Dependable Systems

Inter-dependence of Dependability Properties

* Safe system operation depends on system being
  + Available
  + Operating reliably
* A system may be unreliable due to external attacks
* Denial Of Service attacks
  + Intention: to make it unavailable

Dependability Economics

* High costs for dependable systems
* In some situations, better to accept untrustworthy systems and pau for failure costs
  + However, this depends on system type

Writing Specification for Dependability Properties

* System Requirements
  + Describes what the system must/should/could/won’t do
* Dependability Requirements
  + Functional requirements
    - Defines
      * Error checking
      * Recovery Facilities
      * Protection against system failures
  + Non-functional requirements
    - Defines
      * Required reliability
      * Availability
      * Linked to quality – subjective
  + Excluding Requirements
    - Defines
      * States and conditions that must not arise

Risk-Driven Specification

* Critical systems specification must be risk-driven
* Aim:
  + To understand risks
  + To define requirements that reduce these risks

Stages of Risk-based Analysis

* Risk Identification
  + Identify potential risks
* Risk Analysis and Classification
  + Assess seriousness of each risk
* Risk Decomposition
  + Decompose to discover potential root causes
* Risk Reduction Assessment
  + Define how each risk is eliminated and/or minimised when developing system 🡪 dependability requirements

Phased Risk Analysis

* Preliminary Risk Analysis
  + Identifies risks from system environment
  + Aims to develop initial set of system security and dependable requirements
* Life Cycle Risk Analysis
  + Identifies risks that emerge during design and development
* Operational Risk Analysis
  + Risks associated with user interface and operator errors

Safety Specification

* Identify protection requirements to ensure system failure does not cause:
  + Injury/health issues
  + Death
  + Environmental damage

Risk identification = Hazard identification

Risk analysis = Hazard assessment

Risk decomposition = Hazard analysis

Risk reduction = safety requirements specification

Fault-tree analysis

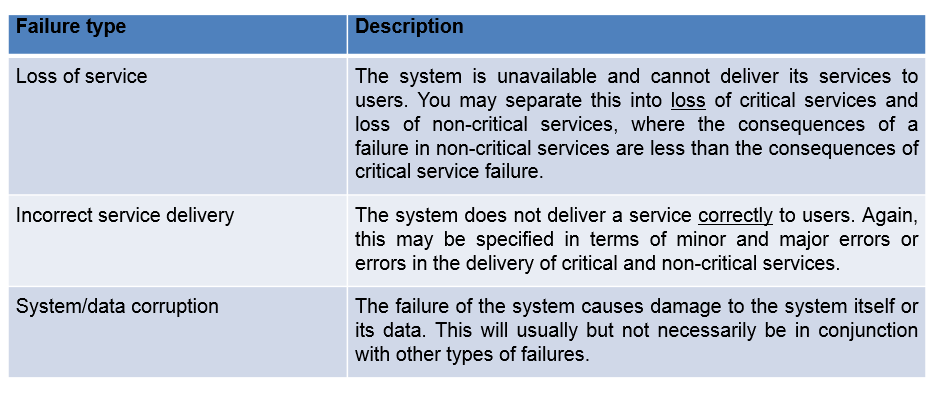
* Aims to minimise the number of single cause of system failure
* Can link with AND and/or OR where appropriate
* 12.4 Fault-tree.epsFind the root cause of risk

Risk Reduction

* Aims to identify dependability requirements that specify:
  + How risks are managed
  + Ensure accidents/incidents do not arise
* Strategies
  + Risk Avoidance
  + Risk Detection and Removal
  + Damage Limitation

System Reliability Specification

* Non-functional Reliability Requirements
  + May be specified quantitatively
    - Defining
      * The number of system failures that are acceptable during normal use of the system
      * The time in which the system must be available
* Functional reliability requirements define system and software functions that avoid, detect or tolerate faults in the software and so ensure that these faults do not lead to system failure.

Types of System Failure

Reliability Metrics

* Quantitative
* System reliability is measured by
  + Counting the number of operational failures
  + The time that the system has been operational.

Probability of Failure on Demand (POFOD)

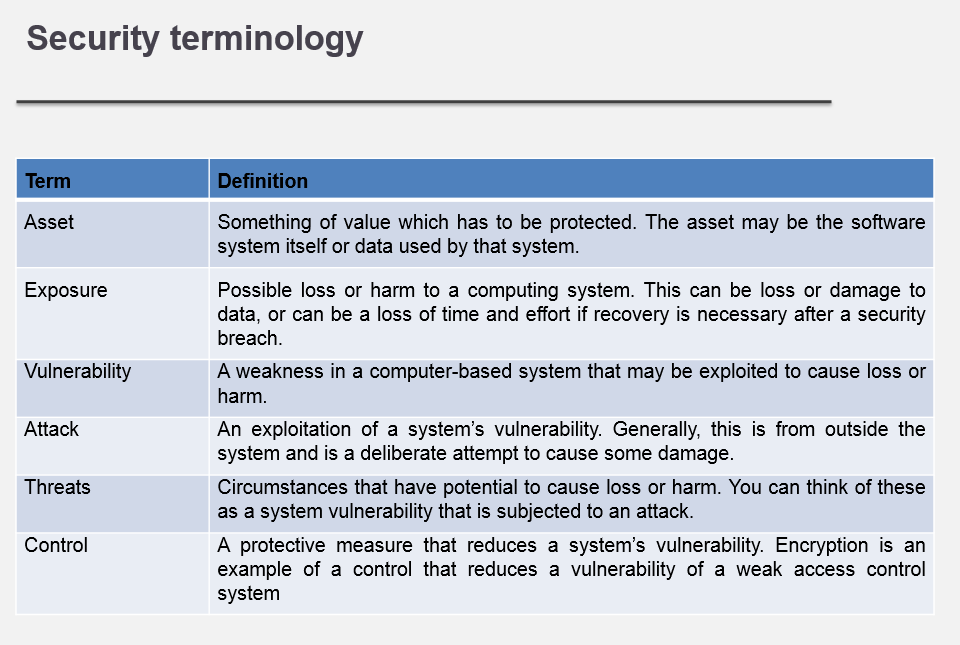
* Probability that a system will fail when a service is requested
* Useful when service is infrequent
* Relevant for many safety-critical

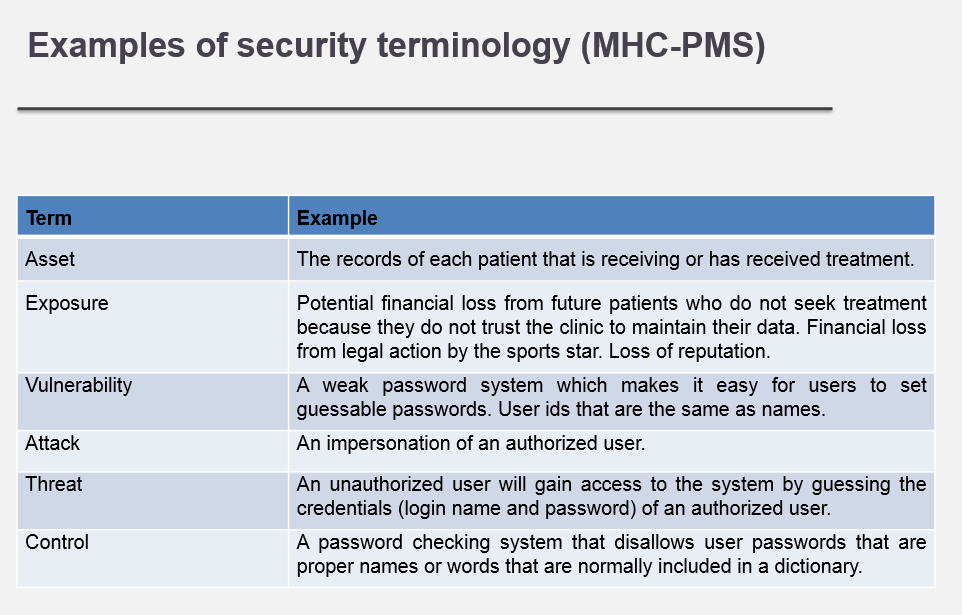
Rate of Fault Occurrence (ROCOF)

* Reflects rate of occurrence in the system (ROCOF)
* ROCOF of 0.002 = 2 failures likely out of 1000 operational time units
  + E.g. 2 failures out of 1000 hours of operation
* Relevant for systems that have a large number of similar requests to process in as short time
* Reciprocal of ROCOF = Mean time to failure (MTTF)
  + Relevant to systems with long transactions
  + MTTF should be longer than expected transaction length

Fundamental Security

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





Threat Classes

* Threats to the confidentiality of the system and its data
  + Can disclose information to people or programs that do not have authorization to access that information.
* Threats to the integrity of the system and its data
  + Can damage or corrupt the software or its data.
* Threats to the availability of the system and its data
  + Can restrict access to the system and data for authorized users.

Damage from Insecurity

* Denial of service
  + The system is forced into a state where normal services are unavailable or degraded
* Corruption of programs or data
  + The programs or data in the system may be modified in an unauthorised way
* Disclosure of confidential information
  + Information that is managed by the system may be exposed to people who are not authorised to read or use that information

Security Assurance

* Vulnerability avoidance
  + The system is designed so that vulnerabilities do not occur.
* Attack detection and elimination
  + The system is designed so that attacks on vulnerabilities are detected and neutralised before they result in an exposure.
* Exposure limitation and recovery
  + The system is designed so that the adverse consequences of a successful attack are minimised.

