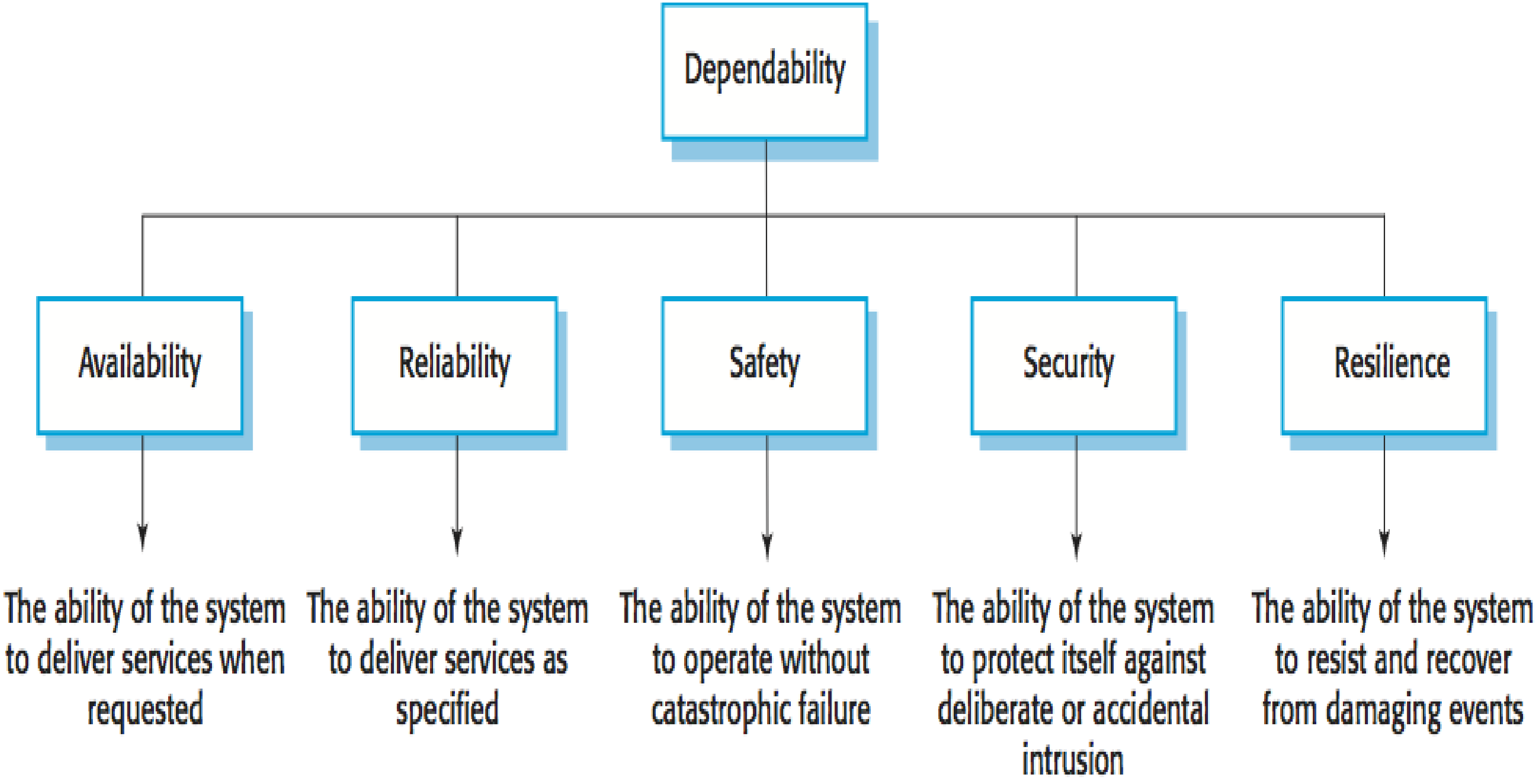
SYSTEM DEPENDABILITY

SYSTEM DEPENDABILITY

- The dependability of a computer system is a property equating to its trustworthiness.


Dependability
Availability
Reliability
Safety
Security
Resilience
The ability of the system to deliver services when requested
The ability of the system to deliver services as specified
The ability of the system to operate without catastrophic failure
The ability of the system to protect itself against deliberate or accidental intrusion
The ability of the system to resist and recover from damaging events

SYSTEM DEPENDABILITY

- It is the property of the system that equals to its trustworthiness. Four principal dimensions to dependability are

  - Availability – To deliver services when required
  - Reliability – To deliver services as specified
  - Safety – To operate without terrible failure
  - Security – To protect itself against accidental or deliberate interruption

Other Dependability Properties

- Reparability : Reflects the extent to which the system can be repaired in the event of a failure.

- Maintainability : Reflects the extent to which the system can be adapted to new requirements.

- Survivability : Reflects the extent to which the system can deliver services while under hostile attack.

- Error Tolerance : Reflects the extent to which user input errors can be avoided and tolerated.

Dependability Specification

Dependability requirements include:

- **Functional requirements** to define error checking and recovery facilities and protection against system failures.
- **Non-functional requirements** defining the required reliability and availability of the system.
- **Excluding requirements** that define states and conditions that must not arise.

A trade-off between system performance and system dependability.

High dependability can only be achieved at the expense of system performance.

Availability and Reliability

- System availability and reliability are closely related properties that can both be expressed as numerical probabilities.
- The reliability of a system is the probability that the systems services will be correctly delivered as specified.
- The availability of the system is the probability that the system will be up and running to deliver these services to users when they request them.

Availability and Reliability

- Availability is usually expressed as a percentage of the time that the system is available to deliver services e.g: 99.95%. However, this does not take into account two factors :

- The **number of users affected** by the service outage. Loss of service in the middle of the night is less important for many systems than loss of service during peakusage periods.

- The **length of the outage**. The longer the outage, the more the disruption. Several short outages are less likely to be disruptive than 1 long outage. Long repair times are a particular problem.

Safety

- These systems that they never damage the people or the systems environment even if the systems fail like monitoring systems in aircraft etc.
- Safety critical software falls in two classes:
  - **Primary safety critical software** – Embedded as a controller in a system. Malfunctioning of such software can cause hardware malfunction which results in human injury or environmental damage.
  - **Secondary safety critical software** – Indirectly results in injury. Example is medical database holding details of drugs administered to patients' error in this could result in wrong dosage of drugs

Safety Achievement

Hazard avoidance : The system is designed so that some classes of hazard simply cannot arise.

Hazard detection and removal : The system is designed so that hazards are detected and removed before they result in an accident.

Damage limitation : The system includes protection features that minimize the damage that may result from an accident.

Safety Specification: Goal is to identify protection requirements that ensure that system failures do not cause injury or death or environmental damage.

Hazard Identification

Identify the hazards that may threaten the system. Types of hazard :

- Physical
- Electrical
- Biological
- Service failure

Security

- Ability of a system to protect itself from external accidental or deliberate attacks. As more systems get connected to Internet it can be attacked by people with unfriendly intentions.

- Without a reasonable level of security, the availability, reliability and safety of the system may be compromised if external attacks can cause some damage to the system.

Types of damage that may be caused through external attack

- **Denial of service** – Forced into a state where its normal services become unavailable affecting the availability of the system.

- **Corruptions of programs or data** – Software components may be altered in unauthorized way affecting the systems behavior and its reliability and safety.

- **Disclosure of confidential information** – External attack may expose confidential information to unauthorized person which affects the safety of the system and later availability or reliability