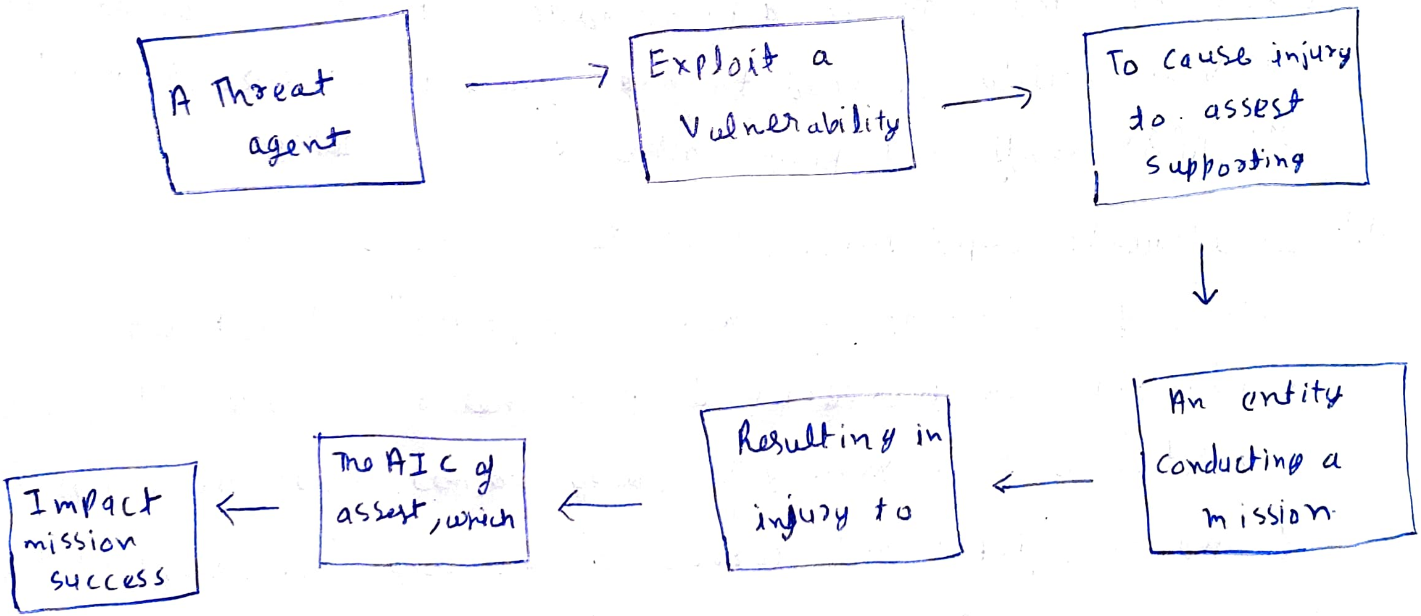
Q1 What is AP&S. Explain the hierarchál structures of vulnerbilitie regarding SCADA system.

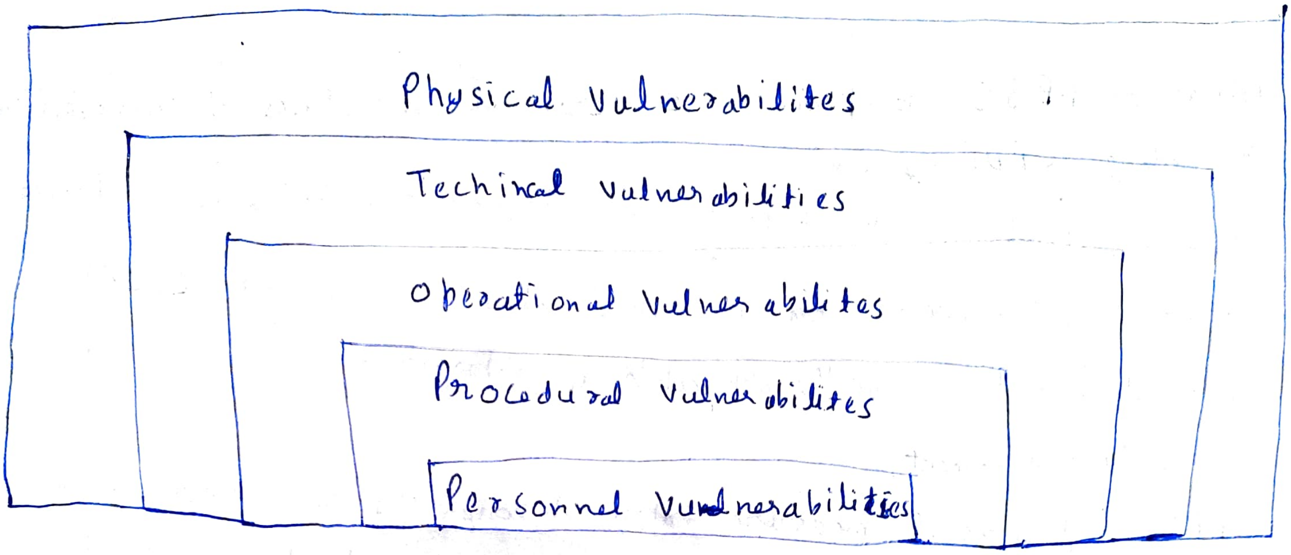
Ans AP&S stand for Assest Protection & Security. AP&S is inclusive term that has been coined in critical infrastruture Protection (CIP) literature and is equally applicable in information system and corporate Security environment.

AP&S refers to all measure taken through the risk ~~magem~~ management life-cycle, include mission analysis, assest valuation, threat assessment, vulnerability assessment, risk assessment, and thereafter, safeguard implementation to protect against, mitigate the effect of, deter, absorb, isolate, respond to, recover from and restore all services and capabilities after an attack or major interruption to operations



Description of AP&S risk broken down.

Hierarchical structure around vulnerabilites regarding SCADA


Physical Vulnerabilites
Techincal Vulnerabilities
Operational Vulnerabilites
Procedural Vulnerabilites
Personnel Vulnerabilities

1) Personnel Vulnerabilites :- It includes the following:

(a) Lack of proper security clearance prior to being granted access to sensitive information. This result in a security breach in all cases.

(b) Lack of or inadequate technical training prior to assuming duties.

(c) Egos and inability to acknowledge that one is not yet cable This Vulnerability can lead to anger, resentment ~~too~~ toward the APSS staff and hiding other vulnerabilites.

(d) Inadequate supervision. Some senior manger in organizations think that "a manager can manage anything" and put untrained, uneducated, an inexperienced personnel in charge of competent practitioners. These manager simply donot have the capability to manage, guide and correct techinically competent staff, especially in APSS.

(e) Lack of ~~secur~~ Security awareness program.

2> Procedural Vulnerabilites :- It include following :

(a) Lack of outdated or distributed security Policies, standards, and directives.

(b.) Lack of inconsistent or conflicting procedures. At the process level, it is critical to ensure consistent, repeatable performance by all operators; otherwise, an apparently minor lack of attention to an anomaly could escalated very quickly to affect the whole process

3> Operational Vulnerabilites :- It include the following:

(a) Lack of alignment of individual operational process. This could result in one process working against another; thereby introducing more operational vulnerabities

(b.) Lack of training in Hazard and accident prevention.

(c) Inadequate personal protective protection Equipment.

(d) Lack of cross-trainning of personnel. This could lead to SPOFs if key personnel with unique knowledge or skills are unavailable for work

(e.) Lack of communication among. and within business lines.

(f) Lack of operational security, which means typically maintainng the confidentially of the workings of the organization, from strategic direction, to operational-level business line, to tactical operation of equipment

~~Technicaly~~

4) Technical Vulnerabilites :- It include following:

(a) Lack of hardening of IT system supporting operations, Hardening include anti-malware, intrusion detection or protection.

system., disabling all unnessary poots and so on.

(b.) Lack of physical separation IT system and lack of integrated. mangement,

(c) Inadequate configuration management.

(d) Inappropriate clipping levels. These setting to determine when an anomaly should set off an alarm. could lead to more vulnerabi-lites, and possibly an attack, if they are set too openaly

(e.) Infrequent maintenance. Not checking and maintainning equipment regularly could lead to pailures, which can affect operational schedules.

5> Physical Vulnerabilites :- It includes following.

(a) Inadequate physical access controls. This could include leaving doors and windows insecure, not challenging unknow indiviual ~~etc~~ etc.

(b) Lack of defense in depth. This could include not having perimeter fencing, signage, and reception areas.

(c) Not physically locking and controlling value assest, such as IT systems, negotiables, IT server room, control rooms, consumables such as fuel, high-value ~~equi~~ equipment and spare parts etc.