Overview of Software Dependability

Er. Rudra Nepal

Nepal College of Information Technology

April 17, 2025

Outline

1. Overview of System Dependability
2. Key Dimensions of Dependability
3. Dependability Achievement and Economics
4. Availability vs Reliability
5. Faults, Errors, and Failures
6. Fault Tolerance and Recovery
7. Safety and Security
8. Comparison: Dependability, Reliability, Safety, Security

What is 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.

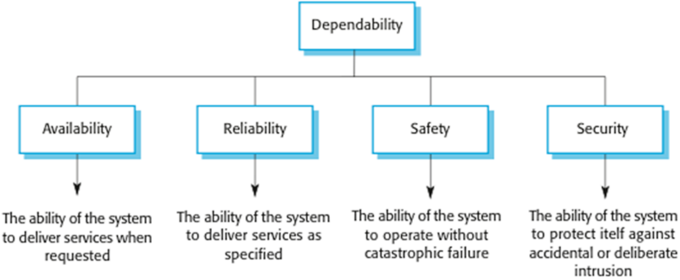
Importance of Dependability

- 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 can fail due to design flaws, manufacturing defects, or simply because the components have worn out over time and reached the end of their useful life.
- **Software failure:** Software may fail because of mistakes in how it's specified, designed, or implemented. These errors can lead to unexpected behavior or complete breakdowns.
- **Operational failure:** These failures happen when people using or operating the system make mistakes. In complex systems, human error is often the biggest cause of failure.

Key Dimensions of Dependability



Dependability
Availability
Reliability
Safety
Security
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 itelf against accidental or deliberate intrusion

Figure: Key Dimensions of Dependability

Principal Dependability Properties

- **Availability:** Probability the system is operational and delivering services.
- **Reliability:** Probability of failure-free operation over a specified period.
- **Safety:** Likelihood the system avoids causing harm to people or the environment.
- **Security:** Ability to resist accidental or deliberate intrusions.

Other Dependability Properties

- **Repairability:** How easily the system can be repaired after failure.
- **Maintainability:** Ease of adapting or repairing the system for new requirements.
- **Survivability:** Ability to deliver services during/after attacks or failures.
- **Error tolerance:** Ability to avoid, detect, and tolerate user errors.

Repairability

- Ability to quickly fix the system after a failure.
- Involves identifying the problem, accessing the failed component, and applying a fix.
- Considered a short-term solution to restore service.
- Difficult to assess before the system is deployed.

Maintainability

- Ease of making long-term changes or repairs to the system.
- Includes fixing bugs and adding new features.
- A highly maintainable system reduces the chance of introducing new faults.
- Critical for systems that undergo frequent updates.

Survivability

- System's ability to keep working during attacks or failures.
- Especially important for distributed systems with security concerns.
- Related to resilience — continuing operation despite component failures.

Error Tolerance

- Describes how well the system handles user mistakes.
- Errors should be detected and corrected automatically.
- Helps prevent user errors from turning into system failures.
- Part of the broader concept of usability.

Dependability Attribute Dependencies

- Safe operation requires availability and reliability.
- Security breaches can undermine reliability and safety.
- Denial-of-service attacks affect availability.
- Virus infections can compromise reliability and safety.

Dependability Achievement

- Avoid accidental errors during development.
- Use effective verification and validation (V&V) processes.
- Implement protection mechanisms against attacks.
- Configure systems correctly for their environment.
- Include recovery mechanisms for restoring service after failure.

Dependability Costs and Economics

- 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.

Dependability costs

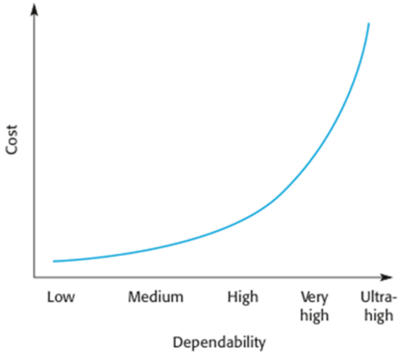


Figure: Cost/dependability curve

Dependability Economics

- Achieving high dependability can be very expensive.
- Sometimes, it's more cost-effective to accept some failures and cover the cost of fixing them.
- However, this approach depends on social and political factors.
- Poor dependability may hurt a company's reputation and future business.
- The required level of dependability also depends on the type of system:
    - For many business systems, moderate dependability may be sufficient.

Availability vs Reliability

- **Reliability:** Probability of failure-free operation over a period.
- **Availability:** Probability the system is operational at a specific time.
- Availability considers repair time; quick repairs can keep availability high even if reliability is low.
- Both can be expressed quantitatively (e.g., 99.9% uptime).

Perceptions of Reliability and Availability

- User perception may differ from formal definitions.
- Environment and consequences of failure affect perception.
- Availability as a percentage does not account for number of users or length of outages.

Faults, Errors, and Failures

- **Human error:** Mistake introducing a fault.
- **System fault:** Defect that can lead to an error.
- **System error:** Erroneous state that can cause unexpected behavior.
- **System failure:** System does not deliver expected service.
- Not all faults cause errors, not all errors cause failures.

Fault Tolerance and Recovery Techniques

- **Fault avoidance:** Minimize introduction of faults during development.
- **Fault detection and removal:** Use V&V to find and correct errors.
- **Fault tolerance:** Run-time techniques to prevent faults from causing errors/failures.
- **Recovery:** Restore normal service after failure (repairability, maintainability, survivability).

Safety and Safety-Critical Systems

- **Safety:** Ability to operate without causing harm.
- **Primary safety-critical:** Failure can directly threaten people (e.g., insulin pump).
- **Secondary safety-critical:** Failure leads to faults in other systems with safety consequences.
- Safety requirements often exclude undesirable situations.

Safety vs Reliability

- Reliability and availability are necessary but not sufficient for safety.
- Reliability: Conformance to specification.
- Safety: Avoidance of harm, even if specification is followed.
- Specification errors or rare faults can make a reliable system unsafe.

Security Concepts

- **Security:** Ability to protect against accidental/deliberate attacks.
- Essential for networked systems.
- Prerequisite for availability, reliability, and safety.
- Insecure systems undermine dependability.

Security Terminology

- **Asset:** Valuable item to be protected (e.g., data).
- **Exposure:** Possible loss/harm (e.g., data loss).
- **Vulnerability:** Weakness that can be exploited.
- **Attack:** Exploitation of a vulnerability.
- **Threat:** Potential cause of loss/harm.
- **Control:** Measure to reduce vulnerability (e.g., encryption).

Threat Classes and Damage from Insecurity

- **Confidentiality:** Unauthorized disclosure of information.
- **Integrity:** Unauthorized modification of software/data.
- **Availability:** Restriction of access for authorized users.
- **Damage:** Denial of service, data corruption, information disclosure.

Security Assurance

- **Vulnerability avoidance:** Design to prevent vulnerabilities.
- **Attack detection and elimination:** Detect and neutralize attacks.
- **Exposure limitation and recovery:** Minimize consequences of successful attacks.

Dependability vs Reliability vs Safety vs Security

Attribute	Focus	Key Points
Dependability	User trust (umbrella term)	Includes availability, reliability, safety, security, repairability, maintainability, etc.
Reliability	Consistent, failure-free service	Necessary but not sufficient for safety; can be formally measured, user perception matters
Safety	Avoidance of harm	May require more than reliability; specification errors can lead to unsafe but ”reliable” systems
Security	Protection from threats	Prerequisite for reliability and safety; an insecure system cannot be considered

Key Points Summary

- Dependability reflects user trust in the system.
- It is achieved through avoidance, detection, and tolerance of faults.
- Security is foundational; without it, other dependability attributes are undermined.
- Balancing cost and required dependability is essential for system design.