Critical Systems

Dong-Ah Lee

Objectives

- To explain what is meant by a critical system where system failure can have severe human or economic consequence.

- To explain four dimensions of dependability - availability, reliability, safety and security.

- To explain that, to achieve dependability, you need to avoid mistakes, detect and remove errors and limit damage caused by failure.

Topics covered

- A simple safety-critical system

- System dependability

- Availability and reliability

- Safety

- Security

Critical Systems

- Safety-critical systems

    - Failure results in loss of life, injury or damage to the environment;

    - Chemical plant protection system;

- Mission-critical systems

    - Failure results in failure of some goal-directed activity;

    - Spacecraft navigation system;

- Business-critical systems

    - Failure results in high economic losses;

    - Customer accounting system in a bank;

System dependability

- For **critical systems**, it is usually the case that **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.

- Usefulness and trustworthiness are not the same thing. A system does not have to be trusted to be useful.

Importance of dependability

- 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**.

- Undependable systems may cause information loss with a high consequent recovery cost.

Development methods for critical systems

- The costs of critical system failure are so high that development methods may be used that are not cost-effective for other types of system.

- Examples of development methods

    – Formal methods of software development

    – Static analysis

    – External quality assurance

Socio-technical critical systems

- 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.
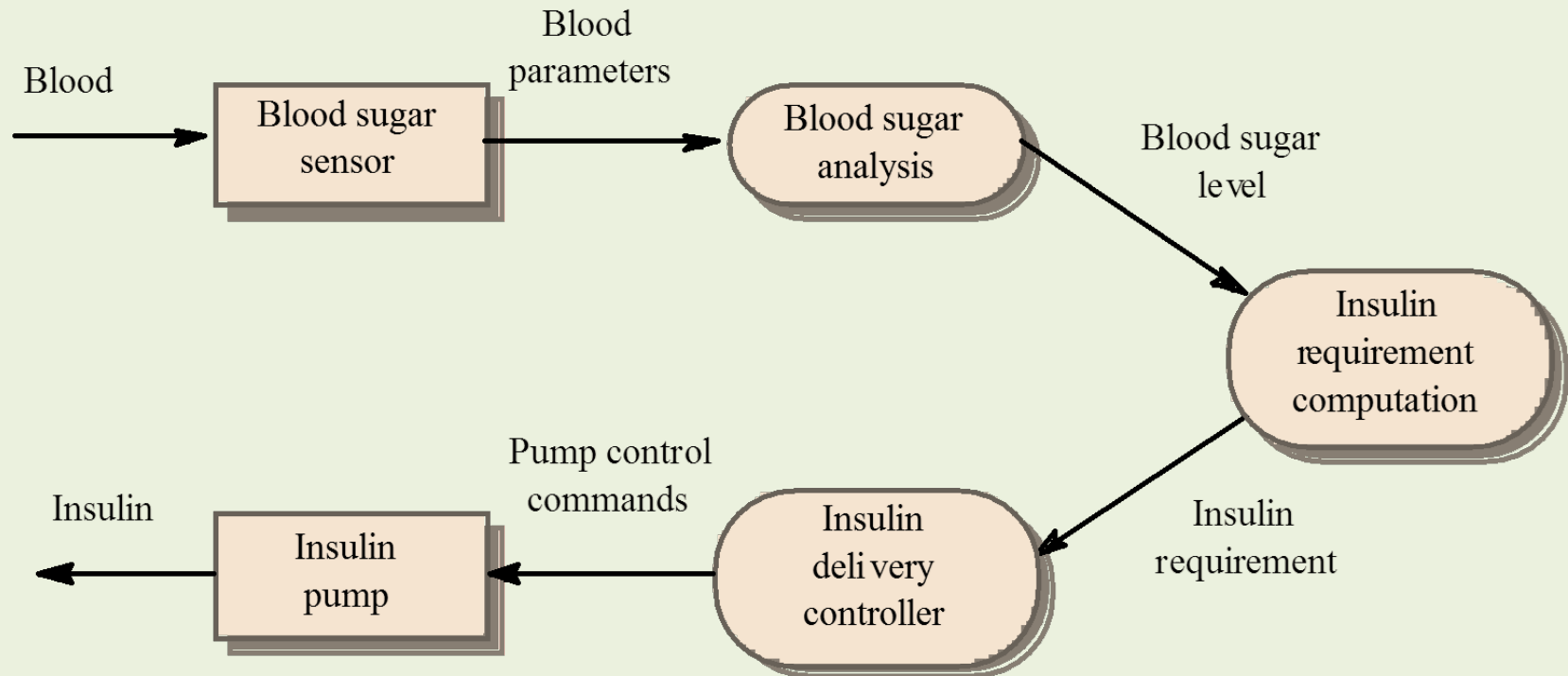
A software-controlled insulin pump

- Used by diabetics to simulate the function of the pancreas which manufactures insulin, an essential hormone that metabolises blood glucose.

- Measures blood glucose (sugar) using a micro-sensor and computes the insulin dose required to metabolise the glucose.

Insulin pump organisation
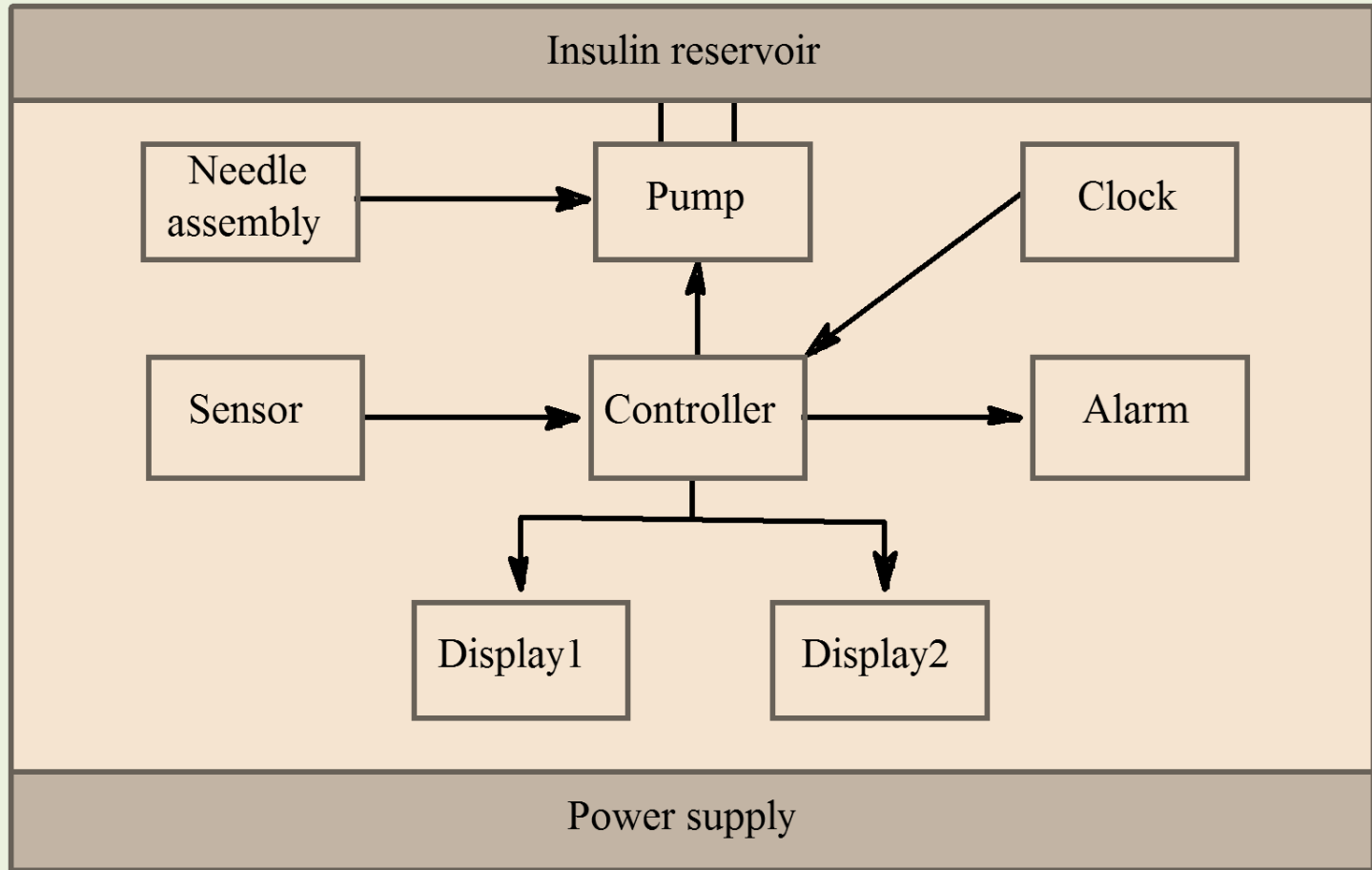
Insulin pump data-flow

Dependability requirements

- The system shall be available to deliver insulin when required to do so.

- The system shall perform reliability and deliver the correct amount of insulin to counteract the current level of blood sugar.

- The essential safety requirement is that excessive doses of insulin should never be delivered as this is potentially life threatening.

Dependability

- The dependability of a system equates to its trustworthiness.

- A dependable system is a system that is trusted by its users.

- Principal dimensions of dependability are:

  - Availability;

  - Reliability;

  - Safety;

  - Security

Dimensions of dependability
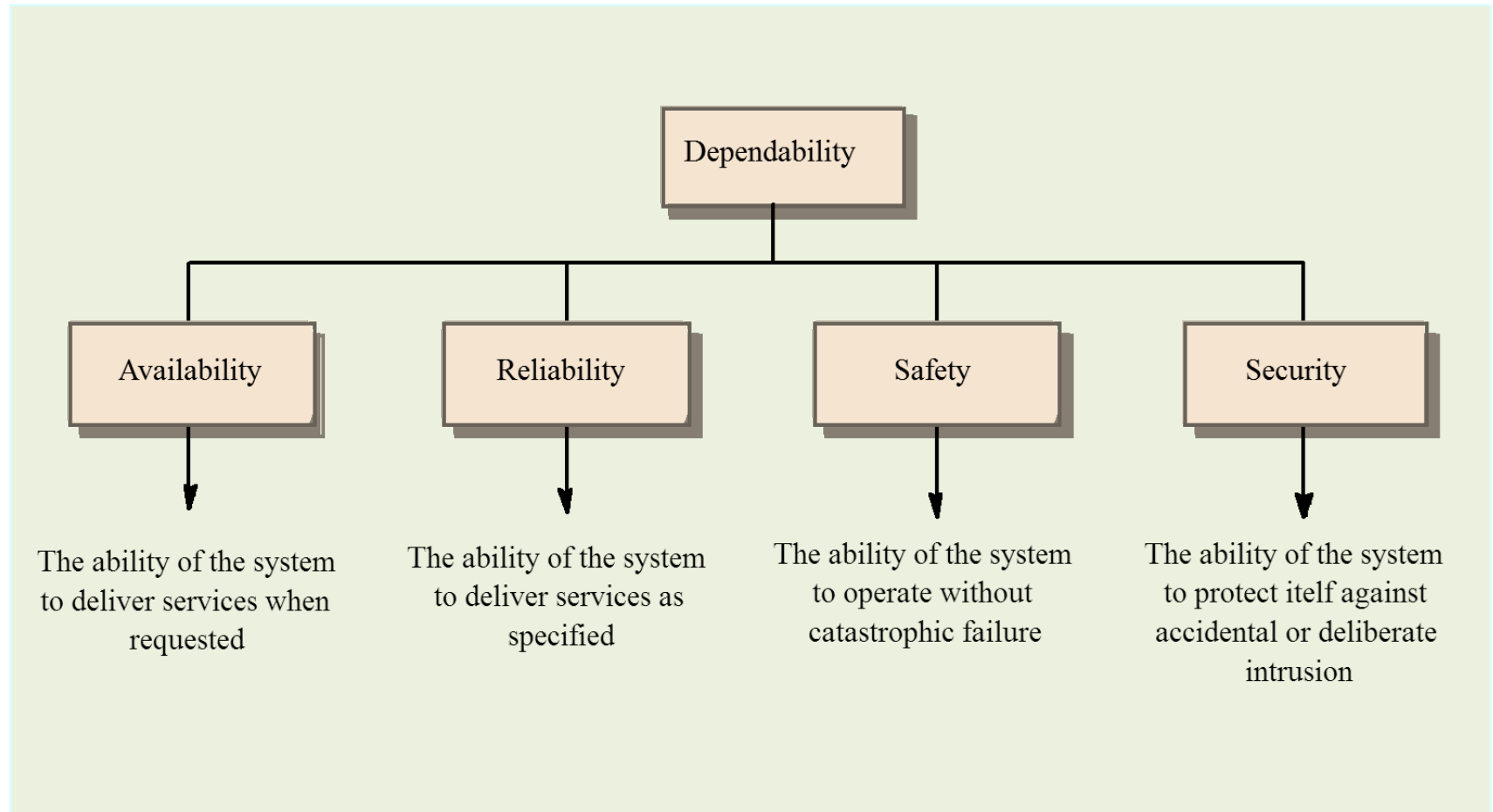
Other dependability properties

- 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.

Dependability vs performance

- Untrustworthy systems may be rejected by their users

- System failure costs may be very high

- It is very difficult to tune systems to make them more dependable

- It may be possible to compensate for poor performance

- Untrustworthy systems may cause loss of valuable information

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 that the required levels of dependability have been achieved

Costs of increasing dependability
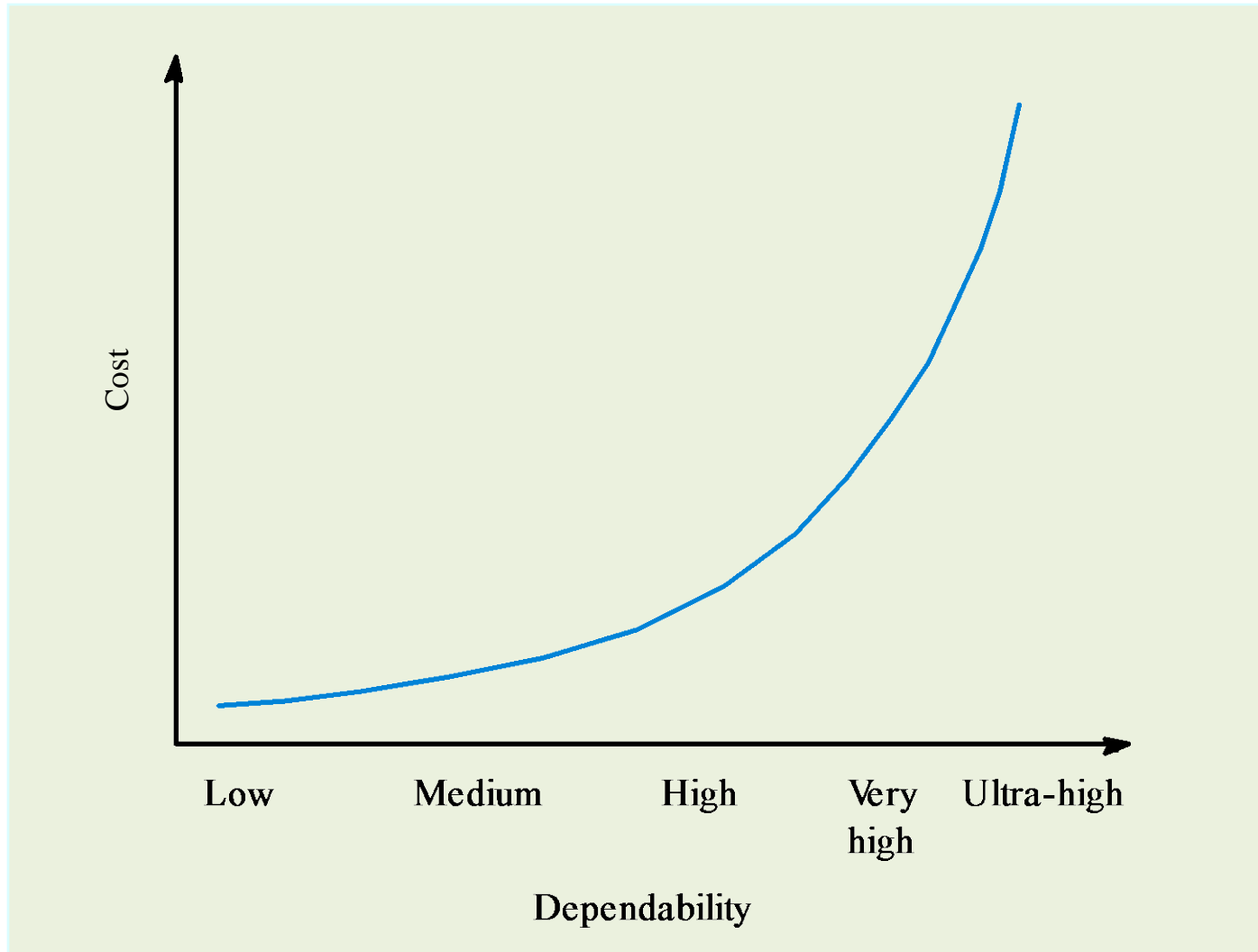
Dependability economics

- 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

Reliability terminology

Term	Description
System failure	An event that occurs at some point in time when the system does not deliver a service as expected by its users
System error	An erroneous system state that can lead to system behaviour that is unexpected by system users.
System fault	A characteristic of a software system that can lead to a system error. For example, failure to initialise a variable could lead to that variable having the wrong value when it is used.
Human error or mistake	Human behaviour that results in the introduction of faults into a system.

Faults and failures

- Failures are a usually a result of system errors that are derived from faults in the system

- However, faults do not necessarily result in system errors

  - The faulty system state may be transient and 'corrected' before an error arises

- Errors do not necessarily lead to system failures

  - The error can be corrected by built-in error detection and recovery

  - The failure can be protected against by built-in protection facilities. These may, for example, protect system resources from system errors

Reliability achievement

- Fault avoidance

  – Development technique are used that either minimize the possibility of mistakes or trap mistakes before they result in the introduction of system faults

- Fault detection and removal

  – Verification and validation techniques that increase the probability of detecting and correcting errors before the system goes into service are used

- Fault tolerance

  – Run-time techniques are used to ensure that system faults do not result in system errors and/or that system errors do not lead to system failures

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

- It is increasingly important to consider software safety as more and more devices incorporate software-based control systems

- Safety requirements are exclusive requirements i.e. they exclude undesirable situations rather than specify required system services

Safety and reliability

- Safety and reliability are related but distinct

  - In general, reliability and availability are necessary but not sufficient conditions for system safety

- Reliability is concerned with conformance to a given specification and delivery of service

- Safety is concerned with ensuring system cannot cause damage irrespective of whether or not it conforms to its specification

Safety terminology

Term	Definition
Accident (or mishap)	An unplanned event or sequence of events which results in human death or injury, damage to property or to the environment. A computer-controlled machine injuring its operator is an example of an accident.
Hazard	A condition with the potential for causing or contributing to an accident. A failure of the sensor that detects an obstacle in front of a machine is an example of a hazard.
Damage	A measure of the loss resulting from a mishap. Damage can range from many people killed as a result of an accident to minor injury or property damage.
Hazard severity	An assessment of the worst possible damage that could result from a particular hazard. Hazard severity can range from catastrophic where many people are killed to minor where only minor damage results.
Hazard probability	The probability of the events occurring which create a hazard. Probability values tend to be arbitrary but range from *probable* (say 1/100 chance of a hazard occurring) to implausible (no conceivable situations are likely where the hazard could occur).
Risk	This is a measure of the probability that the system will cause an accident. The risk is assessed by considering the hazard probability, the hazard severity and the probability that a hazard will result in an accident.

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 minimise the damage that may result from an accident

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 is an essential pre-requisite for availability, reliability and safety

Fundamental security

- If a system is a networked system and is insecure then statements about its reliability and its safety are unreliable

- These statements depend on the executing system and the developed system being the same. However, intrusion can change the executing system and/or its data

- Therefore, the reliability and safety assurance is no longer valid

Security terminology

Term	Definition
Exposure	Possible loss or harm in a computing system. This can be loss or damage to data or can be a loss of time and effort if recovery is necessary after a security breach.
Vulnerability	A weakness in a computer-based system that may be exploited to cause loss or harm.
Attack	An exploitation of a system vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
Threats	Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
Control	A protective measure that reduces a system vulnerability. Encryption would be an example of a control that reduced a vulnerability of a weak access control system.

DEPENDABLE SOFTWARE LABORATORY

KU KONKUK UNIVERSITY

Security assurance

- Vulnerability avoidance

  - The system is designed so that vulnerabilities do not occur. For example, if there is no external network connection then external attack is impossible

- Attack detection and elimination

  - The system is designed so that attacks on vulnerabilities are detected and neutralized before they result in an exposure. For example, virus checkers find and remove viruses before they infect a system

- Exposure limitation

  - The system is designed so that the adverse consequences of a successful attack are minimized. For example, a backup policy allows damaged information to be restored

Key points

- A critical system is a system where failure can lead to high economic loss, physical damage or threats to life.

- The dependability in a system reflects the user's trust in that system

- 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

- Safety is a system attribute that reflects the system's ability to operate without threatening people or the environment

- Security is a system attribute that reflects the system's ability to protect itself from external attack