document shredders

Risk Assessment

- "*Good security is a process, not a product*"

- It requires a balanced approach to be effective

  - 1. <u>Operational measures</u>

    - Such as security policies and procedures, employee awareness training, security officer staffing

  - 2. <u>Electronic systems</u>

    - Such as access control, video surveillance, alarm systems, visitor management systems

  - 3. <u>Site and building design</u>

    - Such as site and facility layout, lighting, landscaping

(See also: http://silvaconsultants.com/buying-the-equipment-is-the-easy-part.html)

Risk Assessment

- Key questions in security assessment:
  - What do we want to protect?
  - What are we protecting against?
  - What are the current or expected asset vulnerabilities?
  - What are the consequences of loss?
  - What specific levels of protection do we wish to achieve?
  - What types of protection measures are appropriate?
  - What are our protection constraints?
  - What are the specific security design requirements?
  - How do the integrated systems of personnel, technologies, and procedures respond to security incidents?

Decisions for Security Risk Managers

*Consequences   *Undesired Events   *Criminal   *Extremist

What's important? Mission

What to protect against?

*Liabilities   *Targets

How Well are you protected?

*Terrorist   *Insider

*Is risk acceptable?

*Reduce Consequences

*Operational trade-off

Decisions

*Improve Protection

*Cost options

Risk Assessment

- Three fundamental questions to answer:
  - 1. What are the bad things that can happen to my facility?
  - 2. How likely are the bad things?
  - 3. How do they affect my facility – its mission, occupants, surroundings, and the larger environment?

- An analytic process to assess security risk
  - Identify and evaluate risk reduction strategies in order to reduce risk

Security risk assessment and management process

$$R = P_A *(1 - P_E)*C$$

(Source: Biringer, B. E., Matalucci, R. V. and O'Connor, S. L., 2007. *Security Risk Assessment and Management*)

Security Planning

- Determine the broad magnitude of the threat and the extent of measures and financial investment appropriate

  - Consult insurers, suppliers and manpower agencies, contractors

- A rational and analytical examination of the aspects influencing the threat, e.g. burglary and theft

  - The intended uses for the building

  - Survey of the building, the immediately adjacent properties and surroundings

Security Planning

- Main categories:
  - Building location and surroundings
  - Building access and structural strength
  - Building contents
  - Occupational pattern
  - Consequence of loss
  - History of loss
  - Existing security measures
  - Recommended level of protection
- Also, the "peace of mind" given to occupants

Security Planning

- Survey of premises
  - To identify any weak points and examine how they may be strengthened
  - Physical security measures include:
    - Quality locks
    - Solid structure doors and surrounds
    - Security bars
    - Blast-resistant curtaining
    - Surveillance and alarm systems
    - Access control

Security Planning

- Steps to formulate a security plan
  - Assemble a risk assessment group/team
  - Decide where to focus security measures
  - Assess the building/facility
  - Assessment of specific risks (probability of occurrence)
- Assess the building/facility
  - Segments of a facility or operation and assets that are most valued and at the greatest risk (critical assets)
  - Events or incidents that may take place
  - Plans that need to be made to safeguard these operations and assets

(* See also: Top 15 Problems Found During a Security Assessment http://silvaconsultants.com/top-15-problems-found-during-a-security-assessment.html)

Security Planning

- Three main objectives
  - Prevent undesirable people, forces, or damaging agents from accessing the facility
  - Prevent acts of injury, damage, or theft from occurring within the facility
  - Develop emergency response contingency plans or strategies for recovering from damage
- If vulnerability is high, risk is increased

Security Planning

- Major considerations
  - Threat/Risk assessments
  - Physical security surveys and audits
  - Contingency planning
  - Emergency operations (e.g. evacuation procedures)
  - Executive protection (protect CEO & key managers)
  - IT & telecommunications security
  - Technical counter measures
  - Guard force deployment
  - Security awareness training

Security Planning

- Planning of security systems
  - Involve the client, architect, security consultant/designer and insurance company
  - Building survey & risk assessment to establish the most appropriate security measures
    - Building location & type
    - Business activities/hours of operation
    - Size, transportability & value of contents
    - Availability of on-site security personnel

Security Planning

- Planning of security systems (cont'd)
  - Careful consideration of physical protection issues can reduce the needs for electronic solutions & provide long-term financial savings ($$)
    - Such as, crime prevention through environmental design (CPTED)
  - Continuous monitoring to ensure fast response to an alarm & rectifying of any faults
  - Physical on-site monitoring
  - Remote monitoring at a central security station
    - Communication link shall be robust & secure
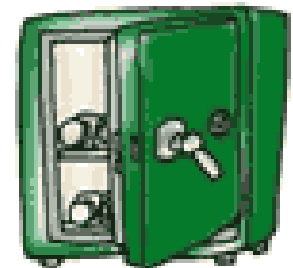
Security Planning

- Seven deadly sins of building security (the top building security mistakes)
  http://www.csoonline.com/article/2124303/physical-security/seven-deadly-sins-of-building-security.html
  - 1. Creating post orders without advanced analysis
  - 2. Placing aesthetics over security
  - 3. Neglecting to properly secure certain entrances
  - 4. Allowing management to ignore security rules
  - 5. Failing to take time to understand your technology
  - 6. Failing to secure important rooms inside the building
  - 7. Overdoing security
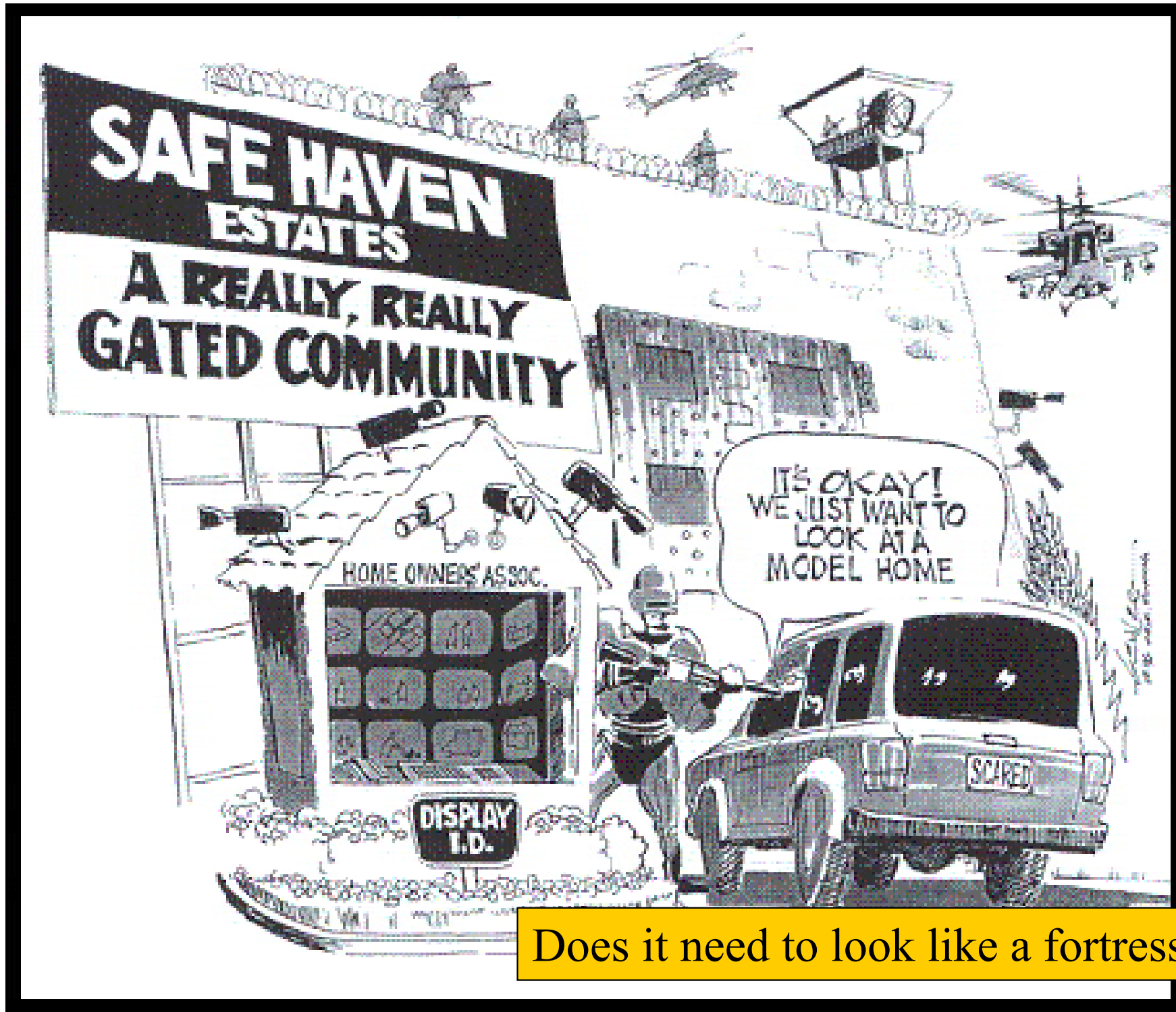
Does it need to look like a fortress?

Security Planning

- How the building plan affects security
  - Restrict unauthorised entry (external doors or windows)
  - Interior layouts: group together secure areas
  - Modification work on existing buildings
    - Scaffolding or ladders are opportunities for access
  - New works must consider existing security practice
    - Ensure revised building configuration does not compromise or undermine any alarm systems

Security Planning

- Example: designing lobbies for good security
  - The lobby is the primary point where visitors and other members of the public enter your facility
  - Many lobbies are designed primarily with aesthetics and convenience in mind
  - Having a poorly designed lobby makes it difficult to properly control access into the building, requiring that additional security measure
  - Problems in lobby design: e.g. visitor control

(Further info: http://silvaconsultants.com/designing-lobbies-for-good-security.html)

Designing a lobby for good security

Private Zone

Security Layer

Lobby

Semi-Public Zone

Receptionist

Security Layer

Public Zone
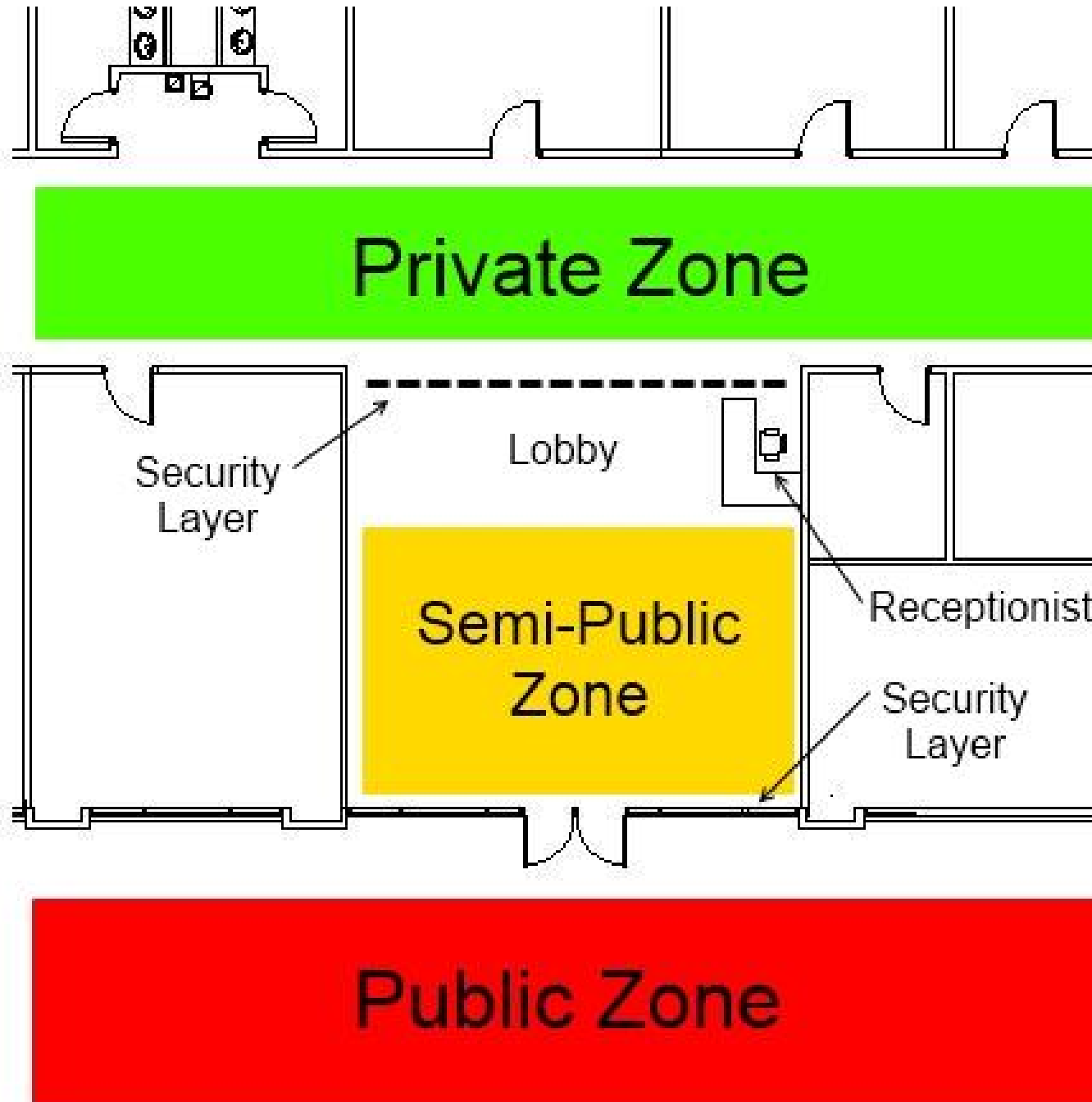
Evaluate the design when you visit a lobby.

(Source: http://silvaconsultants.com/designing-lobbies-for-good-security.html)

Security Planning

- Other examples of security design issues:
  - Security of Public Restrooms
    - http://silvaconsultants.com/security-of-public-restrooms.html
  - Security of Warehouses and Distribution Centers
    - http://silvaconsultants.com/security-of-warehouses-and-distribution-centers.html
  - Weaknesses of Elevator Access Control
    - http://silvaconsultants.com/weaknesses-of-elevator-access-control.html

Security Planning

- Common mistakes in security system design http://silvaconsultants.com/common-mistakes-in-security-system-design.html
  - 1. Security system designed in response to recent crisis
  - 2. Security system designed without supporting human resources in place
  - 3. Security systems designed with too little capacity
  - 4. Security systems designed with too much capacity
  - 5. Security systems too complicated for user
  - 6. Security system designed too specifically around one person

Security Planning

- Site planning and landscape design
  - Vehicular control
    - Such as buffer zone or barriers to restrict vehicle access
  - Perimeter vehicle inspection (prevent tailgating)
  - Site lighting
    - Such as to support CCTV & other surveillance
  - Site signage
  - Landscaping
    - Proper design and use of landscaping elements

(* See also: http://www.gsa.gov/portal/category/21057)

A world without thieves?!
天下無賊?!

Crime Prevention

- Elements necessary for a crime to occur:
  - Desire or motivation on the part of the criminal
  - The skills and tools needed to commit the crime
  - Opportunity
- Crime triangle
  - Criminal – Victim – Opportunity
- Aims to reduce the opportunity
  - By making a potential target of attack inaccessible or unattractive, and by making the attack itself dangerous or unprofitable to the criminal

Crime Prevention

- Types of crimes:
  - Major crimes
    - Such as drug offences, burglary, robbery, indecent assault, thefts
  - Minor crimes
    - Such as graffiti, vandalism, littering, criminal damage
- Crime and loss prevention
  - Affected by the environment
    - High value assets (e.g. cable/manhole cover for sale)
  - Architect, Building Services Engineer and Criminologist must work together

Unattended back lane might attract crime

People commit crime; places permit crime

Crime Prevention

- *Situational* crime prevention techniques:
  - Increase the difficulty or effort of crime
  - Increase the risks of crime
  - Reduce the rewards of crime
  - Reduce provocations 挑釁
  - Remove excuses
- Impact of built environment
  - Barriers and access control
  - Detection and alarm
  - Avoid/protect valuables

(* See also: Situational Crime Prevention http://criminology.wikia.com/wiki/Situational_Crime_Prevention)

Crime Prevention

- ## The Broken Windows Theory

  - A criminological theory of the norm-setting and signaling effect of urban disorder and vandalism on additional crime and anti-social behavior

    - If a building has a broken window that's not repaired, then soon vandals will break more, and perhaps squatters or drug dealers will move in
    - If litter is left on a sidewalk then eventually people will start dumping their trash there

  - Focusing on smaller crime, such as graffiti, is thought to reduce more violent crime

SMALL VANDALISM

URBAN DECAY

CRIME

(See also: http://en.wikipedia.org/wiki/Broken_windows_theory)

Crime Prevention

- [Crime prevention through environmental design (CPTED)](http://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design) 通過環境設計預防犯罪*
  - Proper design & effective use of the built environment can lead to a reduction in the incidence and fear of crime
  - The goal of CPTED is to reduce opportunities for crime that may be inherent in the design of structures or in the design of neighbourhood
  - Deter criminal behaviour and influence offender decisions that precede criminal acts

* See also http://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design

Crime Prevention

- [CPTED Intent](http://www.youtube.com/watch?v=CF_V2S6i30c)
  - The theory of CPTED is based on a simple idea that crime results partly from the opportunities presented by physical environment
  - It is the design or re-design of an environment to reduce crime opportunity & fear of crime through natural, mechanical, and procedural means
  - It is best applied with a multi-disciplinary approach that engages planners, designers, architects, lanscapers, law enforcement and (ideally) residents/space users

Crime prevention through environmental design (CPTED)

LIGHTING

DEFINED SPACE

INFORMAL SURVEILLANCE

LEGIBILITY

DEFINED "PERMEABILITY"
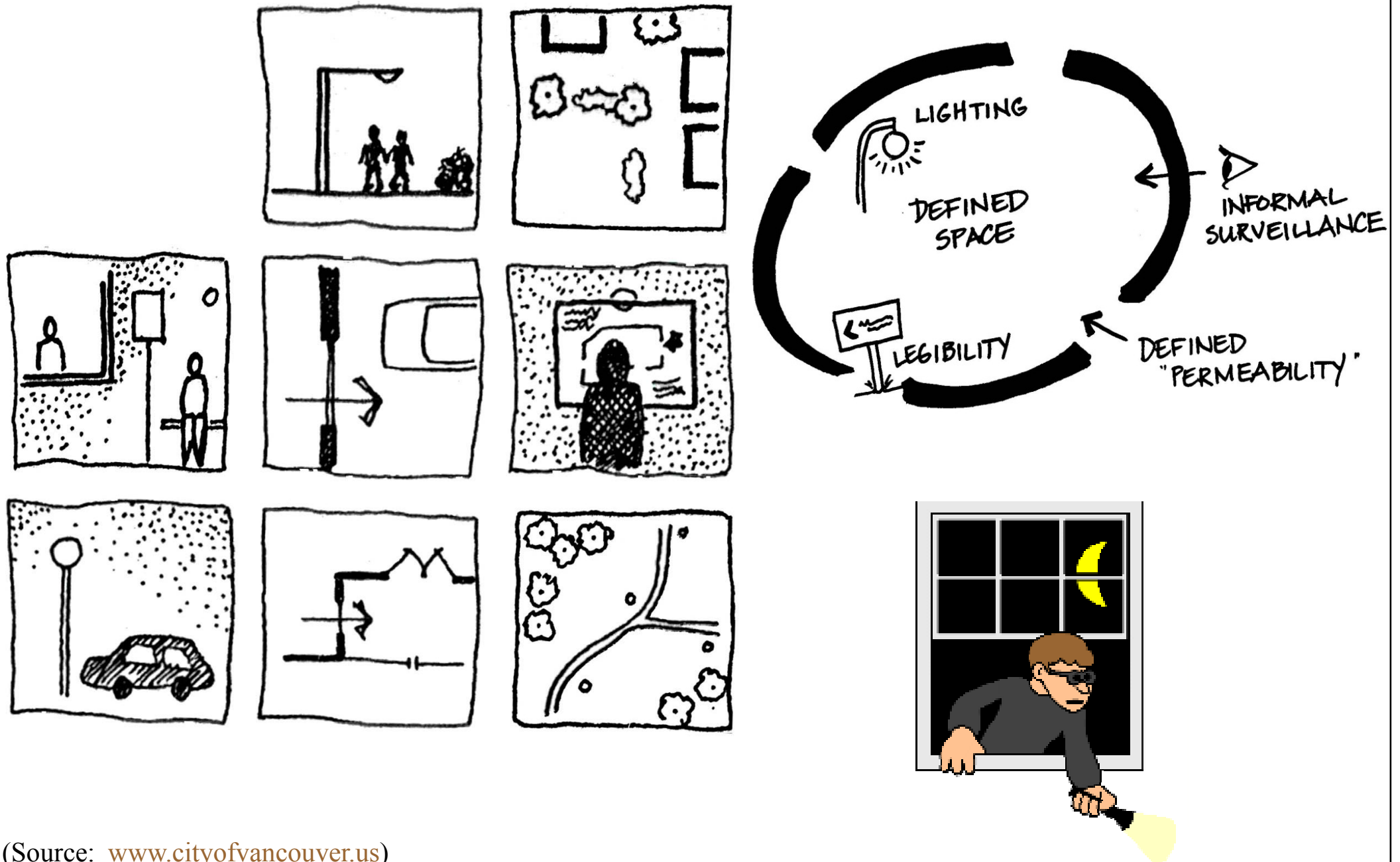
Crime Prevention

- Example: use of light & colour: Blue lighting
  - For areas used by drug addicts to inject drugs
  - The blue lighting makes it impossible to identify veins, thus discouraging the addicts from using that location to "shoot up" and then discard needles

Six key concepts of crime prevention through environmental design (CPTED)
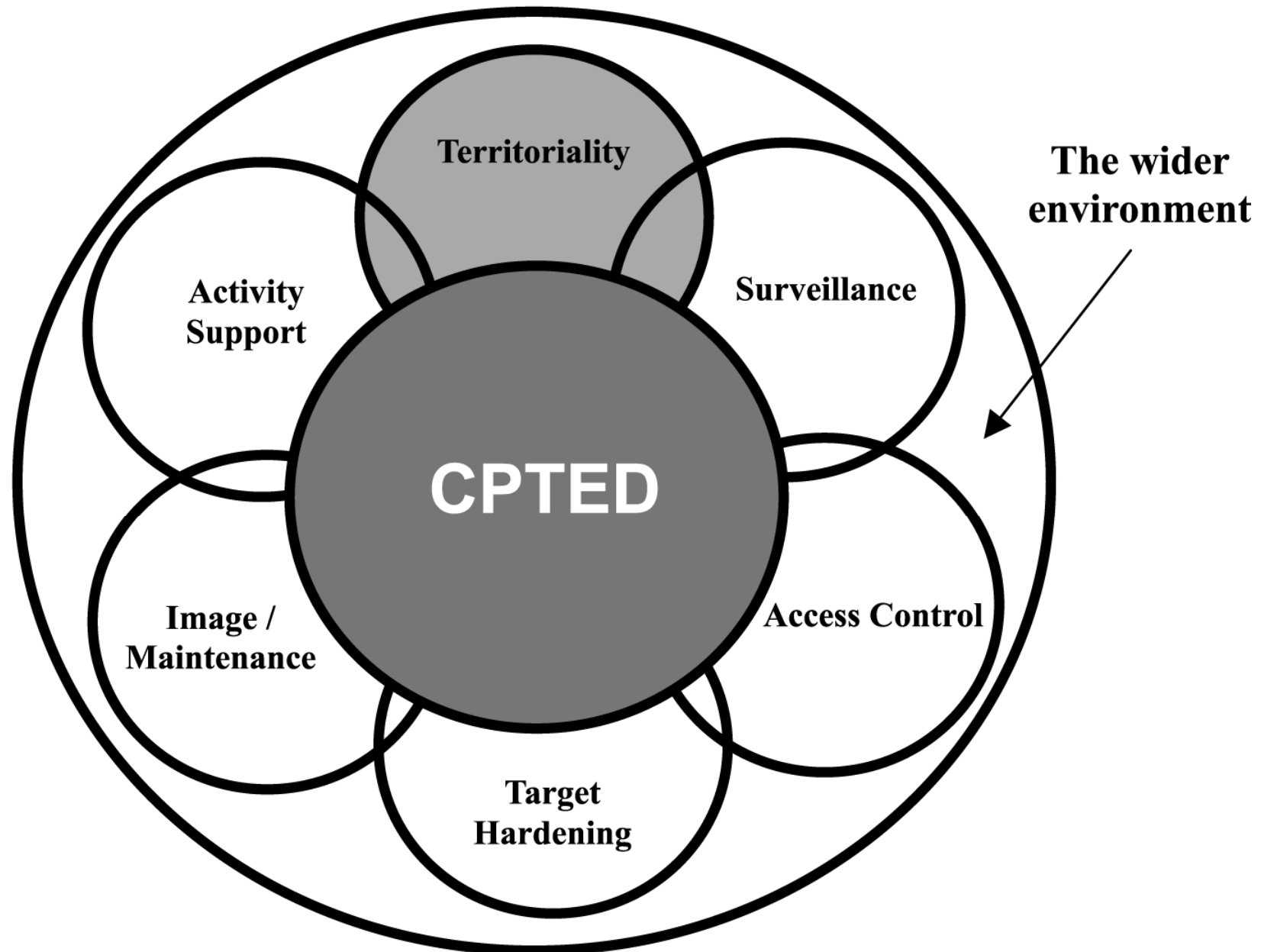
Source: Adapted from Moffat (1983, p. 23)

(Source: Cozens, Saville and Hillier (2005))

Crime Prevention

- "*Designing Out Crime*"
  - To influence offender decisions by affecting the built, social and administrative environment
- Six key concepts of CPTED:
  - 1. Territoriality
  - 2. Surveillance
  - 3. Access control
  - 4. Activity support
  - 5. Image/maintenance
  - 6. Target hardening

Crime Prevention

- 1. <u>Territoriality</u>
  - "Defensible space", to promotes social control
  - Boundaries reinforce a sense of ownership
- 2. <u>Surveillance</u>
  - Natural/CCTV and sightlines ('see and be seen')
  - Increase the threat of apprehension
- 3. <u>Access control</u>
  - Regulated access, limit the opportunity for crime
  - Clearly differentiate between public space and private space

Crime Prevention

- 4. <u>Activity support</u>
  - Encourage and increase "safe" activities
  - Increase the risk of detection of criminal and undesirable activities
- 5. <u>Image/maintenance</u>
  - Promote a positive image and proper maintenance
  - Deterioration indicates less control (e.g. broken window theory)
- 6. <u>Target hardening</u>
  - Use of physical barriers, make less vulnerable

Crime Prevention

- Practical CPTED issues:
    - Land use mix and activity generators
    - Territorial boundaries, screening, edge effects
    - Natural surveillance, sightlines, and signage
    - Concealment and entrapment spaces
    - Gender issues and community safety
    - Lighting (e.g. security or vandal-resistant lighting)
    - Landscaping (e.g. shape and size of plants)
    - Construction phase (e.g. bamboo scafolding)

(See also: Illustrated CPTED Guidelines http://sarkissian.com.au/wp-content/uploads/2010/11/Working-paper-5-CPTED-final.pdf)

Crime Prevention

- Crime risk assessment (CRA) process:
  - 1. <u>Site visit</u>, including interviews/surveys with local residents, prelim. discussions with local police
  - 2. <u>Preliminary reviews</u>, including more in-depth discussions and meetings with CPTED-trained police officers, residents, planners, or CPTED consultants
  - 3. <u>A crime risk assessment</u>, including crime analysis of available statistics, local demographics, mobility patterns and any available forecasts
  - 4. <u>Design reviews</u>, including architectural design workshops and a CPTED review of existing plans. Also technical issues e.g. lighting, target hardening, finishes and detailed landscaping plans

(See also: Illustrated CPTED Guidelines http://sarkissian.com.au/wp-content/uploads/2010/11/Working-paper-5-CPTED-final.pdf)
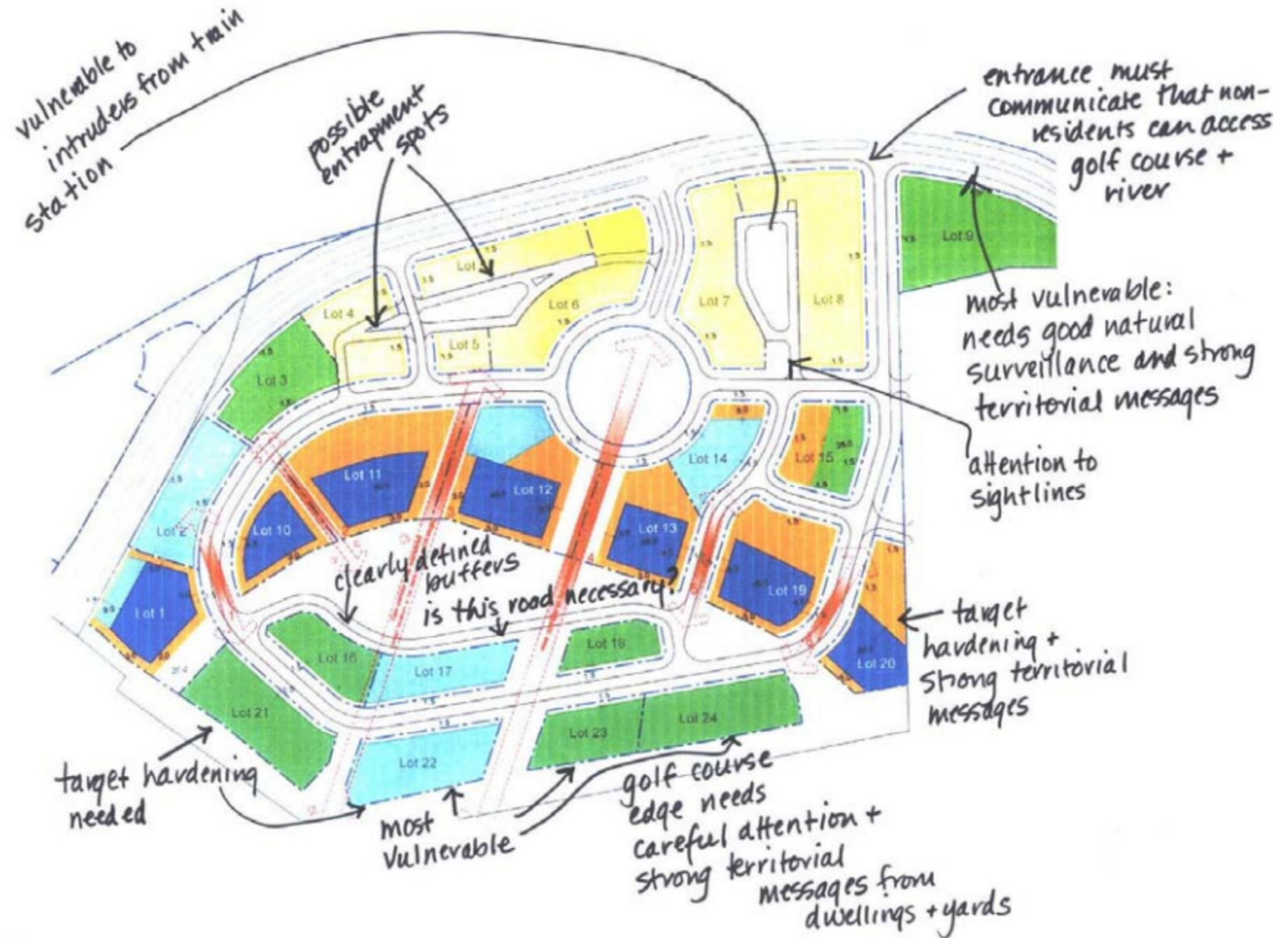
Crime Prevention

- May review proposed development plans for the buildings and look for potential crime risk associated with exterior environment features
  - Building setbacks
  - Fences, walls, hedges, and other boundary markers
  - Trees and shrubbery
  - Streets, sidewalks, and alleys
  - Lighting
  - Public areas and facilities
  - Parking lots and structures

Annotated plan showing potential CPTED issues

vulnerable to intruders from train station

possible entrapment spots

entrance must communicate that non-residents can access golf course + river

most vulnerable: needs good natural surveillance and strong territorial messages

attention to sightlines

clearly defined buffers

is this road necessary?

target hardening + strong territorial messages

target hardening needed

most vulnerable

golf course edge needs careful attention + strong territorial messages from dwellings + yards

<-- N

Crime Prevention

- The law of unintended consequences
  - Unintended outcomes
  - Unexpected benefits (+ve)
  - Unexpected drawbacks (-ve)
  - Perverse results
- Building designers often face such:
  - Need to understand/promote benefits and avoid drawbacks
- Thinking like a *criminal* when designing to reduce crime (rational choice theory)

Crime Prevention

- Physical design can be used to stimulate social attitudes and behaviour, to help reduce both the opportunities for crimes and fear of crime through:
    - Intensified use of streets, parks, and land around structures
    - Increased visibility of intruders to legitimate occupants and users
    - Increased tendency for people to look out for each other and to act if a crime is observed
    - Increased ability to discriminate between people who belong in an area and those who are intruders
    - Increased sense of shared interest in improving and maintaining the quality of the physical and social environment
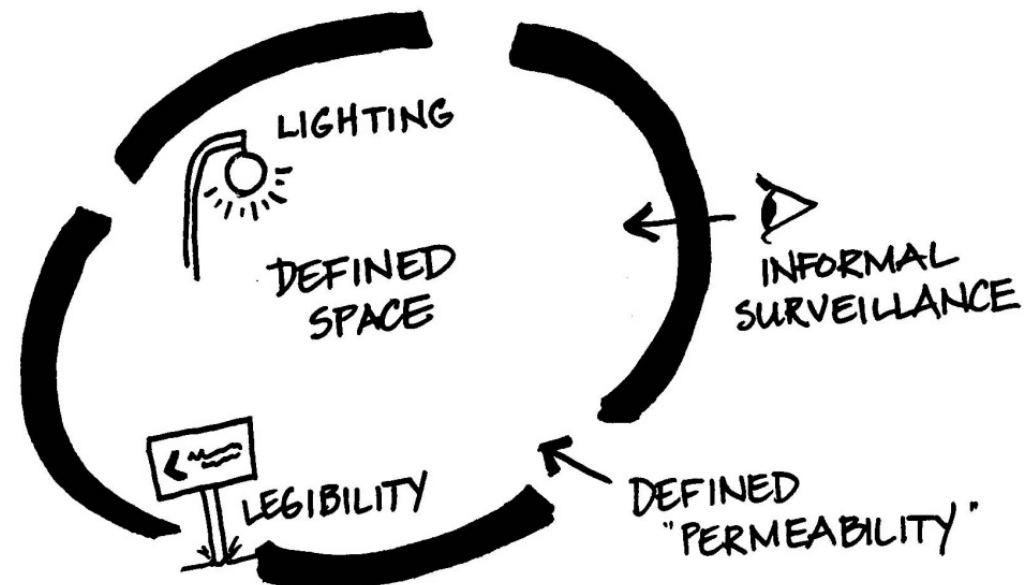
Safe living environment – *Secured by Design*

- Well-designed
- Attractive
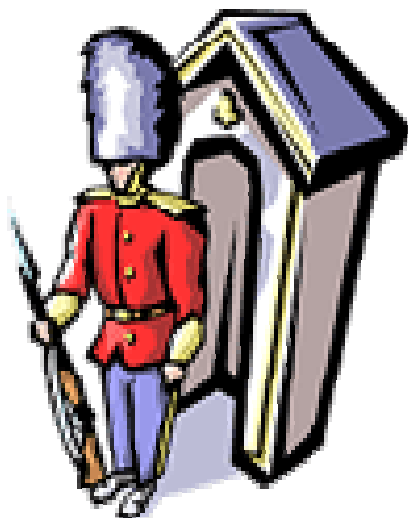- Clearly defined
- Well maintained

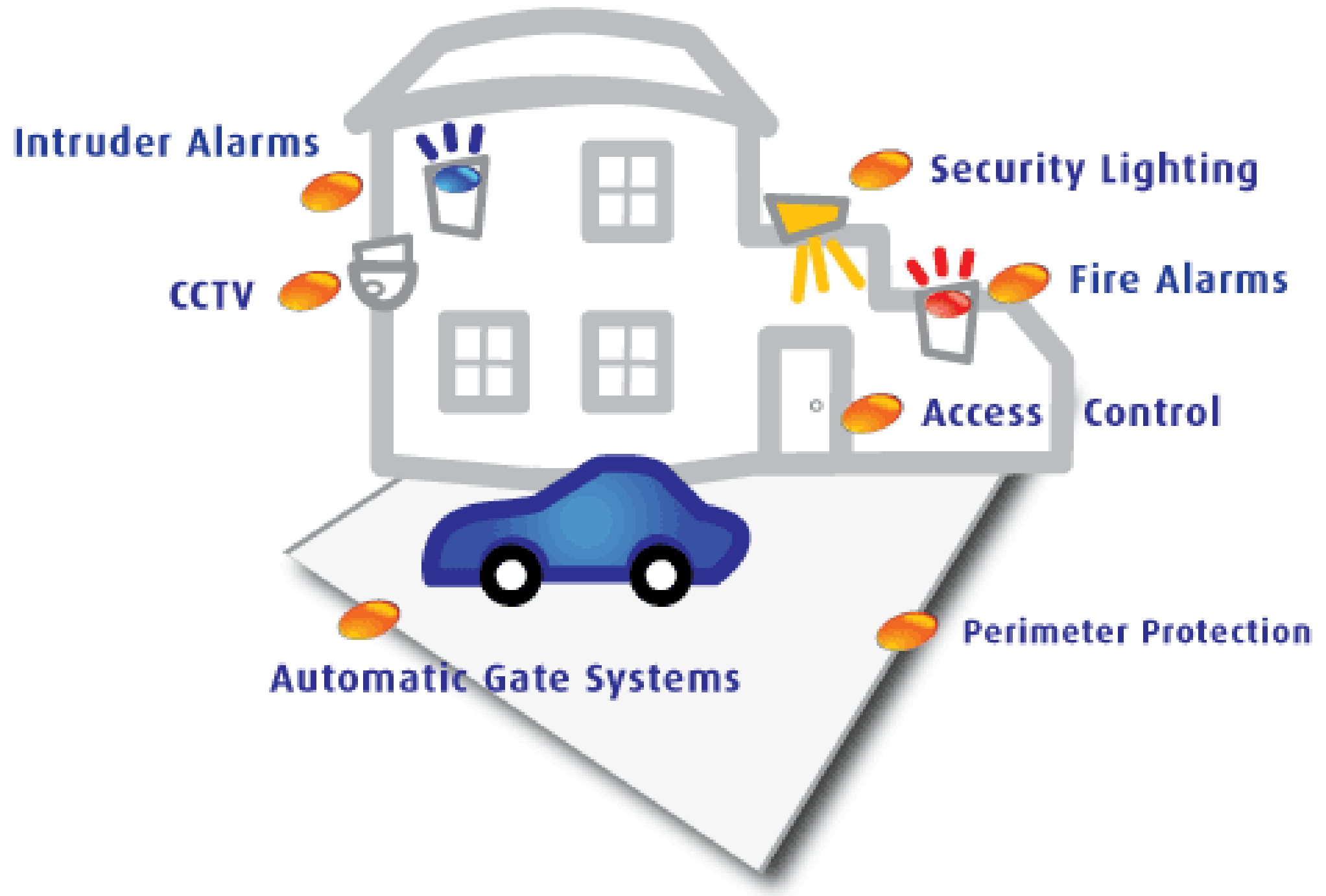(Source: chinapost.com.tw)

Crime Prevention

- Video presentation:
  - "Safe as Houses" (17 minutes)
    - Housing design and layout in achieving security
    - Principles of environmental design for security

Security systems

Intruder Alarms

CCTV

Security Lighting

Fire Alarms

Access Control

Automatic Gate Systems

Perimeter Protection

(Source: www.acesec.co.uk)

Security Systems

- Common types of systems
  - Burglar alarm system
    - Central or local (w/ direct link to police)
  - C.C.T.V. surveillance system
  - Intruder detection & access control
  - Intercom systems (audio/video)
  - Door-phone system & interlocking system
  - P.A. (panic attack) button & sound system
  - Security lighting
  - Guard tour/monitoring system

Typical security and alarm systems

Intrusion Alarms

Closed Circuit Television
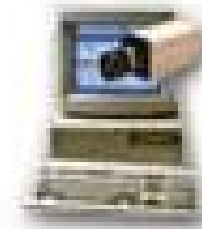
Digital Video Surveillance

Access Control

Critical Process Monitoring

Security Systems

- Burglar alarm system include:
  - Control panel
  - Keypads
  - Intruder detectors and motion detectors (e.g. passive infrared, microwave, or photoelectric)
  - Door and window magnetic contacts
  - Alarm bells or siren
  - Central monitoring station/company (optional)

Security Systems

- Additional items to the basic system

  - Smoke detectors

  - Glass break detectors

  - Panic buttons

  - Pressure mats

  - Closed circuit TV

  - Alarm screens

  - SMS alert service !! →

Basic approach of an alarm system

Input

Control

Output

Sensors	→	Panel	→	- Bell, siren, light - Dialer, email - Police-connect
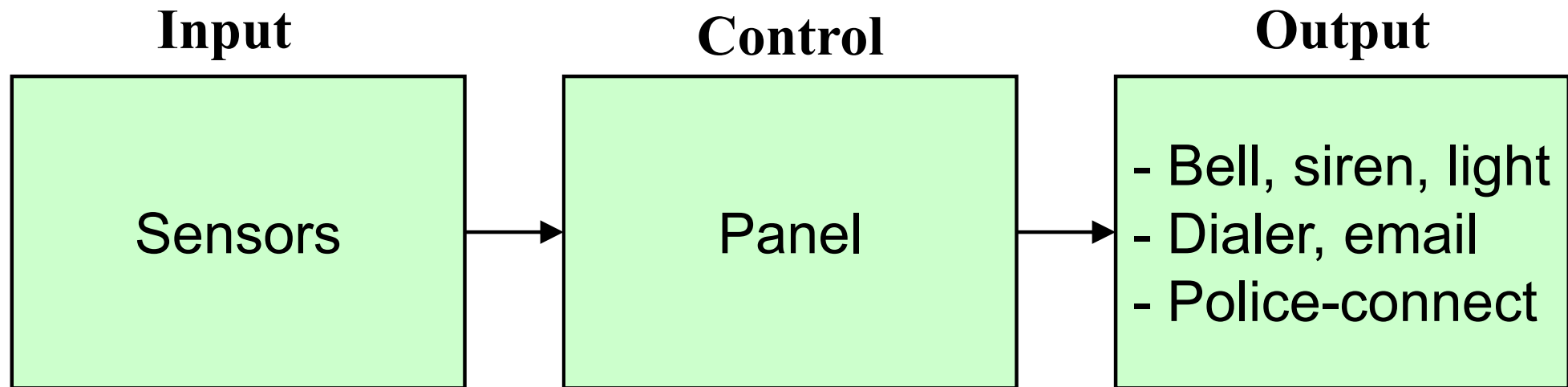
Detection of sensors:
- Infrared
- Ultrasonic
- Microwave (droppler effect)
- Dual technology
- Glass breaks, switches

Annunciation/
alarm signaling

Closed-circuit security alarm system

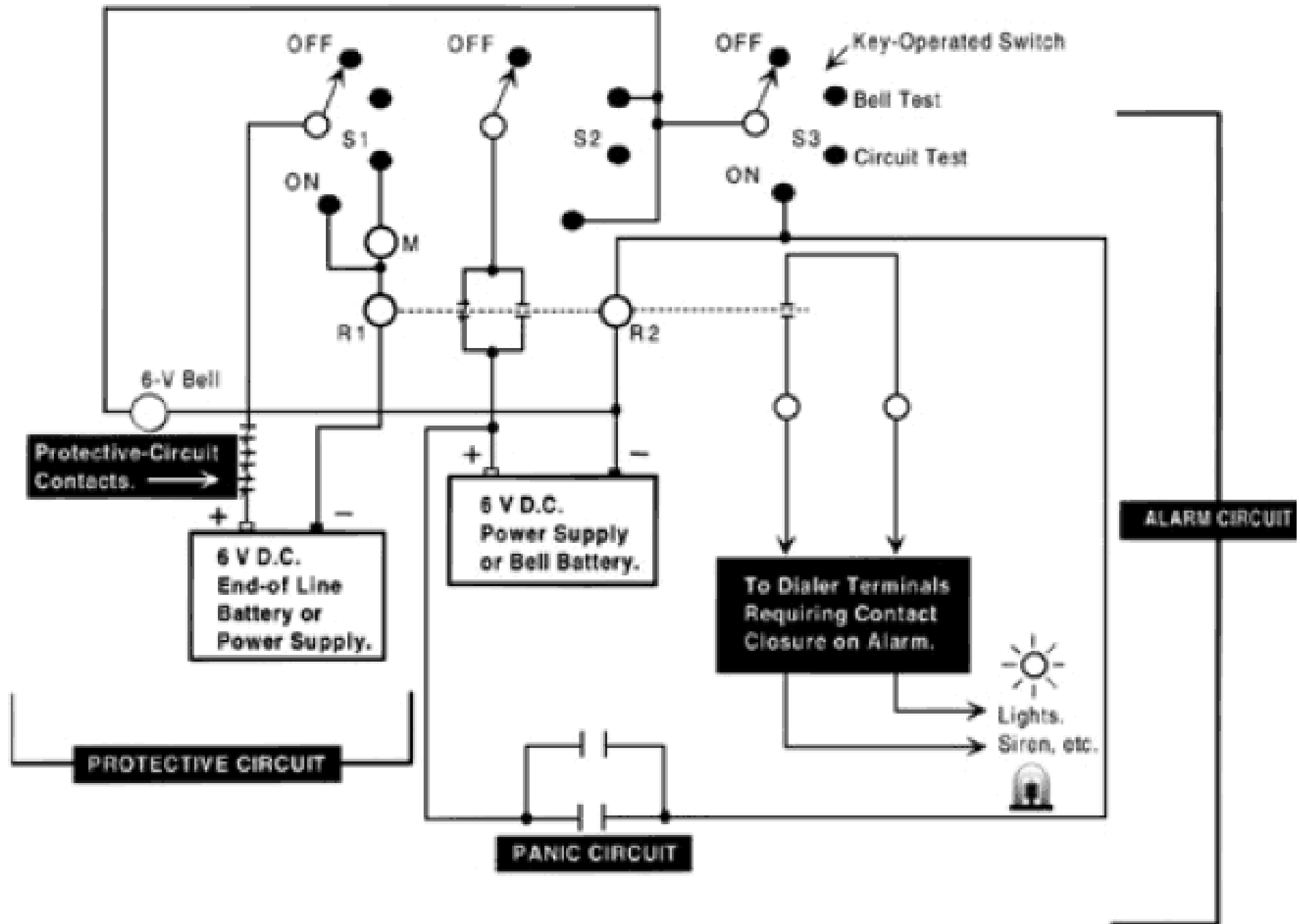OFF — OFF — OFF — Key-Operated Switch

Bell Test

S1 — S2 — S3 — Circuit Test

ON — ON

M

R1 — R2

6-V Bell

Protective-Circuit Contacts. →

+ —

6 V D.C. End-of Line Battery or Power Supply.

+ —

6 V D.C. Power Supply or Bell Battery.

To Dialer Terminals Requiring Contact Closure on Alarm.

ALARM CIRCUIT

Lights. Siron, etc.

PROTECTIVE CIRCUIT

PANIC CIRCUIT

(Source: Kennedy, T. and Traister, J. E., 2002. *Low Voltage Wiring: Security/fire Alarm Systems*)

Components for a typical security/fire-alarm system

Fire Horn

Heat Detector

Burglar Cell

Smoke Detector

Transformer

Control Station

A.C. Supply

Remote-Control Stations with ON-OFF Indication (Lock-Switch or Push Button).

Space Protection Circuit

Surface Magnetic Contacts

Delay loop

Ultrasonic Detectors

Perimeter Protection Circuit

Floor Mat Switch

Infrared Photoelectric Detector
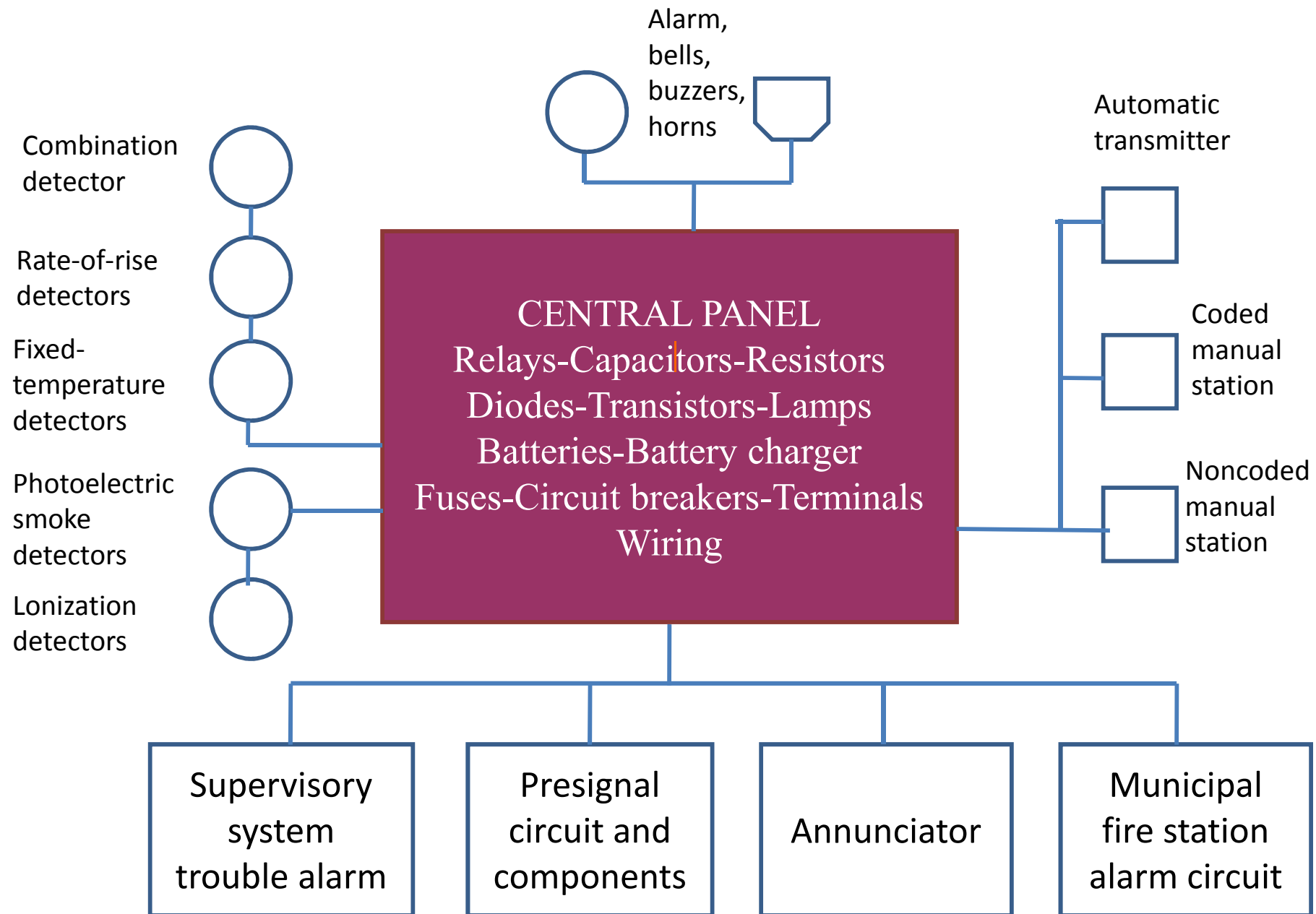
Recessed Magnetic Contacts
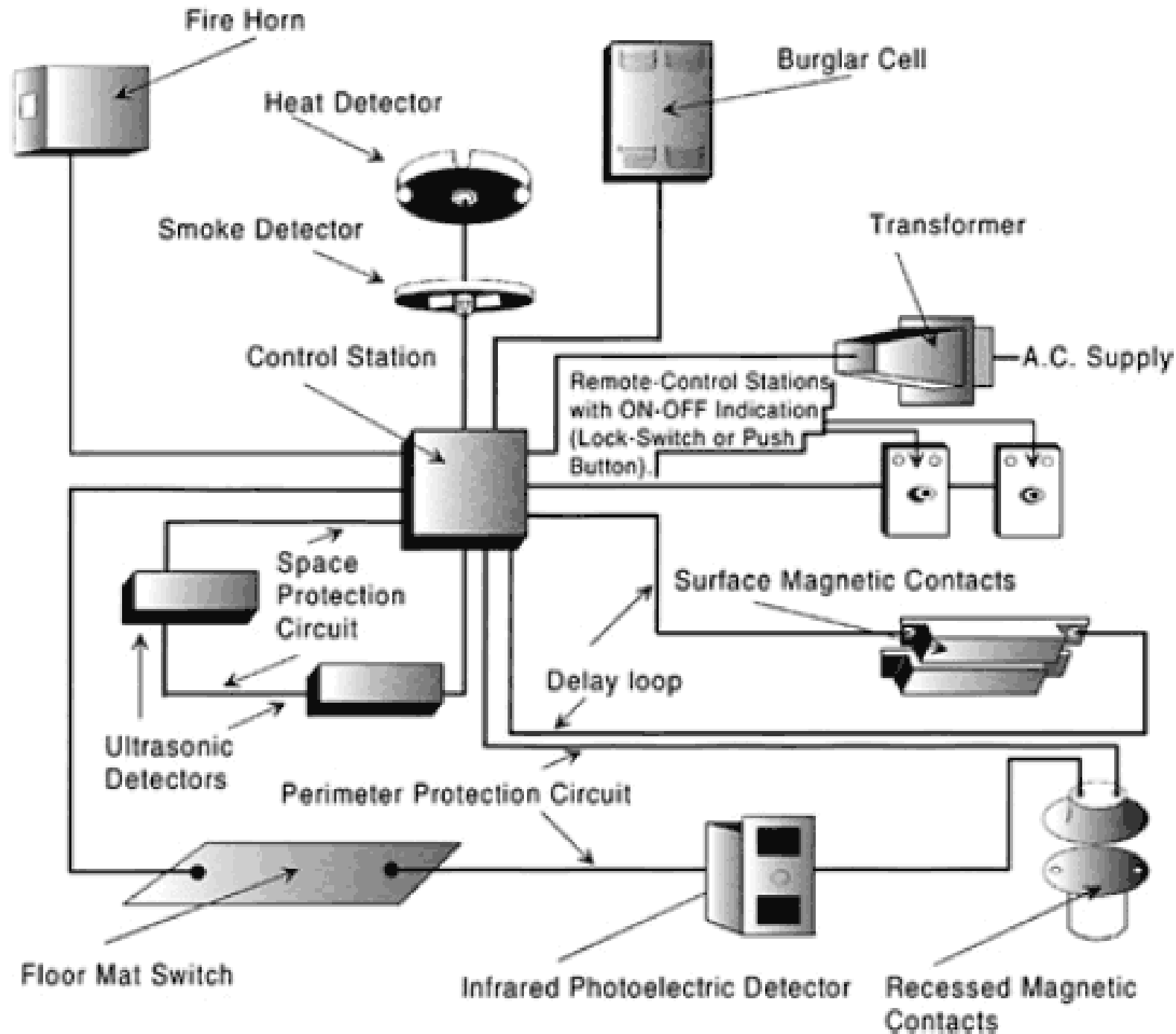
(Source: Kennedy, T. and Traister, J. E., 2002. *Low Voltage Wiring: Security/fire Alarm Systems*)

Schematic diagram of a fire-alarm main control panel

○ = Automatic smoke detector

▢ = Manual pull stations

◉ = Bell, buzzer, or horn annunciator

Station, Detector and Alarm Circuit

Alarm Circuit   Alarm Circuit

MAIN CONTROL PANEL

Station and Detector Circuit

120/240V AC

Supplementary Circuit

(Source: Kennedy, T. and Traister, J. E., 2002. *Low Voltage Wiring: Security/fire Alarm Systems*)
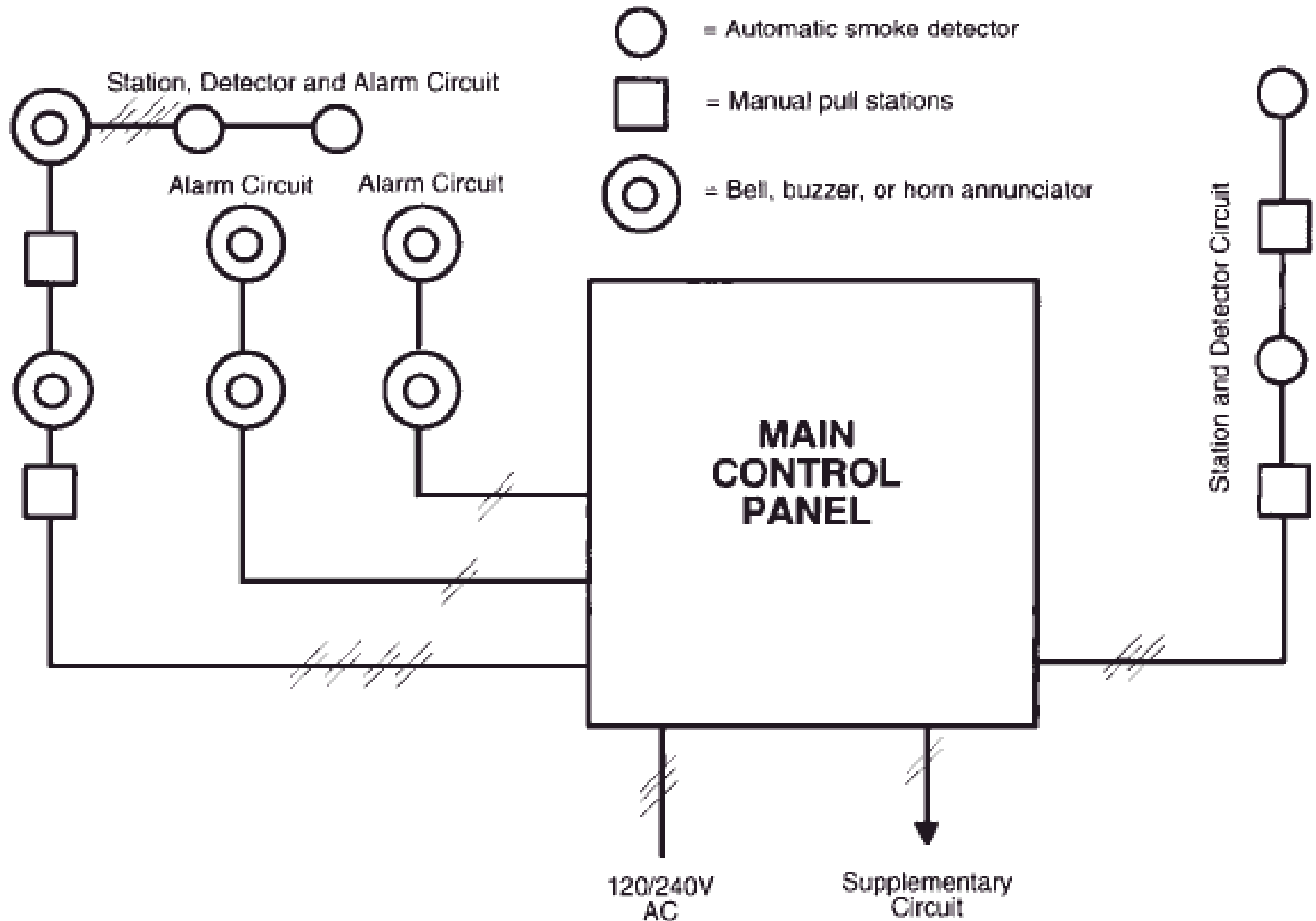
Components of a basic fire-alarm system

Alarm, bells, buzzers, horns

Automatic transmitter

Combination detector

Rate-of-rise detectors

Fixed-temperature detectors

Photoelectric smoke detectors

Lonization detectors

CENTRAL PANEL
Relays-Capacitors-Resistors
Diodes-Transistors-Lamps
Batteries-Battery charger
Fuses-Circuit breakers-Terminals
Wiring

Coded manual station

Noncoded manual station

Supervisory system trouble alarm	Presignal circuit and components	Annunciator	Municipal fire station alarm circuit

(Source: Kennedy, T. and Traister, J. E., 2002. *Low Voltage Wiring: Security/fire Alarm Systems*)

Example of home security system
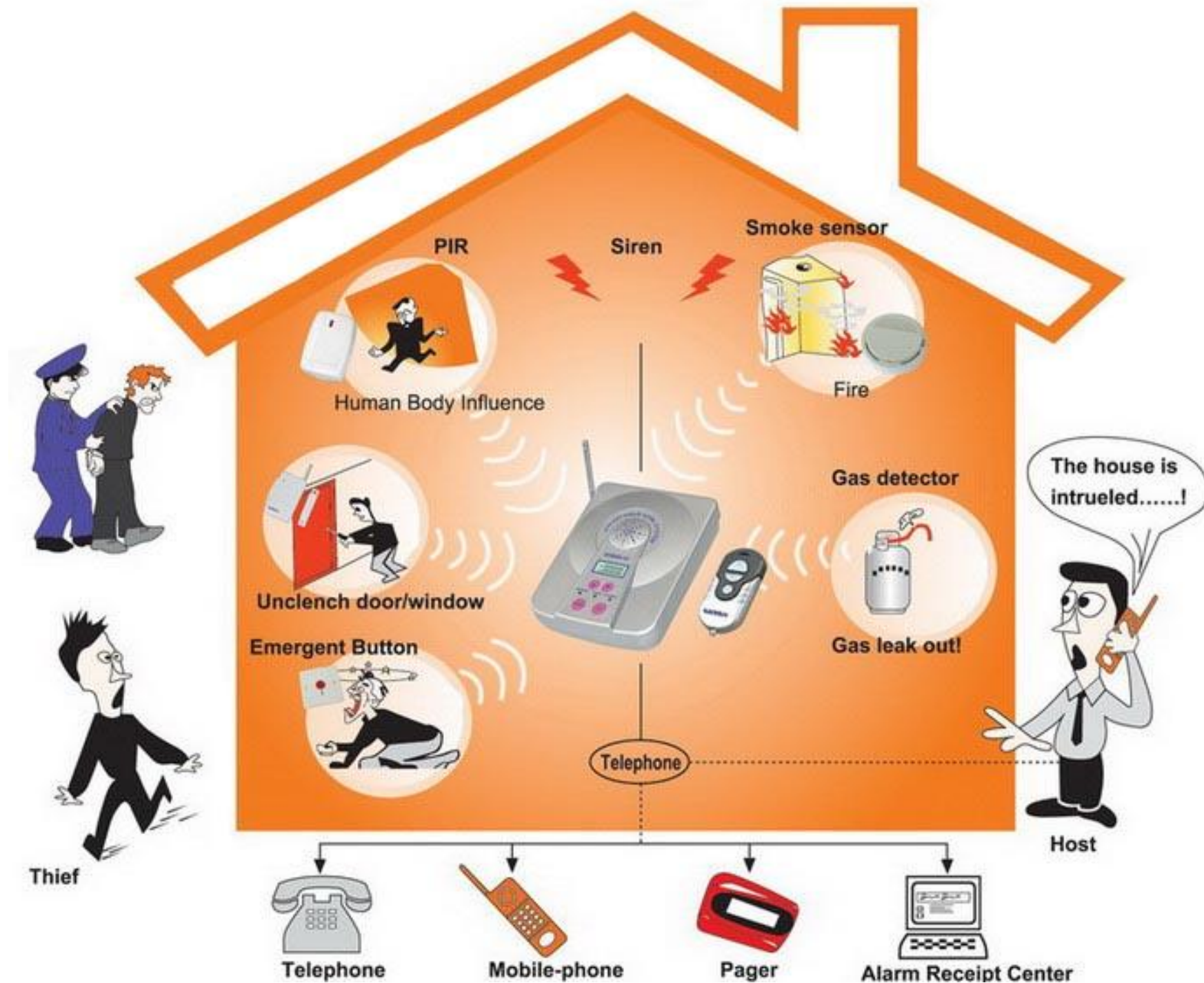
Security Systems

- Monitored systems
  - Contact a monitoring company by telephone
    - The security system senses something
    - The system waits for 30 to 45 seconds before going into alarm allowing the homeowner a chance to deactivate the system to prevent false alarms
    - If not deactivated, the security system goes into alarm and sends a message to the monitoring company over telephone lines
    - The monitoring company receives the message, determines the nature of the alarm and verifies the alarm, generally by placing a phone call to the home. If they do not receive the proper password or do not receive an answer, they call the police
    - The police receive the monitoring company's call and respond

Security Systems

- [Unmonitored](#) systems
  - Typically on-site alarms and/or flashing lights to indicate the security system has been breached
  - Relies on neighbours or passersby as to see or hear the alarms and then to call police
  - A combination of strobe lights and alarms
    - Many burglars will leave once alarms and strobes are activated

Security Systems

- **[False alarms](#)**
    - 95-99% of the alarms received are false
    - Some police departments impose fines for false alarms after a specified number of false alarms
- Common causes of false alarms
    - Environmental conditions e.g. a storm that causes loose windows and doors with sensors to rattle
    - Wandering pets that are not in a "safe" zone and may activate motion sensors
    - Drafts that move objects such as curtains or plants in the home within the motion sensor's detection area

False alarm management scheme in Hong Kong

防盜警鐘分級處理計劃

第一級 — 新警鐘/可靠性系統 new alarm/reliable system

Level 1

（衝鋒隊及巡邏人員 — 留守一小時）

(Emergency Unit & Patrol – stay 1 hour)

第二級 — 30天內 3次誤鳴、180天內 5次誤鳴

Level 2

3 false alarms in 30 days; 5 in 180 days

（巡邏人員 — 不需留守）

(Emergency Unit & Patrol – no stay)

第三級 — 30天內 5次誤鳴、180天內10次誤鳴

Level 3

5 false alarms in 30 days; 10 in 180 days

（通知巡邏人員 — 不需優先處理）

(Patrol – no priority to take care)

Security Systems

- ## Closed circuit television (CCTV) system

  - ### Functions
    - 24 hour surveillance/deterrence
    - Real time or time lapse recording
    - Motion/alarm activated monitoring & recording
    - Area search using remotely controlled cameras
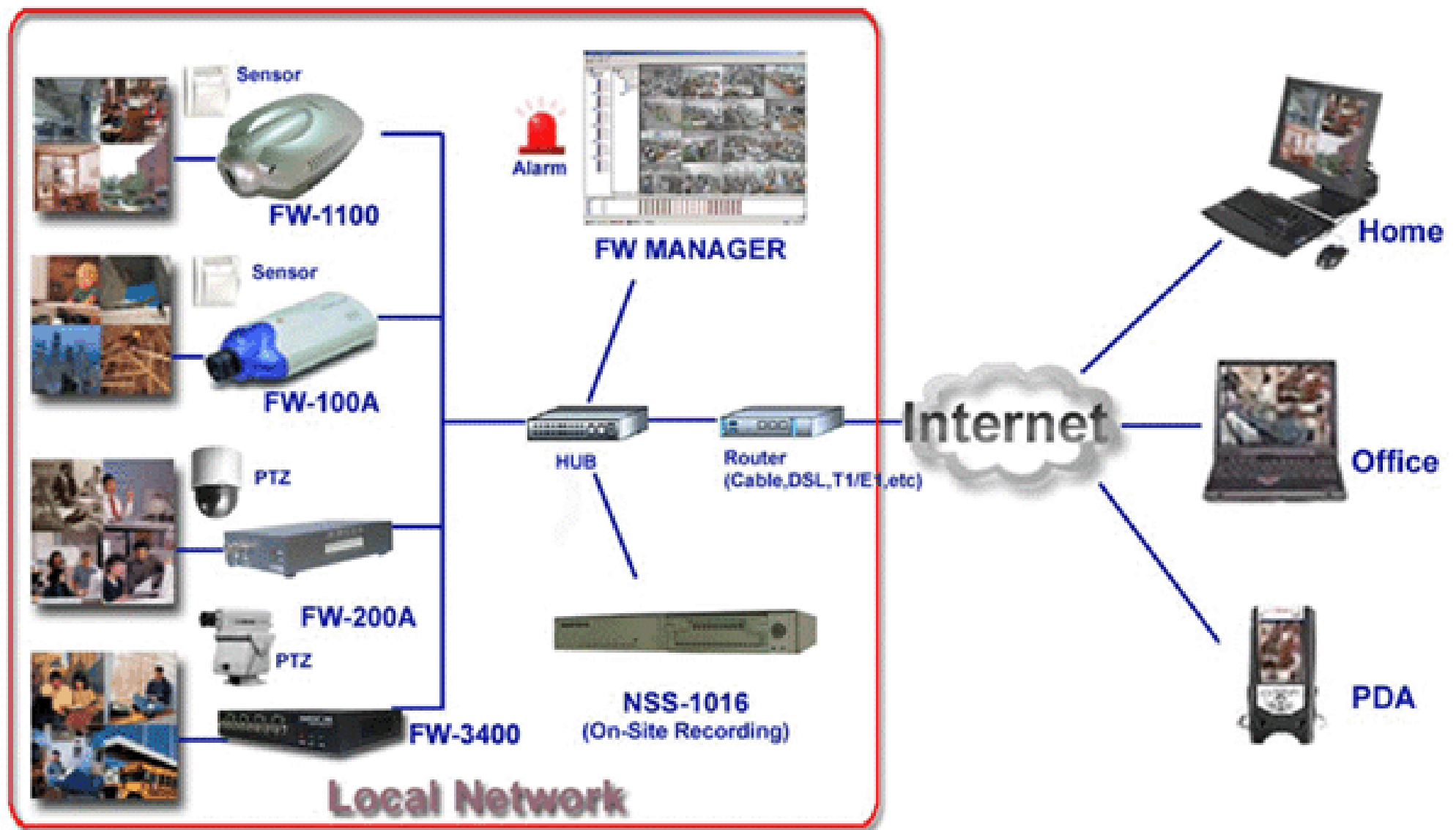   - Integration with access control & other security systems

  - ### Components (now mainly digital)
    - Video camera (colour or monchrome)
    - Monitors, recorders and switchers
    - Multiplexer (triplex operation simultaneous playback and recording)

  - ### Key factors: quality, storage, export, playback

(* See also: HK Police requirements for digital CCTV systems http://www.police.gov.hk/info/doc/cpa/CCTV%20English.pdf)

LAN Networked Multi-Site Monitoring and Security
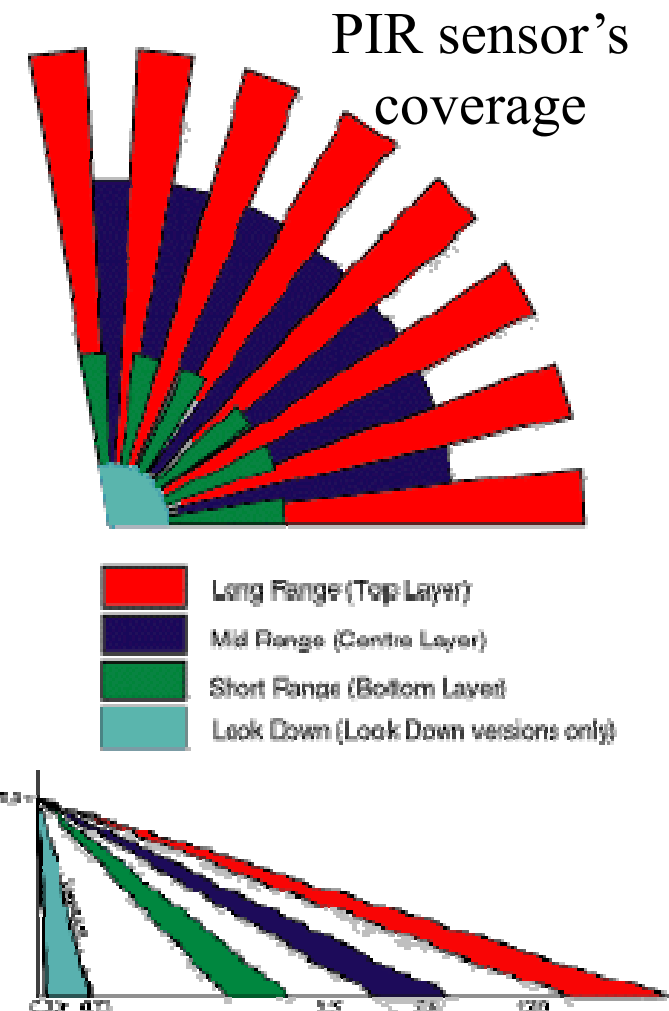
Security Systems

- ## Intruder detection alarm system

  - ### Mechanical contact switch

  - ### Magnetic contact switch

  - ### Glass-break detector

  - ### Photo-electric sensors

  - ### Motion sensors

    - #### e.g. passive infrared (PIR) sensors

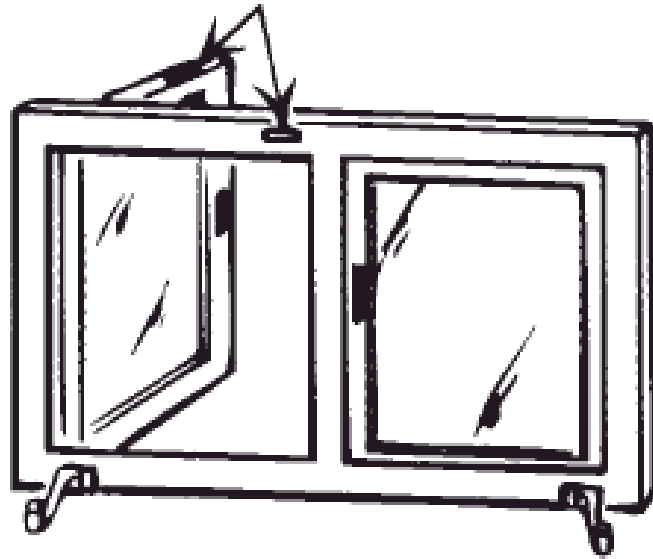 - ### Signaling devices

    - #### Both audible and visual types

PIR sensor's coverage

🟥	Long Range (Top Layer)
🟦	Mid Range (Centre Layer)
🟩	Short Range (Bottom Layer)
🟦	Look Down (Look Down versions only)

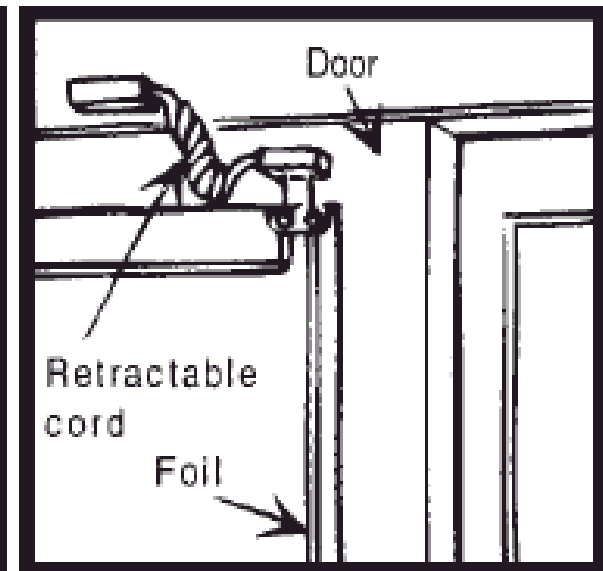# Example of an intruder detection alarm system

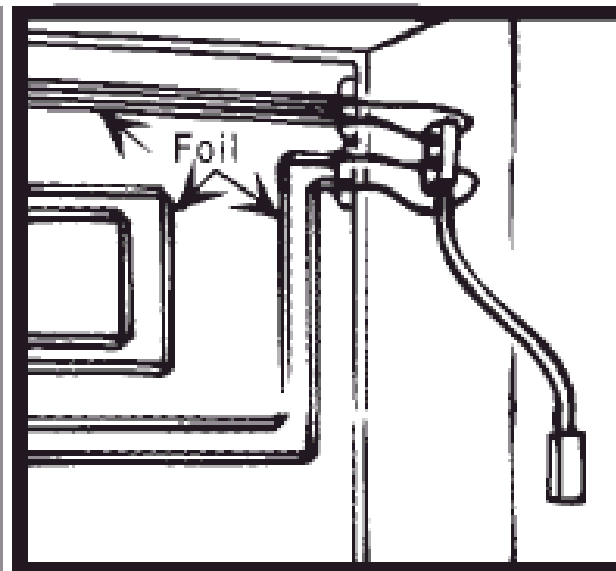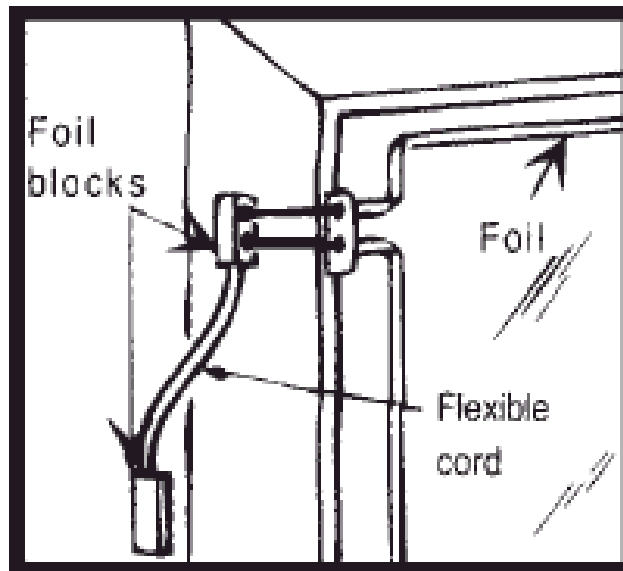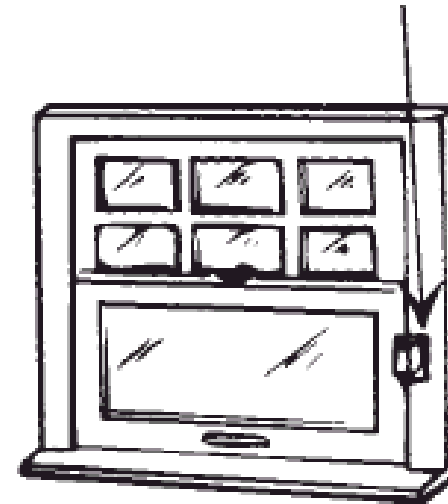# Magnetic contacts on windows and doors

Recessed switch in top casing; magnet in window top

Surface-mounted switch and magnet

Foil blocks

Foil

Flexible cord

Foil

Door

Retractable cord

Foil

(Source: Kennedy, T. and Traister, J. E., 2002. *Low Voltage Wiring: Security/fire Alarm Systems*)
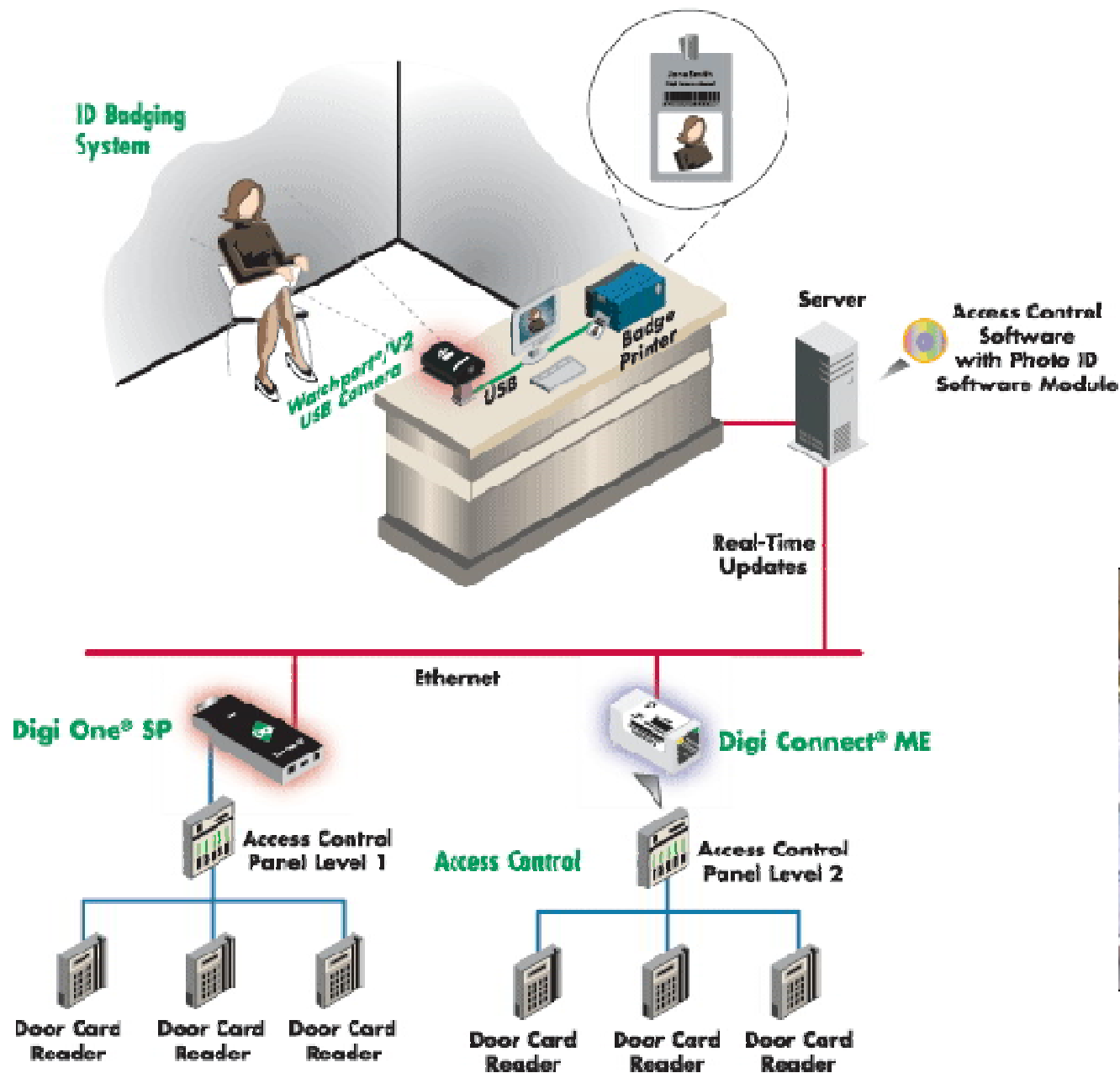
Security Systems

- ## Access control
  - Stand-alone or online systems
  - Methods:
    - Digital codes
    - Magnetic stripe cards
    - Embedded wire cards
    - Proximity cards/tags
    - Biometric access control (e.g. retina, finger prints)
  - Pedestrian turnstiles (like those in subway stations)
  - Car park control (e.g. car park ticket validation)

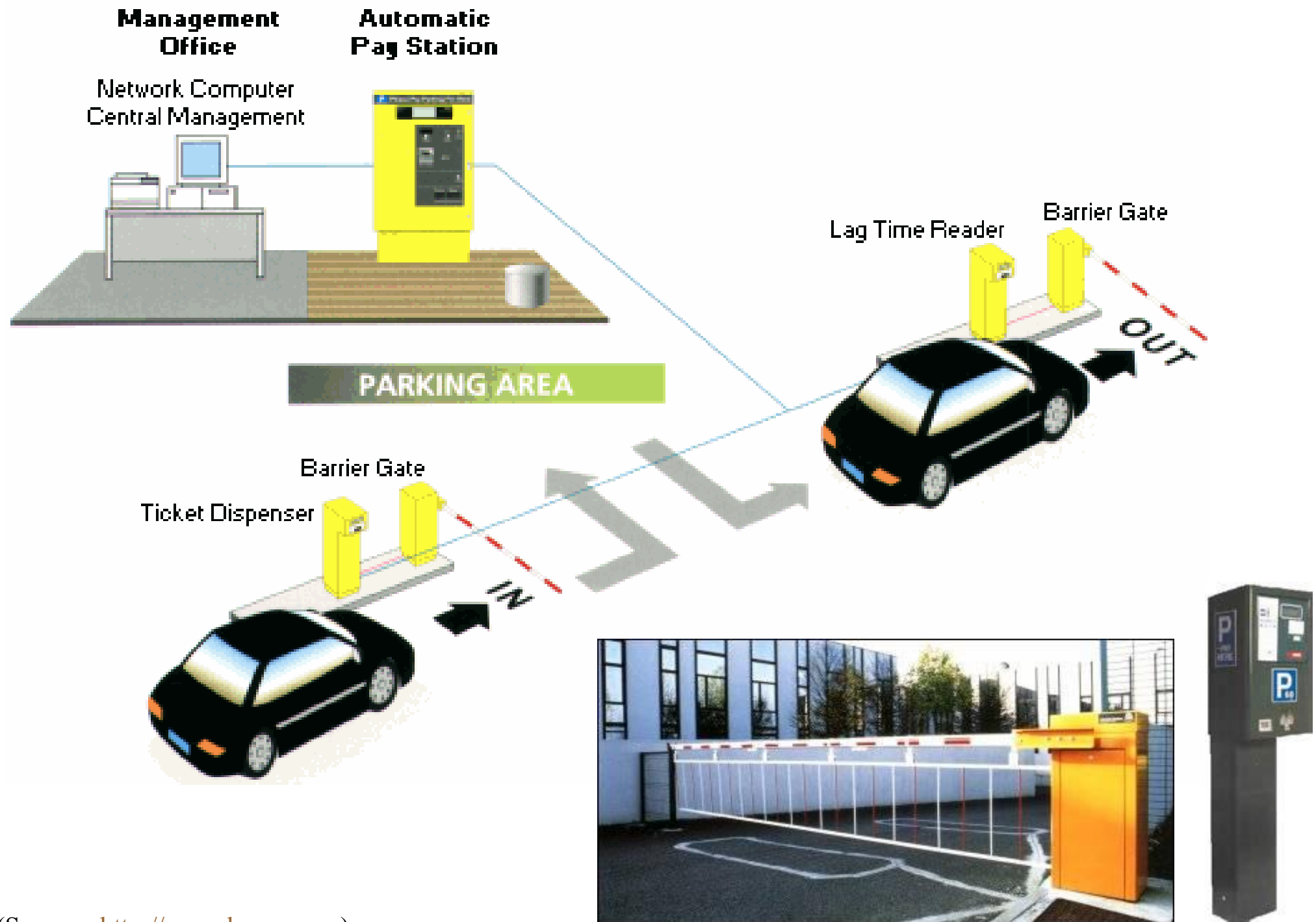**Integrated Photo ID Badge and Access Control System**

Access control system

Pedestrian turnstiles

Car park control system

(Source: http://www.baps.co.nz)

Security Systems

- [Security lighting](#)
  - Good lighting can put off or draw attention to a thief, makes people feel more secure
    - Outdoor floodlight with motion monitor or camera
    - Outdoor motion-activated lighting
      - Passive infra-red (PIR) controlled
  - Recommended design
    - Low consumption lamps
    - Units positioned to reduce glare
    - Avoid light pollution & possible attack

Security Systems

- Guard tour (monitoring) systems
  - Security officers provide periodic patrols of the facility to detect suspicious and abnormal activity
  - Establish a patrol route or "tour" that includes stops at all the important points
  - Three basic types:
    - Watchman's clock system (w/ key stations)
    - Electronic guard tour system (w/ checkpoint stations)
    - Integrated guard tour system (use card readers)
  - Latest technology: e.g. smart phone, GPS

(* See also: Introduction to Guard Tour Systems http://silvaconsultants.com/introduction-to-guard-tour-systems.html)

Security Systems

- Security Products (HK Police Crime Prevention)
  http://www.police.gov.hk/ppp_en/04_crime_matters/cpa/sec_products.html
    - Access control systems, alarms, CCTV
    - Guard monitoring systems
    - Security lighting
    - Locks
    - Perimeter protection (fencing, barriers)
    - Personal panic alarm
    - Property marking
    - Screening, storage
    - Vehicle security system

Security Systems

- Security company licence in HK
  - Type I – provision of security guarding services
  - Type II – provision of armoured transportation services
  - Type III – installation, maintenance and/or repairing of a security device and/or designing (for any particular premises or place) a security system incorporating a security device
- Managed by the Security and Guarding Services Industry Authority (SGSIA)
  http://www.sb.gov.hk/eng/links/sgsia/

A typical building security & car park control system

(1) Building entry access system with intercom system

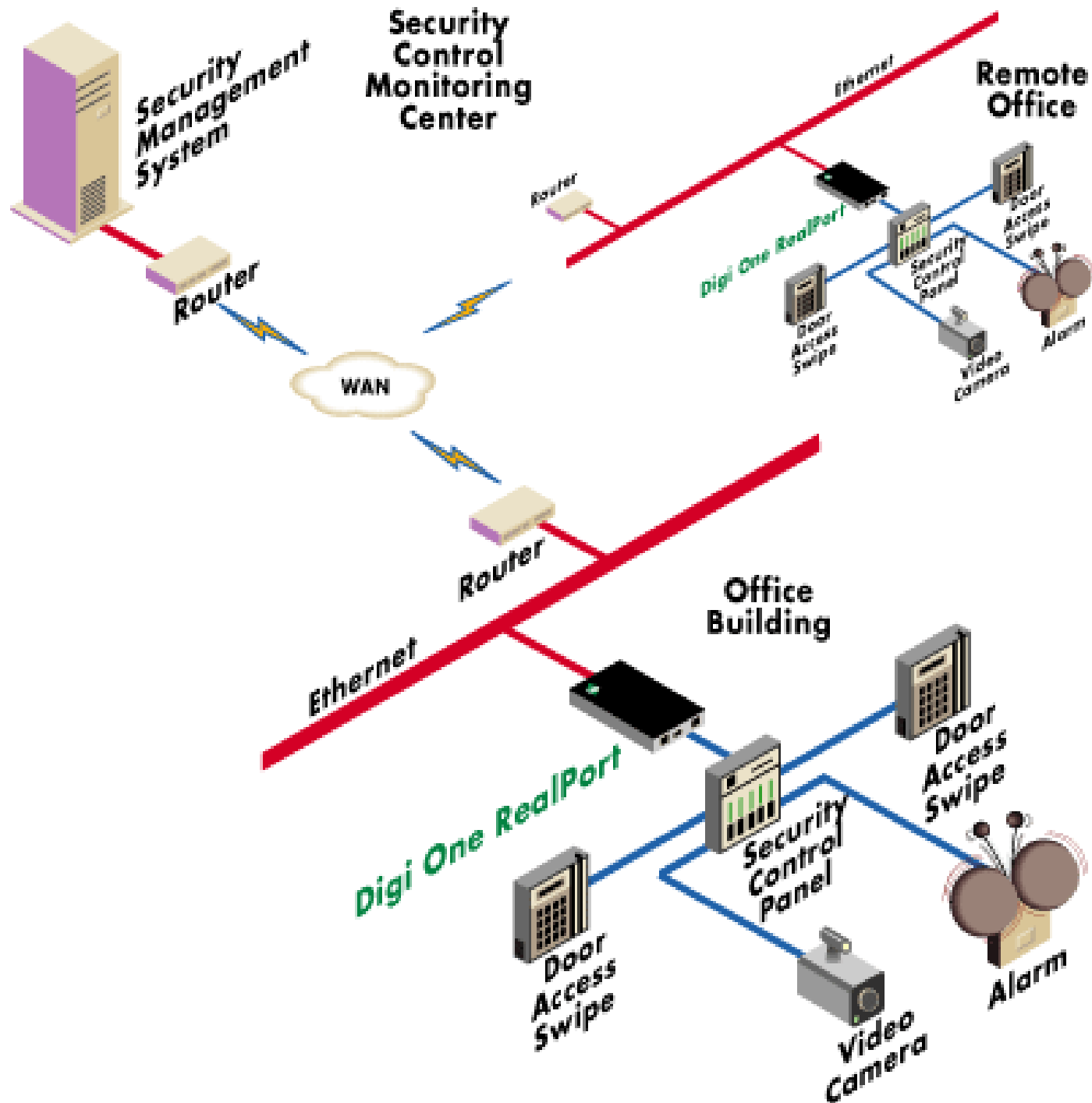(2) Lift access control restricting tenants within floors

(3) Secure alarmed areas within office complexes

(4) Energy management & building service control systems (lighting and air conditioning)

(5) Car park access control for entry and exit

(Source: http://www.baps.co.nz)

Security management network system

Security Systems

- Typical testing & commissioning items
  - Central control unit
  - Interconnecting
  - Uninterrupted power supply
  - Remote alarm transmission to a private security control centre
  - Card access control system
  - Exit control lock
  - Duress button
  - Motion detector, glassbreak detector
  - Magnetic door contact, tamper switch, electric door strike
  - Watchman tour system

Further Reading

- Physical Security Basics
  http://www.shieldjournal.com/physical-security-basics/

- How To Do A Risk Assessment
  http://www.shieldjournal.com/how-to-do-a-risk-assessment/

- Designing Lobbies for Good Security
  http://silvaconsultants.com/designing-lobbies-for-good-security.html

- Alarm Systems – An Overview
  http://www.shieldjournal.com/alarm-systems-an-overview/

- Security Products (HK Police Crime Prevention)
  http://www.police.gov.hk/ppp_en/04_crime_matters/cpa/sec_products.html