Critical System

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 damage caused by failure

Topic covered

- A Simple safety – critical system
- System dependability
- Availability and reliability
- Safety
- Security

Critical Systems

▶ 시스템의 고장(failure)은 비교적 일반적

✓ " 대부분의 경우 고장은 불편하지만 심각한 손해를 입히지 않는다."

▶ Critical System (중대한 시스템 / 중요한 시스템)

✓ "어떤 시스템 고장은 중요한 경제적 손실과, 물질적 피해, 혹은 사람의 생명에 위협이 될 수 있다."

▶ Critical system의 유형

✓ Safety-critical system

- 시스템의 고장으로 인해 부상을 당하거나, 생명을 잃거나, 심각한 결과를 초래
- 예) 화학공장의 제어 시스템, 제초기

✓ Mission-critical system

- 시스템의 고장으로 인해 임무 수행의 활동을 실패
- 예) 화성 탐사 로봇, 무인주차시스템, 무인주행시스템

✓ Business-critical system

- 시스템 고장으로 인해 시스템을 사용하는 사업에 대한 높은 비용을 지불
- 예) 은행의 고객 계정 시스템

System Dependability

▶ Critical system의 중요한 특징

- ✓ Dependability (신뢰성 / 확실성)

▶ Dependability가 critical system에서 가장 중요한 이유

- ✓ 시스템의 신뢰가치(trustworthiness)가 떨어지는 경우 정보의 손실 발생
- ✓ 시스템의 **신뢰성과 보안성이 떨어진다면**, 당신은 그 시스템을 **사용할 수 있겠는가?**

▶ 시스템의 고장으로 인해, 그것을 수리하는 비용이 매우 큼

- ✓ 예) 원자로 시스템, 항공 관제 시스템

▶ Usefulness and Trustworthiness are not the same thing

- ✓ "유용성이 높다고 해서 신뢰성이 높다고 할 수 없다."
- ✓ "신뢰성 높은 critical system은 비용이 많이 든다."

Socio-technical critical systems

▶ Socio-technical critical systems의 특징

✓ 대부분 사람이 감시하고 제어하는 사회 기술 기반 중대한 시스템

- 고장 시 예상치 못한 상황을 복구 할 수 있는 관리자가 필요
- 시스템 운영자는 문제를 복구 할 수 있지만, 문제를 더 일으킬 수 있음

▶ Critical system에서 고장이 일어 날 수 있는 경우 세가지

✓ Hardware failure

- 설계상의 실수, 부속품의 오류, 하드웨어의 수명

✓ Software failure

- 분석, 설계 혹은 구현시의 오류 가능성

✓ Operational failure (가장 큰 문제)

- 운영자의 실수에 의한 오류 가능성

Case study: A software-controlled insulin pump(1/3)

▶ Critical system의 사례연구

✓ **당뇨병**: 췌장이 인슐린을 충분히 생산하지 못기 때문에 생기는 질환

- **저혈당**: 뇌기능 약화
- **고혈당**: 시력 손상, 신장, 심장 기능 약화

▶ 당뇨병에 대한 치료 -> 인슐린을 규칙적으로 투여

✓ 환자의 피 속에 있는 혈당 수치를 측정-> 투여될 인슐린의 양 결정

▶ 소형 센서 기기의 발달로 자동 인슐린 투여 Critical system 개발

✓ 혈당 수치를 측정하여 적당한 양의 인슐린을 투여

✓ 향후 사람의 몸에 영구적으로 내장시킬 수 있는 장비 개발 가능

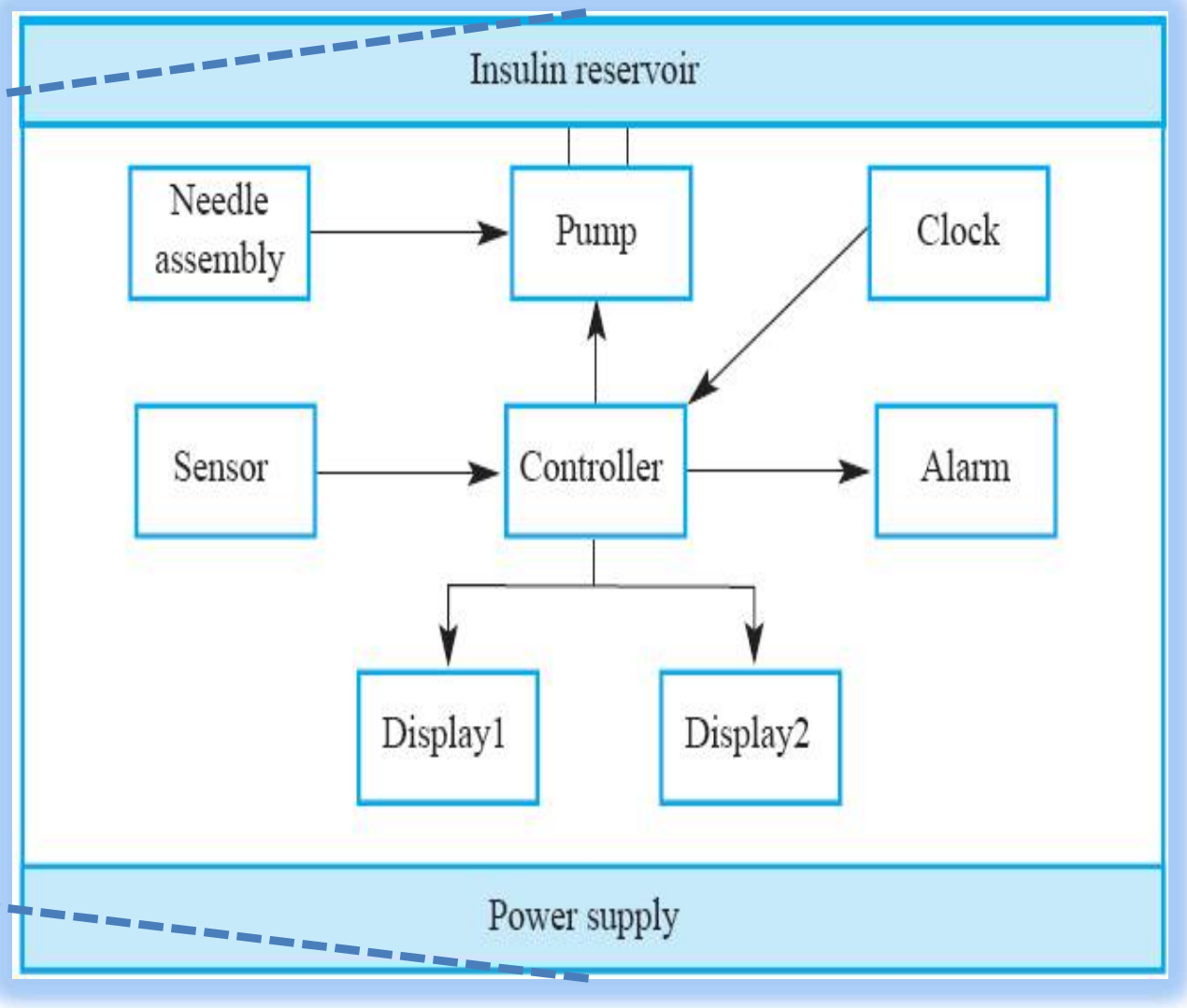
▶ 인슐린 펌프 시스템에 필요한 dependability 는 무엇인가?

✓ **Availability(가용성):** 인슐린이 필요한 시기에 인슐린 공급

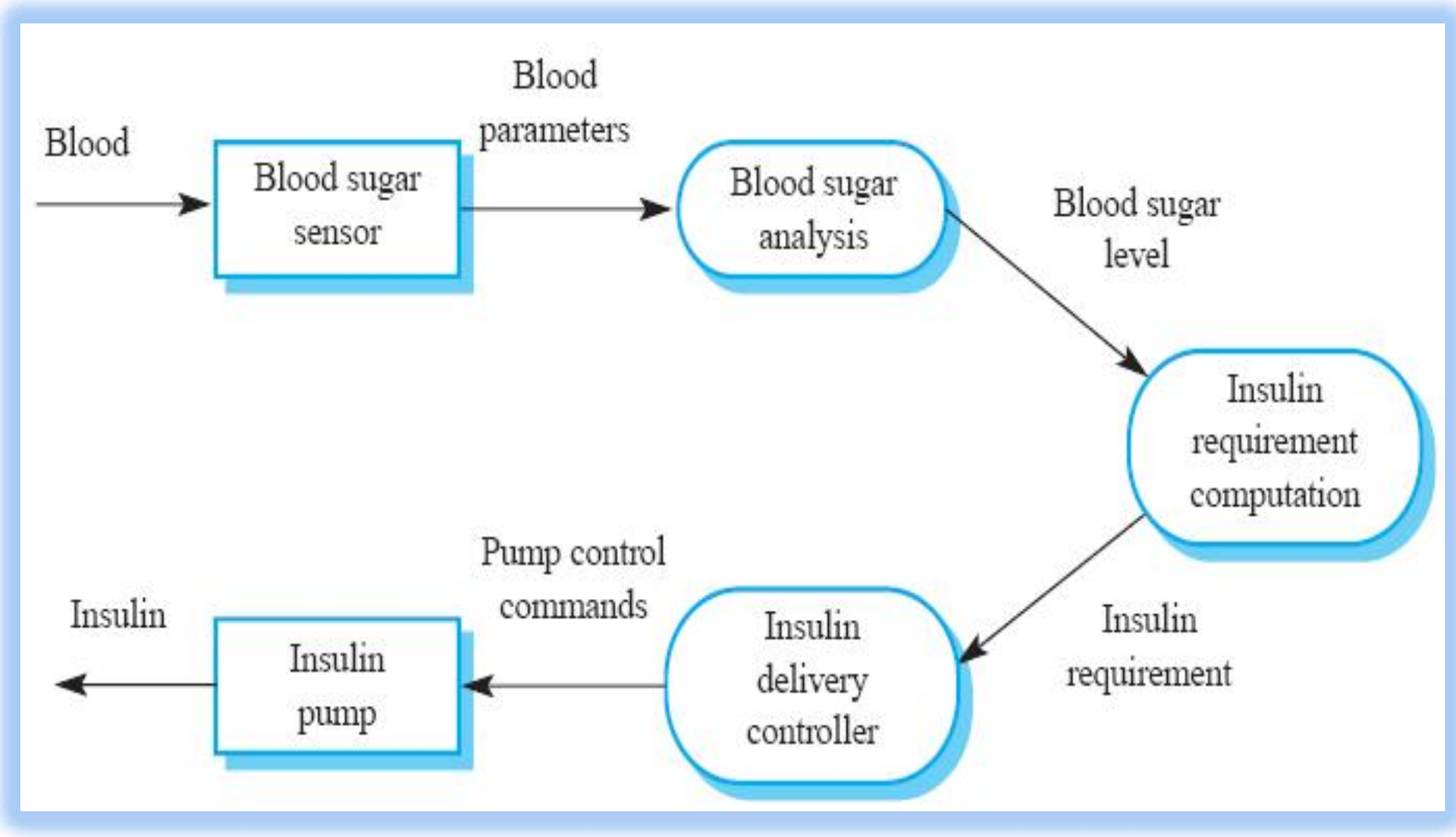
✓ **Reliability(신뢰성):** 혈당 수치에 따라 적당한 양의 인슐린을 투여

✓ **Safety(안정성):** 과다한 인슐린을 투여하면 안됨

Case study: A software-controlled insulin pump(2/3)

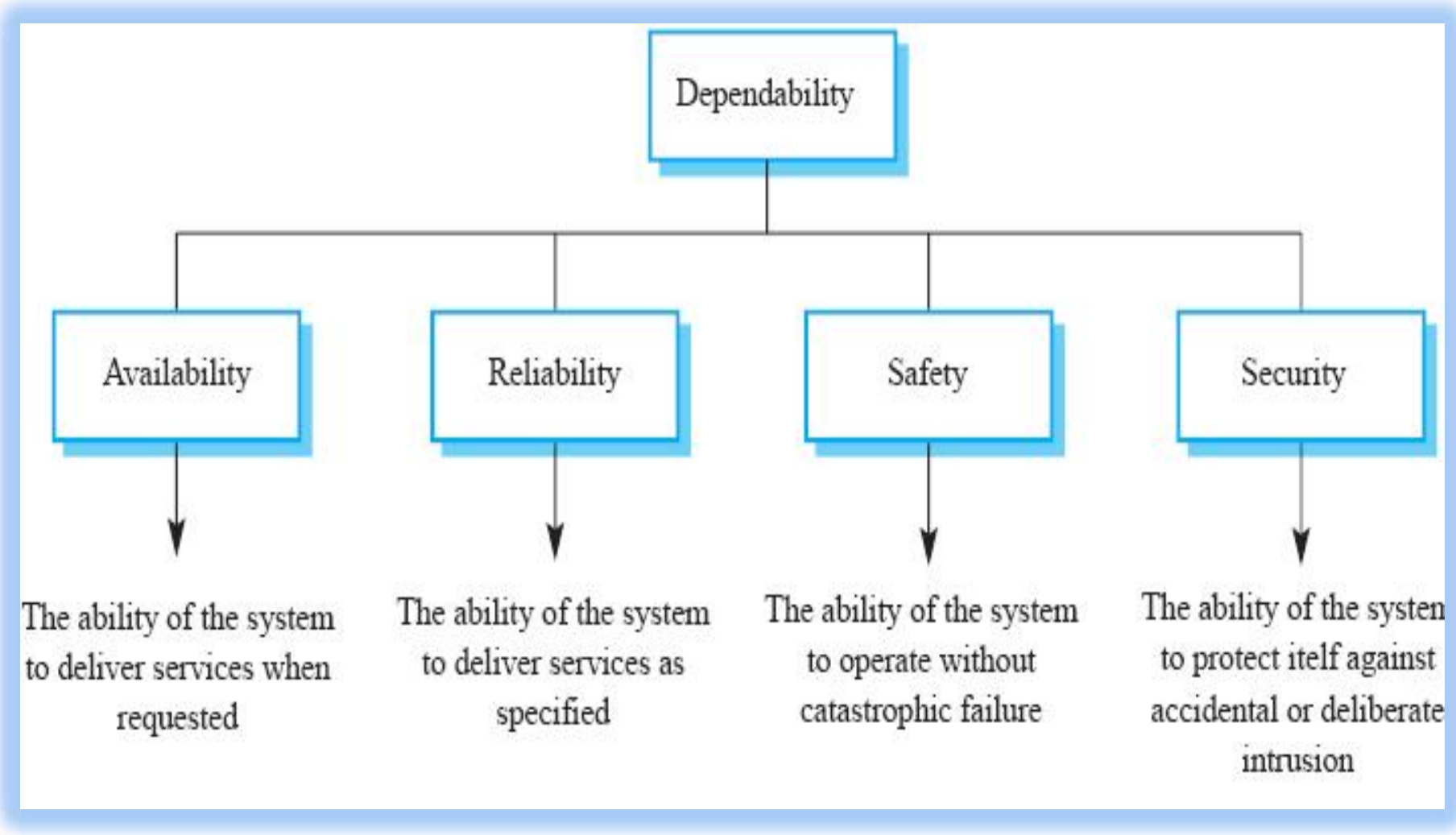


Case study: A software-controlled insulin pump(3/3)



Dimensions of Dependability

► Dependability의 네가지 영역



Dimensions of dependability

► Availability(가용성)

✓ 어느 때라도 서비스를 제공 또는 사용 할 수 있는 확률

► Reliability(신뢰성)

✓ 주어진 시스템 명세대로 서비스를 제공 또는 사용 할 수 있는 확률

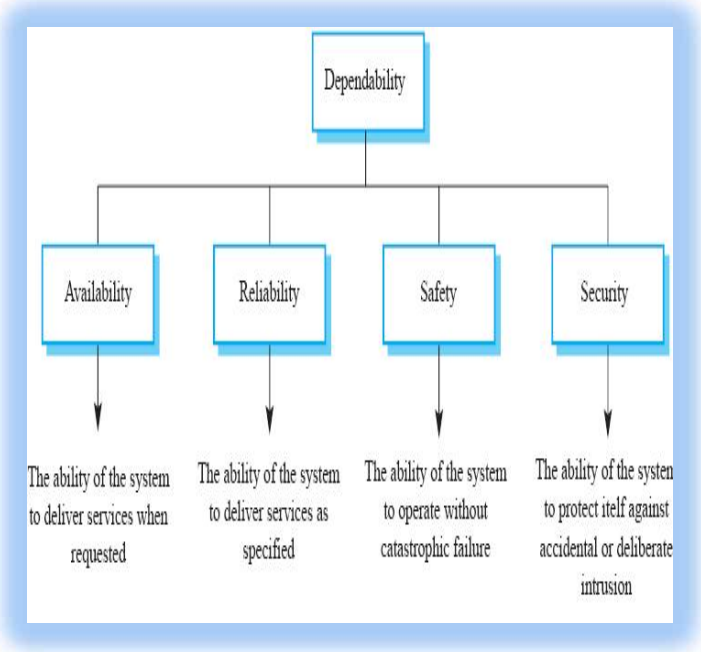
► Safety(안정성)

✓ 사람 또는 환경에 손상을 입히지 않을 확률

► Security(보안성)

✓ 사고 혹은 의도적인 침입을 막을 수 있는 확률

- 무결성 (프로그램과 데이터 미손상)
- 비밀성 (권한자만 정보 접근 가능)



Other dependability properties

► Repairability (수리가능성)

- ✓ Reflects the extent to which the system can be repaired in the event of a failure

► Maintainability (유지보수성)

- ✓ Reflects the extent to which the system can be adapted to new requirements

► Survivability (생존가능성)

- ✓ Reflects the extent to which the system can deliver services whilst under hostile attack

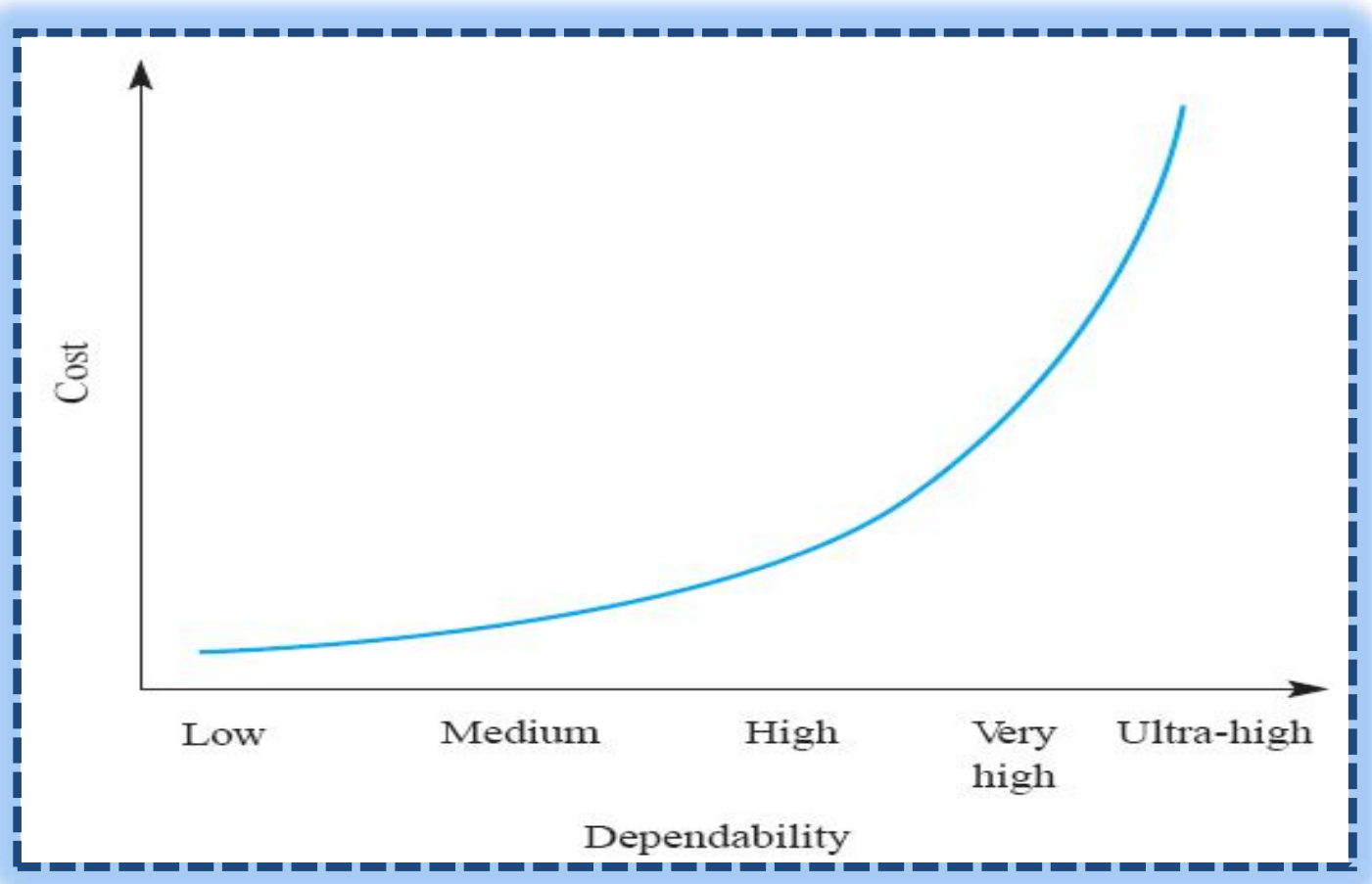
► Error tolerance (오류내성)

- ✓ Reflects the extent to which user input errors can be avoided and tolerated

Costs of increasing dependability

► Costs of increasing dependability

- ✓ 예외적인 상태, 고장 복구에 대한 검사코드의 중복 또는 추가코드가 포함
- ✓ 성능 약화 및 소프트웨어 저장장치 비용증가, 개발 비용 증가
- ✓ 시스템의 성능과 dependability 사이의 trade-off 존재



Dependability economics

- ▶ Dependability가 높은 시스템은 성능이 떨어질 가능성이 높음
- ▶ 시스템 내부에 중복된 작업이 많이 있을 수 있음
- ▶ 시스템 코드가 추가적으로 늘어날 가능성이 큼
- ▶ 높은 기술 개발 비용
- ▶ 높은 테스트 비용

"비용이 많이 들지만, 사회적인 요구에 따라 향후 비즈니스에 치명적인 오류가 있다면 dependability 를 지원하는 기술을 개발해야 하는 필요가 있다."

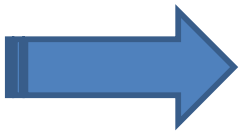
Reliability terminology

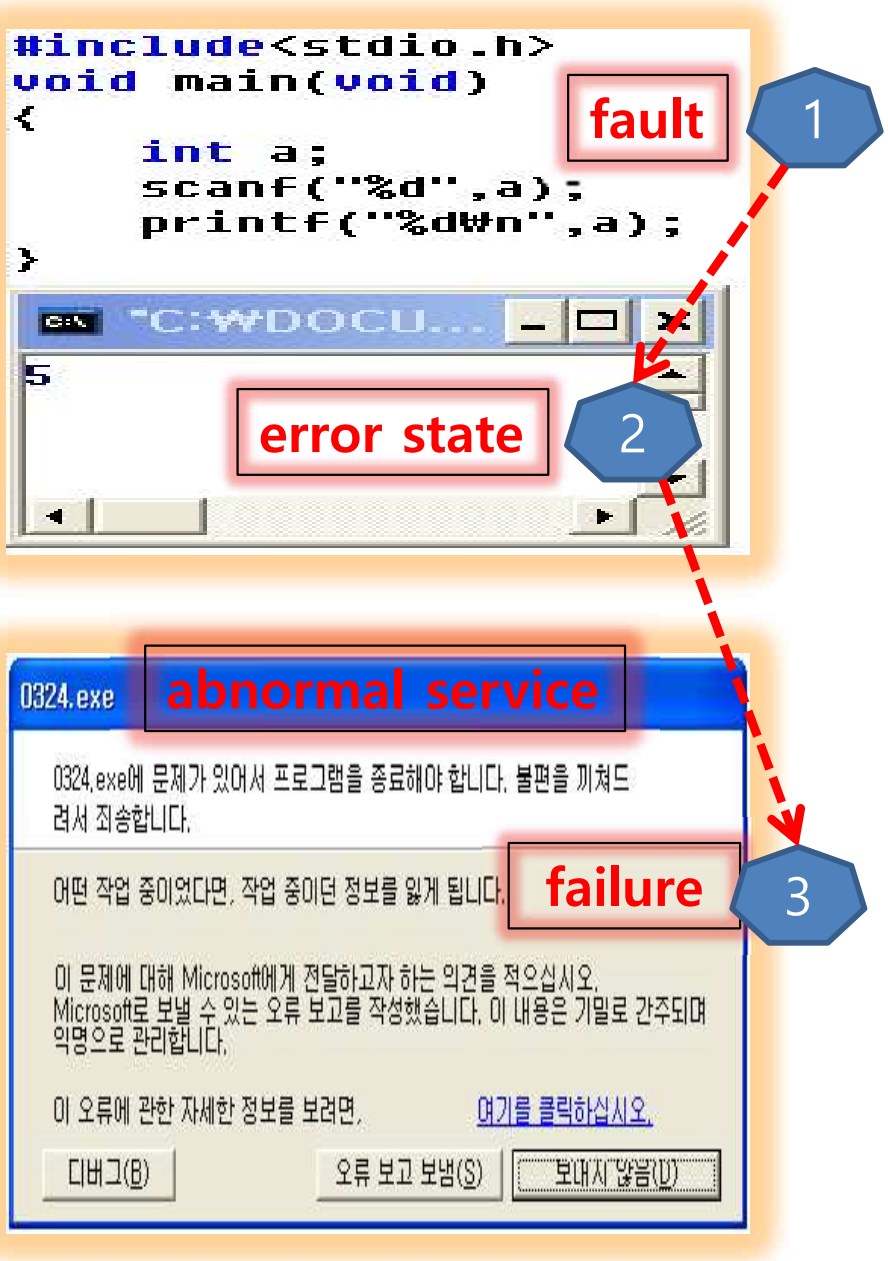
	Term	Description
3	System failure	An event that occurs at some point in time when the system does not deliver a service as expected by its users
2	System error	An erroneous system state that can lead to system behaviour that is unexpected by system users.
1	System fault	A characteristic of a software 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.

Fault, Error and Failure

normal service

```
#include<stdio.h>
void main(void)
{
    int a;
    scanf("%d",&a);
    printf("%d₩n",a);
}
```





Reliability Terminology

▶ 신뢰성관련 용어

✓ 시스템 고장 (system failure)
- 사용자가 기대하는 서비스를 제공하지 못하는 상태

✓ 시스템 오류 (system error)
- 사용자가 예기치 못한 시스템 행동으로 이끄는 상태

✓ 시스템 결함 (system fault)
- 시스템 오류를 이끄는 소프트웨어 특성
- 예) 변수 초기화 실패

✓ 사람의 실수/오류 (human error or mistake)
- 운영자에 의해서 시스템 결함에 이르게 하는 행동

Reliability Achievement

▶ 신뢰성을 이루기 위한 기술

✓ Fault avoidance (결함 회피)

- 시스템 결함 발생 전에, 실수를 할 가능성을 최소화
- 예) 포인터, 정적 분석 (Static analysis)

✓ Fault detection and removal (결함 탐지와 제거)

- 시스템 사용 전, 시스템의 결함을 제거하는 확인과 검증 기술 사용
- 예) 테스트와 디버깅을 통한 시스템 결함 발견

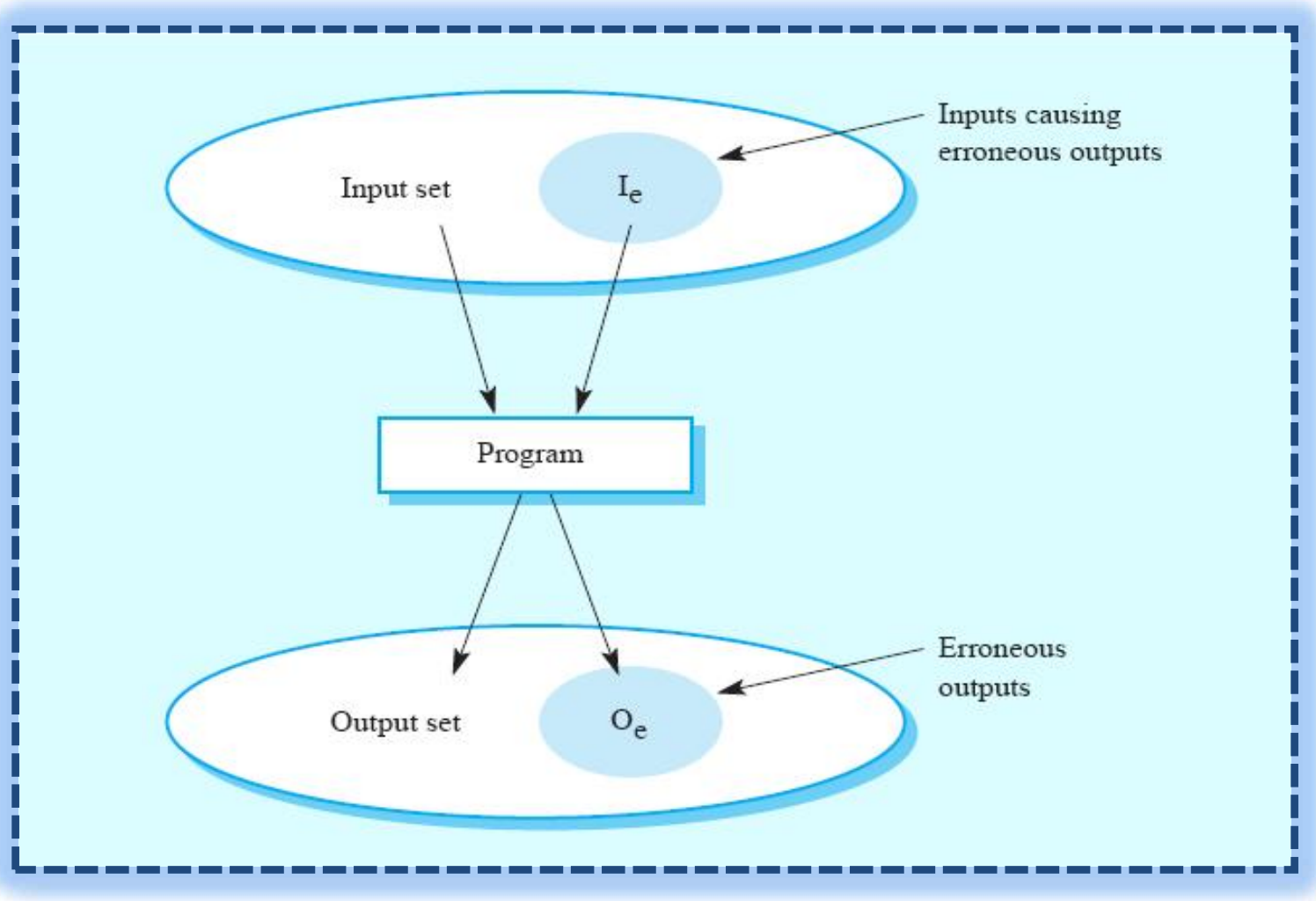
✓ Fault tolerance (결함 내성)

- 시스템에 존재하는 결함이 시스템 오류를 일으키지 않도록 함
- 시스템의 오류가 시스템 고장이 되지 않도록 하는 것
- 예) 시스템 자체 점검기능, 중복시스템 모듈 통합 기술

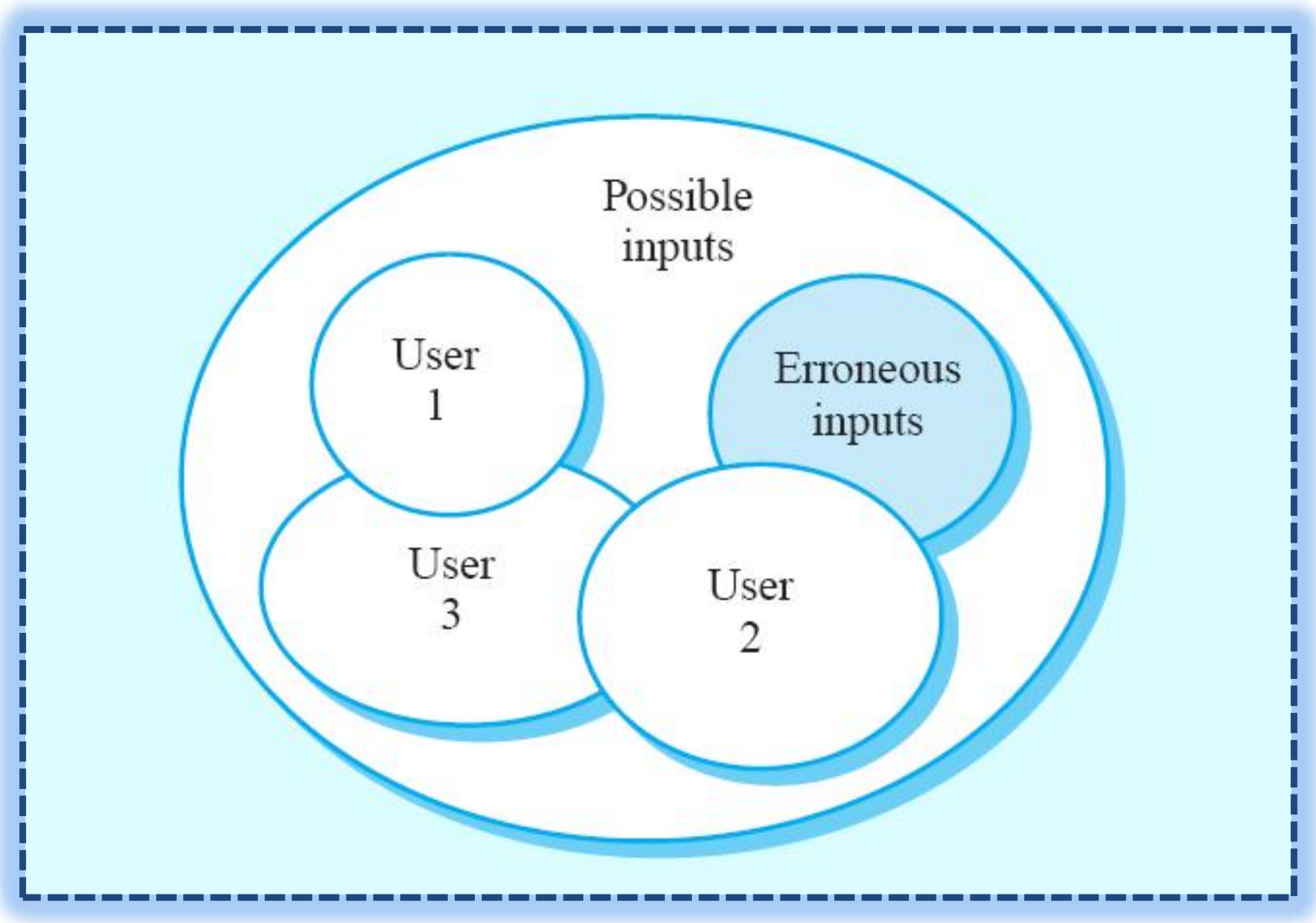
Reliability Modeling

► Input–output mapping

- ✓ 주어진 입력들에 대하여 해당하는 산출물(출력)들을 생산
- ✓ 어떤 입력들은 잘못된 산출물(출력)들을 생산



Reliability perception



Reliability Improvement

- Removing x% of the faults in a system will not necessarily improve the reliability by x%
- A study at IBM showed that removing 60% of product defects results in a 3% improvement in reliability
- A program with known faults may therefore still be seen as reliable by its users

Safety

▶ 안전성은 위험요소들의 작용 없이 시스템을 정상 동작하게 하는 것

✓ 예) 항공관제시스템, 화학공장, 제약공장

✓ Primary safety-critical systems (일차적인 안전성 중심 시스템)

- 시스템에 내장된 결함 소프트웨어의 동작이 하드웨어의 비정상적 문제를 유발
- 인간의 부상, 환경손상

✓ Secondary safety-critical systems (이차적인 안전성 중심 시스템)

- 소프트웨어 설계의 결함으로 간접적으로 손상을 가함
- 예) 환자의 처방 내용을 담고 있는 의료DB의 오류는 약의 오용 유발

✓ Safety terminology

- Hazard (위험), Accident (사고), Damage (손실)
- Hazard severity (위험의 정도), Hazard probability (위험의 확률)
- Risk (위험도)

Safety achievement

▶ Hazard avoidance (위험 회피 기술)

✓ The system is designed so that some hazard cannot arise

- Ex) Cutting system with two separate button

▶ Hazard detection and removal (위험 탐지 및 제거 기술)

✓ The system is designed so that hazards are detected and removed before they result in an accident

- Ex) Chemical plant system detects excessive pressure and opens a relief valve

▶ Damage limitation (피해 최소화 기술)

✓ The system includes protection features that minimize the damage that may result from an accident

- Ex) Aircraft engine including automatic fire extinguishers

Security

▶ 의도적, 비의도적 사고에 대한 외부의 공격에 방어하는 속성

▶ 외부의 공격에 의해 유발되는 피해

✓ Denial of service (서비스 거부)

- 정상적인 서비스를 못하게 함
- 가용성 (availability)에 영향을 미침

✓ Corruption of programs or data (프로그램이나 데이터의 손실)

- 프로그램이나 데이터의 무단 수정
- 신뢰성(reliability) 와 안정성(Safety)에 영향을 미침

✓ Disclosure of confidential information (비밀 정보의 노출)

- 비밀 정보가 외부의 공격에 의해 노출
- 안정성에 영향을 미치고 추후 신뢰성과 가용성에 영향을 미침

Security Terminology

- ▶ Exposure(노출)
- ▶ Vulnerability(취약성)
- ▶ Attack(공격성)
- ▶ Threats(위협)
- ▶ Control(통제)

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 sys tem 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.

Problems from insecurity

- ▶ Denial of Service
- ▶ Corruption of Program or Data
- ▶ Disclosure of Confidential Information

Security achievement

- ▶ Vulnerability avoidance (취약성 회피 기술)
- ▶ Attack detection and elimination (공격 탐지 및 제거 기술)
- ▶ Exposure limitation (노출 최소화 기술)

Homework (1/2)

1. Critical system의 정의

2. Critical system을 세 가지로 구분하여 설명

3. Critical system 에서 dependability가 중요한 이유

4. Critical system 에서 시스템이 고장 날 수 있는 세가지 경우

5. Dependability 와 소프트웨어 개발 비용에 관한 그래프를 작성하고 이를 설명

6. 경제적인 측면에서 dependability 가 높은 시스템은 성능이 떨어질 가능성이 있다. 그 이유는 무엇인가?

Homework (2/2)

7. 시스템의 reliability를 이루기 위한 최소한의 기술 3가지를 설명

8. 시스템의 safety를 이루기 위한 최소한의 기술 3가지를 설명

9. 시스템의 security를 이루기 위한 최소한의 기술 3가지를 설명

10. Critical system 의 사례 연구를 복습하여, 인슐린 펌프의 *System Architecture*를 재설계하고, sub system들의 기능을 설명
    - ✓ 2장 socio-technical system의 burglar alarm system을 참고

11. Critical system의 사례 연구에서 dependability를 위해 필요한 요구사항을 서술 (2가지 이상)