

---

# Dependability Requirements

---

November 2004

©Ian Sommerville 2004

Slide 1

## The concept of dependability

---

- For most complex socio-technical systems, the most important system property is the dependability of the system.
- The dependability of a system is a judgement about the user's trust in that system. It reflects the extent of the user's confidence that it will operate as expected and that it will not 'fail' in normal use.
- Usefulness and trustworthiness are not the same thing. A system does not have to be trusted to be useful, so long as the user is aware of the risks.

November 2004

©Ian Sommerville 2004

Slide 2

## Dependability and environment

---

- Dependability is an emergent system property that cannot be predicted until the system has been integrated.
- Emergent properties are unpredictable because of the complexity of the relationships between components and the environment.
- Environmental factors are particularly important for the perception of system dependability.

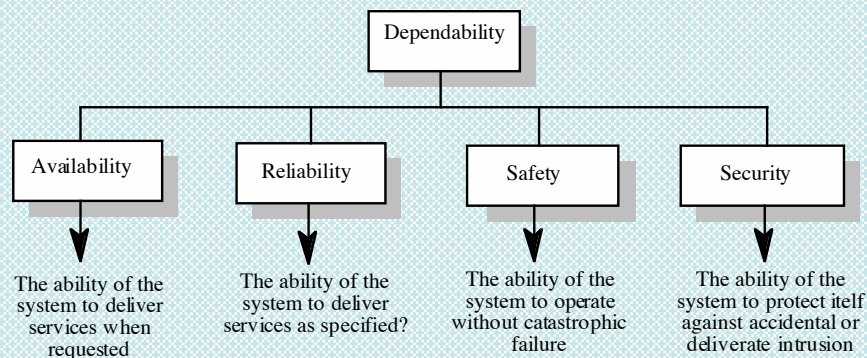
November 2004

©lan Sommerville 2004

Slide 3

## Primary dependability attributes

---



November 2004

©lan Sommerville 2004

Slide 4

## Secondary dependability attributes

---

- **Timeliness**
  - The ability of the system to respond in a timely way to user requests.
- **Survivability**
  - The ability of a system to continue to deliver its services to users in the face of deliberate or accidental attack
- **Recoverability**
  - The ability of the system to recover from user or system errors.
- **Maintainability**
  - The ease of repairing the system after a failure has been discovered or changing the system to include new features.

November 2004

©Ian Sommerville 2004

Slide 5

## Availability

---

- The availability of a system is a measure of whether it can deliver services when requested.
- Used in situations where systems are intended to provide a continuous service.
- High availability is essential for a large class of systems
  - E-commerce systems
  - ISPs
  - Communications systems
- Not meaningful for systems that provide services intermittently. For example, it makes no sense to talk about the availability of Powerpoint.

November 2004

©Ian Sommerville 2004

Slide 6

# Reliability

---

- Intuitively, the reliability of a system is a measure of how often it goes wrong.
- More formally, reliability is the probability of failure free operation in a given environment over a given time.
- Reliability is important in all systems where the costs of system failure are high.
  - Because the actual losses incurred by the user are high.
  - Because the costs of loss of reputation of system vendors is high.
- Reliability is less important where recovery costs are low and recovery can be accomplished quickly.

November 2004

©Ian Sommerville 2004

Slide 7

# Safety

---

- Safety is a property of a system that reflects the system's ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system's environment.
- Safety requirements are often exclusive requirements i.e. they exclude undesirable situations rather than specify required system services. Functional requirements then have to be derived from these.
- More and more systems are safety critical. Not just control systems but also socio-technical systems where the wrong information could result in actions that cause injury.

November 2004

©Ian Sommerville 2004

Slide 8

# Security

---

- The security of a system is a system property that reflects the system's ability to protect itself from accidental or deliberate external attack.
- Security is becoming increasingly important as systems are networked so that external access to the system through the Internet is possible.
- Security requirements are important because security failures may lead to problems of availability, reliability and safety
  - Denial of service attacks - AVAILABILITY
  - Data corruption - RELIABILITY

November 2004

©Ian Sommerville 2004

Slide 9

# Tangled dependability

---

- The primary dependability properties are not independent:
  - Safety may be difficult to achieve if the system does not meet its reliability requirements.
  - Meeting the safety requirements may compromise the availability of the system.
  - Failure of security may compromise availability and reliability of the system.

November 2004

©Ian Sommerville 2004

Slide 10

## Dependability requirements

---

- Exclusion requirements that define undesirable situations that must be excluded by the system.
- System functional requirements that define error checking and recovery facilities and features that provide protection against system failures.
- Non-functional requirements that define the required reliability and availability of the system.

November 2004

©Ian Sommerville 2004

Slide 11

## Exclusion requirements

---

- These are often expressed as 'shall not' requirements. They are usually safety and security related.
  - "The system shall not allow users to modify access permissions on any files that they have not created" (security).
  - "The system shall not allow reverse thrust mode to be selected when the aircraft is in flight" (safety).
  - "The system shall not allow the simultaneous activation of more than three alarm signals" (safety).

November 2004

©Ian Sommerville 2004

Slide 12

## Functional dependability requirements

---

- Requirements that are generated to ensure that the system meets its dependability goals.
- In general, these requirements describe actions that the system should take to detect, avoid and recover from faults or potential system failures.
- These are NOT user requirements but are often generated by system designers in response to user or exclusion requirements.

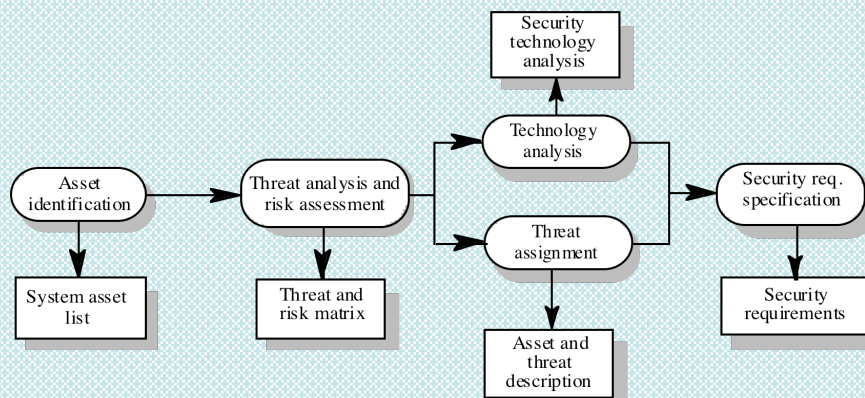
November 2004

©lan Sommerville 2004

Slide 13

## Security requirements

---



November 2004

©lan Sommerville 2004

Slide 14

## Types of security requirement

---

- Identification requirements that specify whether or not a system should identify its users before interacting with them.
- Authentication requirements that specify how users are identified.
- Authorisation requirements that specify the privileges and access permissions of identified users.
- Immunity requirements that specify how a system should protect itself against viruses, worms, etc.
- Integrity requirements that specify how data corruption can be avoided.

November 2004

©Ian Sommerville 2004

Slide 15

## Types of security requirement

---

- Intrusion detection requirements that specify what mechanisms should be used to detect attacks on the system.
- Non-repudiation requirements that specify how a party in a transaction cannot deny their involvement in that transaction.
- Privacy requirements that specify how data privacy is to be maintained.
- Security auditing requirements that specify how system use can be audited and checked.
- System maintenance security requirements that specify how an application can prevent authorised changes from accidentally defeating its security mechanisms.

November 2004

©Ian Sommerville 2004

Slide 16

## Examples of security requirements

---

- SEC1: All system users shall be identified using their library card number and personal password.
- SEC2: Users privileges shall be assigned according to the class of user (student, staff, library staff).
- SEC3: Before execution of any command, LIBSYS shall check that the user has sufficient privileges to access and execute that command.
- SEC4: When a user orders a document, the order request shall be logged. The log data maintained shall include the time of order, the user's identification and the articles ordered.
- SEC5: All system data shall be backed up once per day and backups stored off-site in a secure storage area.
- SEC6: Users shall not be permitted to have more than 1 simultaneous login to LIBSYS.

November 2004

©Ian Sommerville 2004

Slide 17

## Non-functional dependability requirements

---

- Reliability specification
  - Specifies either
    - the probability that the system will fail when a request for a service is made (Probability of failure on demand).
    - the number of failures that are acceptable in a given time period (rate of occurrence of failure).
- Availability specification
  - Specifies the probability that the system will be available to deliver services when a request is made.
  - Therefore, an availability of 0.999 means that the system must be available 99.9% of the time.

November 2004

©Ian Sommerville 2004

Slide 18

## Reliability specification

---

- Probability of failure on demand
  - Used for systems that provide intermittent rather than continuous service. For example, a protection system that is intended to shut down equipment in the event of a power surge.
  - A POFOD of 0.001 means that, on average, 1 in 1000 demands on the system will result in failure.
  - The level of POFOD required depends on the predicted number of demands on the system. If it is expected that there will be no more than 1 demand per year, then a POFOD of 0.001 may be acceptable. If there is 1 demand per hour, then a higher value for POFOD would normally be required.

November 2004

©Ian Sommerville 2004

Slide 19

## Reliability specification

---

- Rate of occurrence of failures
  - Specifies the acceptable number of system failures over a given time period or over a given number of service requests.
    - 2 failures / operational hour
    - 2 failures / 1000 service requests
  - Does not take type of failure into account. Separate values could be produced for serious/non-serious failures.
- Mean time to failure
  - Reciprocal of ROCOF. 2 failures per operational hour gives a MTTF of 30 minutes.
  - MTTF used when a system supports long transactions e.g. a CAD system. The MTTF must be significantly longer than the average transaction length.

November 2004

©Ian Sommerville 2004

Slide 20

## Availability specification

---

- Availability specification of 0.999 means that system must not be unavailable for more than 1.5 minutes in a 24 hour period.
- But we can also meet this availability if the system is unavailable for a 9 hour period over a year.
- The first of these may be acceptable, the second may not.
- The specification also does not take into account periods of degraded service.

November 2004

©Ian Sommerville 2004

Slide 21

## Example

---

- In a railway signalling system, the track is divided into segments. Each segment is controlled by a signal (red, amber, green) and has an associated speed limit.
- An on-board train protection system automatically applies the brakes of a train if the speed limit for a segment of track is exceeded or if the train enters a track segment that is currently signalled with a red light (i.e. the segment should not be entered).
- The speed limit and signal status are transmitted to the train before it enters a controlled segment of track.

November 2004

©Ian Sommerville 2004

Slide 22

## Dependability requirements

---

- What reliability metric should be used to specify the required reliability for this type of system?
- What safety requirements might apply to the system in this case.

November 2004

©Ian Sommerville 2004

Slide 23

## Reliability metric

---

- The most appropriate reliability metric is Probability of Failure on demand (POFOD).
- This is the probability that the system will respond correctly when a request is made for service at a given point in time.
- This metric is used for protection systems where demands for service are intermittent and relatively infrequent over the lifetime of the system.
- In this case, if we assume that there are 100 trains on the network and each has a 0.001% chance of passing a red light, then the probability that some train will pass a red light is 0.1. If the system has a POFOD of 0.001 this means that the probability of some train failing to stop at a red light is 0.0001.

November 2004

©Ian Sommerville 2004

Slide 24

## Safety requirements

---

- The system shall ensure that the train brakes are applied when a 'red signal' is received.
- The system shall sound an alarm in the driver's cabin when a 'red signal' is received.
- The system shall compare the train speed with the segment speed limit once per second.
- If the train speed exceeds the segment speed limit and the train throttle position is not zero then the throttle position should be reset to zero.
- If the train speed exceeds the segment speed limit and the train deceleration is less than the comfortable deceleration limit then the train brakes should be applied.

November 2004

©Ian Sommerville 2004

Slide 25

## Key points

---

- Dependability is a judgement on the trustworthiness of a system.
- Key dependability attributes are:
  - Availability and reliability
  - Safety and security
- Non-functional dependability requirements can define the expected availability and reliability.
- Functional dependability requirements are generated to ensure that a system meets its dependability goals.

November 2004

©Ian Sommerville 2004

Slide 26