CHAPTER 7

UNIT II

Critical System

Syllabus

Critical System : Types of critical system A simple safety critical system, Dependability of a system, Availability and Reliability, Safety and Security of Software systems.

7.1 Critical System

Q. What is a Critical System ?

- Critical System are the systems that are considered the one on which a business or organization is almost totally dependent for its very survival and prosperity.
- Critical systems require highly good quality, reliable, cost effective software for their integration.
- Successful development of critical systems is dependent on well-defined and managed software development and highly capable professionals.

7.1.1 Types of Critical System

Q. State the types of critical system.

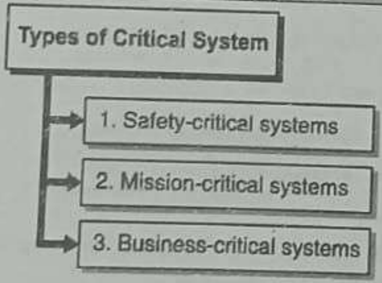
Types of Critical System
1. Safety-critical systems
2. Mission-critical systems
3. Business-critical systems

Fig. 7.1.1 : Types of Critical System

1. **Safety-critical systems**

- Any failure in these systems result in injury, death or damage to the environment.
- **Example :** Chemical Plant system

2. **Mission-critical systems**

- Any failure in these systems result in the failure of some expected goals.
- **Example :** Spacecraft navigation system.

3. **Business-critical systems**

- Any failure in these systems result in high financial loss.
- **Example :** Bank Accounting system.

7.2 System Dependability

Q. Describe system dependability. What is its importance in critical systems ?

- The system dependability is the trustworthiness on the system i.e. the user's degree of trust in that system.
- Usefulness and Trustworthiness are different - A system need not have to be trusted to be useful.

A. Importance of Dependability

- Systems those are not dependable that means, systems that are not trustworthy, unreliable, unsafe or insecure are rejected by their users.
- Undependable systems may cause loss of valuable information resulting in a high recovery cost.

B. Various Dimensions of Dependability

1. **Availability :** Ability of the system to deliver the services whenever required at any given point of time.
2. **Reliability :** Ability of the system to deliver the services as specified and expected by the user without any failure in normal use.
3. **Safety :** Ability of the system to operate without catastrophic failure.
4. **Security :** Ability of the system to protect itself against accidental intrusions or malicious attacks.
5. **Reparability :** It is the extent to which the system can be repaired in the event of a failure.
6. **Maintainability :** It is the extent to which a system can be adapted to new requirements.
7. **Survivability :** It is the extent to which a system can deliver services under the condition of an accidental attack.
8. **Error Tolerance :** It is the extent to which user input errors can be avoided and tolerated.

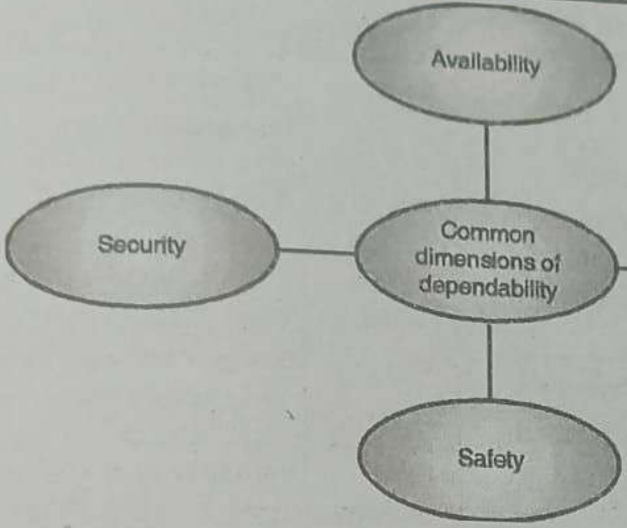

Fig. 7.2.1 : Dimensions of dependability

7.3 A Simple Safety Critical System

- Example of a simple safety critical system is a software-controlled insulin pump. It is used by diabetic patient to measure the sugar level.
- **Data flow in this system is as follows :** The blood sugar sensor observes the blood and analyzes the sugar level in the blood by examining the blood parameters it then computes the insulin requirement and communicates it to the insulin delivery controller which commands the insulin pump to inject the insulin.
- Dependability factors of this insulin system are :
  - **Availability :** The insulin pump is available to deliver insulin whenever required to do so.
  - **Reliability :** The insulin pump performs its function reliably and delivers the correct amount of insulin.
  - **Safety :** The insulin pump does not deliver the excessive doses of insulin and it is potentially life threatening.

7.4 Availability and Reliability

- **Availability :** Ability of the system to be operational and able to deliver the requested services at a point of time.
- **Reliability :** Ability of the system to deliver the requested services over a specified time in a given environment without any failure in normal use.

A. Influences on reliability

1. **Hardware reliability :** What is the failing probability of a hardware component and how long does it take to repair that component?
2. **Software reliability :** How frequently a software component produces an incorrect output?
3. **Operator reliability :** How likely the operator of a system makes an error?

B. Reliability Terminologies

1. **System failure :** Occurs when the system does not deliver the requested service as expected by its users.
2. **System error :** The system behaviour that is unexpected by system users
3. **System fault :** Characteristic of a software system that can lead to a system error. Use of + instead of – can result in wrong calculations.
4. **Human error or mistake :** Human behaviour that results in the introduction of faults into a system.

C. Approaches for Reliability Improvement

1. **Fault avoidance :** Use development techniques to minimize the possibility of mistakes before they result in the introduction of the faults.
2. **Fault detection and removal :** Use of verification and validation techniques to increase the probability of detecting and correcting the errors before the system is delivered. Removing A% of faults do not improve the reliability by A%. A study at IBM showed that removing 60% of faults improve the reliability by 3%.

3 **Fault tolerance :** Use run-time techniques to ensure that the system faults do not result in system errors and do not lead to system failures.

7.5 Safety of the System

- Safety is a property that says that the system should never damage the people or system's environment.
- **Example :** Aircraft – the control and monitoring systems of the Aircraft.

Q. State the two types of Safety-critical systems and how can safety be achieved?

There are two types of safety critical systems :

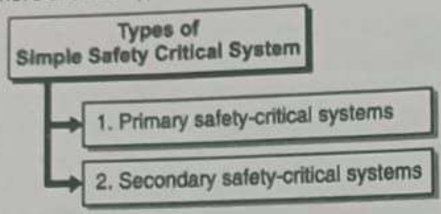
Types of Simple Safety Critical System
1. Primary safety-critical systems
2. Secondary safety-critical systems

Fig. 7.5.1 : Types of Simple Safety Critical System

1. **Primary safety-critical systems**

   These are the embedded software systems whose failure causes the associated hardware to fail and directly threaten then users. .

2. **Secondary safety-critical systems**

   These are the systems whose failure indirectly results in faults in other systems which can threaten the users of the system.

Q. Describe the safety terminologies: hazard severity and hazard probability.

Table 7.5.1 : Safety Terminology

Term	Description
Accident	An unexpected event which results in human death or injury, damage to property or to the environment. ***Example:*** *A computer-controlled machine injuring its operator.*
Hazard	A condition that causes or contributes to an accident. ***Example:*** *A failure of the sensor that detects an obstacle in front of the machine.*
Damage	Measure of loss resulting from an accident. ***Example:*** *Many people killed as a result of an accident to minor injury or property damage.*
Hazard Severity	The worst possible damage that could result from a particular hazard. ***Example:*** *Many people are killed just only due to minor damage.*
Hazard Probability	Probability of the events occurring which create a hazard. Probability values range from probable (say, 1/100th chance) to unbelievable.
Risk	Probability that the system will cause an accident.

Ways to achieve Safety

Safety in a system can be achieved by following ways :

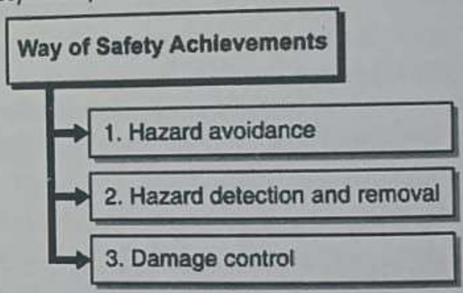

Fig. 7.5.2 : Way of Safety Achievements

1. **Hazard avoidance**

   The system is designed so that some classes of hazards cannot arise.

2. **Hazard detection and removal**

   The system is designed so that hazards are identified and deleted before the system meets any accidental failure or damage.

3. **Damage control**

   The system contains protection features that minimize the damage that may occur due to a hazard.

7.6 Security of the System

Security is an ability to protect the system from accidental or intentional malicious attack such as viruses, unauthorized use of service/data modification.

Table 7.6.1 : Security Terminology

Term	Description
Exposure	Loss or harm of data, time and efforts put to recover after a security breach.
Vulnerability	Weakness of the system that leads to any loss or harm
Attack	Exploitation from the outside of the system to breach the security and cause some damage
Threats	Circumstances that have potential to cause loss or harm
Control	Protective measure to reduce the vulnerabilities and threats such as the encryption of the data.

A. Damage due to insecurity

1. **DoS (Denial of Service) :** It is an attack meant to shut down a machine or network, making it inaccessible to its intended users. This is accomplished by flooding the target with traffic, or sending it information that triggers a crash
2. **Corruption of data:** The system components may be altered due to hardware of software malfunction, malware or virus infection.
3. **Leakage of confidential information:** Personal information or confidential information may be exposed to unauthorized people.

B. Ways to achieve Security

1. **Vulnerability avoidance:** Design safe systems so that the vulnerabilities can be avoided such as avoiding the external network connection.
2. **Attack detection and elimination:** Design safe systems which can detect and remove the attacks before they result in an data exposure.
3. **Exposure limitation:** The consequences of an attack should be immediately reduced by use of backup policies which can help to restore the damaged information.

Review Questions

Q. 1 What is a Critical System? State the types of critical system.

Q. 2 Describe system dependability. What is its importance in critical systems?

Q. 3 Explain the various factors of dependability in detail.

Q. 4 State the two types of Safety-critical systems and how can safety be achieved ?

Q. 5 Describe the safety terminologies: hazard severity and hazard probability.