10. Physical Security Requirements

Purpose of Physical Security :: Protection against physical threats.

- Smoke
- Fire
- Water
- Storm

Earthquake

Theft
Equipment failure
Personal loss

Vandalism, Explosion, Building collapse

Toxic material using loss.

PERSPECTIVE

Identify Physical Threats ⟹ Implement safeguards

Apply Security Principles To Site & Facility Design

First line of defence, People are last.

Start with Designing Secure Facility + operations

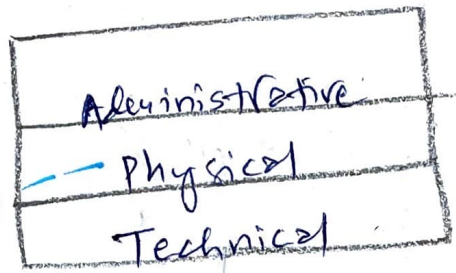
- Secure Facility Plan
  - Developed through critical path Analysis
  - what to secure?
- Site selection
- Facility Design
  - Crime prevention through Environmental Design (CPTED)
  - guidelines to design physical structure environment
- visibility
- Natural disasters

- Technology Convergence
  - Provide efficiency + cost saving but watch-out for single point of failure
  - when technology merge overtime e.g single connection for voice, vide, data = SPOF

IMPLEMENT SITE & FACILITY SECURITY CONTROLS

Physical Security perspective

Access control perspective



Remember below order when implementing Security for physical Environment.

1. Deterrent – Fencing
2. Denied – Locked Door
3. Detect – Sensor Alarms
4. Delay – Enough control to delay while police is on the way.

* Equipment Failure

One day it will = Prepare mentally for AVAILABILITY.

Response time to return system to Functional level ∝ cost involved in to maintain that Solution

if onsite replacement ≠ Fesible

⇩

Lock SLA with vendor.

Aging Hardware = schedule for replacement / repair

MTTF (mean time to failure)

- Router last for 10 years

Replace device before MTTF expires

MTTR (mean time for Repair)

- Router needs repair / maintenance every 1 year

while device sent for replacement, Prepare alternate / Backup Hardware

MTBF (mean time between failures)

- Estimation of time between first and subsequent failures

* wiring closet
(Intermediate distribution Facilities - IDF)
(Premise wire Distribution Room)

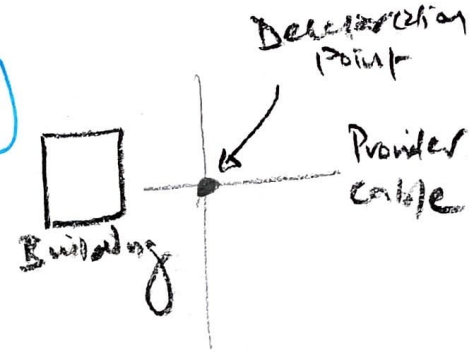
→ Physical security Focus ⟹ Prevent Unauthorised Access

→ Have wiring closet security policy ⟹ Provide to Building mgmt staff

Element of

Cable Plant Management Policy

→ Entrance Facility

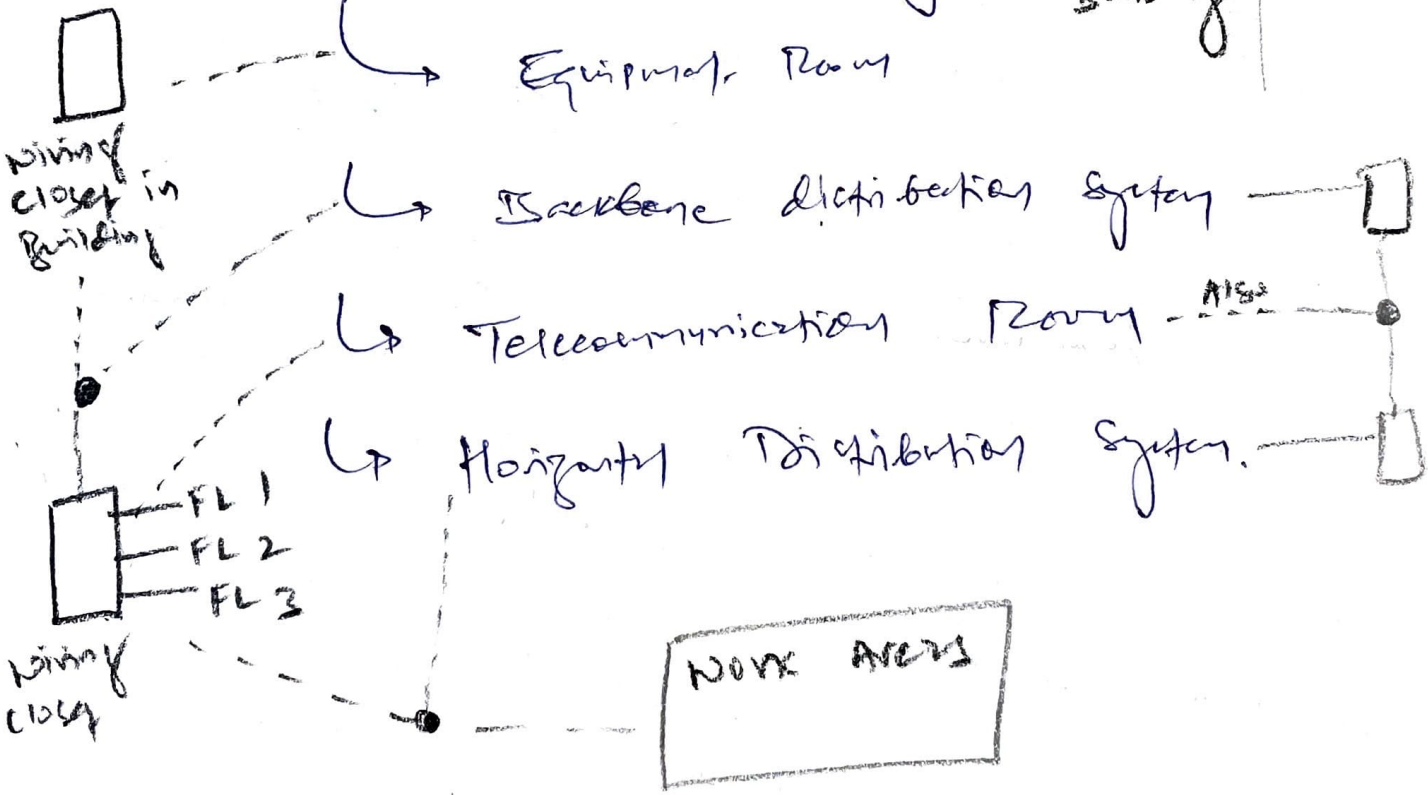


→ Equipment Room

→ Backbone distribution System

→ Telecommunication Room

→ Horizontal Distribution System.



EE

Wiring closet Security concern = Prevent physical Unauthorised access

→ Update building mgmt about wiring closet security policy

* Server Rooms / Data Centers

- can be human incompatible
  = low temp, low light
- Don't put on ground Floor / Basement = should be at care of building (heart)

Technical controls for Datacentre

Smart cards
- Used for Authentication purpose
- mostly for multi-factor: "something you have"

IDS
- only useful when connected to intrusion alarm
- 2 aspects of IDS
  (a) How it gets power
  (b) How it communicates
  - Battery Backup
  - Heartbeat sensor

Proximity Readers
- Passive Device
  - NO electronics
- Field-power Device
  - Has electronic, activates when device enters to electromagnetic field
- Transponder device = self-powered & transmit signal
  - Garage Door Remote

Prevention:
- Audit trails + access logs are helpful

Access Abuse

- Piggybacking
- Masquerading
  - Using someone else' security ID

Manual
- CCTV + security guards.

Automatic

TEMPEST

Emanation Security

- Read ch: 9 Electromagnetic Radiation for Basics / Intro

Called TEMPEST countermeasures

Safeguards to Protect Emanation Attacks

Faraday cage

BOX

mobiles / TV Broadcast don't work here

Blocks Electromagnetic signals (EM)

White Noise

Broadcasts false traffic in the time to mask and hide the presence of real emanations.

white Noise

non-confidential signal (fake signal)

Control Zones

- outside control zone, Emanation is blocked
- within control zone, EM signals are supported.

* Media Storage Facilities

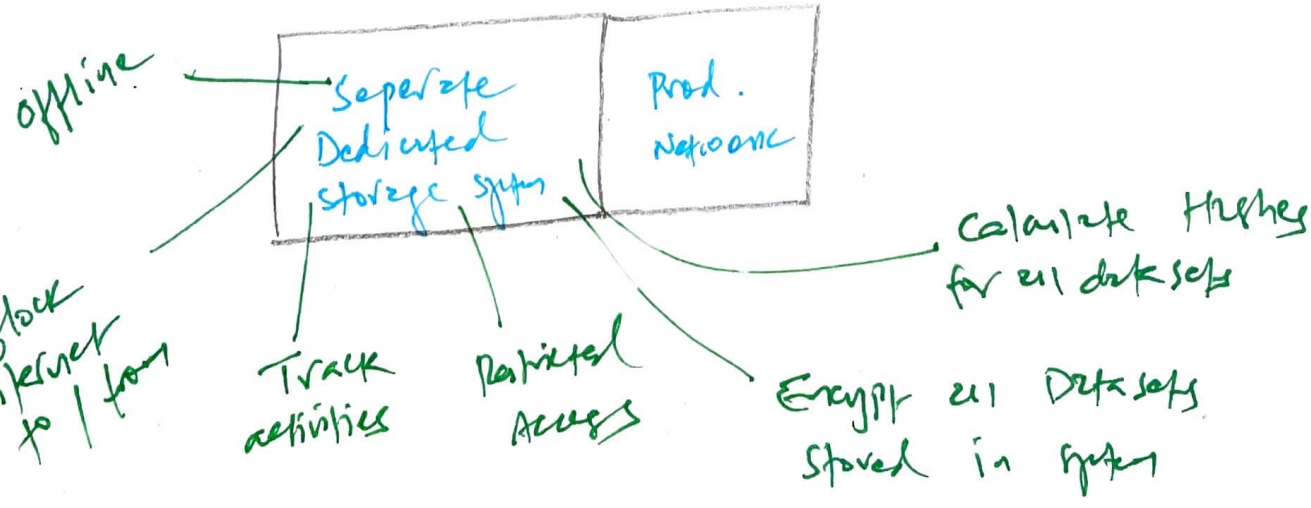
Security concerns
- theft
- corruption
- Data Remnant Recovery

(To Reduce Risk)
How to secure media storage?

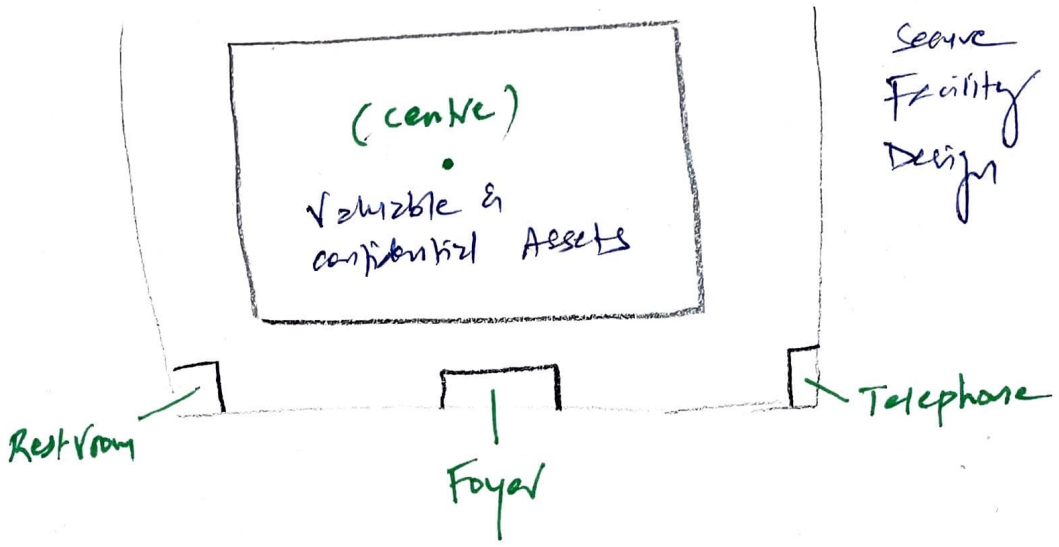
- Restrict Access
- Physical security (from stealing)
  - locked cabinet
- Secure wiping (Avoid Data Remance)
  - Zeroization
    - Erase data by replacing with zeros
- Lable media
  - classification
- From Malware
  - Patching
- Higher protection
  - Fire, Flood, EM field, Temp monitoring
- Verify media with Hash-based integrity
  - To ensure valid file remains valid

* Evidence storage

Cyber crime ↑↑↑ ⟹ Retain logs, audit trails & records of digital events.



* Restricted and Work Area Security



Secure Facility Design

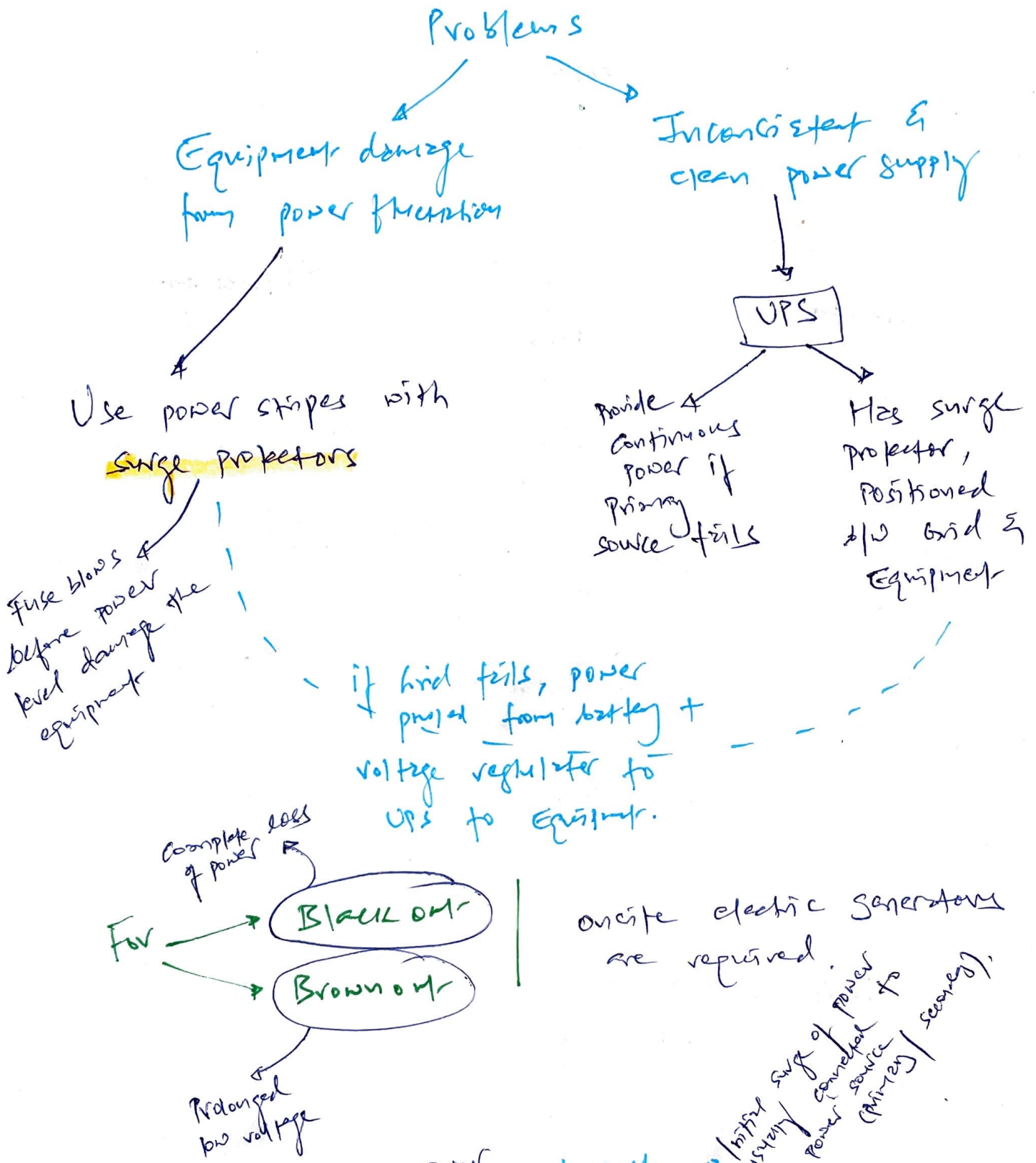
Something to consider

- Wall partition to avoid shoulder surfing
- Classified work Areas (similar to data & Asset)
  - only personals with valid clearance can access
- Address visitors & visitor control
- Physical security.
  - RFID ID
  - Cards
  - Mantrap
  - CCTV
  - written logs
  - Keys / locks

Sensitive Compartmented Information Facility (SCIF)

- military
- government
- Concept for restricted work area
- no photography, video allowed
- Purpose: Provide restricted access to only those with fewness need based on clearance level
  - store, view & update sensitive compartmented information (SCI)

* Utilities and HVAC Considerations



* Noise

→ from Equipment = Affect Data Transmission

- Telephone
- TV
- Cellular
- Radio / Audio
- Network mechanisms

Noise

2 Types of Electromagnetic Interference (EMI)

Common mode noise

- Generated by difference in power b/w hot & ground wire of power source

Traverse mode noise

- Generated by difference in power b/w hot & neutral wire of power source

Noise

Radio Frequency Interference (RFI)

- All electronic appliances generate RFI

So far problem Equipment from

Power loss

Noise

* Temperature, Humidity & Static

→ 15 to 23°C (60 to 75 °F)

DC — 40 to 60%.

Too much humidity → corrosion / moisture / Equipment Damage

Too little humidity → static electricity

(static voltage)
Static electricity → 2000 volt = system shutdown

4000 = printer jam

17,000 = permanent circuit damage

Min. level of static discharge can destroy electronic equipment.

* Water Issues

- leakage
- flooding

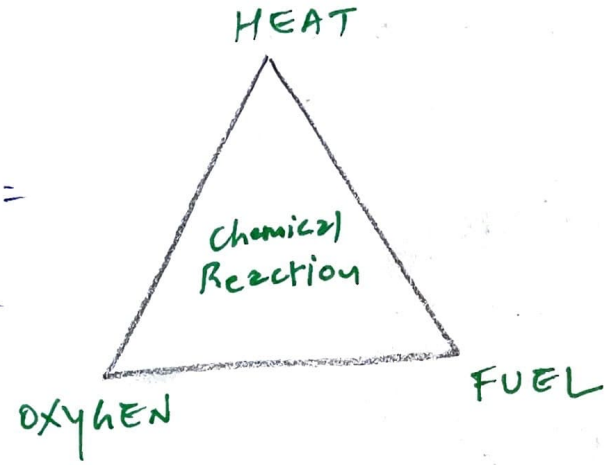
Water + Electricity = danger
(Serious risk of Electrocution)

- Install water detection circuit
- Be familiar with shutoff valves & drainage locations.
- Monitoring for plumbing leaks.

* Fire prevention, Detection & Suppression

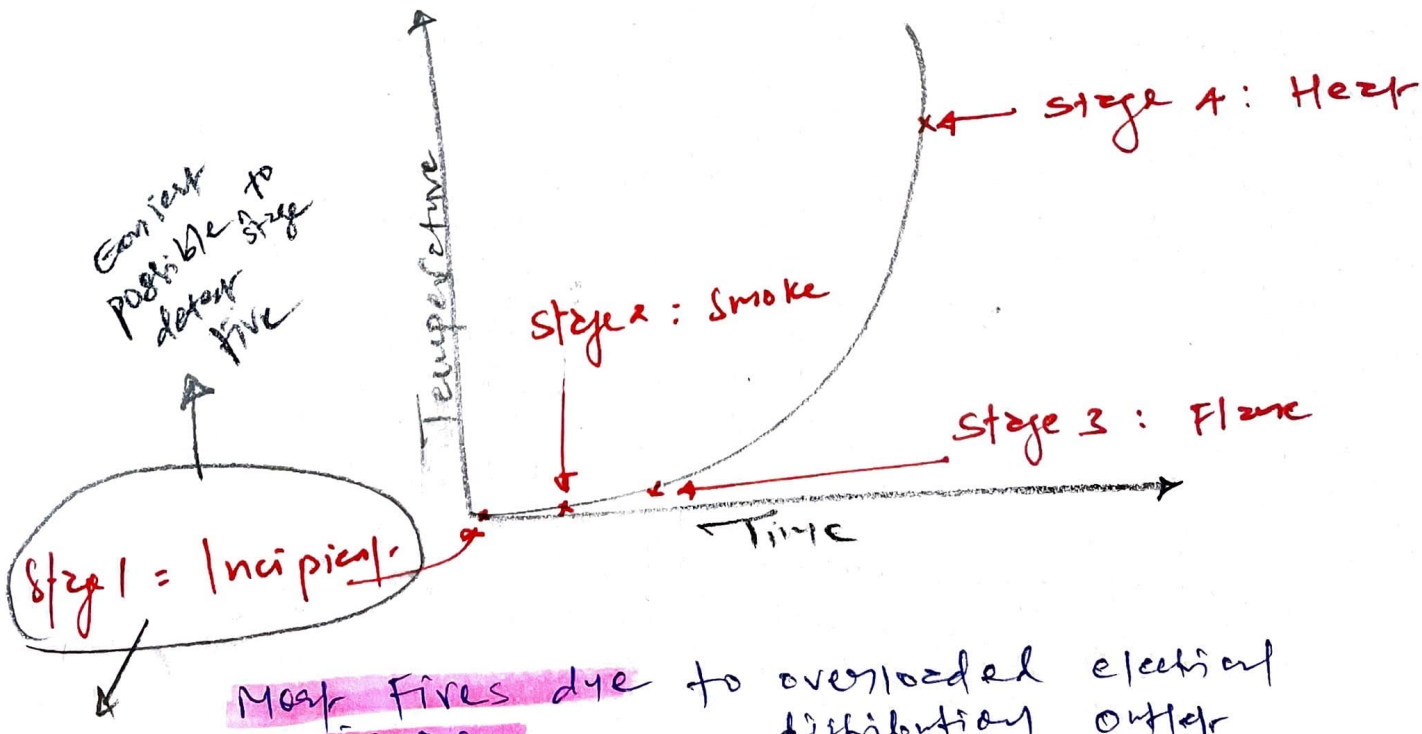
The Fire Triangle

- Remove any one of four = fire can be extinguished



Various suppression mechanism exist but Consider what aspect of fire triangle it addresses

Stages of FIRE



Most Fires dye to overloaded electrical distribution outlet in DC

only ones Ionization no smoke

Fire Mgmt → Evacuation route (at least two)
→ Awareness Training (Suppressing mechanisms)
→ Use of Fire Ex.

* Five Extinguishers

→ only use in Incipient stage

By Types

A
Common Combustibles
Water, Soda Acid, Dry Powder

B
Liquids
CO_2, Halon, Soda Acid

C
Electrical
CO_2, Halon

water can't used for class B or C

D
Metal
Dry powder

Oxygen suppression can't use on metal fire because metal produces its own oxygen.

* Fire Detection Systems

→ To prevent Fire

- Automatic Detection
- Suppression System

Fixed-Temperature Detection System

Triggers when specific temp is reached.

Rate-of-Rise Detection System

Triggers suppression when the speed at which temp reaches to specific level.

$23^\circ \rightarrow 38^\circ$

Flame-Actuated System

Suppression based on infrared energy of flames.

Smoke-Actuated System

Use of photoelectric or radioactive ionization sensors as triggers.

* Water Suppression Systems

most common cause = Human Error

4 Types

Wet Pipe System (closed head)

- Pipe full of water discharge when triggers suppression

Dry Pipe System

- Filled with compressed air
- Suppression trigger to escape air = open valve = fill the water

Deluge System

- Large dry pipes but bigger
- Not ideal for offices that has electronics & computers.

Preaction System

- Combination of Dry + wet pipes
- Dry in the initial stage (2 steps) of fire, then filled with water

Best for environment that house computers & Humans together.

Used for Sprinklers head heat activation before dispensing water

* Gas Discharge Systems

Removes oxygen from air = Don't use where people are located.

Halon = Effective fire suppression compound but becomes toxic @ 900°F

Use substitutes:

- FM-200
- CEA-410
- NAF-S-III
- FE-13
- Low pressure water mist
- Argon / Argonite / Inergen / Aero-K

* Damage caused by Fire

Smoke

- Damage any storage device

Heat

- Damage any electronic or computer component

Suppression media

- cause short circuit
- initiate corrosion
- render equipment useless

Implement & Manage Physical Security.

Designate Facility Areas As

- Public
- Private
- Restricted

- Public → Physical Access controls
- Private → Monitoring
- Restricted → Prevention Mechanisms

* Perimeter Security Controls

- Fence
- Gate
- Turnstile
  - Revolving Door
- Mantrap
  - Prevents piggybacking
  - Remember NATO
  - Delay Feature
- Security Bollards
  - Prevents vehicles ramming access points.

* Lighting — ~~Security lights~~ — Light poles should be placed the same distance apart as diameter of illuminated area

* Security Guards & Dogs

- Guards: Vulnerable to social Engg Attack + they are expensive
- Dogs: Most effective as deterrent & detection.

* Internal Security Controls

Escort assigned to visitors.

Monitor their access + activities closely.

Keys & Combination locks

- + Key card for shared Entry points (Building)
- Access to individual entry (storage, cabinets)

Preset locks

Programmable + combination locks

more control

Anybody can pick the lock, called Shimming

Badges

- Simple ID with photo
- smart-card as multifactor AAA

Motion Detectors (MD)

- Infrared or (heat-based MD heat level & Patterns
- Wave pattern motion (transmit constant ultrasonic signal low
- Capacitance motion detector (changes in electrical or magnetic field)
- Photoelectric MD
- Passive Audio MD (listen to Abnormal sounds)

changes in light, for dark rooms

Intrusion Alarms

Alarm Types:
- Deterrent Alarm
- Repellent A.
- Notification A.

Alarm categories:
- Local Alarm system
- central station System
- Auxiliary station

P.t.o (cont..)

Secondary Verification Mechanisms – to get rid of false positives

Sensors
Alarms ⇒ False Alarm (Bird, Animal)
MD

Need more than one triggers to confirm

E.g CCTV = secondary mechanism
- Need manual review after trigger

CCTV is preventive measure.
Reviewing footage is detective measure.

Environment and Life Safety

Physical security
└ primary focus
- Protect human life

└ Secondary focus
– Restore IT systems

* First Protect people. BCP comes later.
– OEP (occupant emergency plan) used to minimize threat to life

Privacy Responsibilities & Legal Requirements

Safety of PII ← Address in organization's security policy

NIST 800-122

Privacy = Protecting PII from unauthorised Access

GDPR from EU

Regulatory Requirements

Country / jurisdiction	Industry (BANK, HEALTH CARE)
Legal Requirements	

Foundation of security framework

Notes

- Soda Acid + other dry powders: Extinguishers work to remove fuel supply
- Water: Suppresses the temperature
- Halon & CO_2: Remove oxygen supply from fire.
  - is Bad / Banned
- Humidity: DC range 40 - 60 %.
  - lower = static electricity
  - high = moisture / Equipment Damage
- Capacitance: Type of motion detector that monitor the electromagnetic field in monitored area, it senses the disturbance that corresponds to motion.

→ Halon use CFC suppressant material that was banned in Montreal protocol because it depletes ozon layer.

SCADA - Supervisory Control and Data Acquisition