Critical Systems Specification

Objectives

- To explain how dependability requirements may be identified by analysing the risks faced by critical systems
- To explain how safety requirements are generated from the system risk analysis
- To explain the derivation of security requirements
- To describe metrics used for reliability specification

Topics covered

- Risk-driven specification
- Safety specification
- Security specification
- Software reliability specification

Dependability requirements

- Functional requirements to define error checking and recovery facilities and protection against system failures.
- Non-functional requirements defining the required reliability and availability of the system.
- Excluding requirements that define states and conditions that must not arise.

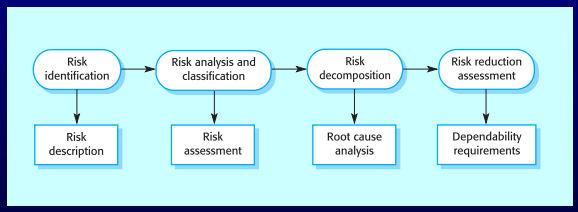
Risk-driven specification

- Critical systems specification should be risk-driven.
- This approach has been widely used in safety and security-critical systems.
- The aim of the specification process should be to understand the risks (safety, security, etc.) faced by the system and to define requirements that reduce these risks.

Stages of risk-based analysis

- Risk identification
  - Identify potential risks that may arise.
- Risk analysis and classification
  - Assess the seriousness of each risk.
- Risk decomposition
  - Decompose risks to discover their potential root causes.
- Risk reduction assessment
  - Define how each risk must be taken into eliminated or reduced when the system is designed.

Risk-driven specification



Risk identification

- Identify the risks faced by the critical system.
- In safety-critical systems, the risks are the hazards that can lead to accidents.
- In security-critical systems, the risks are the potential attacks on the system.
- In risk identification, you should identify risk classes and position risks in these classes
  - Service failure;
  - Electrical risks;
  - …

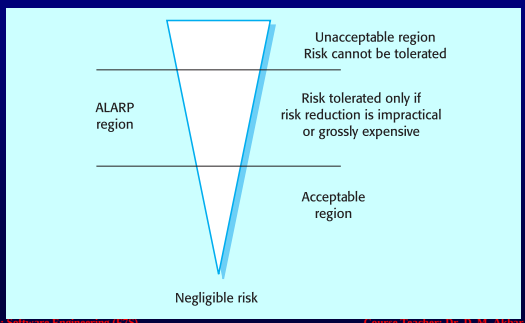
Insulin pump risks

- Insulin overdose (service failure).
- Insulin underdose (service failure).
- Power failure due to exhausted battery (electrical).
- Electrical interference with other medical equipment (electrical).
- Poor sensor and actuator contact (physical).
- Parts of machine break off in body (physical).
- Infection caused by introduction of machine (biological).
- Allergic reaction to materials or insulin (biological).

Risk analysis and classification

- The process is concerned with understanding the likelihood that a risk will arise and the potential consequences if an accident or incident should occur.
- Risks may be categorised as:
  - Intolerable. Must never arise or result in an accident
  - As low as reasonably practical(ALARP). Must minimise the possibility of risk given cost and schedule constraints
  - Acceptable. The consequences of the risk are acceptable and no extra costs should be incurred to reduce hazard probability

Levels of risk



Social acceptability of risk

- The acceptability of a risk is determined by human, social and political considerations.
- In most societies, the boundaries between the regions are pushed upwards with time i.e. society is less willing to accept risk
  - For example, the costs of cleaning up pollution may be less than the costs of preventing it but this may not be socially acceptable.
- Risk assessment is subjective
  - Risks are identified as probable, unlikely, etc. This depends on who is making the assessment.

Risk assessment

- Estimate the risk probability and the risk severity.
- It is not normally possible to do this precisely so relative values are used such as ‘unlikely’, ‘rare’, ‘very high’, etc.
- The aim must be to exclude risks that are likely to arise or that have high severity.

Risk assessment - insulin pump

Identified hazard	Hazard probability	Hazard severity	Estimated risk	Acceptability
1. Insulin overdose	Medium	High	High	Intolerable
2. Insulin underdose	Medium	Low	Low	Acceptable
3. Power failure	High	Low	Low	Acceptable
4. Machine incorrectly fitted	High	High	High	Intolerable
5. Machine breaks in patient	Low	High	Medium	ALARP
6. Machine causes infection	Medium	Medium	Medium	ALARP
7. Electrical interference	Low	High	Medium	ALARP
8. Allergic reaction	Low	Low	Low	Acceptable

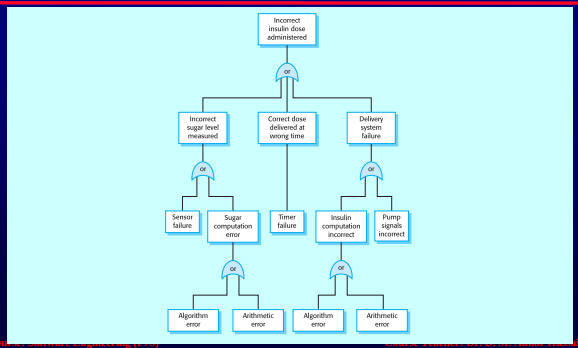
Risk decomposition

- Concerned with discovering the root causes of risks in a particular system.
- Techniques have been mostly derived from safety-critical systems and can be
  - Inductive, bottom-up techniques. Start with a proposed system failure and assess the hazards that could arise from that failure;
  - Deductive, top-down techniques. Start with a hazard and deduce what the causes of this could be.

Fault-tree analysis

- A deductive top-down technique.
- Put the risk or hazard at the root of the tree and identify the system states that could lead to that hazard.
- Where appropriate, link these with ‘and’ or ‘or’ conditions.
- A goal should be to minimise the number of single causes of system failure.

Insulin pump fault tree



Risk reduction assessment

- The aim of this process is to identify dependability requirements that specify how the risks should be managed and ensure that accidents/incidents do not arise.
- Risk reduction strategies
  - Risk avoidance;
  - Risk detection and removal;
  - Damage limitation.

Strategy use

- Normally, in critical systems, a mix of risk reduction strategies are used.
- In a chemical plant control system, the system will include sensors to detect and correct excess pressure in the reactor.
- However, it will also include an independent protection system that opens a relief valve if dangerously high pressure is detected.

Insulin pump - software risks

- Arithmetic error
  - A computation causes the value of a variable to overflow or underflow;
  - Maybe include an exception handler for each type of arithmetic error.
- Algorithmic error
  - Compare dose to be delivered with previous dose or safe maximum doses. Reduce dose if too high.

Safety requirements - insulin pump

SR1: The system shall not deliver a single dose of insulin that is greater than a specified maximum dose for a system user.
SR2: The system shall not deliver a daily cumulative dose of insulin that is greater than a specified maximum for a system user.
SR3: The system shall include a hardware diagnostic facility that shall be executed at least 4 times per hour.
SR4: The system shall include an exception handler for all of the exceptions that are identified in Table 3.
SR5: The audible alarm shall be sounded when any hardware or software anomaly is discovered and a diagnostic message as defined in Table 4 should be displayed.
SR6: In the event of an alarm in the system, insulin delivery shall be suspended until the user has reset the system and cleared the alarm.

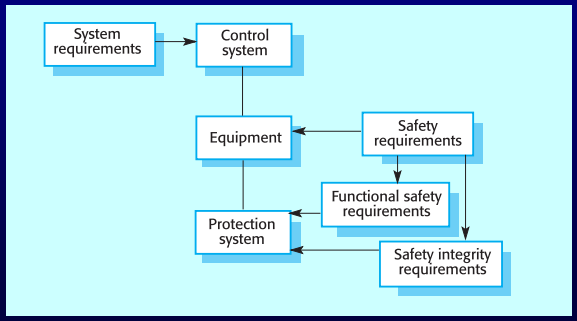
Safety specification

- The safety requirements of a system should be separately specified.
- These requirements should be based on an analysis of the possible hazards and risks as previously discussed.
- Safety requirements usually apply to the system as a whole rather than to individual sub-systems. In systems engineering terms, the safety of a system is an emergent property.

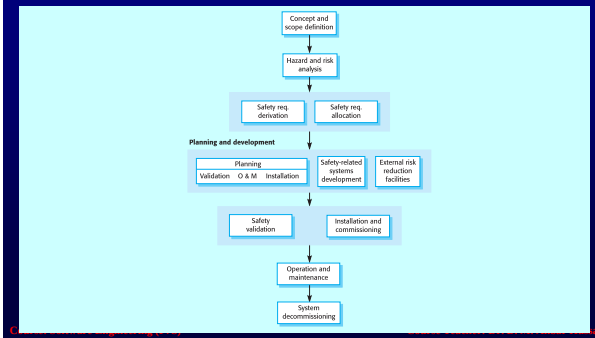
IEC 61508

- An international standard for safety management that was specifically designed for protection systems - it is not applicable to all safety-critical systems.
- Incorporates a model of the safety life cycle and covers all aspects of safety management from scope definition to system decommissioning.

Control system safety requirements



The safety life-cycle



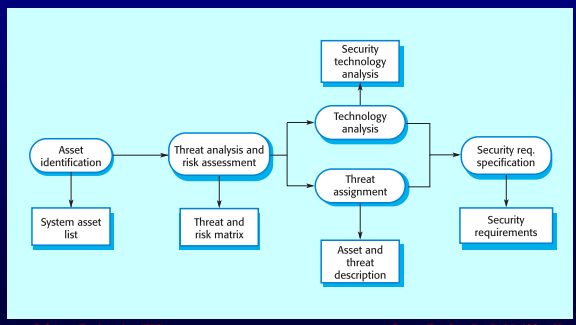
Safety requirements

- Functional safety requirements
  - These define the safety functions of the protection system i.e. the define how the system should provide protection.
- Safety integrity requirements
  - These define the reliability and availability of the protection system. They are based on expected usage and are classified using a safety integrity level from 1 to 4.

Security specification

- Has some similarities to safety specification
  - Not possible to specify security requirements quantitatively;
  - The requirements are often 'shall not' rather than 'shall' requirements.
- Differences
  - No well-defined notion of a security life cycle for security management; No standards;
  - Generic threats rather than system specific hazards;
  - Mature security technology (encryption, etc.). However, there are problems in transferring this into general use;
  - The dominance of a single supplier (Microsoft) means that huge numbers of systems may be affected by security failure.

The security specification process



Stages in security specification

- Asset identification and evaluation
  - The assets (data and programs) and their required degree of protection are identified. The degree of required protection depends on the asset value so that a password file (say) is more valuable than a set of public web pages.
- Threat analysis and risk assessment
  - Possible security threats are identified and the risks associated with each of these threats is estimated.
- Threat assignment
  - Identified threats are related to the assets so that, for each identified asset, there is a list of associated threats.

Stages in security specification

- Technology analysis
  - Available security technologies and their applicability against the identified threats are assessed.
- Security requirements specification
  - The security requirements are specified. Where appropriate, these will explicitly identified the security technologies that may be used to protect against different threats to the system.

Types of security requirement

- Identification requirements.
- Authentication requirements.
- Authorisation requirements.
- Immunity requirements.
- Integrity requirements.
- Intrusion detection requirements.
- Non-repudiation requirements.
- Privacy requirements.
- Security auditing requirements.
- System maintenance security requirements.

LIBSYS security requirements

SEC1: All system users shall be identified using their library card number and personal password.
SEC2: Users privileges shall be as signed according to the class of user (student, staff, library staff).
SEC3: Before execution of any command, LIBSYS shall check that the user has sufficient privileges to access and execute that command.
SEC4: When a user orders a document, the order request shall be logged. The log data maintained shall include the time of order, the user's identification and the articles ordered.
SEC5: All system data shall be backed up once per day and backups stored off-site in a secure storage area.
SEC6: Users shall not be permitted to have more than 1 simultaneous login to LIBSYS.

System reliability specification

- Hardware reliability
  - What is the probability of a hardware component failing and how long does it take to repair that component?
- Software reliability
  - How likely is it that a software component will produce an incorrect output. Software failures are different from hardware failures in that software does not wear out. It can continue in operation even after an incorrect result has been produced.
- Operator reliability
  - How likely is it that the operator of a system will make an error?

Functional reliability requirements

- A predefined range for all values that are input by the operator shall be defined and the system shall check that all operator inputs fall within this predefined range.
- The system shall check all disks for bad blocks when it is initialised.
- The system must use N-version programming to implement the braking control system.
- The system must be implemented in a safe subset of Ada and checked using static analysis.

Non-functional reliability specification

- The required level of system reliability required should be expressed quantitatively.
- Reliability is a dynamic system attribute- reliability specifications related to the source code are meaningless.
  - No more than N faults/1000 lines;
  - This is only useful for a post-delivery process analysis where you are trying to assess how good your development techniques are.
- An appropriate reliability metric should be chosen to specify the overall system reliability.

Reliability metrics

- Reliability metrics are units of measurement of system reliability.
- System reliability is measured by counting the number of operational failures and, where appropriate, relating these to the demands made on the system and the time that the system has been operational.
- A long-term measurement programme is required to assess the reliability of critical systems.

Reliability metrics

Metric	Explanation
POFOD Probability of failure on demand	The likelihood that the system will fail when a service request is made. A POFOD of 0.001 means that 1 out of a thousand service requests may result in failure.
ROCOF Rate of failure occurrence	The frequency of occurrence with which unexpected behaviour is likely to occur. A R OCOF of 2/100 means that 2 f ailures are likely to occur in each 100 operational time units. This metric is sometimes called the failure intensity.
MTTF Mean time to failure	The average time between observed system failures. An MTTF of 500 means that 1 failure can be expected every 500 time units.
AVAIL Availability	The probability that the system is available for use at a given time. Availability of 0.998 means that in every 1000 time units, the system is likely to be available for 998 of these.

Probability of failure on demand

- This is the probability that the system will fail when a service request is made. Useful when demands for service are intermittent and relatively infrequent.
- Appropriate for protection systems where services are demanded occasionally and where there are serious consequence if the service is not delivered.
- Relevant for many safety-critical systems with exception management components
  - Emergency shutdown system in a chemical plant.

Rate of fault occurrence (ROCOF)

- Reflects the rate of occurrence of failure in the system.
- ROCOF of 0.002 means 2 failures are likely in each 1000 operational time units e.g. 2 failures per 1000 hours of operation.
- Relevant for operating systems, transaction processing systems where the system has to process a large number of similar requests that are relatively frequent
  - Credit card processing system, airline booking system.

Mean time to failure

- Measure of the time between observed failures of the system. Is the reciprocal of ROCOF for stable systems.
- MTTF of 500 means that the mean time between failures is 500 time units.
- Relevant for systems with long transactions i.e. where system processing takes a long time. MTTF should be longer than transaction length
  - Computer-aided design systems where a designer will work on a design for several hours, word processor systems.

Availability

- Measure of the fraction of the time that the system is available for use.
- Takes repair and restart time into account
- Availability of 0.998 means software is available for 998 out of 1000 time units.
- Relevant for non-stop, continuously running systems
  - telephone switching systems, railway signalling systems.

Non-functional requirements spec.

- Reliability measurements do NOT take the consequences of failure into account.
- Transient faults may have no real consequences but other faults may cause data loss or corruption and loss of system service.
- May be necessary to identify different failure classes and use different metrics for each of these. The reliability specification must be structured.

Failure consequences

- When specifying reliability, it is not just the number of system failures that matter but the consequences of these failures.
- Failures that have serious consequences are clearly more damaging than those where repair and recovery is straightforward.
- In some cases, therefore, different reliability specifications for different types of failure may be defined.

Failure classification

Failure class	Description
Transient	Occurs only with certain inputs
Permanent	Occurs with all inputs
Recoverable	System can recover without operator intervention
Unrecoverable	Operator intervention needed to recover from failure
Non-corrupting	Failure does not corrupt system state or data
Corrupting	Failure corrupts system state or data

Steps to a reliability specification

- For each sub-system, analyse the consequences of possible system failures.
- From the system failure analysis, partition failures into appropriate classes.
- For each failure class identified, set out the reliability using an appropriate metric. Different metrics may be used for different reliability requirements.
- Identify functional reliability requirements to reduce the chances of critical failures.

Bank auto-teller system

- Each machine in a network is used 300 times a day
- Bank has 1000 machines
- Lifetime of software release is 2 years
- Each machine handles about 200, 000 transactions
- About 300, 000 database transactions in total per day

Reliability specification for an ATM

Failure class	Example	Reliability metric
Permanent, non-corrupting.	The system fails to operate with any card that is input. Software must be restarted to correct failure.	ROCOF 1 occurrence/1000 days
Transient, non-corrupting	The magnetic stripe data cannot be read on an undamaged card that is input.	ROCOF 1 in 1000 transactions
Transient, corrupting	A p attern of transactions across the network causes database corruption.	Unquantifiable! Should never happen in the lifetime of the system

Specification validation

- It is impossible to empirically validate very high reliability specifications.
- No database corruptions means POFOD of less than 1 in 200 million.
- If a transaction takes 1 second, then simulating one day's transactions takes 3.5 days.
- It would take longer than the system's lifetime to test it for reliability.

Key points

- Risk analysis is the basis for identifying system reliability requirements.
- Risk analysis is concerned with assessing the chances of a risk arising and classifying risks according to their seriousness.
- Security requirements should identify assets and define how these should be protected.
- Reliability requirements may be defined quantitatively.

Key points

- Reliability metrics include POFOD, ROCOF, MTTF and availability.
- Non-functional reliability specifications can lead to functional system requirements to reduce failures or deal with their occurrence.