Threats

- Human errors
  - Configuration errors
  - Operator/user error
  - Loss of hardware
  - Non compliance with policies or procedures
- System failures
  - Failures of devices or systems
  - Failures or disruptions of communication links (communication networks)
  - Failures of parts of devices
  - Failures or disruptions of main supply
  - Failures or disruptions of the power supply
  - Malfunctions of parts of devices
  - Malfunctions of devices or systems
  - Failures of hardware
  - Software bugs
- Natural and social phenomena
  - Earthquakes
  - Fires
  - Extreme weather (e.g. flood,heavy snow, blizzard, high temperatures, fog, sandstorm)
  - Solar flare
  - Volcano explosion
  - Nuclear incident
  - Dangerous chemical incidents
  - Pandemic (e.g. Ebola)
  - Social disruptions (e.g. ndustrail actions,civil unrest, strikes, military actions, terrorist attacks, political instability)
  - Shortage of fuel
  - Space debris & meteorites
- Third party failures
  - Internet service provider
  - Cloud service provider (SaaS / PaaS / SaaS/IaaS/SecaaS)
  - Utilities (power / gas / water)
  - Remote maintenance provider
  - Security testing companies (i.e. penetration testing/vulnerability assessment)
- Malicious actions
  - Denial of Service attacks
    - Amplification/Reflection
    - Flooding
    - Jamming
  - Malicious software on IT assets (including passenger and staff devices)
    - Worm / Trojan / Virus / Rootkit / Exploitkit / Botnet / Spyware / Ransomware / Scareware / Adware
    - Remote arbitrary code execution (device under attacker control)
  - Exploitation of (known or unknown) software vulnerabilities
    - Implementation flaws in IT assets (flaw in code)
    - Design flaws in IT assets (flaw in logic)
    - Advanced Persistent Threats (APT)
  - Misuse of authority / authorisation
    - Unauthorised use of software
    - Unauthorised installation of software
    - Repudiation of actions
    - Abuse of personal data/Identity Fraud
    - Using information from an unreliable source
    - Unintentional change of data in an information system
    - Inadequate design and planning or lack of adoption
    - Data leakage or sharing (exfiltration, discarded, stolen media)
  - Network/interception attacks
    - Manipulation of routing information (incl. redirection to malicious sites)
    - Spoofing
    - Unauthorised access to network / services
    - Authentication attacks (against insecure protocols or PKI)
    - Replay attacks
    - Repudiation of actions
    - Wiretaps (wired)
    - Wireless comms (eavesdropping/interception/jamming/electromagnetic interference)
    - Network reconnaissance/information gathering
  - Social attacks
    - Phishing / Spearphishing
    - Pretexting
    - Untrusted links (fake websites / CSRF / XSS)
    - Baiting
    - Reverse social engineering
    - Impersonation
  - Tampering with devices
    - Unauthorised modification of data (incl. compromising smart sensor data and threat image projection))
    - Unauthorised modification of hardware or software (including tampering with kiosk devices, inserting keyloggers, or malware)
    - Data deletion / corruption
  - Breach of physical access controls / administrative controls
    - Bypassing authentication
    - Privilege escalation
  - Physical attacks on airport assets
    - Vandalism
    - Sabotage
    - Explosives / bomb threats
    - Malicious tampering or control of assets resulting in damage