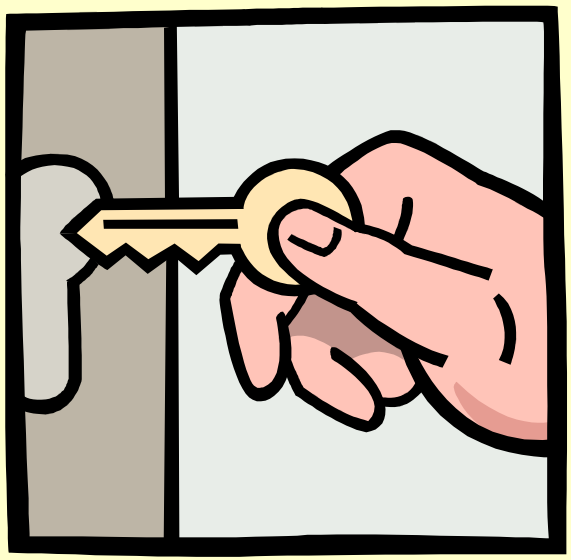
MECH3422 Building Services Engineering I

http://me.hku.hk/bse/MECH3422/



Security Systems

Dr. Sam C. M. Hui

Department of Mechanical Engineering

The University of Hong Kong

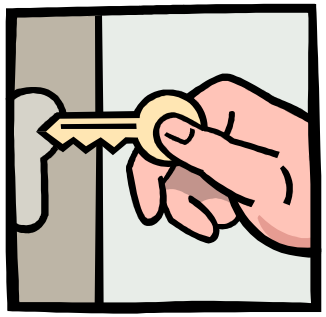
E-mail: cmhui@hku.hk

Sep 2015

Contents

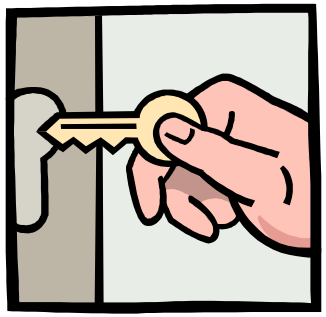
- Basic Concepts
- Risk Assessment
- Security Planning
- System Components

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

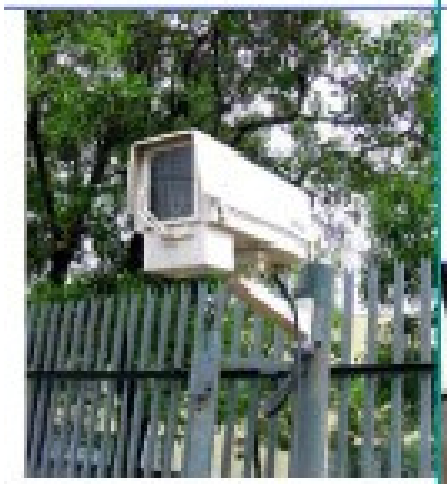
Basic Concepts



- 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 & data)

[* See also: Information security - Wikipedia http://en.wikipedia.org/wiki/Information_security]

Highly secured premises

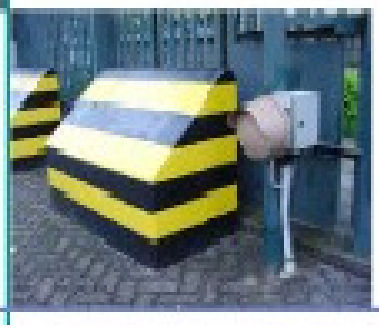


CCTV

Security control centre

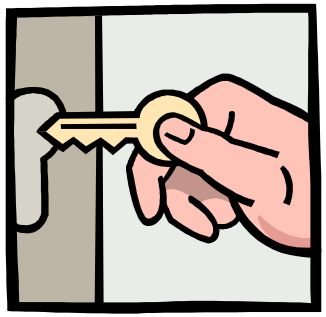
Access control

Blocks & fencing



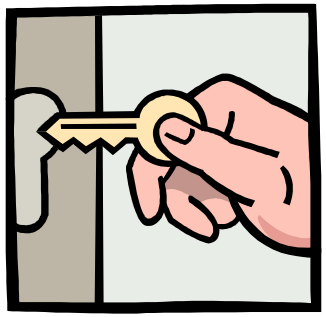
[Source: Hong Kong Note Printing Limited]

Basic Concepts

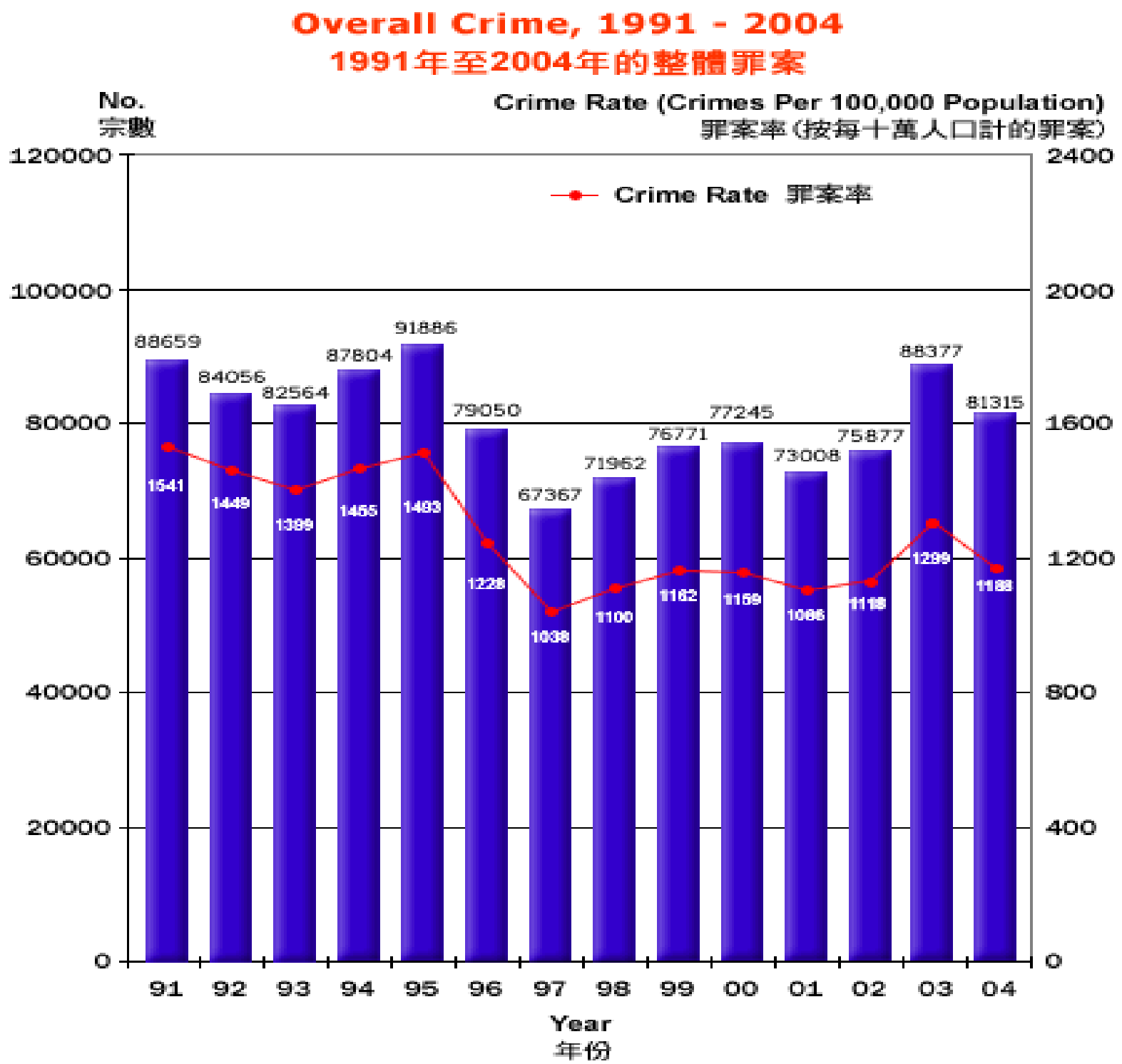


- Elements of physical security
  - Explosion protection & obstacles, to frustrate trivial attackers and delay serious ones
  - Alarms, security lighting, security guard patrols or closed-circuit television cameras, to make it likely that attacks will be noticed
  - Security response, to repel, catch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

Basic Concepts



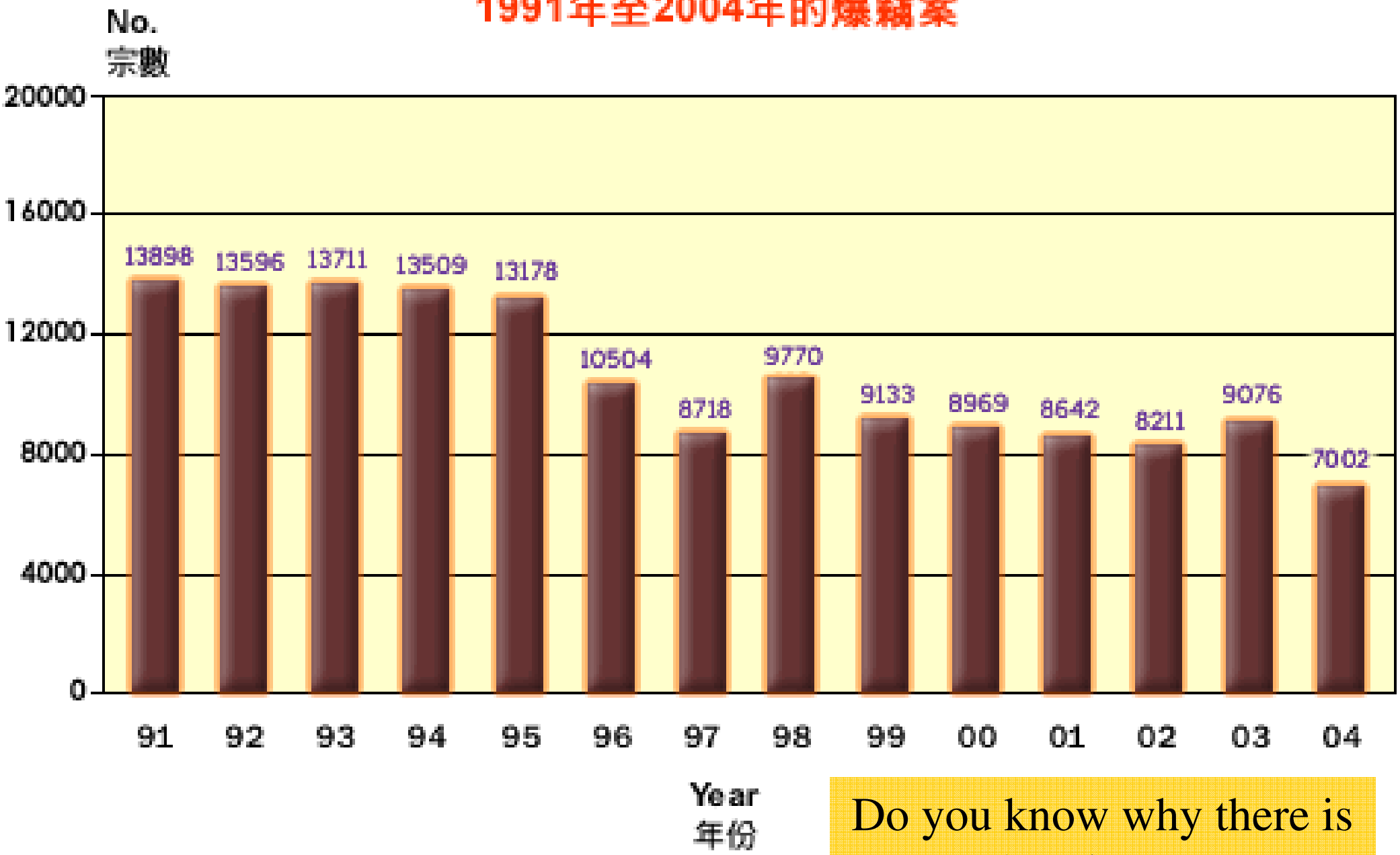
- Why security and alarm systems?
  - Decrease the chances of a burglary (if a burglar is aware a house has a system, he she might move on to another home)
  - Decrease the number of items stolen and the extent of damage done
- Objectives of security design
  - Crime prevention: aim to minimise, in and around the building, risks of theft, criminal damage, vandalism, personal attack and sabotage, both during the construction of the building and throughout its life



Crime in Hong Kong

Source: http://www.info.gov.hk/police/

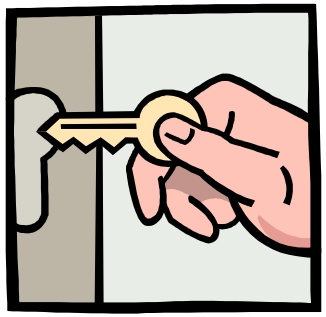
Burglary, 1991 - 2004
1991年至2004年的爆竊案



Do you know why there is a drop in 1997?

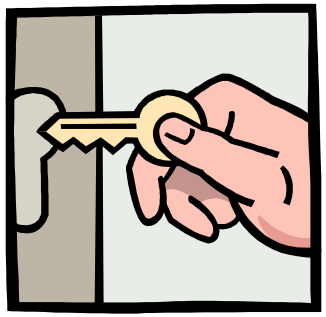
Source: http://www.info.gov.hk/police/

Basic Concepts



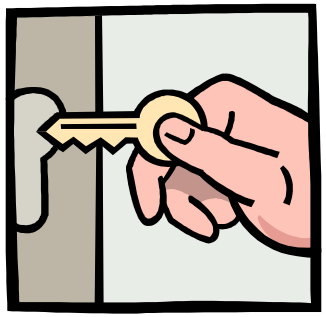
- Four layers of physical security
  - 1. Environmental design (to deter threats)
  - 2. Mechanical and electronic access control (e.g. locks and access cards)
  - 3. Intrusion detection (monitors for attacks)
  - 4. Video monitoring (for incident verification and historical analysis)
- The goal is to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

Basic Concepts



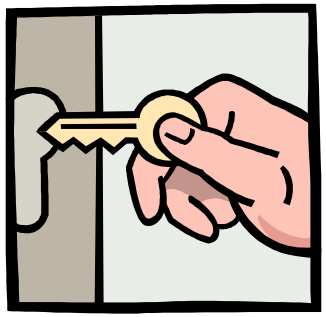
- Key concerns of security design
  - Must be fully *co-ordinated*, at all stages of building design
  - Design of physical protection
    - Building design (e.g. landscaping, building inter-relationships, access)
    - Physical security components (e.g. doors and windows)
  - Design of security devices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

Basic Concepts



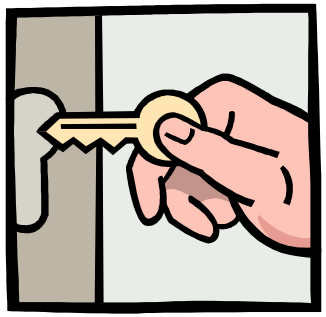
- Remember: security systems do not 100% prevent thieves from breaking into buildings
- A good security plan should include:
  - Strong window, door, and lock products
  - Good security habits and lifestyles (e.g. always lock doors at night or when the house is vacant)
  - Natural surveillance, e.g. neighbourhood watches
- Conflicts between security and fire safety
  - Security requires lock-up; safety requires open

Basic Concepts



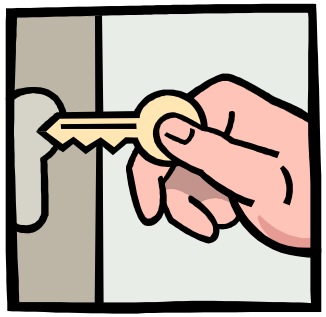
- Major issues
  - 1. Evaluate the risk
    - Assess all possible risks e.g. damage by fire, water, vandalism, burglary (and terrorism), and the inconvenience suffered as a result
    - Estimate the required level of investment in security measures by evaluating the risk of burglary
    - Take into account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

Basic Concepts



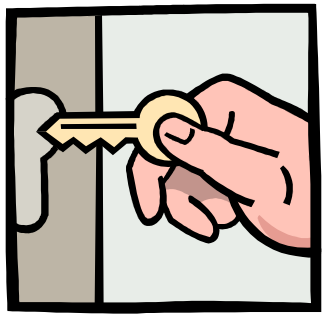
- Major issues (cont'd)
  - 2. Physical protection
    - Form of fencing or building elements (e.g. walls, partitions, doors, windows, barriers, screens, bolts, locks, safes, and so on) which discourage and delay unauthorised entry
  - 3. Detection
    - Consider the assessed risk, the time needed to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

Basic Concepts



- Major issues (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

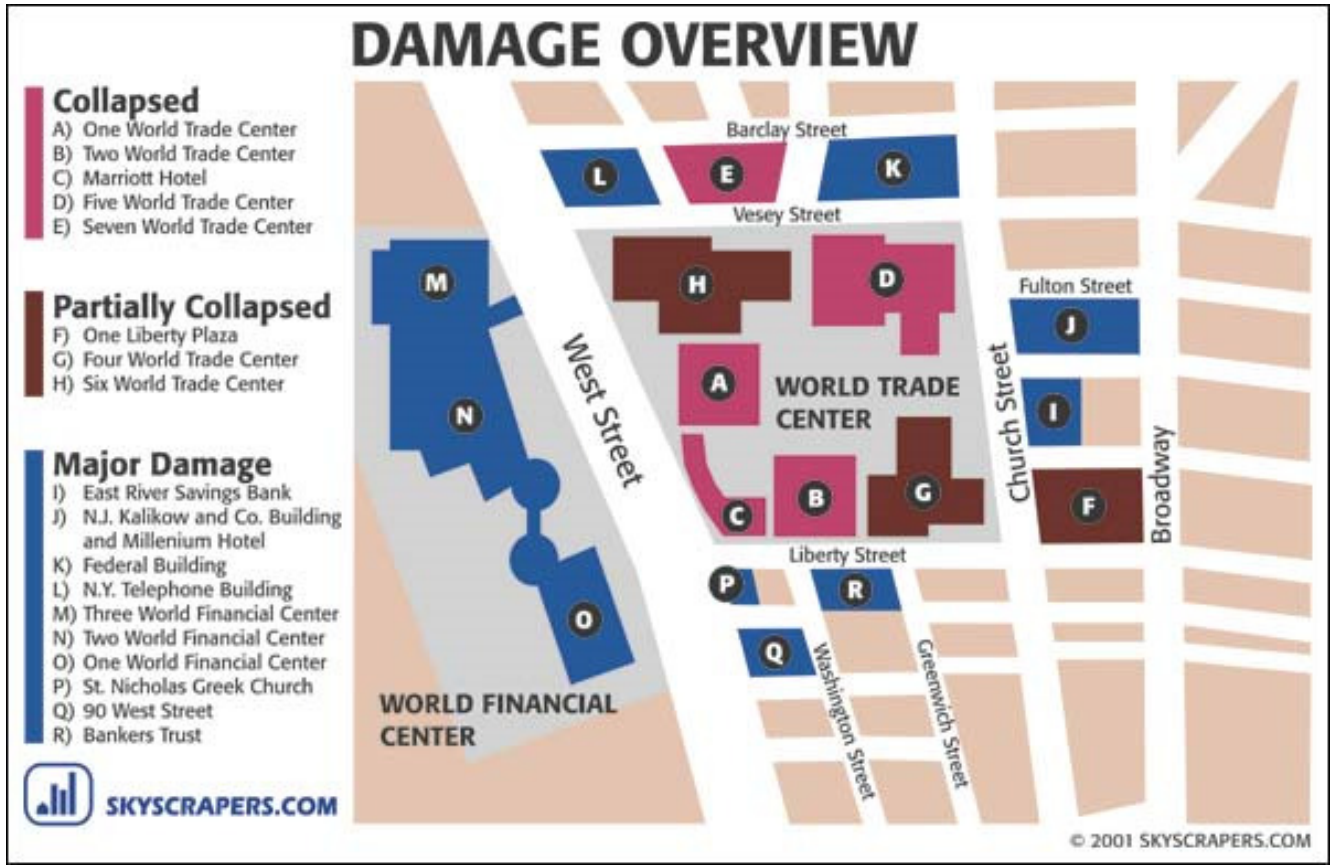


- Major issues (cont'd)
  - 6. Maintenance and review
    - Frequent testing & competent maintenance minimise the possibility of system failure
    - Periodic reviews to determine the changes, if any, to the building's structure, usage, personnel, or to the items being protected

Risk Assessment

- Identify security risks/threats
  - What can happen
  - Threats to personnel safety
  - Theft of property
  - Vandalism and sabotage
- Since "9/11", terrorism has become a major focus in many countries (e.g. homeland security in USA)
  - "Terrorism" = unlawful use or threatened use of force or violence by a person or an organised group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons

Impact of 9/11 on security design & requirements



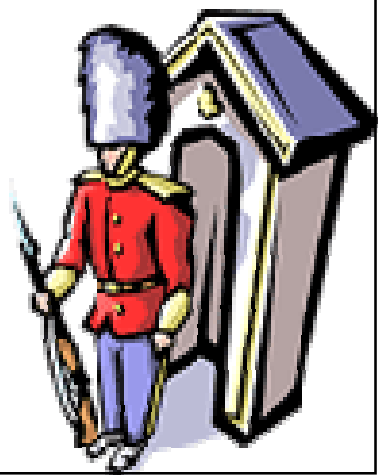
[Source: http://www.skyscrappers.com]

Risk Assessment

- 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

Risk Assessment

- 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



Risk Assessment

- 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

Risk Assessment

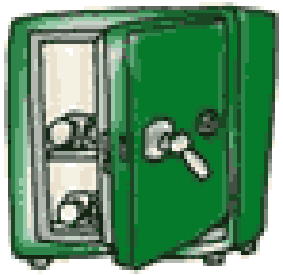
- Main categories:
  - Building location and surroundings
  - Building access and structural strength
  - Building contents
  - Occupational pattern
  - Consequence of loss
  - History of loss
  - Existing security measures
  - Recommended level of protection
- Also, the “peace of mind” given to occupants

Security Planning

- 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

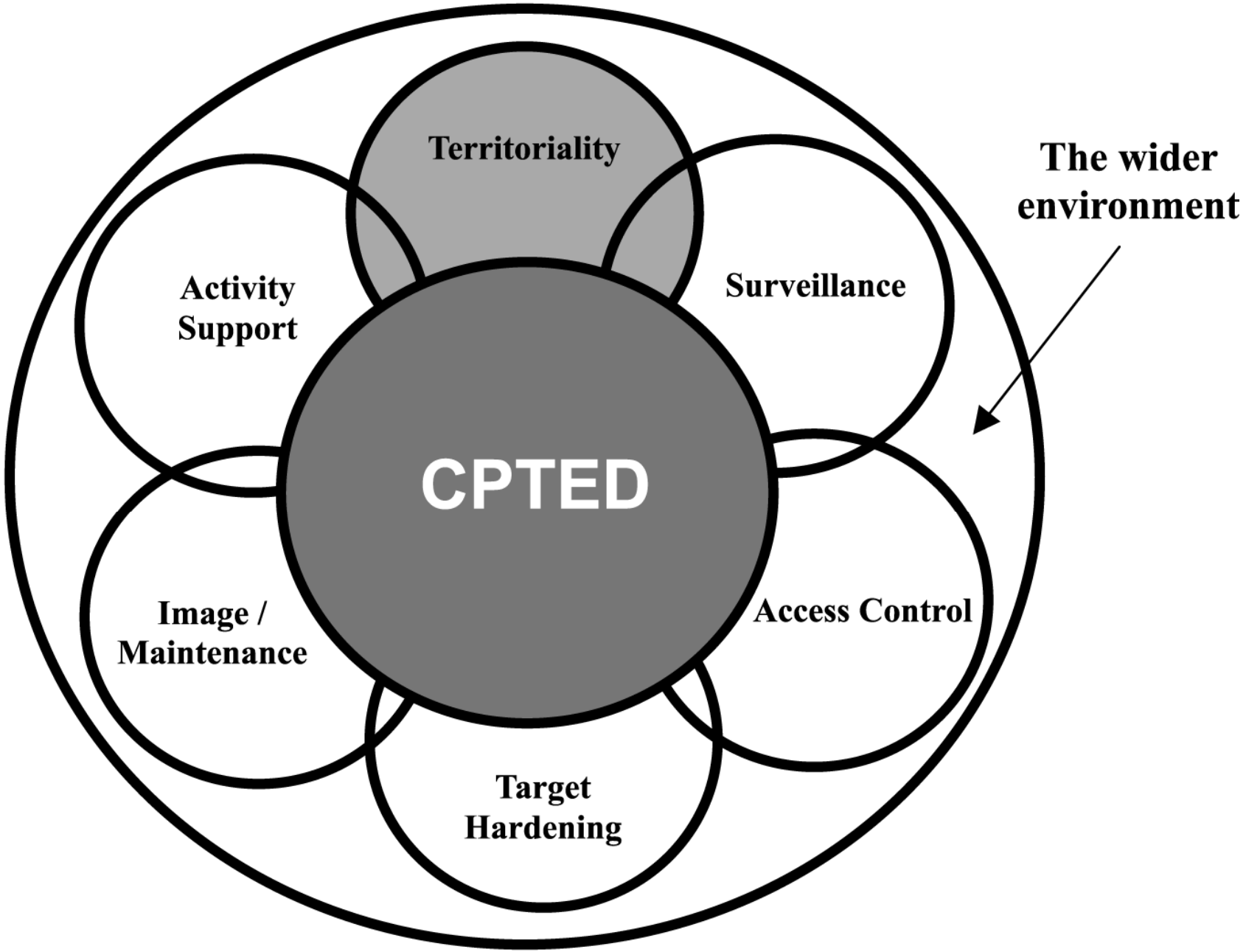
- Planning of security systems
  - Careful consideration of physical protection issues can reduce the needs for electronic solutions & provide long-term financial savings
    - Such as, crime prevention through environmental design (CPTED)
  - Continuous monitoring to ensure fast response to an alarm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

Security Planning

- Crime prevention through environmental design (CPTED) 通過環境設計預防犯罪*
  - A multi-disciplinary approach to deterring criminal behavior through environmental design
    - Relationship between the built environment and criminal behaviour
    - Deter criminal behaviour and influence offender decisions that precede criminal acts
  - Proper design & effective use of the built environment can lead to a reduction in the incidence and fear of crime

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

Concepts of crime prevention through environmental design (CPTED)



Source: Adapted from Moffat (1983, p. 23)

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

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

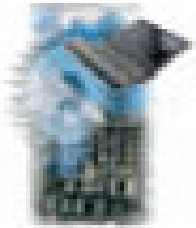
Typical security and alarm systems

Intrusion Alarms

Closed Circuit Television

Digital Video Surveillance

Access Control



Critical Process Monitoring

System Components

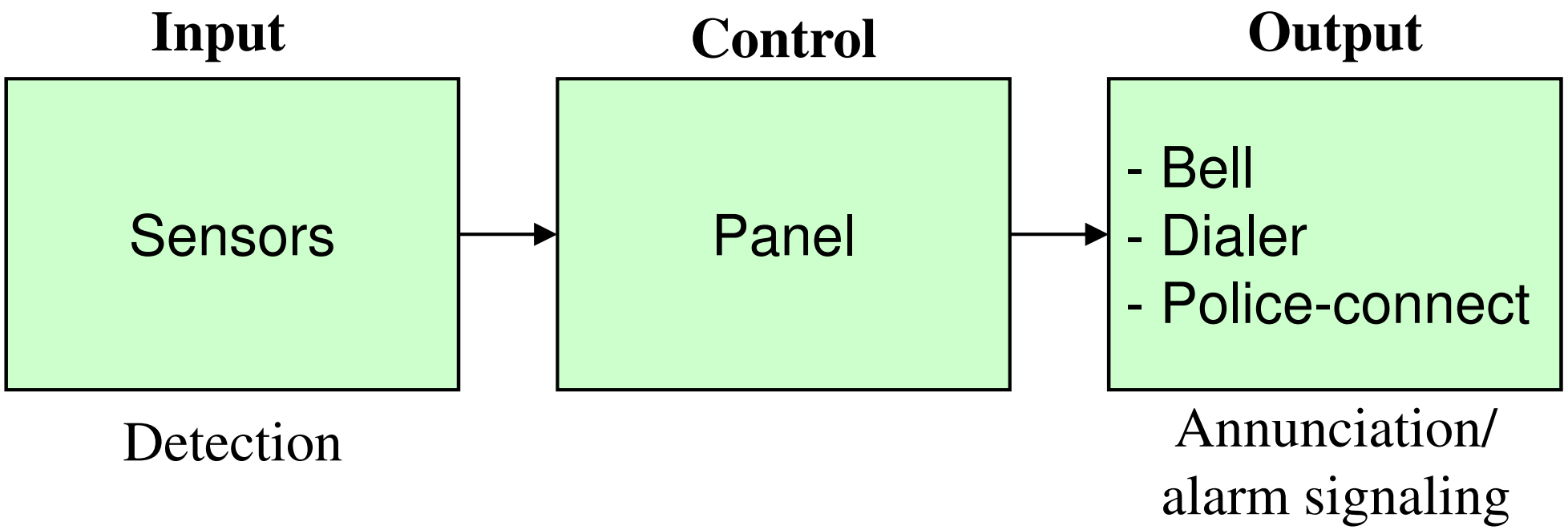
- Common types of systems
  - Burglar alarm system
    - Central or local (w/ direct link to police)
  - Fire alarm & detection system
  - C.C.T.V. surveillance system
  - Intruder detection & access control
  - Intercom systems (audio/video)
  - Door-phone system & interlocking system
  - P.A. (panic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

System Components

- 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)

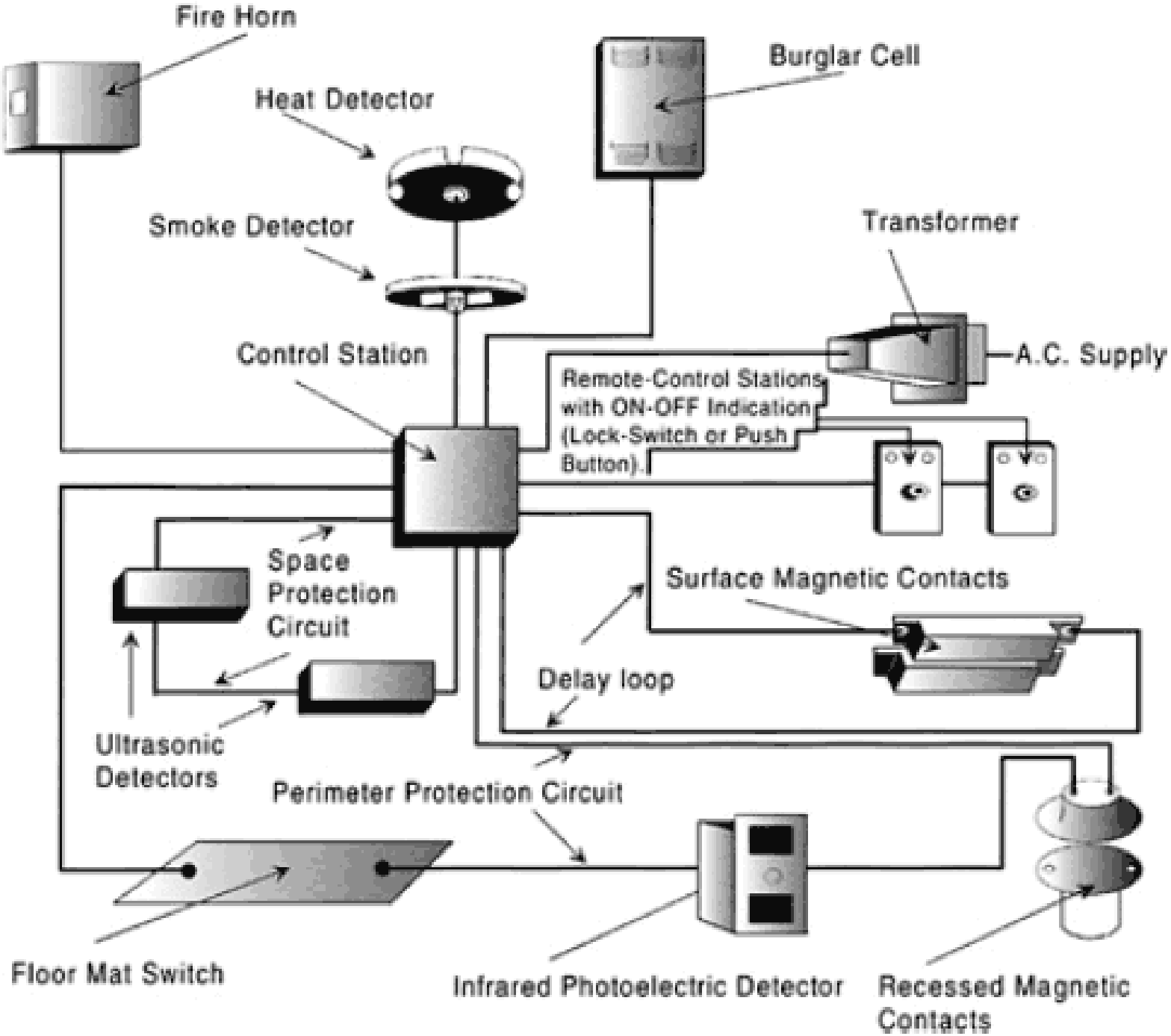
System Components

- Additional items to the basic system
  - Smoke detectors
  - Glass break detectors
  - Panic buttons
  - Pressure mats
  - Closed circuit TV
  - Alarm screens
  - SMS alert service !! →



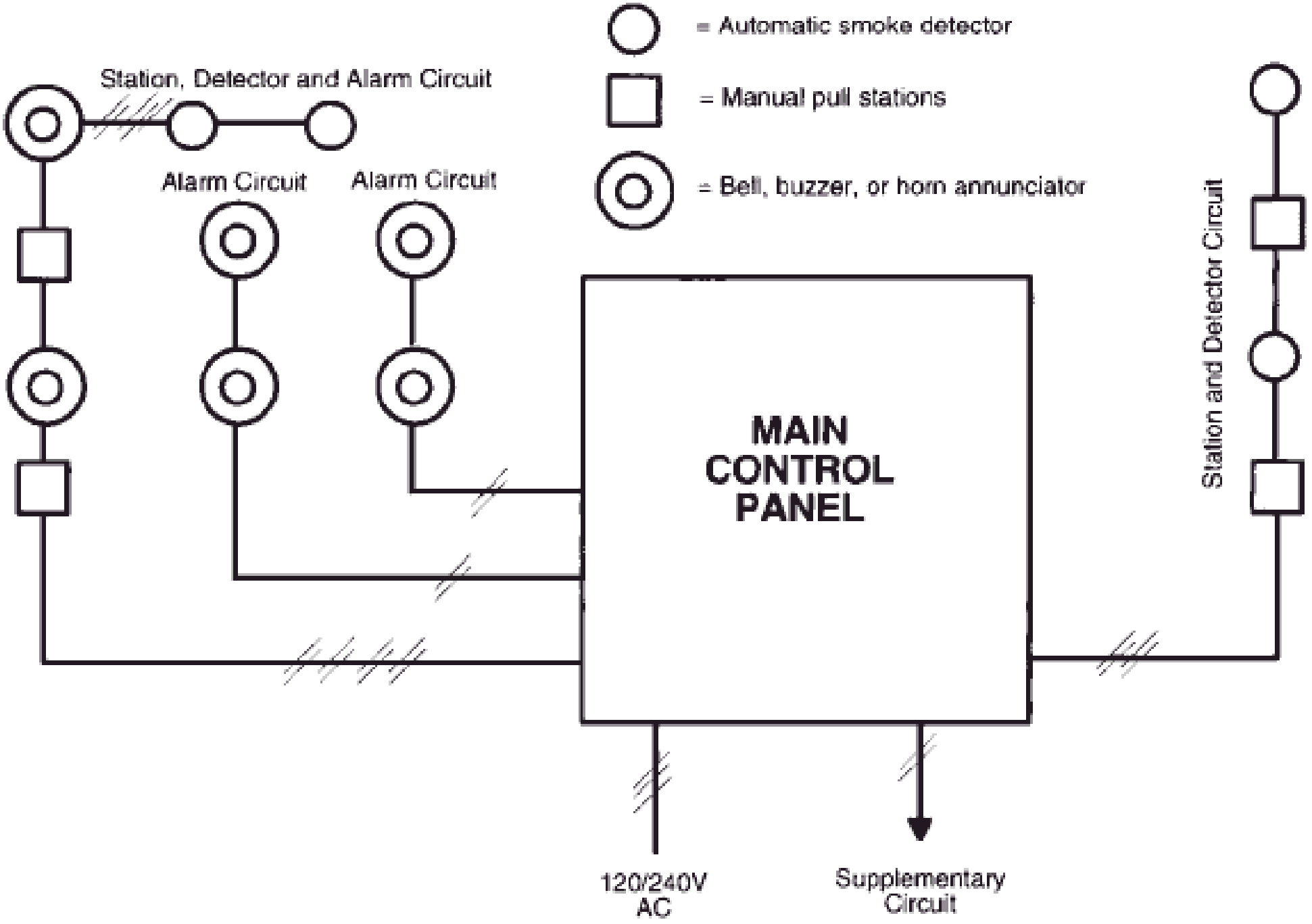
Basic approach of an alarm system

Components for a typical security/fire-alarm system



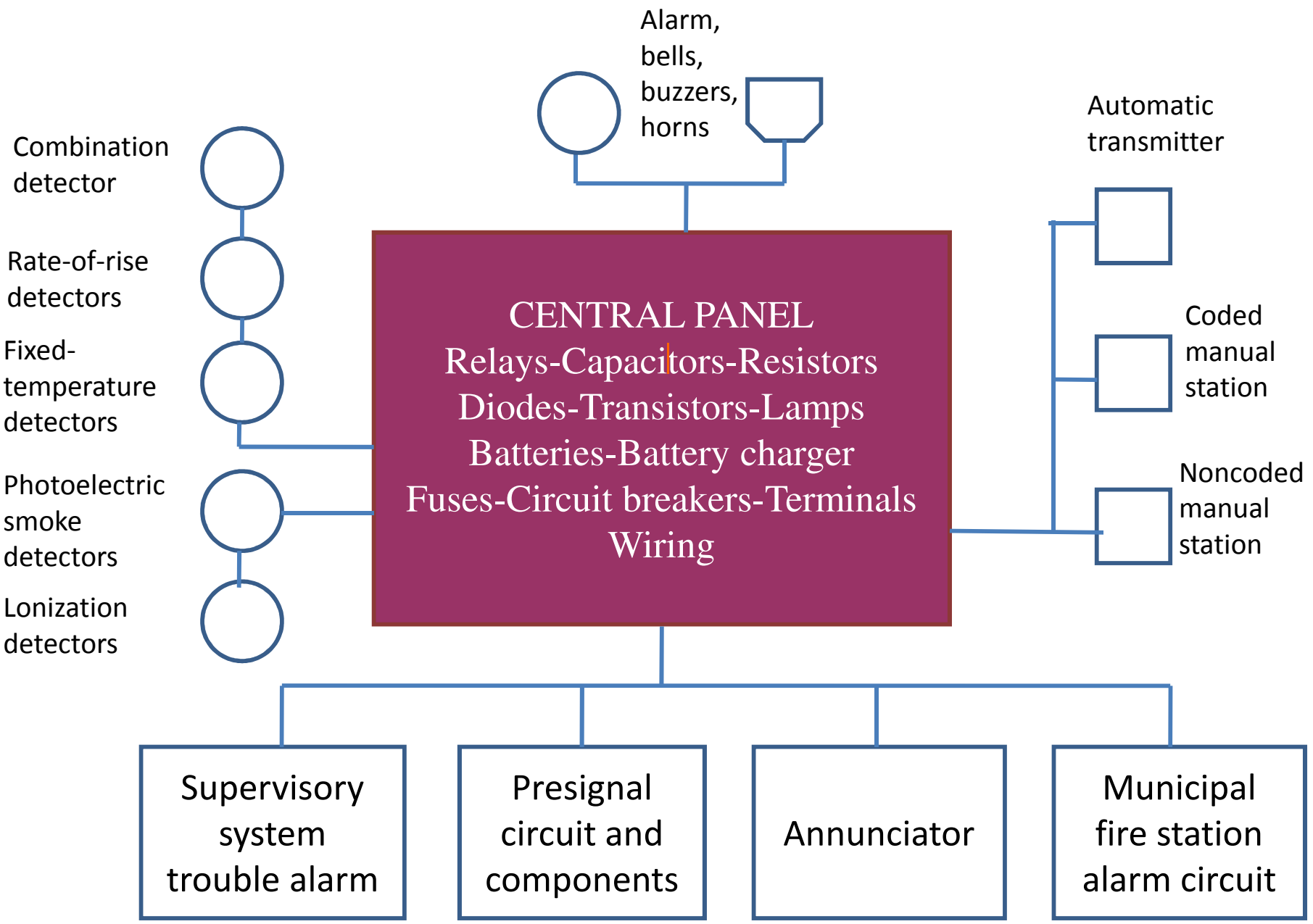
[Source: Kennedy, T. and Traister, J. E., 2002. Low Voltage Wiring: Security/fire Alarm Systems]

Schematic diagram of a fire-alarm main control panel



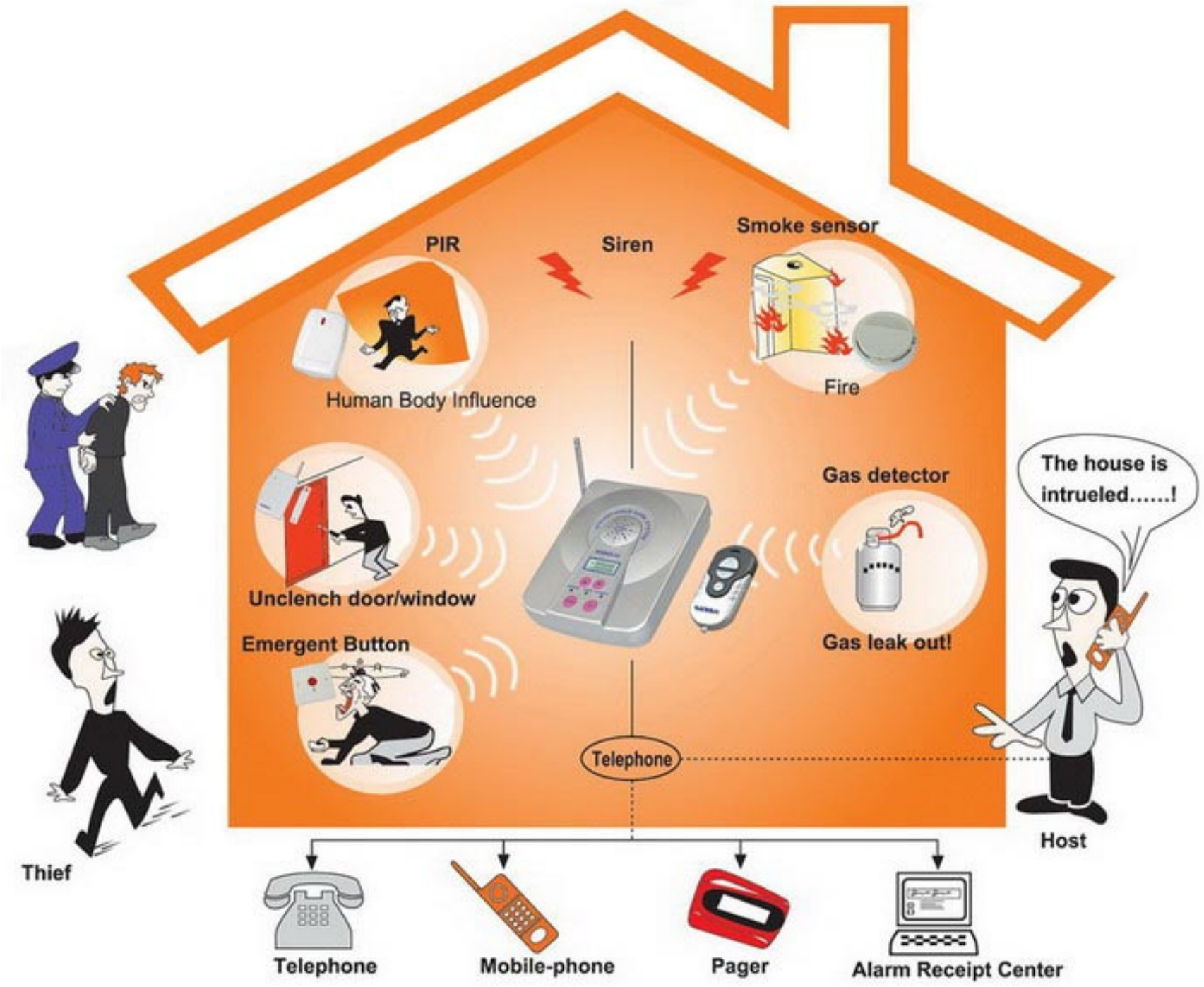
[Source: Kennedy, T. and Traister, J. E., 2002. Low Voltage Wiring: Security/fire Alarm Systems]

Components of a basic fire-alarm system



[Source: Kennedy, T. and Traister, J. E., 2002. Low Voltage Wiring: Security/fire Alarm Systems]

Example of home security system



[Source: http://pubs.sciepub.com/jit/1/1/1/]

System Components

- 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

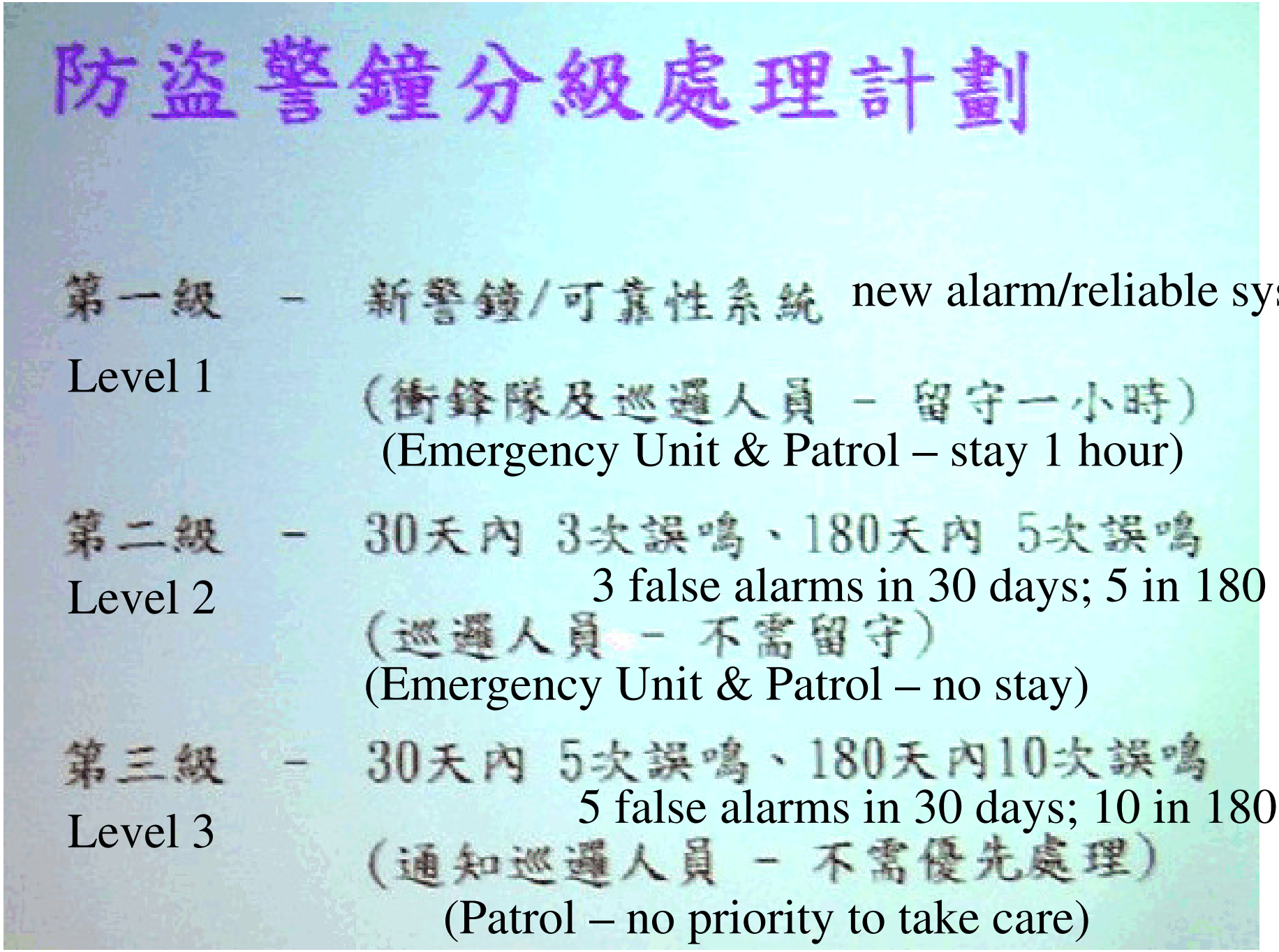
System Components

- 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

System Components

- 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



new alarm/reliable system

(Emergency Unit & Patrol – stay 1 hour)

3 false alarms in 30 days; 5 in 180 days

(Emergency Unit & Patrol – no stay)

5 false alarms in 30 days; 10 in 180 days

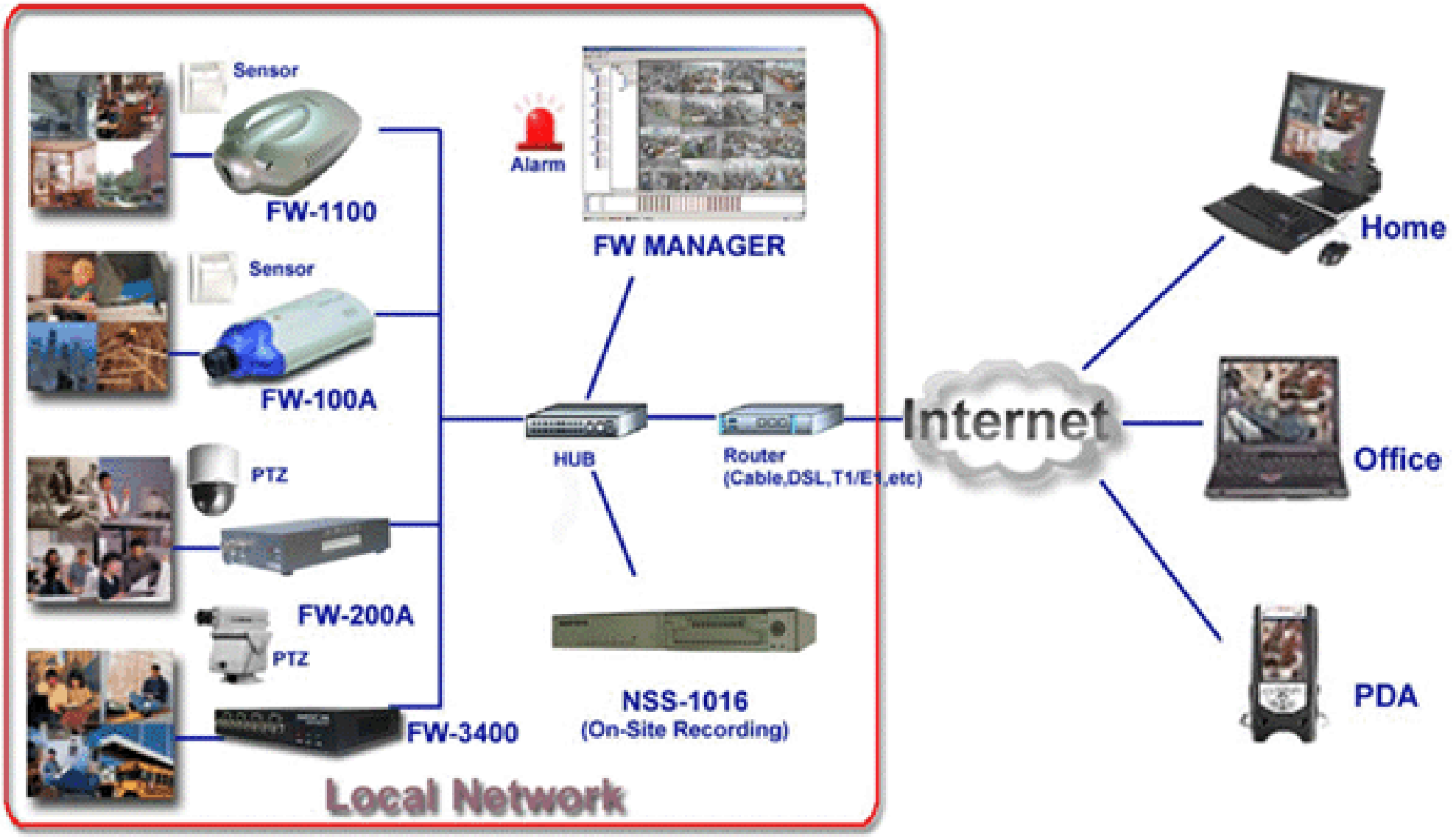
(Patrol – no priority to take care)

[Source: Hong Kong Police Crime Prevention Bureau]

System Components

- 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
    - Video camera (colour or monchrome)
    - Monitors
    - Recorders and switchers
    - Multiplexer (triplex operation simultaneous playback and recording)

LAN Networked Multi-Site Monitoring and Security

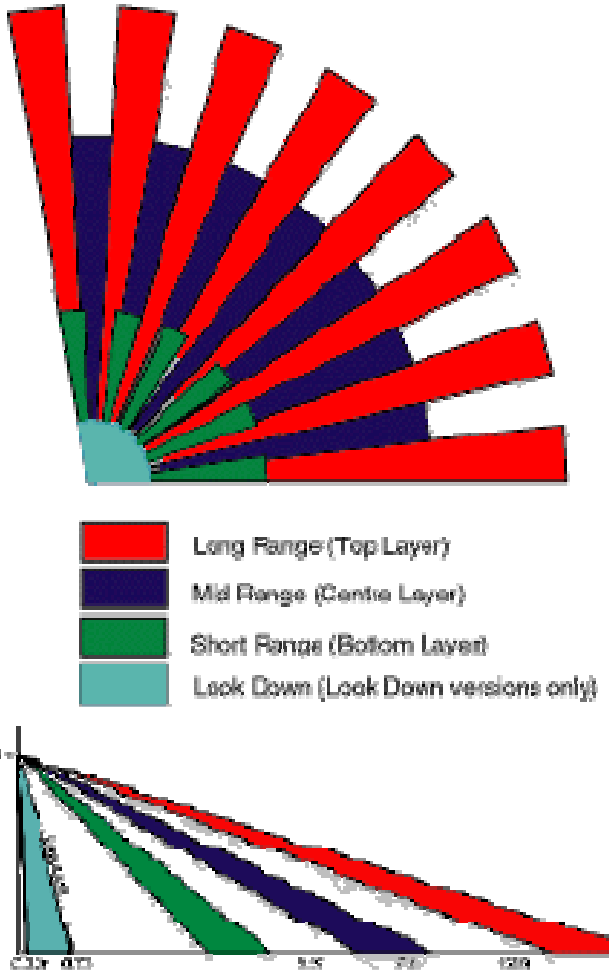


[Source: http://www.flexwatch.com]

System Components

- Intruder detection
  - Mechanical contact switch
  - Magnetic contact switch
  - Glass-break detector
  - Photo-electric sensors
  - Motion sensors
    - e.g. passive infrared (PIR) sensors

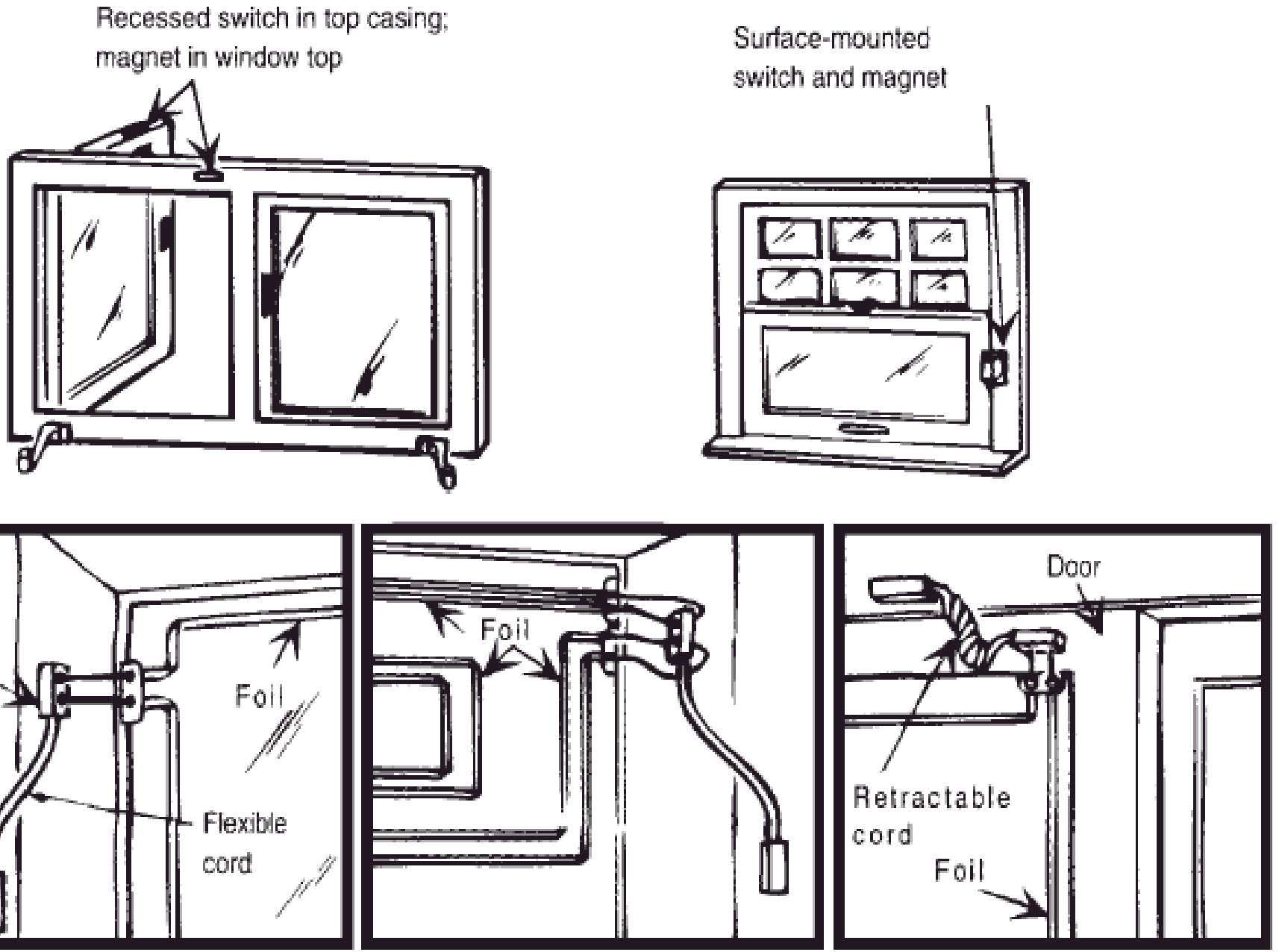
PIR sensor's coverage



Example of an intruder detection alarm system

[Source: http://www.xpertsecurity.com]

Magnetic contacts on windows and doors



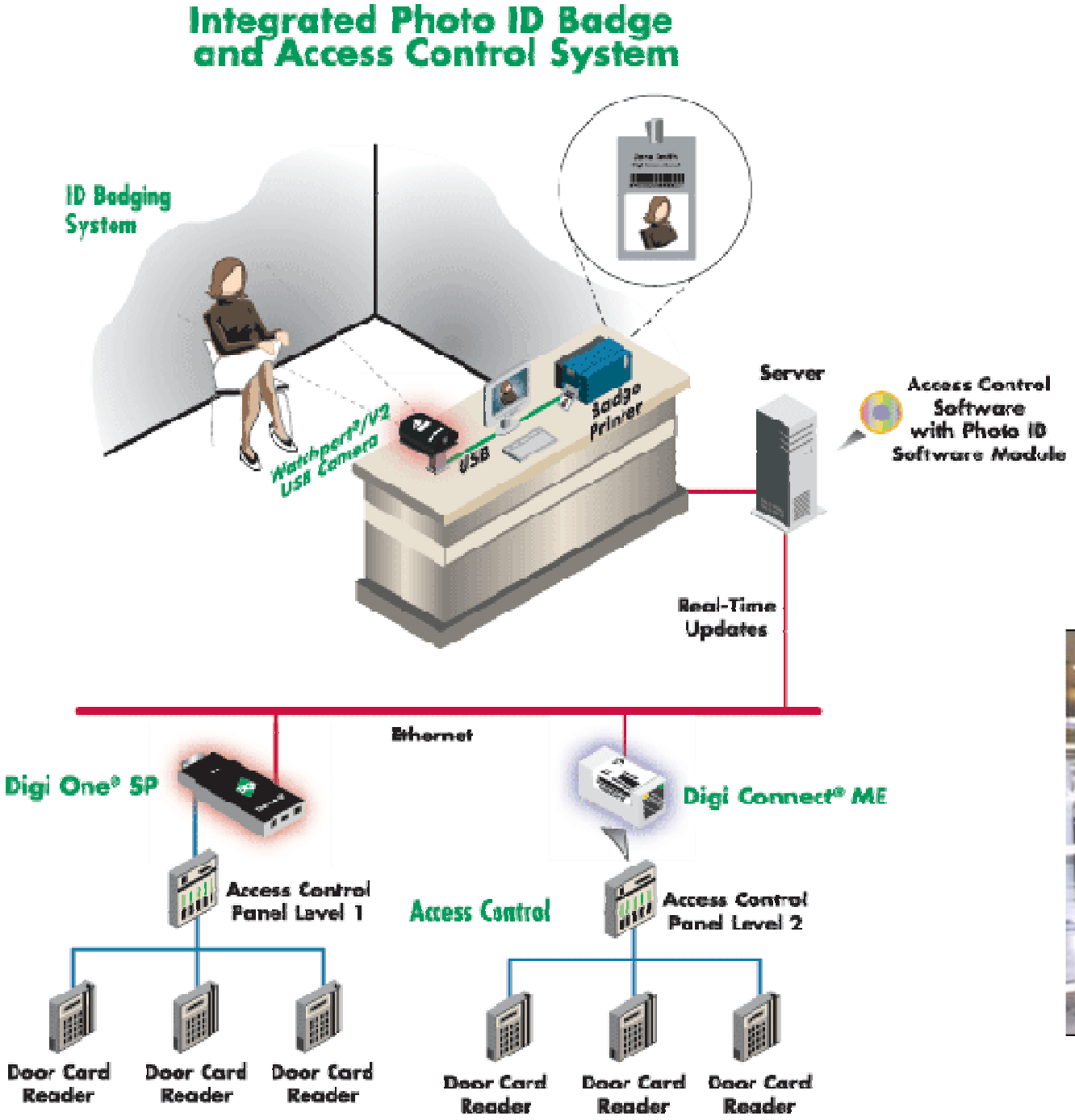
[Source: Kennedy, T. and Traister, J. E., 2002. Low Voltage Wiring: Security/fire Alarm Systems]

System Components

- 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)

Access Control Terminal

Access control system

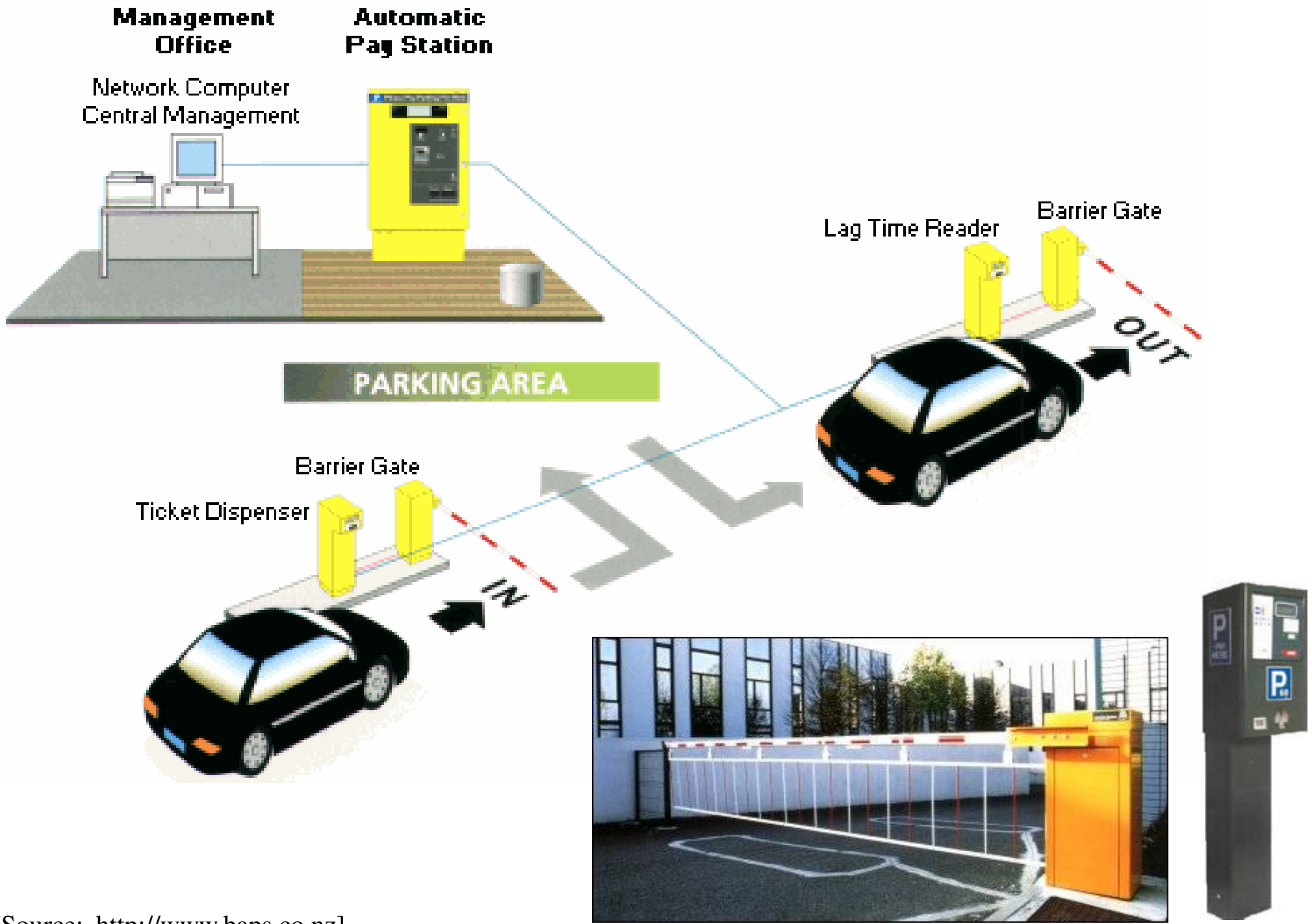


[Source: http:// www.digi.com]

Pedestrian turnstiles

[Source: http://www.baps.co.nz]

Car park control system



[Source: http://www.baps.co.nz]

System Components

- 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

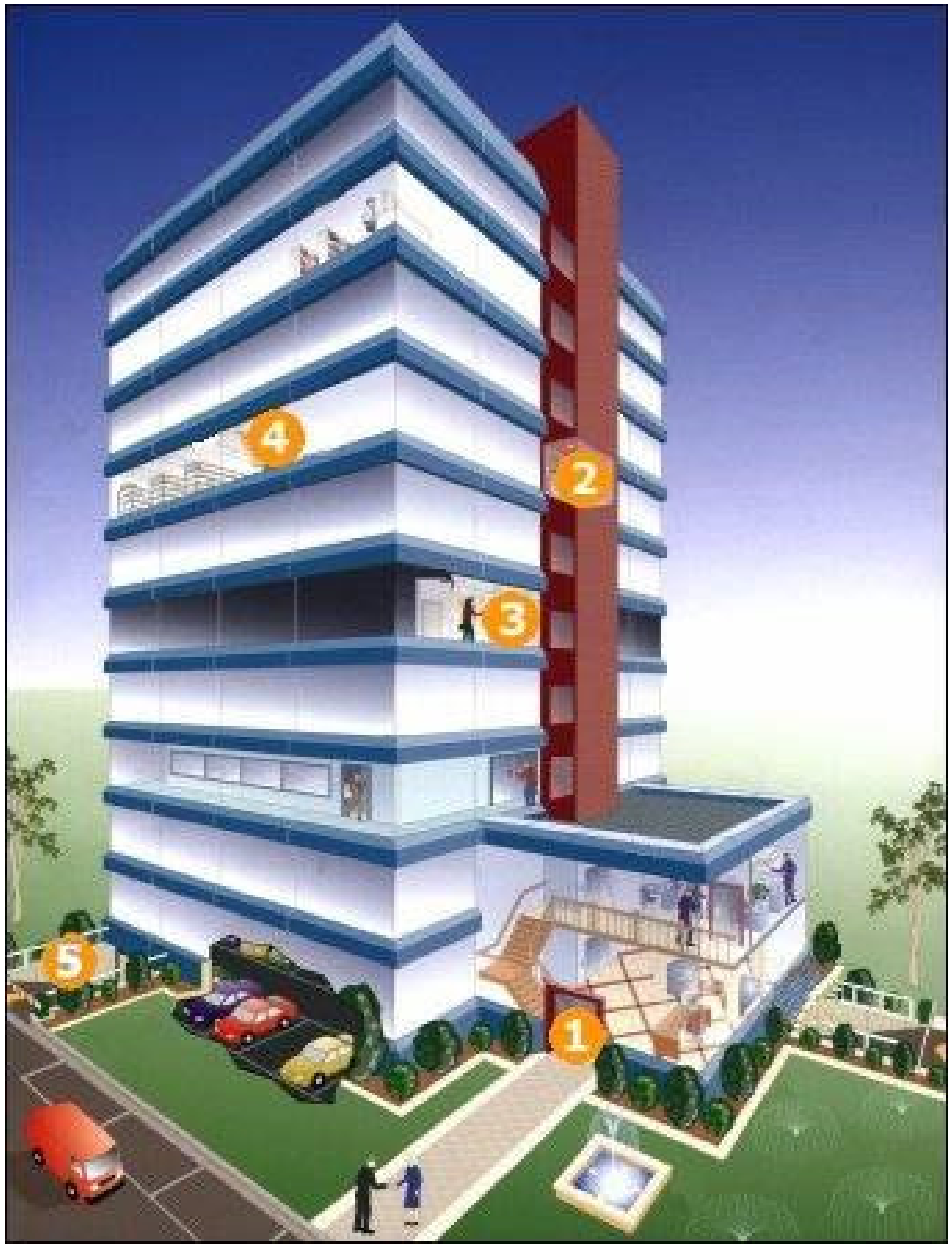
System Components

- Security Products: Yellow Pages (HK Police Crime Prevention Bureau) http://www.police.gov.hk/hkp-home/english/cpb/yellow.htm
  - Access control systems, alarms, CCTV
  - Guard monitoring systems
  - Security lighting
  - Locks, storage
  - Perimeter protection (fencing, barriers)
  - Property marking
  - Screening
  - Vehicle Protection

System Components

- 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)

A typical building security & car park control system



(1) Building entry access system with intercom system

(2) Lift access control restricting tenants within floors

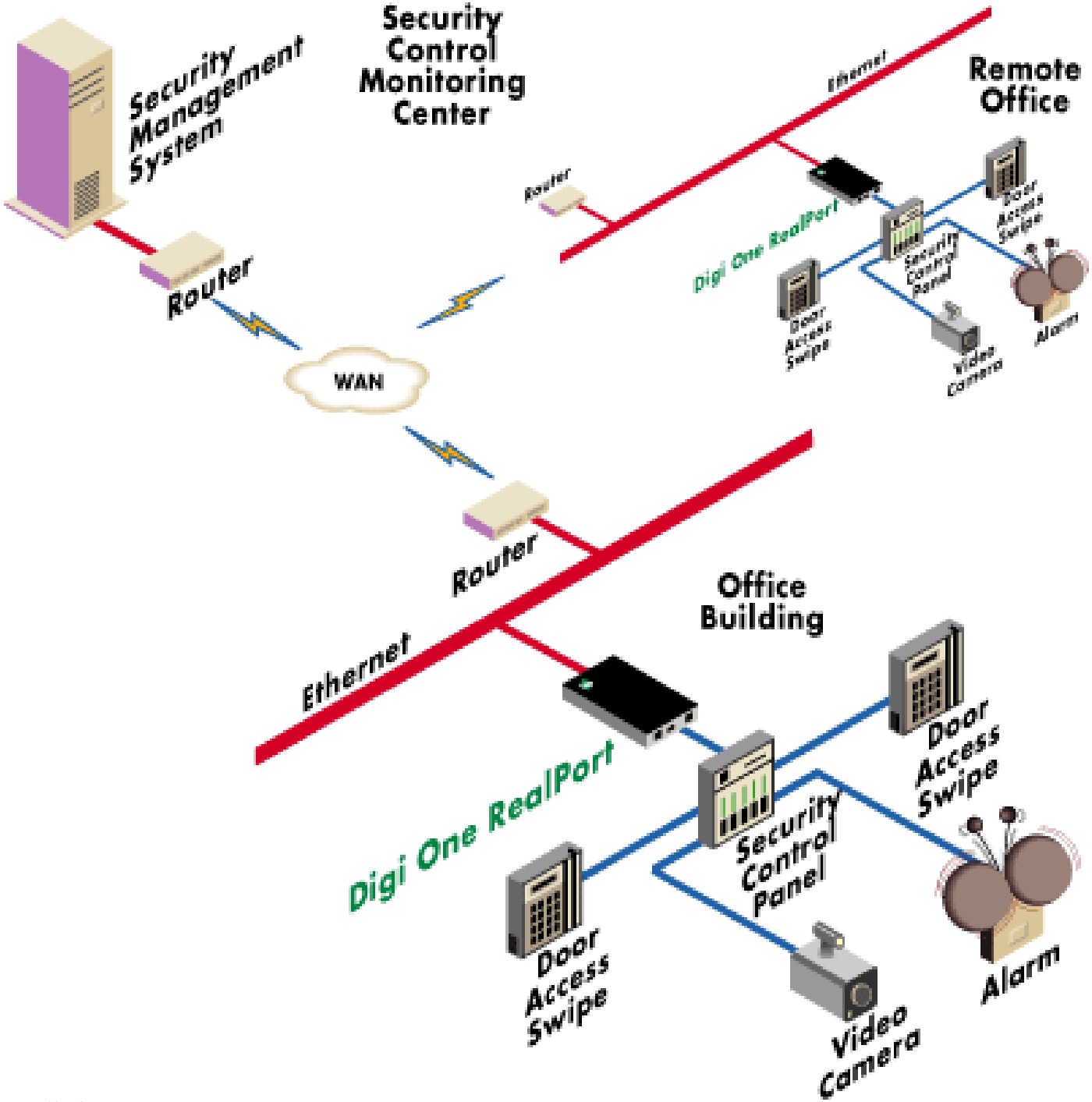
(3) Secure alarmed areas within office complexes

(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



[Source: http:// www.digi.com]