**Chapter 10: Physical Security Requirements**

A secure facility plan outlines the security needs of your organization and emphasizes

methods or mechanisms to employ to provide security. Such a plan is developed through risk assessment and critical path analysis.

Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements.

The top priority of security should always be the protection of the life and safety of personnel.

Crime Prevention Through Environmental Design (CPTED) addresses secure architecture and facility design. CPTED has three main strategies: natural access control, natural surveillance, and natural territorial reinforcement.

Server rooms should be located at the core of the building. Try to avoid locating these

rooms on the ground floor, on the top floor, and in the basement whenever possible. Additionally, the server room should be located away from water, gas, and sewage lines.

Physical intrusion detection systems, also called burglar alarms, detect unauthorized

activities and notify the authorities. Intrusion detection systems used to monitor physical activity may include security guards, automated access controls, and motion detectors as well as other specialty monitoring techniques.

**Intrusion Alarms**

Deterrent alarms: Alarms that trigger deterrents may engage additional locks, shut doors, and so on.

Repellent alarms: Alarms that trigger repellents, usually sound an audio siren or bell and turn on lights.

Notification alarms: Alarms that trigger notification are often silent from the intruder/attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement.

Rooms intended primarily to house computers should generally be kept between 59 and 89.6 degrees Fahrenheit (15 and 32 degrees Celsius) .

Positive air pressure in the data center should be maintained to avoid dust particles movement inside the data center. Air should move out from the high pressure area inside the data center to low pressure area outside the facility when doors are open.

Humidity should be maintained between 20 and 80 percent.

The purpose of the fire triangle is to illustrate that if you can remove any one of the four items from the fire triangle, the fire can be extinguished. Different suppression mediums address different aspects of the fire:

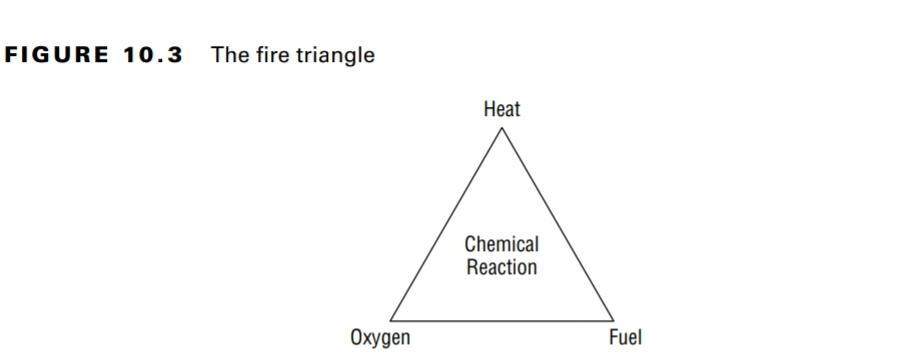
■ Water suppresses the temperature.

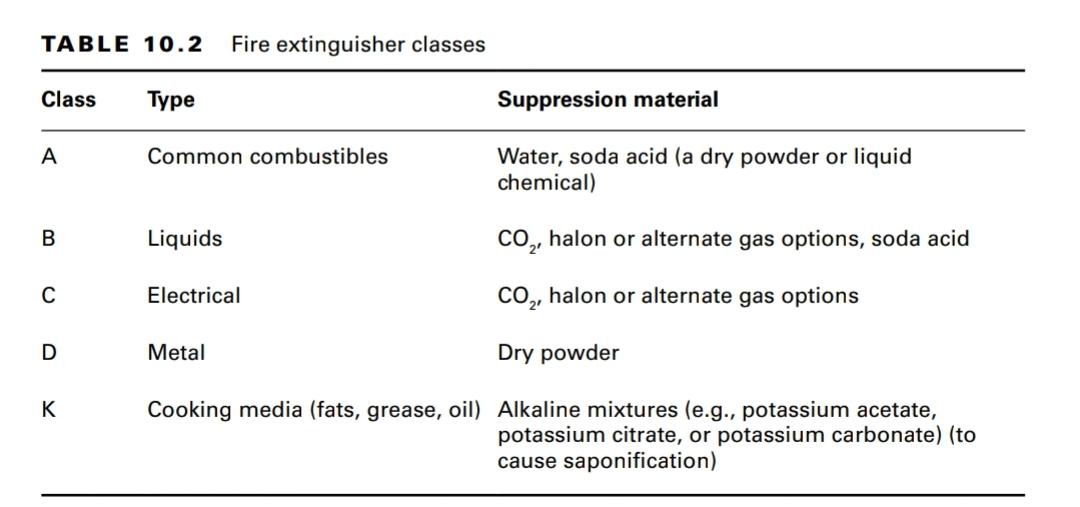
■ Soda acid and other dry powders suppress the fuel supply.

■ Carbon dioxide (CO2) suppresses the oxygen supply.

■ Halon substitutes and other nonflammable gasses interfere with the chemistry of

combustion and/or suppress the oxygen supply.





Fixed-temperature fire detectionsystems trigger suppression when a specific temperature is reached. This is the most common type of detector and present in most office buildings.

There are four main types of water suppression systems:

* A wet pipe system (also known as a closed head system) is always full of water. Water discharges immediately when suppression is triggered.
* A dry pipe system contains compressed inert gas. Once suppression is triggered, the inert gas is released, opening a water valve that in turn causes the pipes to fill and discharge water into the environment moments later.
* A preaction system is a variation of the dry pipe system that uses a two-stage. At the initial stage (smoke, heat, and so on) the dry pipe is allowed to fill. At a later stage (sufficient heat), the water is released. If the fire stops at the smoke stage, the pipe can be emptied manually. It's best for tackling false positives.
* Deluge systems contain very large pipes and deliver large volumes of water.

Gas discharge fire suppressionsystems use a compressed gas to effectively extinguish fire. However, gas discharge systems should not be used in environments in which people are located. Gas discharge systems usually remove the oxygen from the air, thus making them hazardous to personnel.

**Perimeter Security Controls**

Fences - Defines perimeter boundaries

Gates - Track movement of resources

Turnstiles - Allow entry of one individual at a time

Access Control Vestibules (Mantrap) - Two gates, Internal gate opens only after user is authenticated and authorized

Barricades - Controls movement of traffic and peoples

Lighting - Proper lighting deters unauthorized activities, it is the dark places that attract more criminal activities.

Security Guards and Guard Dogs - To keep a watch on facility

Humans are the most common cause of a false positive for a water-based fire suppression.

Gas-based fire suppression may be more effective and faster than a water-based system.

The correct order of the six common physical security control mechanisms is Deter, Deny, Detect, Delay, Determine, Decide.

Key locks are the most common and inexpensive form of physical access control device for both interior and exterior use.

After key locks, lighting is often claimed to be the most commonly deployed physical security mechanism. However, lighting is only a deterrent and not a strong deterrent.

A capacitance motion detector senses changes in the electrical or magnetic field surrounding a monitored object.

A wave pattern motion detector monitors for significant or meaningful changes or disturbances in the reflected pattern.

A photoelectric motion detector senses changes in visible light levels for the monitored area.

An infrared PIR (passive infrared) or heat-based motion detector monitors for significant or meaningful changes in the heat levels and patterns in a monitored area.