Security and Dependability

WK 9

Topics covered

- Dependability properties
  - The system attributes that lead to dependability.
- Availability and reliability
  - Systems should be available to deliver service and perform as expected.
- Safety
  - Systems should not behave in an unsafe way.
- Security
  - Systems should protect themselves and their data from external interference.

System dependability

- For many computer-based systems, the most important system property is the dependability of the system.
- The dependability of a system reflects the user's degree of trust in that system. It reflects the extent of the user's confidence that it will operate as users expect and that it will not 'fail' in normal use.
- Dependability covers the related systems attributes of reliability, availability and security. These are all inter-dependent.

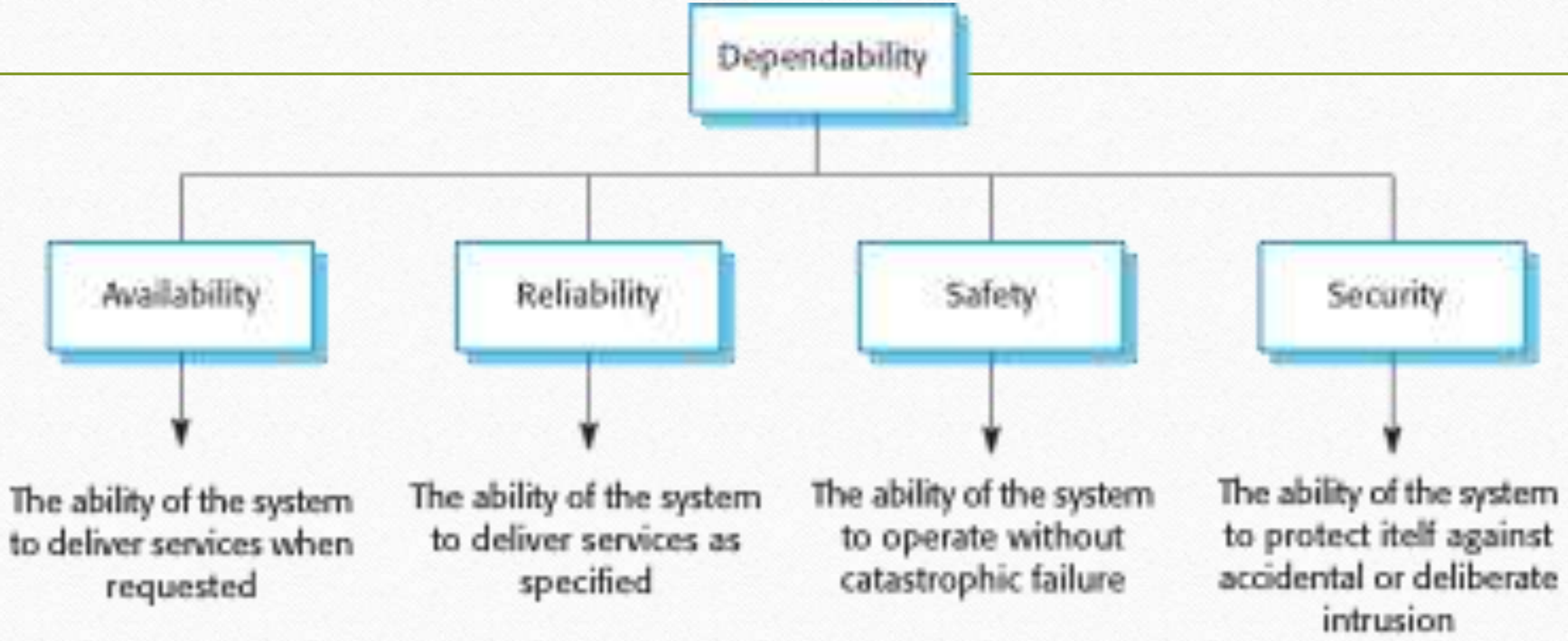
Importance of dependability

- System failures may have widespread effects with large numbers of people affected by the failure.
- Systems that are not dependable and are unreliable, unsafe or insecure may be rejected by their users.
- The costs of system failure may be very high if the failure leads to economic losses or physical damage.
- Undependable systems may cause information loss with a high consequent recovery cost.

Causes of failure

- Hardware failure
  - Hardware fails because of design and manufacturing errors or because components have reached the end of their natural life.
- Software failure
  - Software fails due to errors in its specification, design or implementation.
- Operational failure
  - Human operators make mistakes. Now perhaps the largest single cause of system failures in socio-technical systems.

Principal dependability properties



Dependability

Availability

The ability of the system to deliver services when requested

Reliability

The ability of the system to deliver services as specified

Safety

The ability of the system to operate without catastrophic failure

Security

The ability of the system to protect itelf against accidental or deliberate intrusion

Principal properties

- Availability
  - The probability that the system will be up and running and able to deliver useful services to users.
- Reliability
  - The probability that the system will correctly deliver services as expected by users.
- Safety
  - A judgment of how likely it is that the system will cause damage to people or its environment.
- Security
  - A judgment of how likely it is that the system can resist accidental or deliberate intrusions.

Other dependability properties

- Repairability
    - 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 whilst under hostile attack;
- Error tolerance
    - Reflects the extent to which user input errors can be avoided and tolerated.

Repairability

- The disruption caused by system failure can be minimized if the system can be repaired quickly.
- This requires problem diagnosis, access to the failed component(s) and making changes to fix the problems.
- Repairability is a judgment of how easy it is to repair the software to correct the faults that led to a system failure.
- Repairability is affected by the operating environment so is hard to assess before system deployment.

Maintainability

- A system attribute that is concerned with the ease of repairing the system after a failure has been discovered or changing the system to include new features.
- Repairability – short-term perspective to get the system back into service; Maintainability – long-term perspective.
- Very important for critical systems as faults are often introduced into a system because of maintenance problems. If a system is maintainable, there is a lower probability that these faults will be introduced or undetected.

Survivability

- The ability of a system to continue to deliver its services to users in the face of deliberate or accidental attack
- This is an increasingly important attribute for distributed systems whose security can be compromised
- Survivability subsumes the notion of resilience - the ability of a system to continue in operation in spite of component failures

Error tolerance

- Part of a more general usability property and reflects the extent to which user errors are avoided, detected or tolerated.
- User errors should, as far as possible, be detected and corrected automatically and should not be passed on to the system and cause failures.

Dependability attribute dependencies

- Safe system operation depends on the system being available and operating reliably.
- A system may be unreliable because its data has been corrupted by an external attack.
- Denial of service attacks on a system are intended to make it unavailable.
- If a system is infected with a virus, you cannot be confident in its reliability or safety.

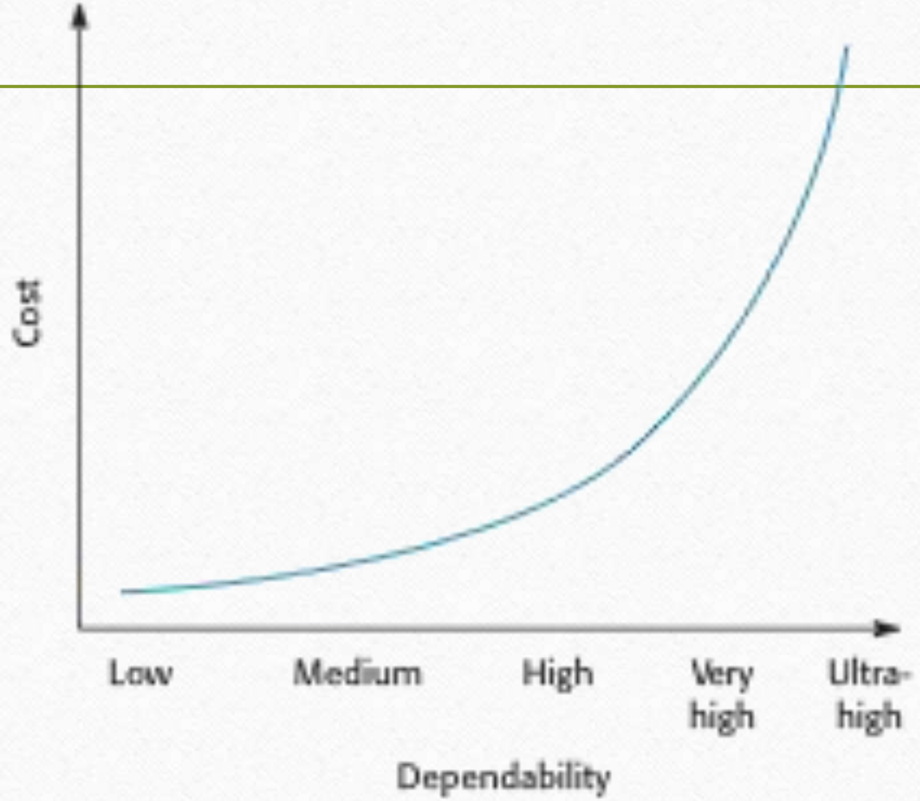
Dependability achievement

- Avoid the introduction of accidental errors when developing the system.
- Design V & V processes that are effective in discovering residual errors in the system.
- Design protection mechanisms that guard against external attacks.
- Configure the system correctly for its operating environment.
- Include recovery mechanisms to help restore normal system service after a failure.

Dependability costs

- Dependability costs tend to increase exponentially as increasing levels of dependability are required.
- There are two reasons for this
  - The use of more expensive development techniques and hardware that are required to achieve the higher levels of dependability.
  - The increased testing and system validation that is required to convince the system client and regulators that the required levels of dependability have been achieved.

Cost/dependability curve



Dependability economics

- Because of very high costs of dependability achievement, it may be more cost effective to accept untrustworthy systems and pay for failure costs
- However, this depends on social and political factors. A reputation for products that can't be trusted may lose future business
- Depends on system type - for business systems in particular, modest levels of dependability may be adequate

Availability and reliability

- Reliability
  - The probability of failure-free system operation over a specified time in a given environment for a given purpose
- Availability
  - The probability that a system, at a point in time, will be operational and able to deliver the requested services
- Both of these attributes can be expressed quantitatively e.g. availability of 0.999 means that the system is up and running for 99.9% of the time.

Availability and reliability

- It is sometimes possible to subsume system availability under system reliability
  - Obviously if a system is unavailable it is not delivering the specified system services.
- However, it is possible to have systems with low reliability that must be available.
  - So long as system failures can be repaired quickly and does not damage data, some system failures may not be a problem.
- Availability is therefore best considered as a separate attribute reflecting whether or not the system can deliver its services.
- Availability takes repair time into account, if the system has to be taken out of service to repair faults.

Perceptions of reliability

- The formal definition of reliability does not always reflect the user's perception of a system's reliability
  - The assumptions that are made about the environment where a system will be used may be incorrect
    - Usage of a system in an office environment is likely to be quite different from usage of the same system in a university environment
  - The consequences of system failures affects the perception of reliability
    - Unreliable windscreen wipers in a car may be irrelevant in a dry climate
    - Failures that have serious consequences (such as an engine breakdown in a car) are given greater weight by users than failures that are inconvenient

Reliability and specifications

- Reliability can only be defined formally with respect to a system specification i.e. a failure is a deviation from a specification.
- However, many specifications are incomplete or incorrect – hence, a system that conforms to its specification may ‘fail’ from the perspective of system users.
- Furthermore, users don’t read specifications so don’t know how the system is supposed to behave.
- Therefore perceived reliability is more important in practice.

Availability perception

- 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 peak usage 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.

Key points

- The dependability in a system reflects the user’s trust in that system.
- Dependability is a term used to describe a set of related ‘non-functional’ system attributes – availability, reliability, safety and security.
- The availability of a system is the probability that it will be available to deliver services when requested.
- The reliability of a system is the probability that system services will be delivered as specified.