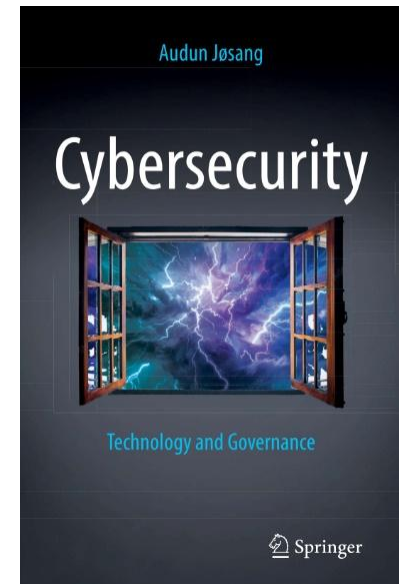


Chapter 12: Physical Security

Cybersecurity: Technology and Governance

Audun Jøsang,

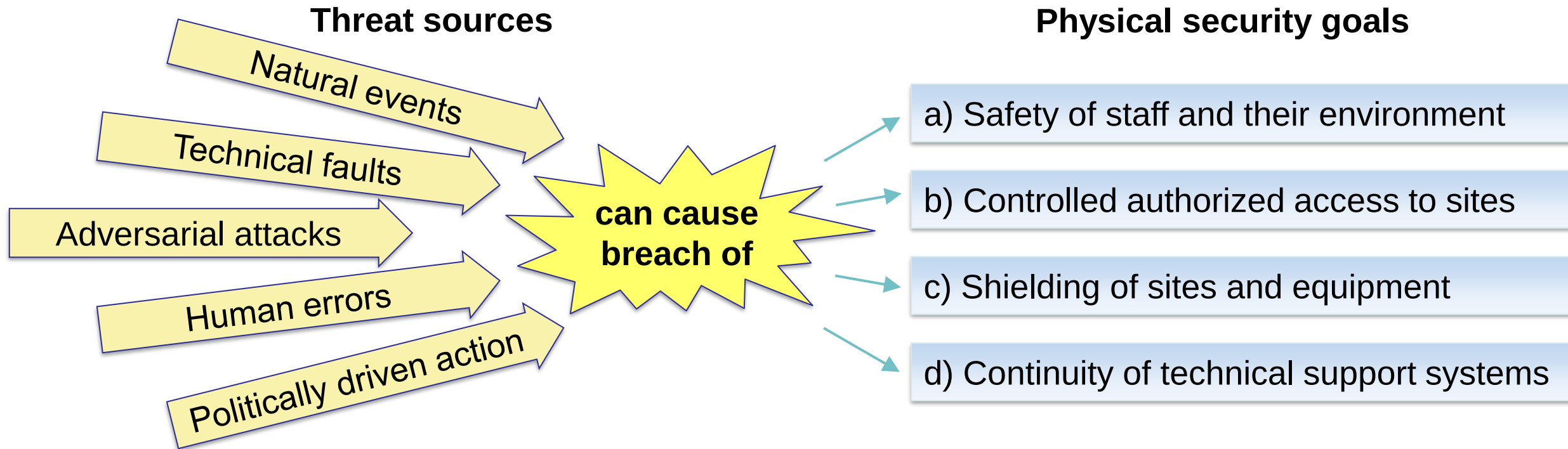
1st Edition, Springer Nature, 2024.



Overview

- Threat sources and physical security goals
- Technologies for physical security goals
 - Safety of staff and the environment
 - Controlled authorized access
 - CPTED: Crime Prevention Through Environmental Design
 - Shielding of sites and equipment
 - Continuity of technical support systems

Threat Sources and Physical Security Goals



Threats to Physical Security

- Natural events - forces of nature
- Technical failures
 - technical hardware & equipment failures or errors
 - technical software failures or errors
- Adversarial acts
 - espionage or trespass,
 - theft and compromises to intellectual property
- Human error - unintentional acts
 - acts of human error or failure,
 - deviations in quality of service,
- Politically driven action
- Management failures
 - technical obsolescence.

Safety of staff and their environment

- Life safety goals should always take precedence over all other types of security goals. Safety deals with the protection of life and assets against fire, natural disasters, and devastating accidents.
- HSE (Health, safety and environment) is an interdisciplinary field covering the study and implementation of environmental protection and safeguard of people's health and safety, especially in organizations, but also in public spaces. It is what organizations must do to make sure that their activities do not cause harm.
- The HSE discipline is well regulated in most countries. HSE managers must identify and understand relevant EHS regulations, which then must be communicated through the organization in order for suitable measures to be implemented.

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire
- Fires account for more property damage, personal injury, and death than any other threat
- It is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards

Controlled authorized access

- Physical access control ensures that only authorized staff can enter sites and restricts their movements within the site and movements from one security zone to the next.
- There should be a limited and well-defined set of entry points to sites. For guests there should be a single entry point with a front desk and procedures for sign-in before entering the site. Depending on the sensitivity of the zone, the policy can require guests to be escorted at all times inside the site.
- Access mechanisms include the use of access cards, biometrics or two-factor authentication such as an access card combined with a secret PIN, as described in Chapter 8. Mantraps (double security doors) should be considered for access to sensitive areas.

Physical Perimeter Defenses

- Physical perimeter defenses consists of making buildings more difficult or less attractive targets. It does not necessarily mean the construction of an impenetrable bunker, although this would be the extreme case of target hardening.



Physical perimeter defenses

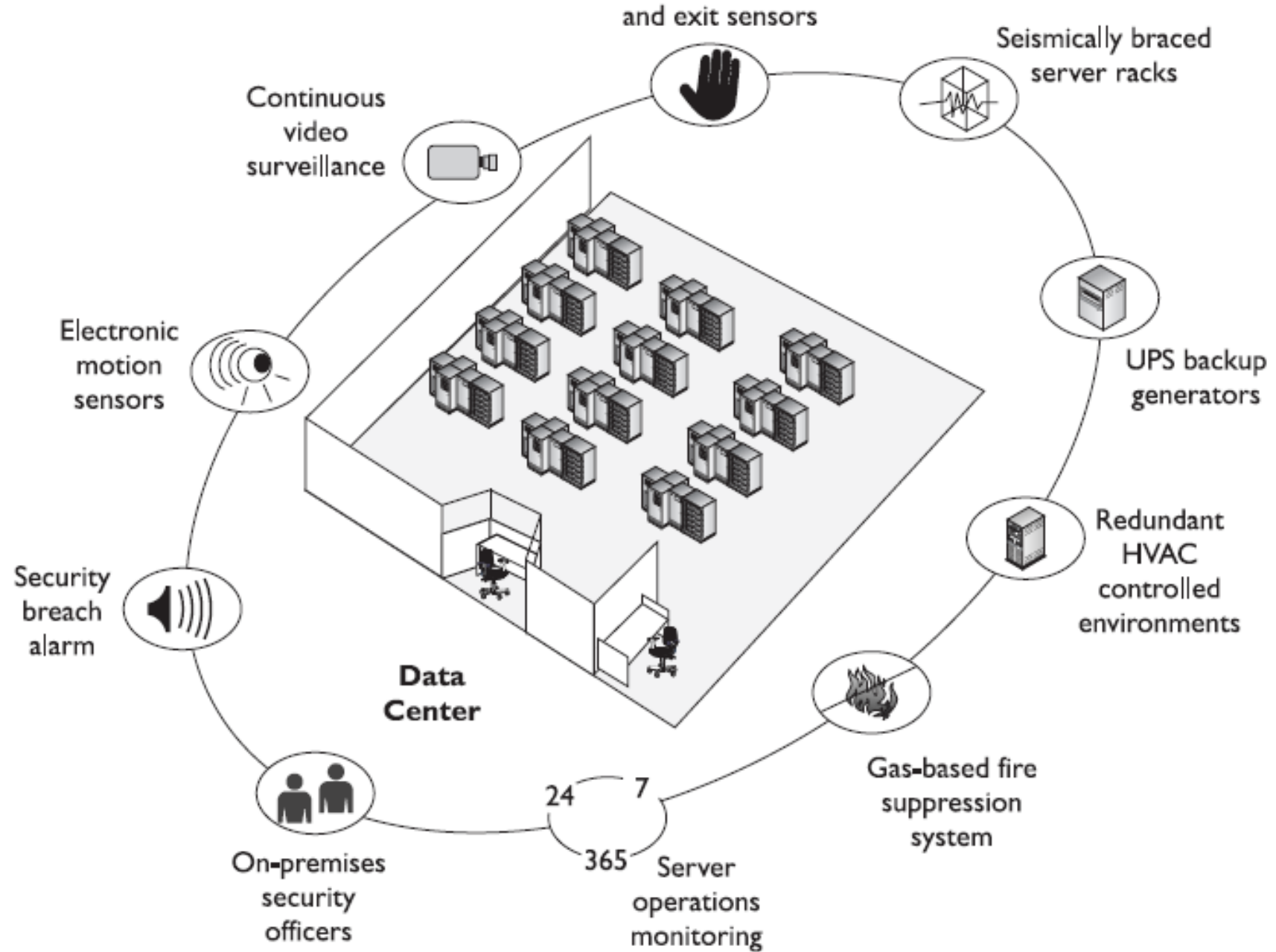
- Walls, Fencing, and Gates
- Guards
- Dogs, ID Cards, and Badges
- Locks and Keys
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

- *To ensure that no unauthorized person can get physical access to facilities and systems, or damage and steal equipment.*

Multilayered Physical Security

- Defence in depth
 - Requires that the organisation establish multiple layers of controls
 - Attackers will have to penetrate many protection layers in order to access sensitive information and systems
 - Slows down, and makes successful attacks much harder

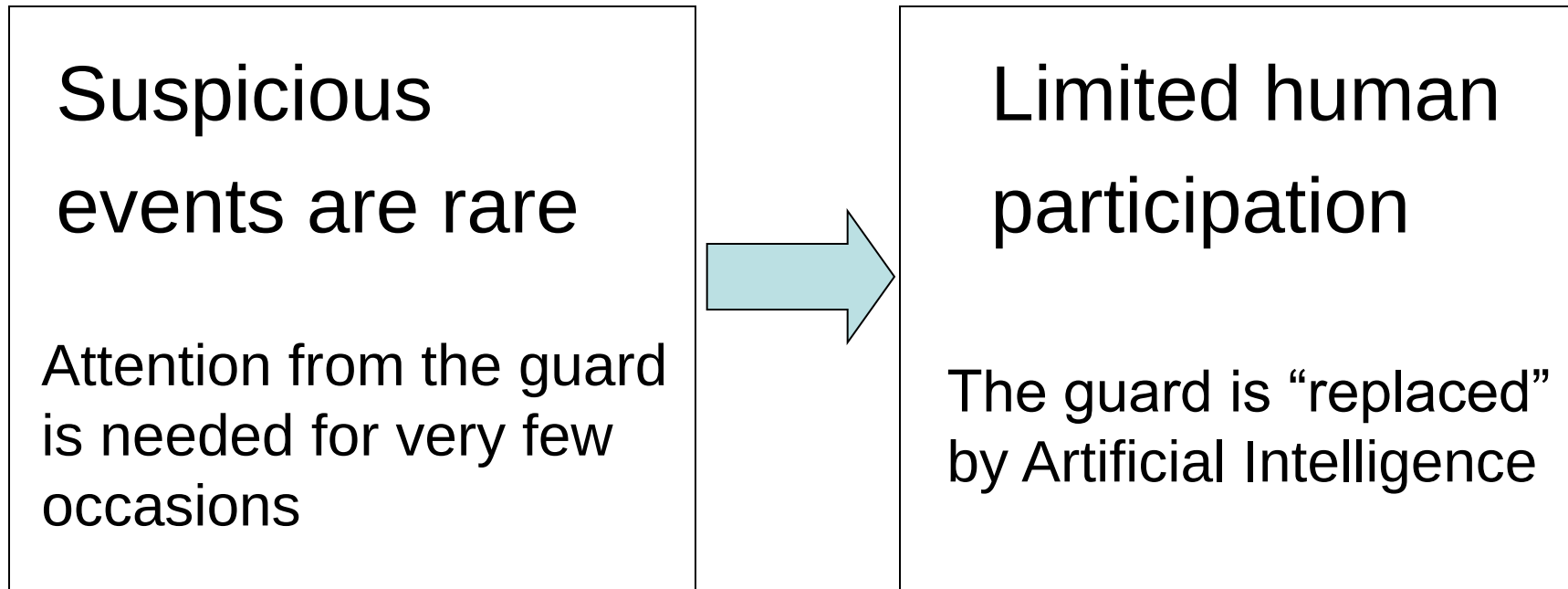
Defence in Depth



Electronic Monitoring

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks:
 - reactive and do not prevent access or prohibited activity
 - recordings often not monitored in real time and must be reviewed to have any value
 - Human security guards tire quickly and will no longer react to events recorded by video surveillance

Automated video surveillance



Automated Video Surveillance

- Large scale video surveillance systems using AI for analysing camera feeds and other sensors
- System of scattered low-cost video sensors
 - Focus on the design of AI classifiers and fusion algorithms
 - Stream full quality video or just images
- Alarms triggered by vision systems to get human attention to suspicious events.

Mobile and Portable Systems

- With the increased threat to overall information security for laptops, handhelds, and PDAs, mobile computing requires even more security than the average in-house system
- Many of these mobile computing systems not only have corporate information stored within them, many are configured to facilitate the user's access into the organization's secure computing facilities

Stopping Laptop Theft

- Inventory all laptops, and register with vendor
- Harden the OS / Platform
- Password protect the BIOS
- Don't check laptops in as luggage when flying
- Never leave a laptop unattended
- Carry laptop in a non-descriptive case or bag
- Engrave the laptop with identification signs
- Lock to stationary object with slot lock and cable
- Back up data from laptop
- Use special safe if left in vehicles
- Encrypt sensitive data
- Use laptop tracing service

Laptop Tracing Service



- Laptop tracing can act as a strong theft deterrent

Remote Computing Security

- Remote site computing - distant from the organizational facility
- Telecommuting - computing using telecommunications including Internet, dial-up, or leased point-to-point links
- Employees may need to access networks on business trips
- Telecommuters need access from home systems or satellite offices
- To provide a secure extension of the organization's internal networks, all external connections and systems must be secured

CPTED

Crime Prevention Through Environmental Design

- *CPTED is the proper design and effective use of the built environment which may lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life.* –
US National Crime Prevention Institute

CPTED Strategies

- Natural Surveillance
- Natural Access Control
- Territorial Reinforcement
- Activity Support

CPTED Natural Surveillance

- A design concept directed primarily at keeping intruders easily observable. Promoted by features that maximize visibility of people, parking areas and building entrances: doors and windows that look out on to streets and parking areas; pedestrian-friendly sidewalks and streets; front porches; adequate night time lighting.

CPTED Natural Surveillance

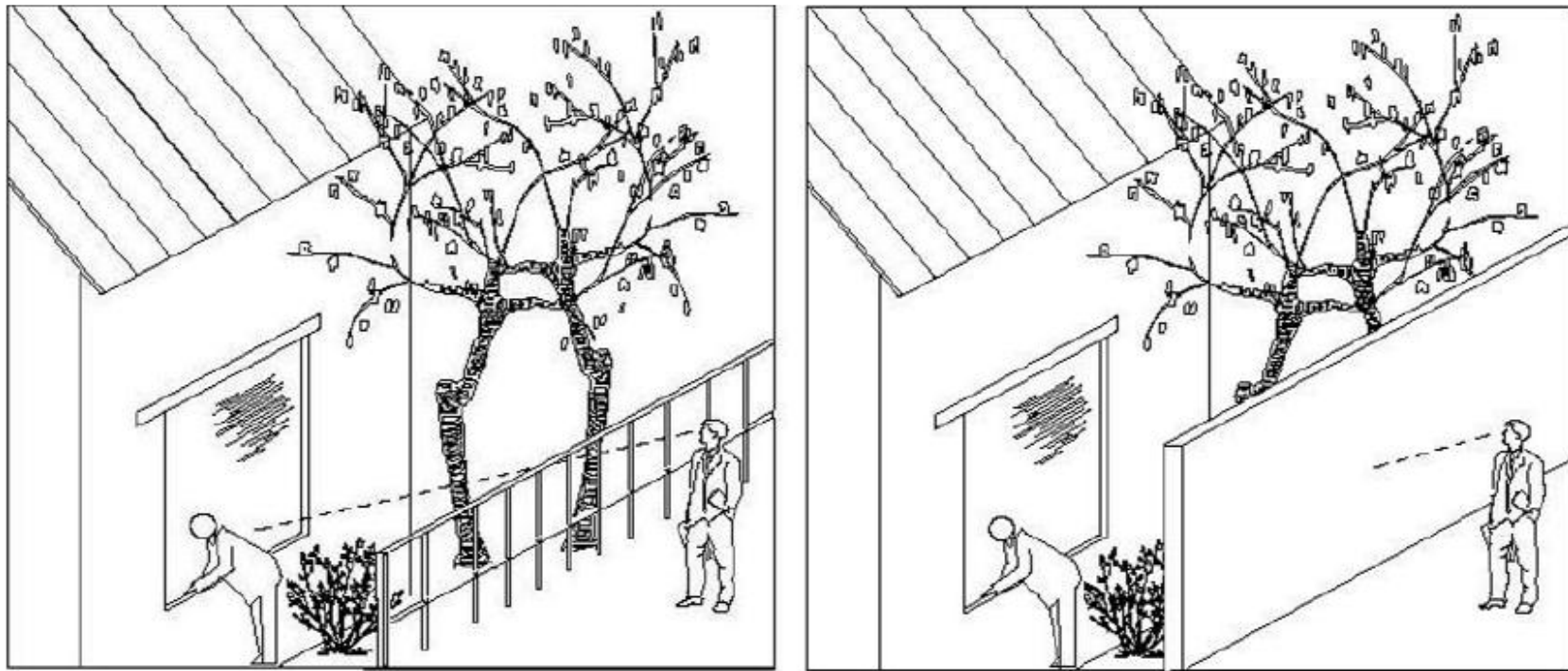
- This stairwell design providing access to a parking garage creates opportunities for surveillance as well as creating the opportunity to be heard if assistance is needed.
-



Source: Harris, Textbook

CPTED Natural Surveillance

- **Permeable fencing allows surveillance**



CPTED Natural Access Control

- A design concept directed primarily at decreasing crime opportunity by denying access to crime targets and creating in offenders a perception of risk. Gained by designing streets, sidewalks, building entrances and neighbourhood gateways to clearly indicate public routes and discouraging access to private areas with structural elements.

CPTED Natural Access Control

- The bollard lights placed at the entrance to this office building provide Natural Access Control because they guide you toward the building's entrance. There are no signs to indicate the building's entrance, but the combination of a walkway, landscaping, and bollard lights forces visitors to follow the path to the entrance.



Source: Harris, Textbook

CPTED Territorial Reinforcement

- Physical design can create or extend a sphere of influence. Users then develop a sense of territorial control while potential offenders, perceiving this control, are discouraged. Promoted by features that define property lines and distinguish private spaces from public spaces using landscape plantings, pavement designs, gateway treatments, and "CPTED" fences.

CPTED Territorial Reinforcement



Painting over graffiti immediately sends a message that the area is cared for and will be well maintained.



This shop front clearly defines the barrier from the public area to the office building.

CPTED Activity Support

- Planned activities for the areas that need to be protected.
Designed to get people to work together to increase the overall awareness of acceptable and unacceptable activities in the area.
 - E.g.
 - Sport courts in parks attract healthy activity
 - Company BBQ parties on company grounds

CPTED Activity Support

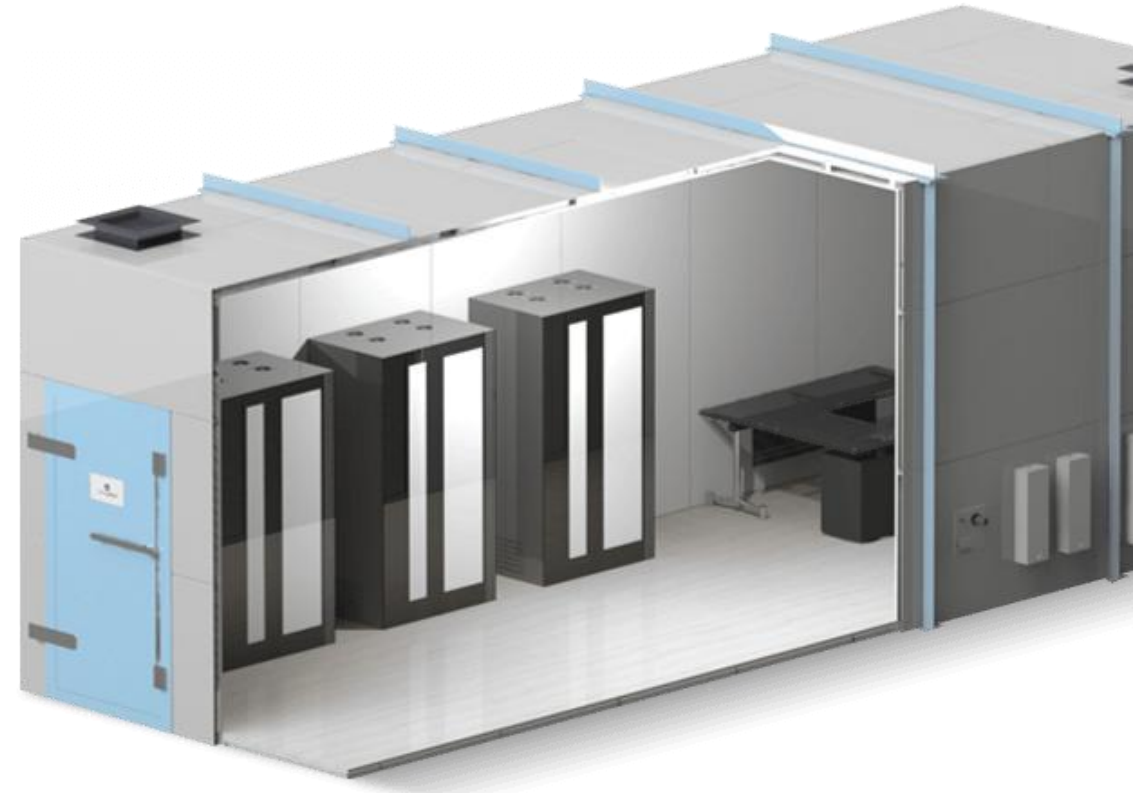
- This company BBQ gives staff and neighbours the perception that the area is being actively used and cared for, which discourages trespassing and littering.



Source: Officeworks Intranet
<http://www.bkmsd.com/>

RF (Radio Frequency) Emission Security

- Electromagnetic emission from computer screens can be picked up from several hundred meters away with sensitive antennas and receptors.
- Solid walls dampen the signals, but only a Faraday cage blocks emissions.
- Carrying cases can be Faraday cages, where e.g. smartphones can be shielded from mobile base stations and other radio-detection equipment.

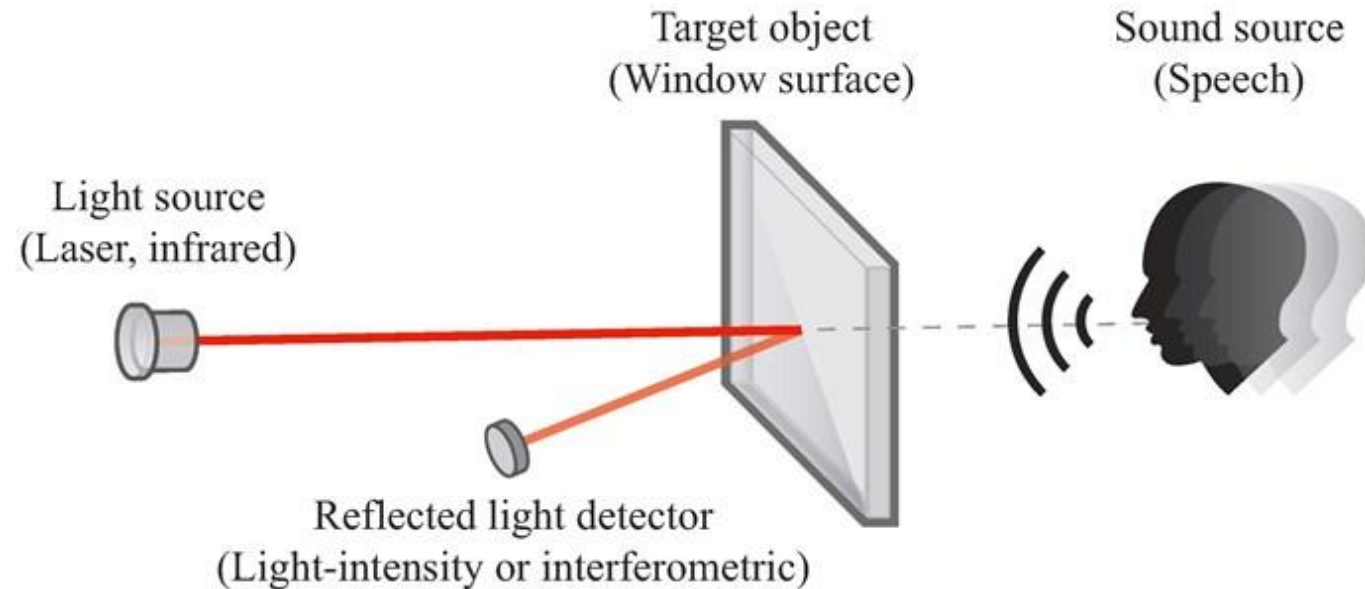


Faraday cage: RF shielded room

Source: <https://globalemc.co.uk/shielded-rooms/faraday-cages/rfi-emi-shielded-rooms/>

Sound Emission Security

- Oral conversation generates soundwaves which cause minute vibrations in windows and objects in the room.
- Attackers on the outside can point laser beams on windows or other objects, where the perturbations in the reflected light caused by the vibrations can be detected.
- Attackers can regenerate the sound of the conversations. A mitigation strategy against such attacks is e.g. to ensure that sensitive conversations are held in rooms without exterior windows, or with shielded windows.



Surveillance with laser microphones

Source: <https://www.extrica.com/article/16943>

Continuity of technical support systems

- Good physical security should protect resources against **accidental damage and forces of nature**, as well as deliberate acts, so include protection against
 - Fire & Smoke
 - Water damage
 - Power failure,
 - Structural collapse



Heating, Ventilation, and Air Conditioning

HVAC areas that can cause damage to IT systems:

- Temperature
 - Optimal temperature for IT equipment (and people) is 20-24°C
- Dust
 - Can obstruct cooling, can cause device malfunctioning
- Humidity
 - Optimal humidity for IT equipment is 40%-55%
- Static
 - One of the leading causes of damage to sensitive circuitry is electrostatic discharge (ESD)
 - A person can generate up to 12,000 volts of static current by walking across a carpet
 - Often caused by low air humidity

Power Management and Conditioning

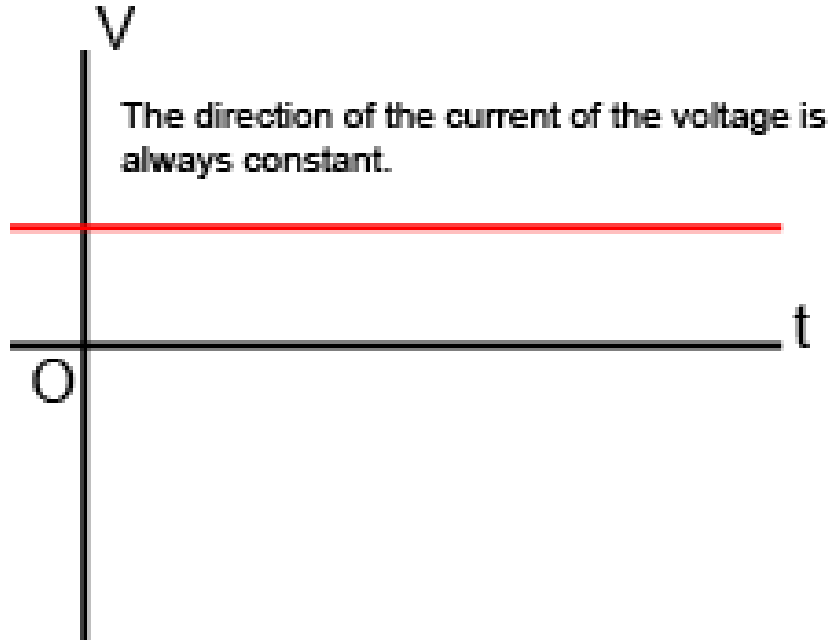
- Electrical quantity (voltage level and amperage rating) and quality (cleanliness and proper installation) of the power are important
- Any noise that interferes with the normal 50 Hertz (or 60 Hertz) cycle can result in inaccurate time clocks or unreliable internal clocks inside the CPU
- Grounding
 - Grounding ensures that the returning flow of current is properly discharged
 - If not properly installed could cause damage to equipment and injury or death to the person
- Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire

Electrical Terms

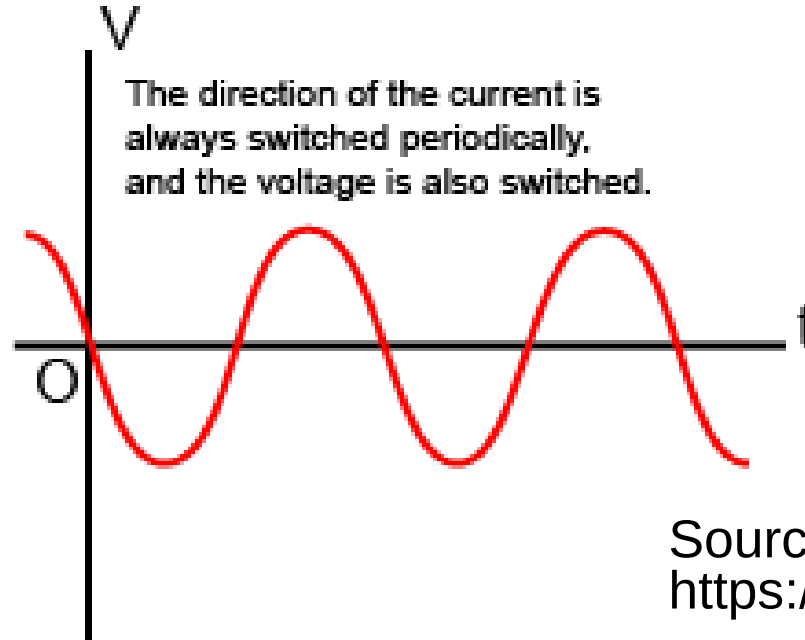
- **Fault:** momentary interruption in power
- **Blackout:** prolonged interruption in power
- **Sag:** momentary drop in power voltage levels
- **Brownout:** prolonged drop in power voltage levels
- **Spike:** momentary increase in power voltage levels
- **Surge:** prolonged increase in power voltage levels

Electric Power: AC and DC

Direct Current (DC)



Alternating Current (AC)



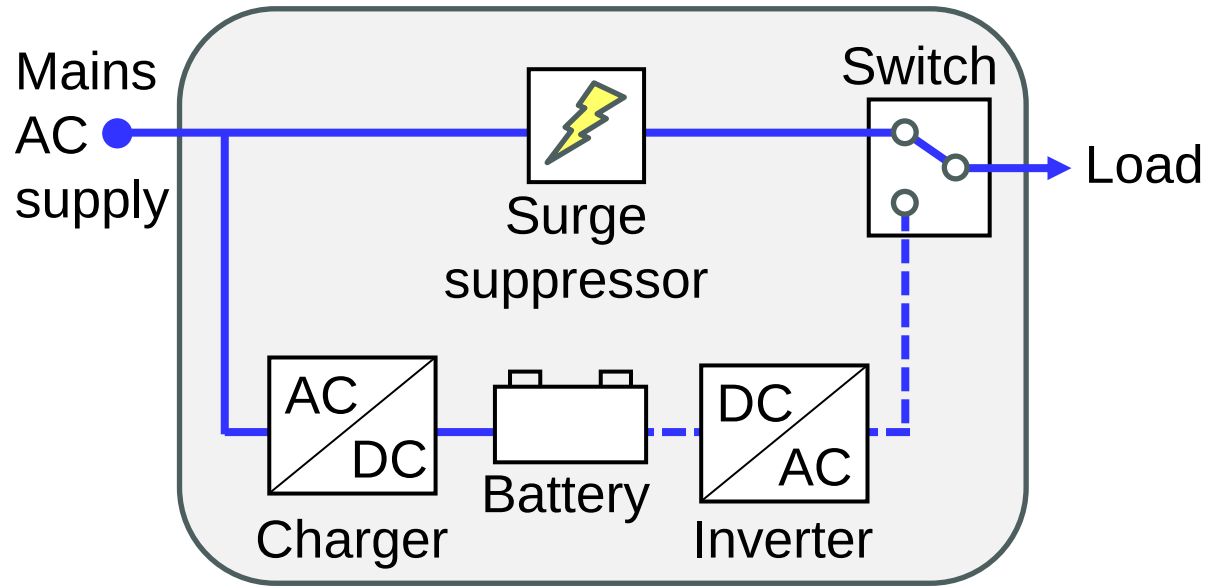
Source:
<https://www.extrica.com/article/16943>

- DC: Direct Current, provided by battery or power supply
- AC: Alternating Current, provided by power company
 - 220V, 50Hz (Europe) or 110V, 60Hz (US)

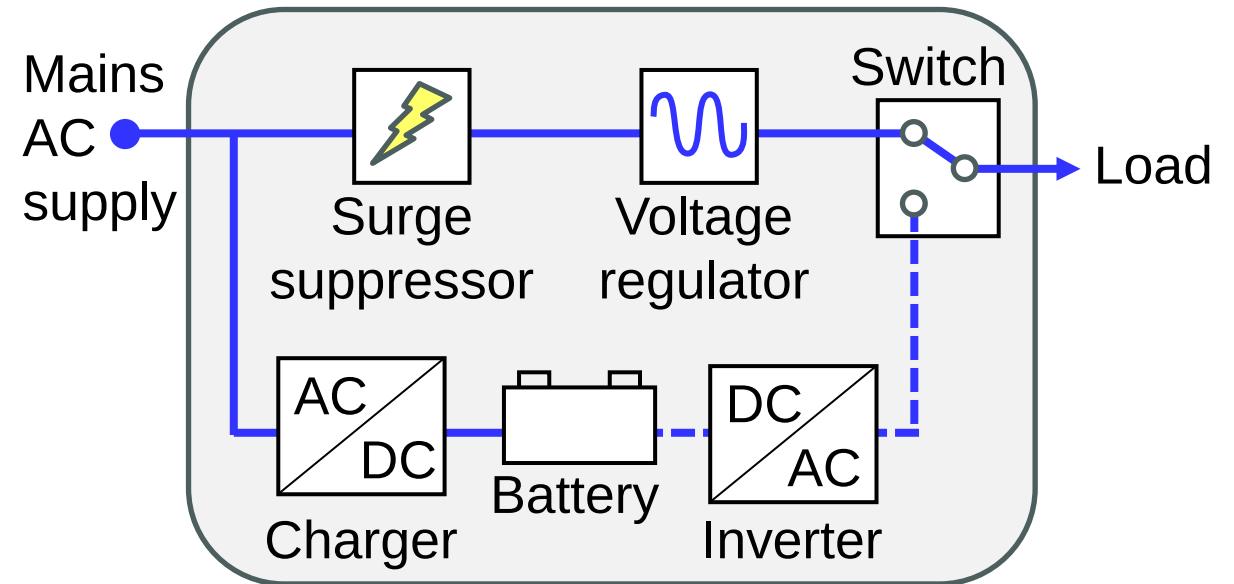
Uninterruptible Power Supplies (UPSs)

- In case of power outage, a UPS is a backup power source for major computer systems
- There are four basic configurations of UPS:
 - **Standby:** battery, causes short interruption
 - **Line-interactive:** minimal interruption
 - **Online double conversion UPS:** no interruption
 - **Generator combined with UPS:** long-time power supply

UPS 1

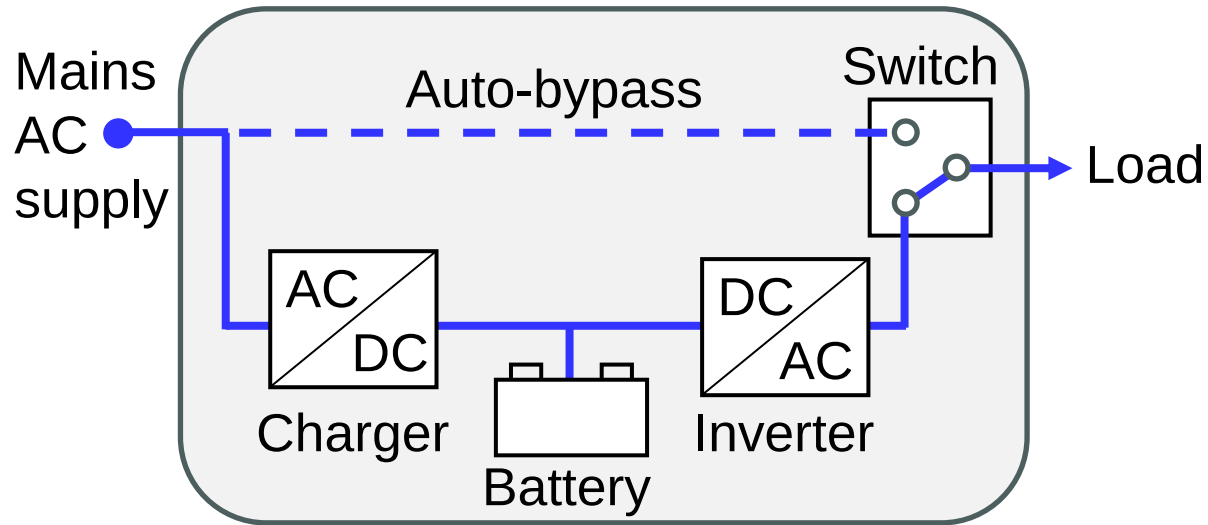


a) Standby UPS

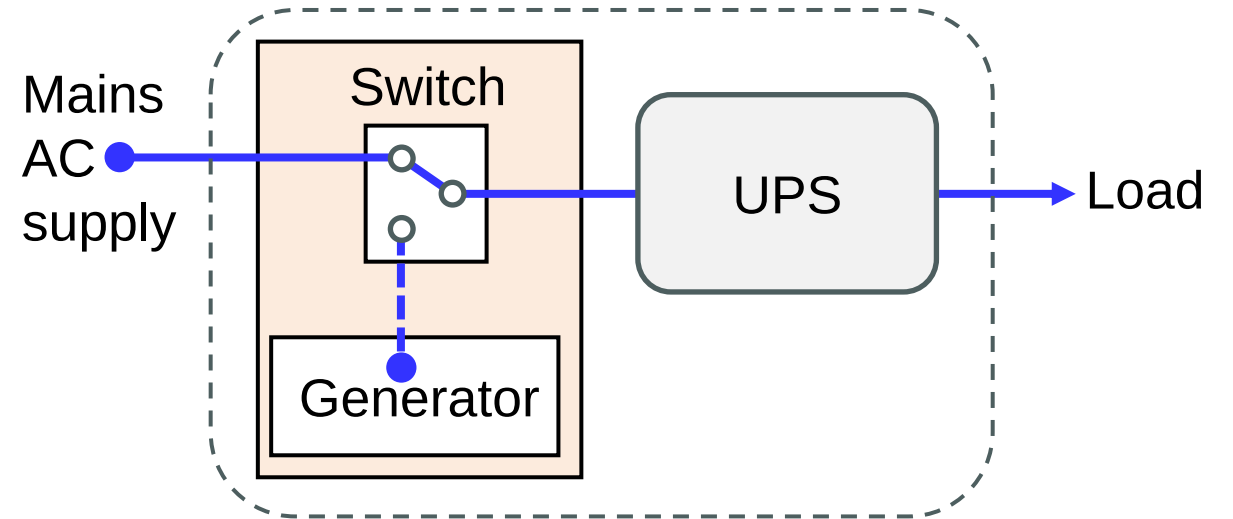


b) Line-interactive UPS

UPS 2



c) Online double conversion UPS



d) Generator combined with UPS

UPS and protection from power supply problems

Tabellen nedenfor viser forslag til hvilke typer UPS som løser hvilke strømproblemer

	Line-interactive UPS		Generator combined with O-UPS	
	Standby UPS		Online UPS	
	S-UPS	LI-UPS	O-UPS	G-UPS
Fault			✓	✓
Blackout	✓	✓	✓	✓
Persistent blackout				✓
Sag		✓	✓	✓
Brownout		✓	✓	✓
Spike	✓	✓	✓	✓
Surge	✓	✓	✓	✓
Frequency instability and noise		✓	✓	✓

End of presentation

