Information Systems Security

Arrianto Mukti Wibowo, M.Sc.,
Faculty of Computer Science
University of Indonesia
amwibowo@cs.ui.ac.id

Physical Security

Objectives

- To address the threats, vulnerabilities, and countermeasures which can be utilized to physically protect an enterprise's resources and sensitive information to include people, facilities, data, equipment, support systems, media, and supplies.

- To discuss considerations for choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

Agenda

- Physical Security Threats
- Site Design and Configuration
- Physical Security Requirements
  - For Centralized Computing Facilities
  - For Distributed Processing Facilities
  - For Extended Processing

What Does Physical Security Include?

- Physical Access Controls
  - Guards
  - Fences
  - Barriers
  - Lighting
  - Keys and Locks
  - Badges
  - Escorts
  - Property Controls
  - Monitoring/Detection Systems

What Else Does Physical Security Cover?

- Environmental Protection
  - Power Protection
  - Water Protection
  - Fire Detection
  - Fire Suppression
  - Evacuation
  - Environmental Monitoring/Detection

Physical Security Threats

- External Threats
  - Wind/Tornado
  - Flooding
  - Lightning
  - Earthquake
  - Cold and Ice
  - Fire
  - Chemical

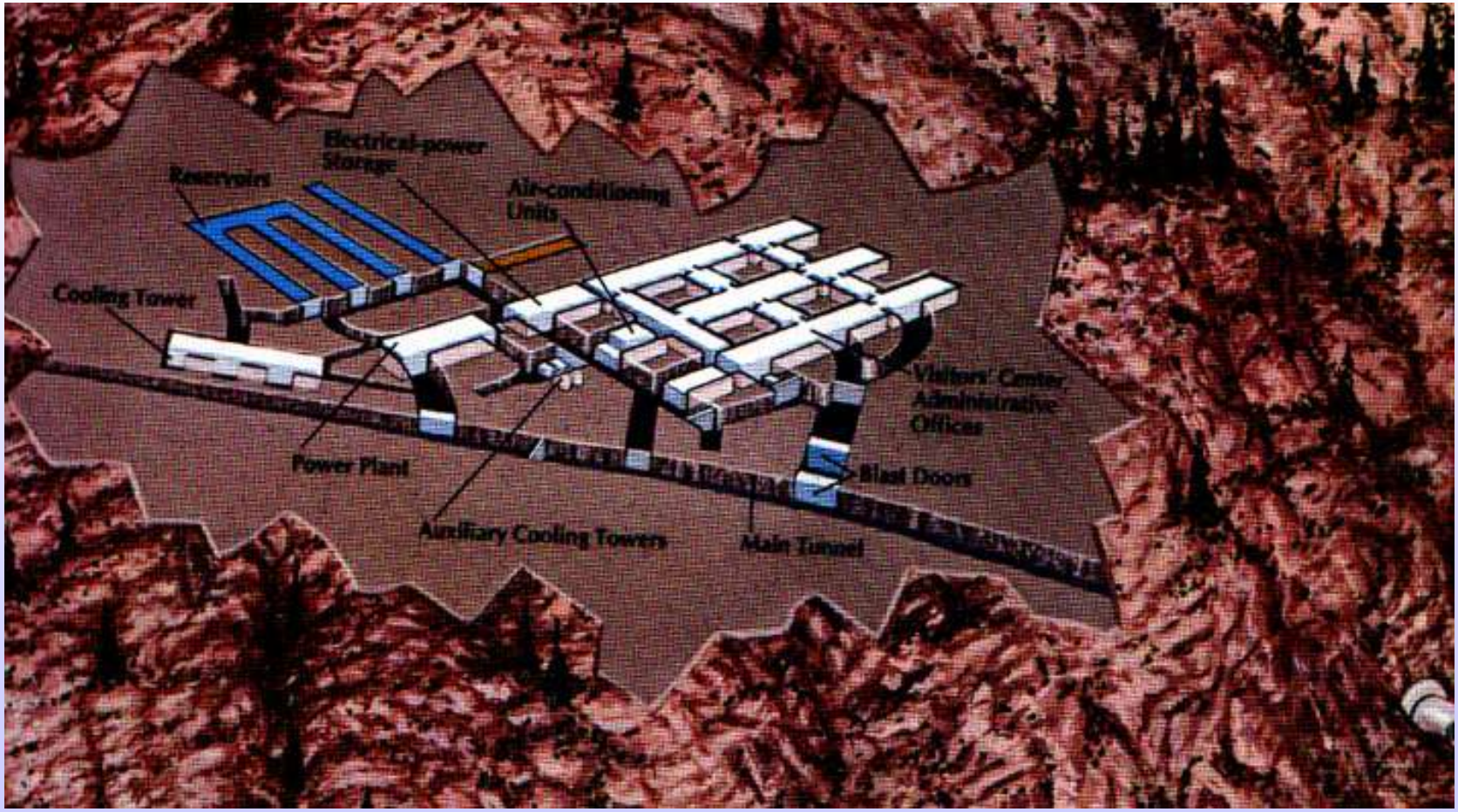
Threat Identification (continued)

- Internal Physical Threats
  - Fire
  - Environmental Failure
  - Liquid Leakage
  - Electrical Interruption
- Human Threats
  - Theft
  - Vandalism
  - Sabotage
  - Espionage
  - Errors

Selecting Facility Site

- Location and Access to highway, trains or airport
- Local Crime
- Visibility
- Emergency Access
- Natural Hazards
- Air and Surface Traffic
- Stable Power Supply
- Existing Boundary Protection: Barriers/Fencing/Gates
- Surrounding Terrain
- Joint Tenants
- Hospital, Fire Dept, Police Station

Bunker Komputer Dalam Gunung



Computing Facility Requirements / Design Considerations

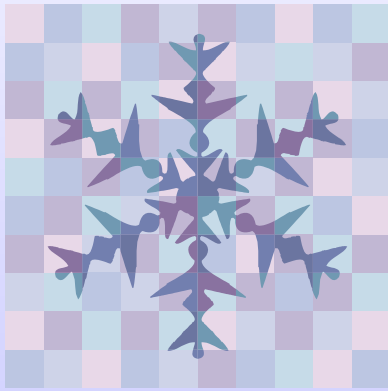
- Load: berapa berat beban yang dapat ditanggung oleh lantai? Langit-langit?
- Walls
  - Combustibility of material
  - Fire Rating
  - True Floor to Ceiling
  - Penetrations
  - Adjacent Areas (apakah rembes air?)
- Doors
  - Resistance to forcible entry
  - Hinges
  - Fire Rating
  - Alarms
  - Monitoring
  - Fail-safe-stance at emergency

Computing Facility Requirements (continued)

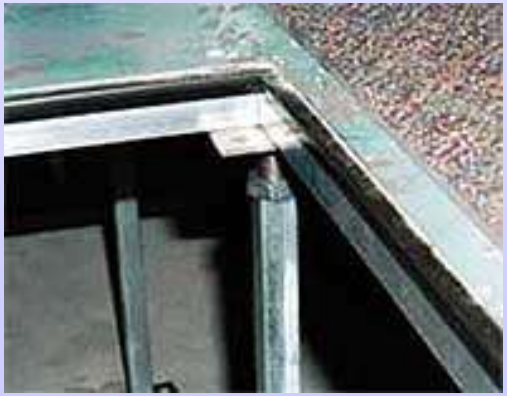
- Windows/Openings
  - Opaque
  - Shatterproof
  - Bulletproof
  - Placement
- Computer and Equipment Room Lay Out
  - Equipment Access
  - Storage
  - Occupied Areas
  - Cable Routing

Computing Facility Requirements (continued)

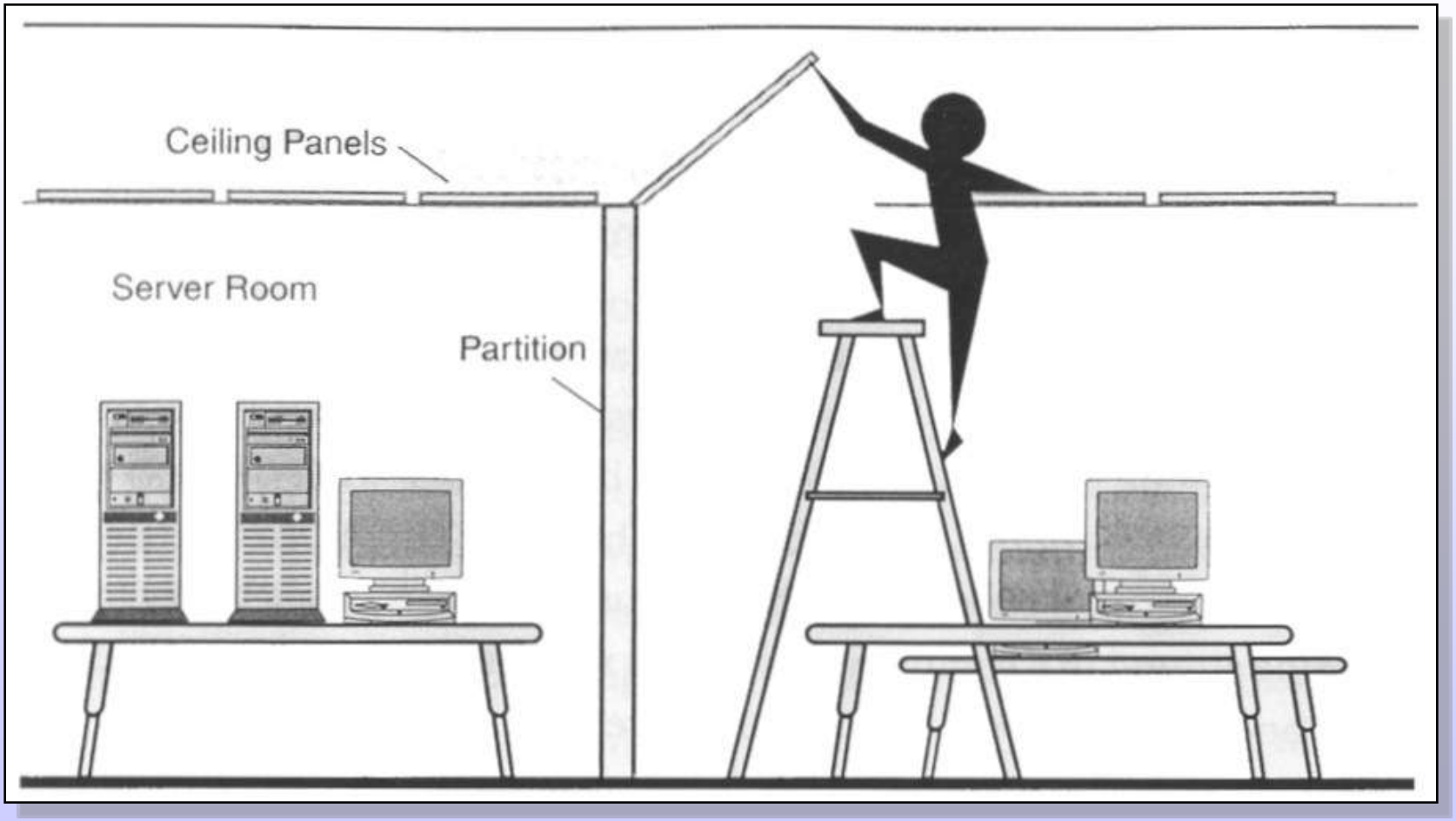
- Air Conditioning
  - Positive Pressure
  - Protected Air Intakes
  - Independent Power
  - Emergency Shut Off Controls
  - Monitoring



- Flooring
  - Load bearing rating
  - Raised floor?
  - Fire rating
  - Non-electric-conducting material
- Electrical design
- Fire considerations



Internal Partition Problems



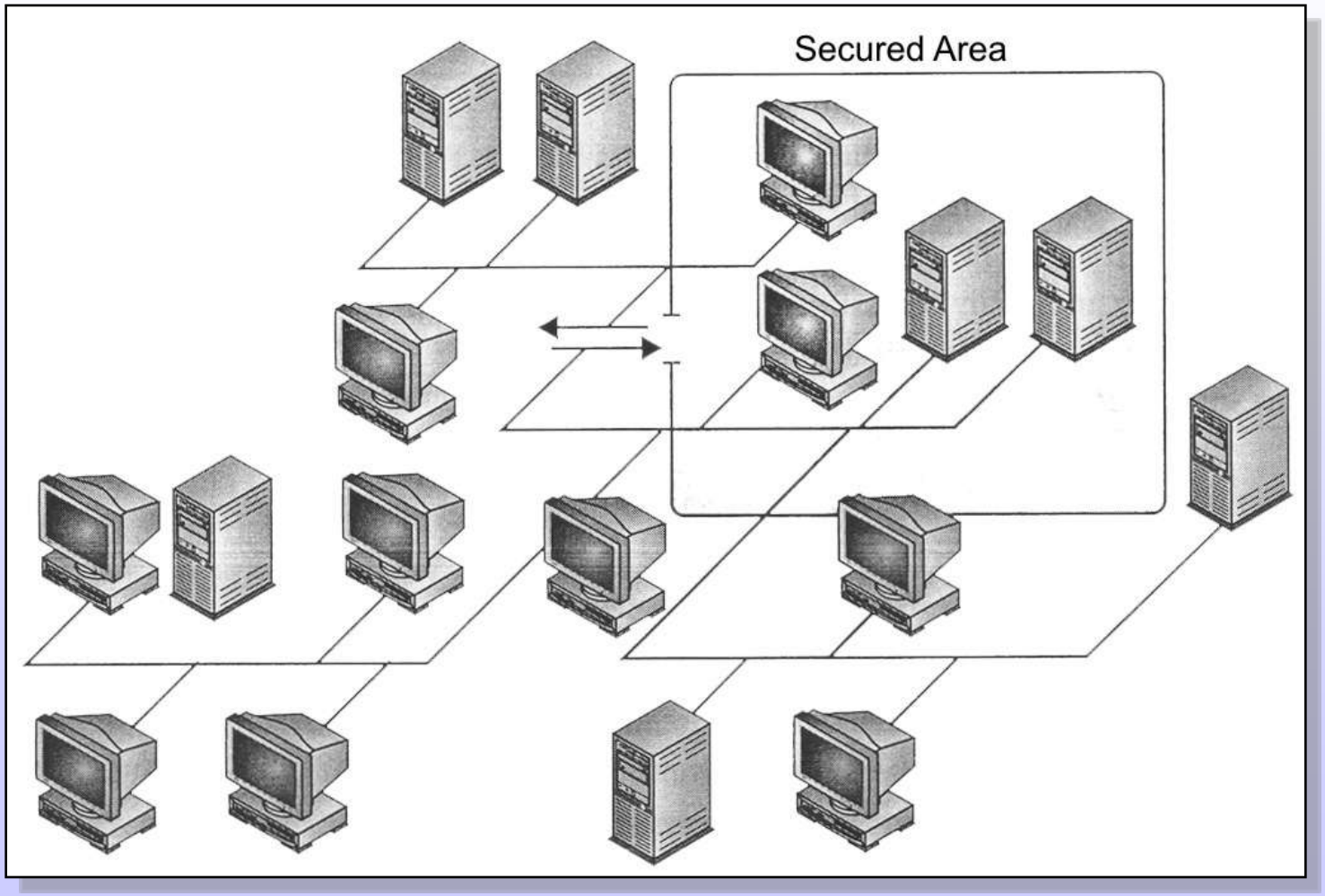
Data Centre Placement

- Jangan diletakkan di puncak gedung (preventif kebakaran)
- Jangan diletakkan di basement gedung (preventif banjir)
- Sebaiknya di tengah (core) bangunan

Computer Room

- Dulu mainframe dikendalikan operator dari dekat, sekarang remote
- Ruangan bisa lebih kecil dan efisien, kurang penting memperhatikan faktor manusia (karena tidak ada manusia!)
- Rack mounted system
- Close to wiring distribution centre
- Single point of entry

Single Point of Entry to Computer Room



Backup

- Data
- O/S, Application
- Manuals
- Forms
- Hardware
- Electrical supplies
- Personnel

MTBF & MTTF

- Mean Time Before Failure
- Mean Time Before Repair
- Semakin lama, makin bagus

MTBF 654 days
MTTF 160 days

MTBF 500 days
MTTF 120 days

Electrical Power

Definitions:

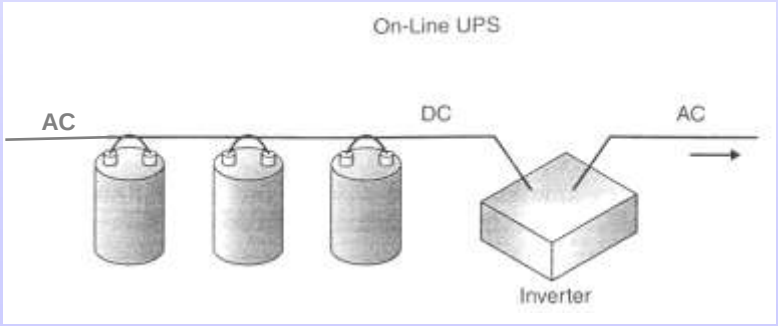
- Blackout - Loss of Power
- Brownout - Prolonged Period of Below Normal Voltage
- Noise - Random Disturbance that Interferes with a Device
- Sag - Short Period of Low Voltage
- Spike - Momentary High Voltage
- Surge - Prolonged High Voltage

Electrical Power

- Dedicated Circuits
- Controlled Access to:
  - Power Distribution Panels
  - Master Circuit Breakers
  - Transformers
  - Feeder Cables
- Emergency Power Off Controls
- Voltage Monitoring/Recording
- Surge Protection
- Voltage regulator → clean power

Sumber power bila gagal

- Alternate Feeders
- Uninterruptible Power Supply
  - Online UPS
  - Standby UPS: memiliki sensor power failure
- Emergency Power Generator / Backup Power
  - Fuel Consideration
  - Costs
- Semua harus selalu dicoba!

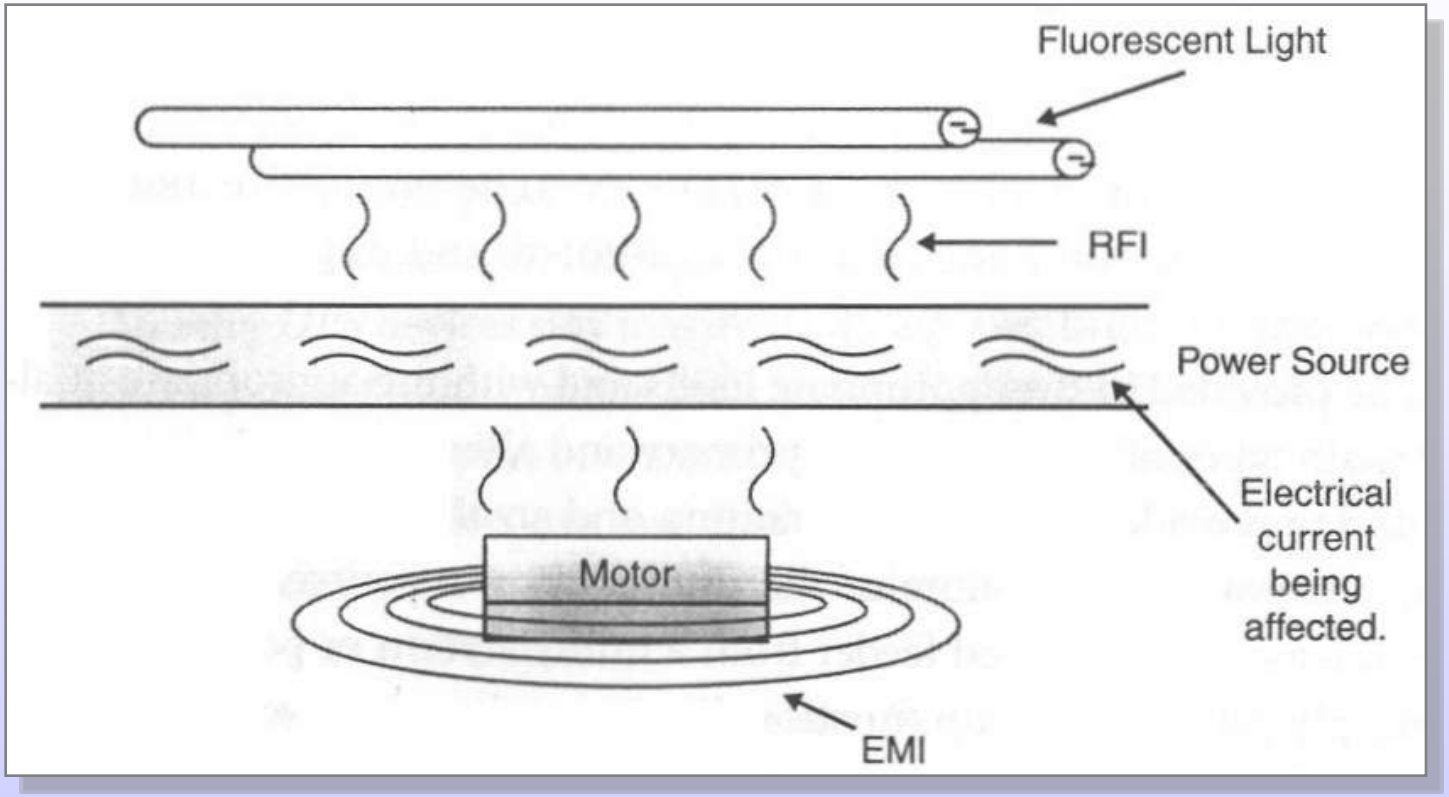


Backup Power Function

- Lighting
- Physical Access Control Systems
- Fire Protection Systems
- Computing equipment
  - Mainframes
  - Servers
  - Workstations
- Communications Equipment
- Telephone Systems

Hati-hati, penggunaan backup power supply juga bisa menyebabkan spike…!

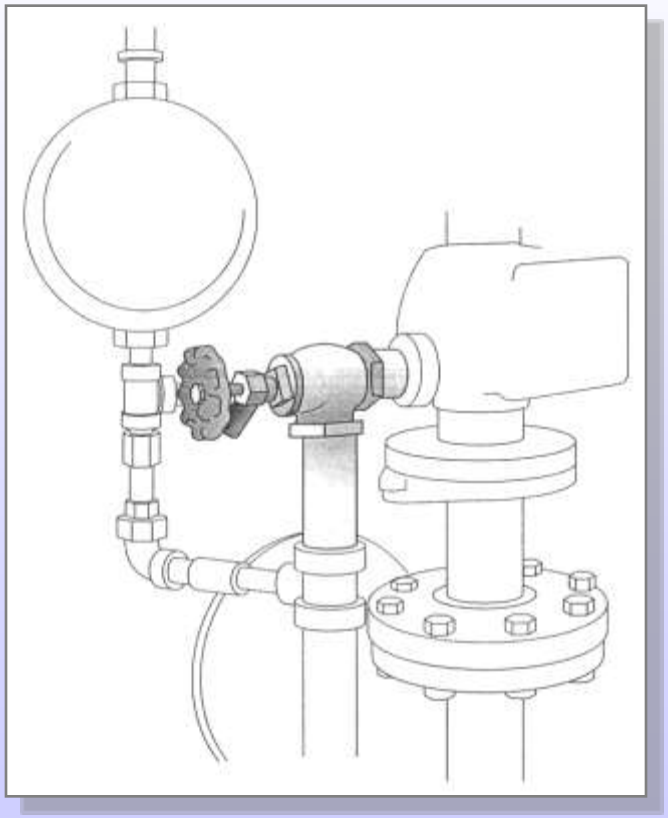
Gangguan aliran listrik



Faraday cage, apakah perlu?

Environmental Issues

- Humidity Controls
- Air Quality (Dust), bisa membuat kipas kotor lalu macet…
- Water Protection
  - Falling Water
  - Rising Water
  - Drains
  - Protective Coverings
  - Positive drains → flow out
  - Shutoff valves
- Ventilation: positive pressurization



Fire

- Fire prevention:
  - Pelatihan pegawai
  - Ketersediaan peralatan / sarana yg memadai
  - Akses ke sumber air dg mudah
- Fire detection
  - Pull box alarm
  - Smoke detectors

Fire Prevention & Protection

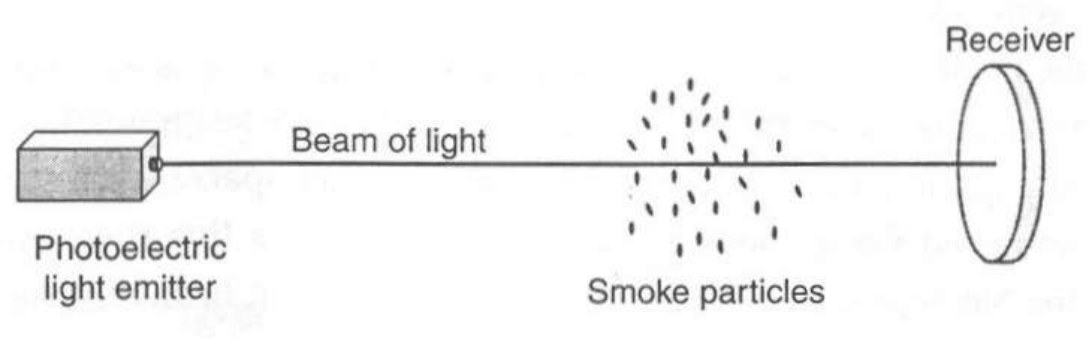
- Fire Elements:
  - Fuel
  - Oxygen
  - Temperature
- Causes Of Computer Center Fires
  - Electrical Distribution Systems (korslet)
  - Equipment → cegah overheating dengan sekring / fuse
  - Puntung rokok
- Fire Classes
  - A: Common Compustibles (use Water/Soda Acid)
  - B: Liquid (CO_2/Soda Acid/Halon)
  - C: Electrical (CO_2/Halon)

Fire Prevention & Protection (continued)

- Temperatures When Damage Occurs
  - Paper Products: 350°
  - Computer Equipment: 175°
  - Disks: 150°
  - Magnetic Media: 100°
- Fire Detection
  - Manual
  - Optical (Photoelectric-Smoke Blocking Light)
  - Temperature
  - Ionization (Reaction to Charged Particles in Smoke)

Fire Detectors

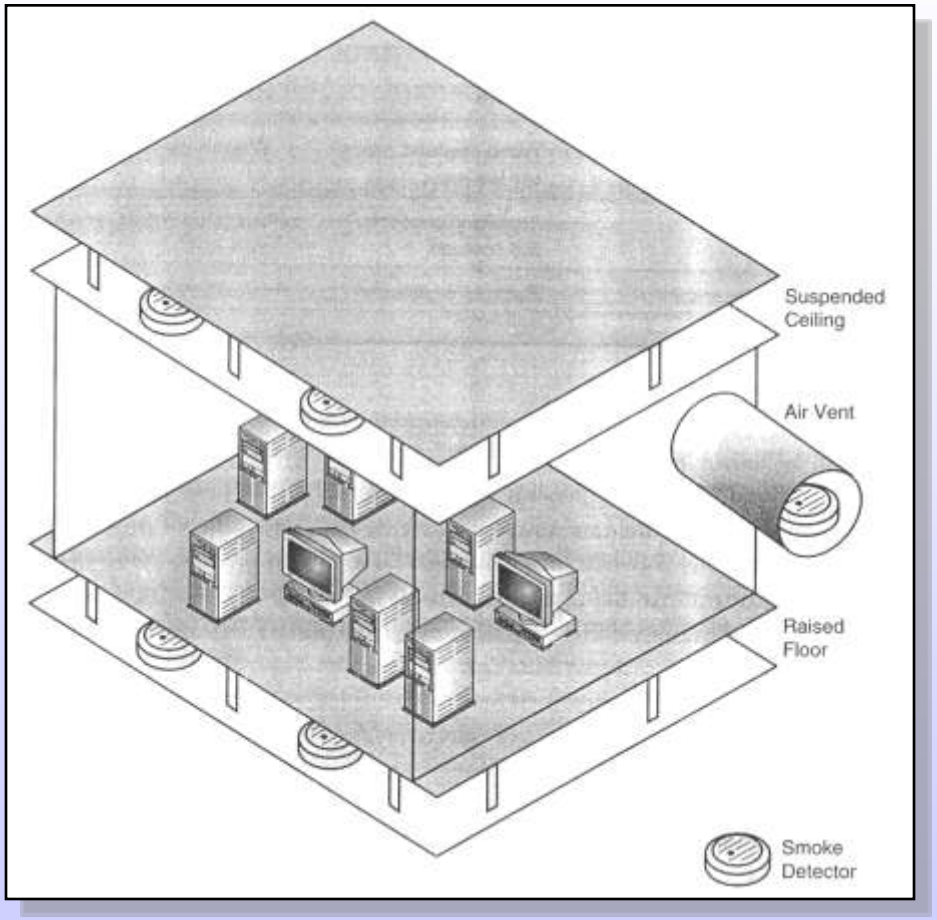
- Smoke activated, dgn photoelectric device, akan aktif kalau sinar terhalang asap



- Heat activated
  - Fixed temprature sensor
  - Rate-of-rise temprature sensor
- Flame activated, menggunakan pulsa-pulsa inframerah
- Automatic dial-up to fire departments

Detectors

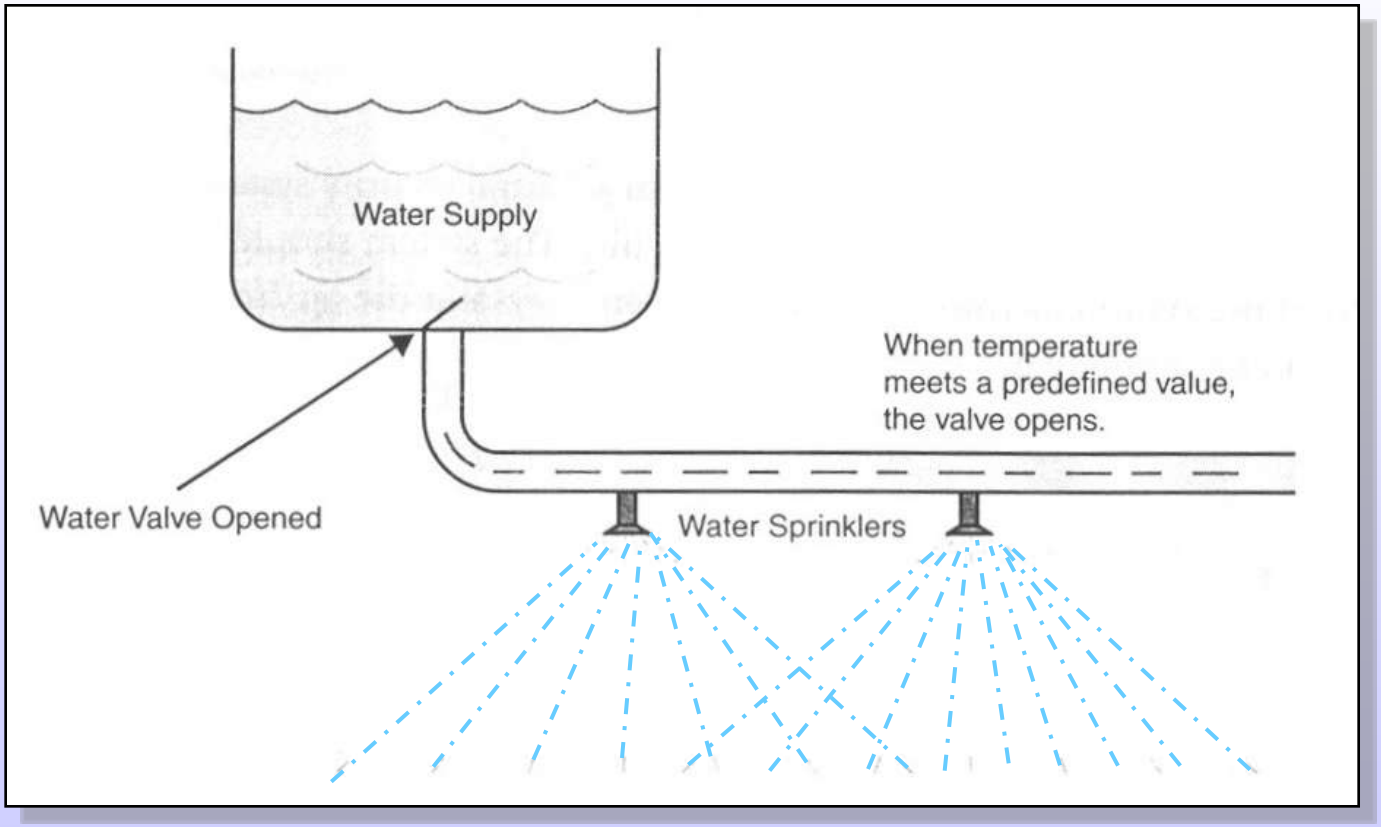
- On Ceilings
- Above Suspended Ceilings
- Beneath Raised Floors
- Return Air Ducts



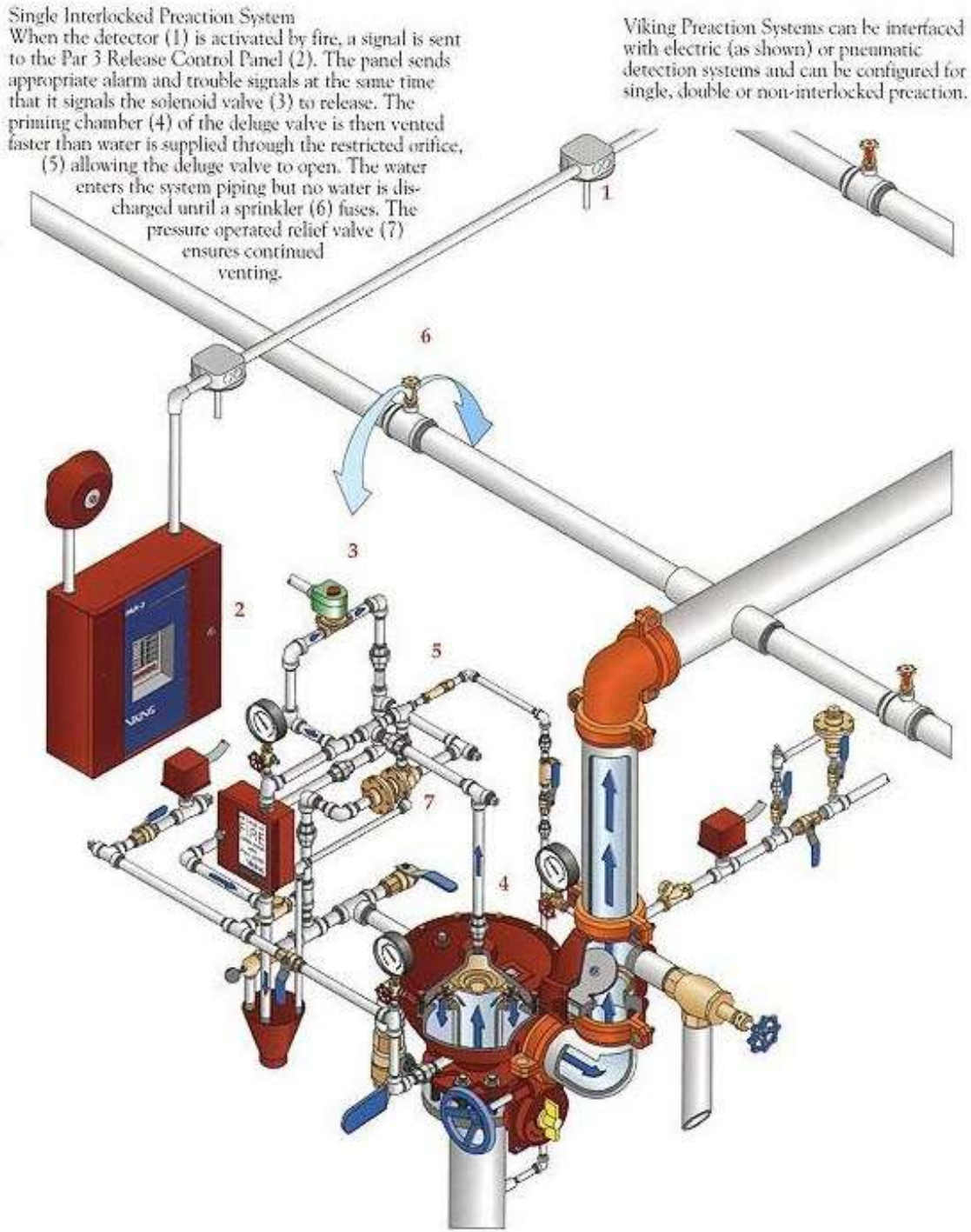
Fire Suppression

- Portable Extinguishers
  - At Exits
  - Mark Locations and Type
  - Types A, B & C
  - Need to Inspect
- Water Sprinkler Systems
  - Works to Lower Temperature
  - Most Damaging to Equipment
  - Conventional Systems
  - Wet Pipe
  - "Dry Pipe" Systems: Less Risk of Leakage
  - Preaction: suhu x_1 akan mengalirkan air ke pipa, suhu x_2 akan menyemprotkan air
  - Employ in Throughout Building and in all Spaces

Dry Pipe


Water Supply
When temperature
meets a predefined value,
the valve opens.
Water Valve Opened
Water Sprinklers

Preaction Water System



Carbon Dioxide (CO_2)

- Colorless/Odorless
- Potentially Lethal
- Removes Oxygen
- Best for Unattended Facilities
- Delayed-Activation in Manned Facilities

Halon

- Best Protection for Equipment
  - Inside Equipment Cabinets/Vaults
  - Special Areas
  - Above Suspended Ceilings
  - Under Raised Floors
- Concentrations <10% are Safe

- Becomes Toxic at 900^{o}
- Depletes Ozone (CFCs)
- Montreal Protocol (1987)
- Halon 1301: Requires Pressurization
- Halon 1211: Self-Pressurization (Portable Extinguishers)
- Penggantinya:
  - FM-200
  - Argon, Argonite
  - Inergen
  - CEA-410

Other Considerations

- Training
- Testing
- National Fire Prevention Association (NFPA) Standards
- Local Fire Codes
- Drainage

Securing Storage Areas

- Forms Storage Rooms
  - Increased Threat of Fire
  - Combustibles
  - Access Controls
- Media Storage Rooms
  - Media Sensitivity
  - Segregation
  - Access Controls
  - Environmental Controls

Media Protection

- Storage
  - Media Libraries/Special Rooms
  - Cabinets
  - Vaults
- Location
  - Operational
  - Off-Site
- Transportation

Protecting Wiring

- Optical Fiber
- Copper Wire
- Certifying the Wiring and Cabling
- Controlling Access to Closets and Riser Rooms

Other Considerations

- Dealing with Existing Facilities
  - Planning
  - Upgrade/Renovation
  - Incremental New Construction
- Protecting the Protection
  - Implement Physical and Environmental Controls for Security Systems
  - Protect against both Intentional and Inadvertent Threats

Personnel Access Controls

- Position Sensitivity Designation
- Management Review of Access Lists
- Background Screening/Re-Screening
- Termination/Transfer Controls
- Disgruntled Employees

Access Controls – Locks

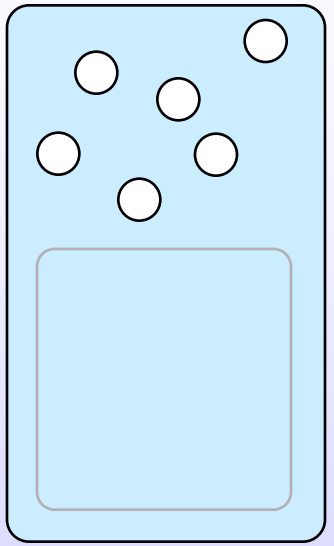
- Preset Locks and Keys
- Programmable Locks
  - Mechanical (Cipher Locks)
  - Electronic (Keypad Systems): Digital Keyboard
    - Number of Combinations
    - Number of Digits in Code
    - Frequency of Code Change

Access Controls - Tokens

- Security Card Systems
  - Dumb Cards
    - Photo Identification Badges
    - Manual Visual Verification
    - Can be Combined with Smart Technology
  - Digital Coded (Smart) Cards
    - Often Require Use of PIN Number with Card
    - Readers: Card Insertion, Card Swipe & Proximity

Types of Access Cards

- Photo ID Cards
- Optical Coded Cards
- Electric Circuit Cards (Embedded Wire)
- Magnetic Cards (Magnetic Particles)
- Metallic Stripe Card (Copper Strips)



Access Controls - Biometrics

- Fingerprint/Thumbprint Scan
- Blood Vein Pattern Scan
  - Retina
  - Wrist
  - Hand
- Hand Geometry
- Facial Recognition
- Voice Verification
- Keystroke Recorders
- Problems
  - Cost
  - Speed
  - Accuracy

Physical Security in Distributed Processing

- Threats
  - To Confidentiality
    - Sharing Computers
    - Sharing Diskettes
  - To Availability
    - User Errors
  - To Data Integrity
    - Malicious Code
    - Version Control

Distributed Processing Physical Security Controls (continued)

- Office Area Controls
  - Entry Controls
  - Office Lay-Out
  - Personnel Controls
  - Hard-Copy Document Controls
  - Electronic Media Controls
  - Clean-Desk Policy

Office Area Physical Security Controls (continued)

- Printer/Output Controls
- Property Controls
- Space Protection Devices
- Equipment Lock-Down

Distributed Processing Physical Security Controls (continued)

- Cable Locks
- Disk Locks
- Port Controls
- Power Switch Locks
- Keyboard Locks
- Cover Locks

Distributed Processing Physical Security Controls (continued)

- Isolated Power Source
  - Noise
  - Voltage Fluctuations
  - Power Outages
- Heat/Humidity Considerations
- Fire/Water
- Magnetic Media Controls

Extended Processing Physical Security Controls

- User Responsibilities Paramount
  - Protection against Disclosure
    - Shoulder Surfing
    - Access to Sensitive Media and Written Material
  - Integrity Protection
  - Protection against Loss or Theft
    - Locks
    - Practices
- Management Responsibilities
  - Approval
  - Monitoring

Boundary Protection

- Area Designation: Facilitates Enforcement
- Vehicular Access
- Personnel Access
  - Occupants
  - Visitors (Escort & Logging)
- Dogs
- Fences
  - Deter Casual Trespassing
  - Compliments Other Access Controls
  - Aesthetics
  - Won't Stop Determined Intruder

Boundry Protection (continued)

- Lighting
  - Entrances
  - Parking Areas
  - Critical Areas
- Perimeter Detection Systems
  - Does Not Prevent Penetration
  - Alerts Response Force
  - Requires Response
  - Nuisance Alarms
  - Costly

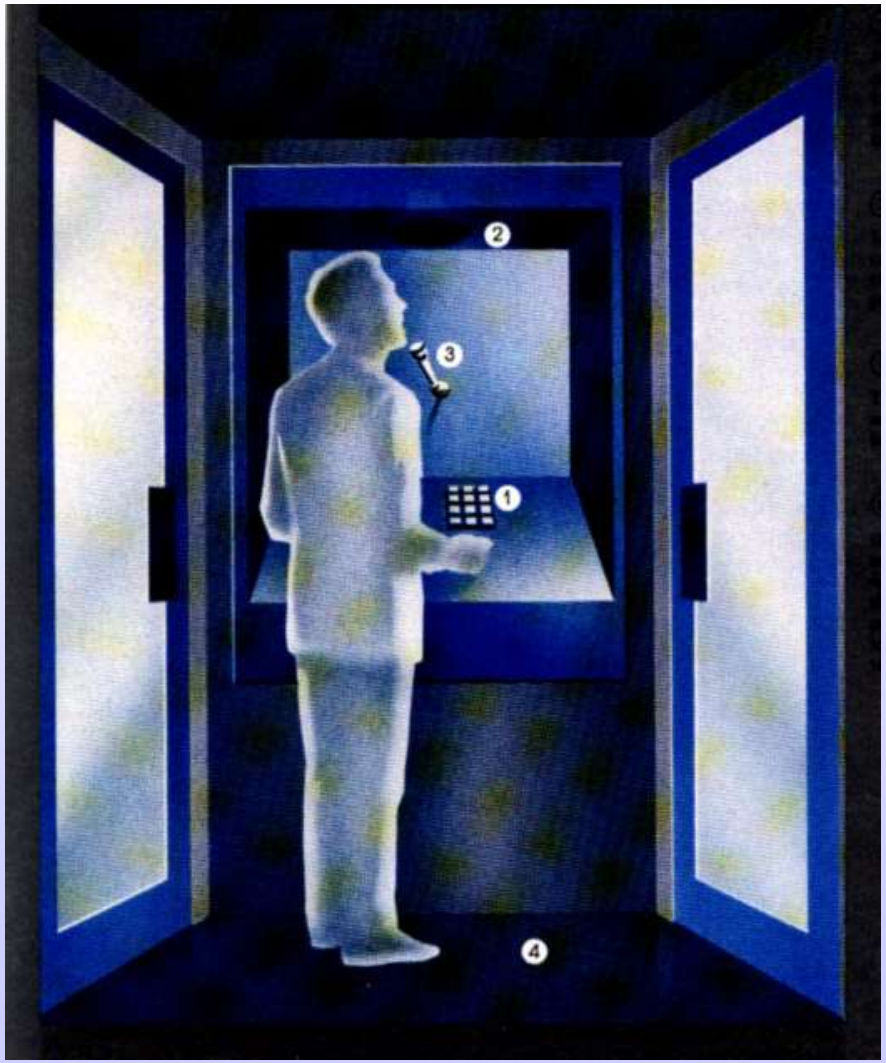
Boundry Protection (continued)

- CCTV
  - Efficiency
  - Requires Human Response
  - Limitations
- Staffing
  - Access Control Points
  - Patrols
  - Employees

Detection Systems

- Photoelectric systems, dalam ruang gelap, kalau ada yang pakai senter, akan alarm
- Wave pattern: seperti dalam film-film action. Ada transmiter, mirror dan reciever. Bisa pakai inframerah, ultrasonic, atau microwave
- Passive infrared: membaca perubahan panas dalam ruangan
- Acoustic-seismic detection
- Metal di jendela, kalau jendela dibuka akan bunyi alarm.

Man Trap



1. Memeasukkan kartu identifikasi (what you have)
2. Mengetikkan 12 digit angka rahasia (what you know)
3. Komputer secara acak akan memilihkan kata-kata yang harus diucapkan ulang (who you are)

Man Trap