
Risk-based requirements analysis

Discusses how to use an analysis of risks to the system to derive the system requirements

November 2004

©Ian Sommerville 2004

Slide 1

Risk-based requirements analysis

- The safety-critical systems community and the security critical systems community have independently developed similar techniques for generating dependability requirements (hazard analysis and vulnerability analysis)
- These focus on what problems might arise and what can be done to avoid, tolerate or reduce the impact of these problems
- The techniques can be generalised as risk-based requirements analysis - as well as safety and security, it can also be used for risks that threaten the availability, performance, etc. of the system

November 2004

©Ian Sommerville 2004

Slide 2

Risks

- A risk is, informally, something that you do not want to happen. They range from trivial to extremely serious:
 - Risk of dropping a cup of coffee
 - Risk that the files on your computer will be corrupted
 - Risk that an on-line banking system will reveal your accounts to others
 - Risk of an aircraft crashing into a residential area
- The acceptability of a risk depends on what is threatened by the risk, the probability of the causes of the risk arising and the probability that these causes will result in an incident

Terminology

- **Assets**
 - The things that are threatened by a risk. These can be the system itself, things controlled or managed by the system or things in the systems environment. An example of an asset would be an aircraft and its passengers.
- **Hazard or vulnerability**
 - A fundamental threat to an asset. A hazard is a system state that, given adverse environmental conditions, will lead to an accident or an incident.
 - Therefore, a hazard that threatens an aircraft is engine failure.
- **Accident or incident**
 - The possible consequence of the hazard arising. An accident involves loss of life or damage; An incident is a 'near miss' where there is a potential for damage
 - An incident that could arise from engine failure is an emergency landing
 - An accident that could arise from engine failure in an aircraft is an air crash.

Risk assessment

- When assessing risk we need to consider:
 - The value of the assets that are threatened
 - The probability that a threat to these assets will arise (the hazard probability)
 - The probability that the threat will develop into an incident (the accident probability)
 - The probable extent of the damage to the assets
 - The costs of repairing or replacing the assets or compensating the asset owners
 - The circumstances of use. Our view of what is an acceptable risk depends on the circumstances where that risk is being evaluated

November 2004

©Ian Sommerville 2004

Slide 5

Risk mitigation strategies

- The focus of the safety requirements engineering process is to move from a statement of the risks to system requirements that ensure these risks are reduced to a commercially (and socially) acceptable level
- Risk avoidance
 - Design the system so that an accident cannot occur
 - This may involve hazard avoidance (the threat cannot occur) or accident avoidance (the threat cannot result in an accident)
- Risk management
 - Reduce the probability of threats (hazards) arising
 - Reduce the probability that a hazard results in an accident
- Damage reduction
 - Reduce the damage caused by the incident
 - Reduce the costs of recovery of the damaged assets

November 2004

©Ian Sommerville 2004

Slide 6

Risk analysis process

- Identify the assets at risk and the risks that threaten these assets
- Identify the critical incidents i.e. those incidents where there is a high probability of occurrence or where damage from an accident is severe
- Identify the hazards that could result in these incidents arising
- Discover the root causes of these hazards
- Wherever possible, generate requirements that ensure these root causes are avoided or detected and corrected
- Requirements for safety can be:
 - System requirements
 - Design constraints
 - Requirements for a separate protection system
 - Requirements for the operational process
 - Requirements for organisational processes, procedures or equipment

November 2004

©Ian Sommerville 2004

Slide 7

Asset identification

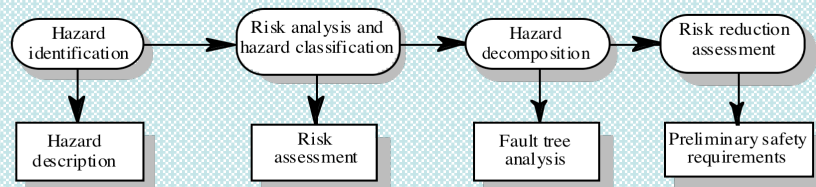
- The assets that must be protected may be:
 - The operators of the system - people using the system must not be damaged by system failure
 - People and things in the system's environment. The term asset is used quite loosely here
 - The system itself. It may be essential that the system should always be available
 - Other systems controlled or protected by the system being analysed. Many software systems are controllers or protection systems. Software failure may mean that other systems are threatened
 - The data that is managed by the system

November 2004

©Ian Sommerville 2004

Slide 8

Hazard and risk analysis



November 2004

©Ian Sommerville 2004

Slide 9

Hazard and risk analysis

- Identification of hazards which can arise which compromise the safety of the system and assessing the risks associated with these hazards
- Structured into various classes of hazard analysis and carried out throughout software process from specification to implementation
- A risk analysis should be carried out and documented for each identified hazard and actions taken to ensure the most serious/likely hazards do not result in accidents

November 2004

©Ian Sommerville 2004

Slide 10

Hazard analysis stages

- Hazard identification
 - Identify potential hazards which may arise
- Risk analysis and hazard classification
 - Assess the risk associated with each hazard
- Hazard decomposition
 - Decompose hazards to discover their potential root causes
- Risk reduction assessment
 - Define safety or safe system requirements that reduce the risks associated with the use of the system

November 2004

©Ian Sommerville 2004

Slide 11

Hazard identification

- During this stage, you identify hazards that could result in an incident. Hazards are things that can go wrong in the system itself.
- Hazard identification can be top-down or bottom-up
 - Top-down identification. From potential risks, identify the system and environmental states that could cause these
 - Bottom-up identification. Start with the things that might go wrong with the system and work out what incidents these could cause
- You should remember that incidents sometimes arise from a combination of hazards and not simply a single hazard

November 2004

©Ian Sommerville 2004

Slide 12

Insulin system risks

- Insulin overdose
- Insulin underdose
- Electrical interference with other medical devices
- Infection
- Physical damage to user
- Allergic reaction

November 2004

©Ian Sommerville 2004

Slide 13

Hazard classes

- Physical hazards
 - Hazards that are associated with physical states of the system
 - In a cutting machine, an exposed blade is a physical hazard
- Electrical hazards
 - Hazards that are associated with electrical states of the system
 - A fuse of the wrong type in a device is an electrical hazard
- Control hazards
 - Hazards that are associated with the software controlling the system
 - An arithmetic overflow is a control hazard
- Data hazards
 - Hazards that are associated with the data processed by a system
 - An incorrect diagnosis of a medical condition in a medical record is a data hazard

November 2004

©Ian Sommerville 2004

Slide 14

Insulin system hazards

- Incorrect computation of insulin dose (control)
 - Insulin overdose or underdose
- Incorrect sensor signals (data)
 - Insulin overdose or underdose
- Syringe blockage (physical)
 - Insulin underdose
- Physical damage to machine (physical)
 - Parts of needle break off in patients body
- Power failure (electrical)
 - Insulin underdose
- Dirty needle/sensor (physical)
 - Infection caused by introduction of machine
- Inappropriate materials (physical)
 - Allergic reaction to the materials or insulin used in the machine

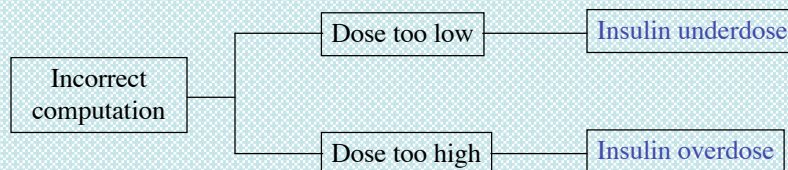
November 2004

©Ian Sommerville 2004

Slide 15

Hazard breakdown

- Where there is more than one possible consequence or different levels of damage associated with a consequence, then the hazard may be further decomposed



November 2004

©Ian Sommerville 2004

Slide 16

Risk assessment

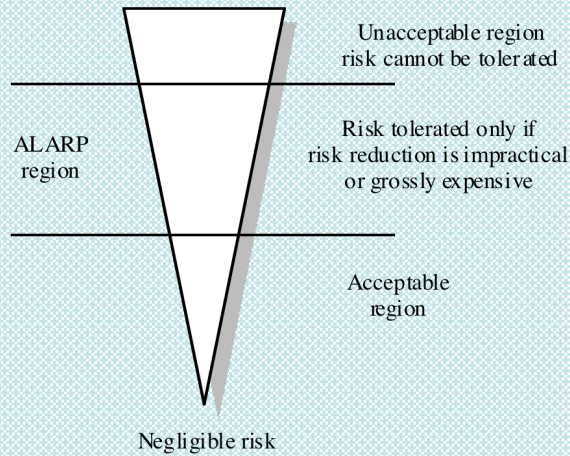
- Assesses the hazard probability, the accident probability and the accident severity
- The outcome of a risk assessment is a statement of acceptability
 - Intolerable. Must never arise or result in an accident
 - As low as reasonably practical(ALARP) Must minimise possibility of hazard given cost and schedule constraints
 - Acceptable. Consequences of hazard are acceptable and no extra costs should be incurred to reduce hazard probability

November 2004

©Ian Sommerville 2004

Slide 17

Risk classification



November 2004

©Ian Sommerville 2004

Slide 18

Risk analysis example

- Insulin overdose
 - High probability, Serious, Unacceptable
- Insulin underdose
 - High probability, Moderate, ALARP
- Electrical interference with other medical devices
 - Low probability, Serious, ALARP
- Infection
 - High probability, Moderate/serious, Unacceptable
- Physical damage
 - Low probability, serious, ALARP
- Allergic reaction
 - Low probability, Moderate, Acceptable

November 2004

©Ian Sommerville 2004

Slide 19

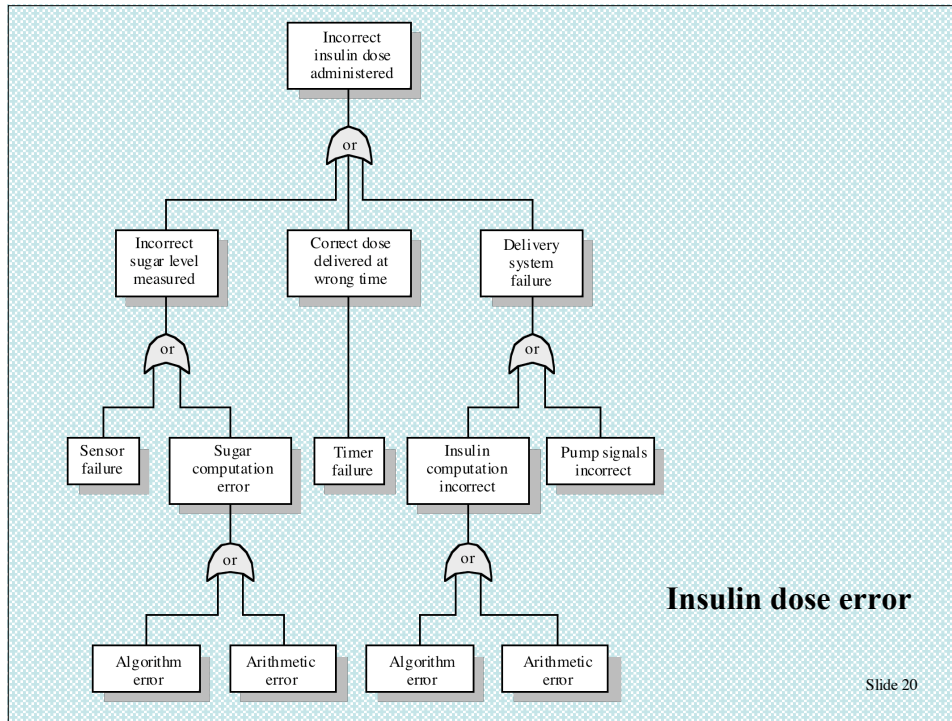
Fault-tree analysis

- Method of hazard analysis which starts with an identified risk and works backward to the root causes of the problem.
- Can be used at all stages of hazard analysis from preliminary analysis through to detailed software checking
- Top-down hazard analysis method. May be combined with bottom-up methods which start with system failures and lead to hazards

November 2004

©Ian Sommerville 2004

Slide 20



Risk reduction assessment

- Generate requirements that:
 - Ensure that the hazard does not arise
 - Ensure that, if the hazard arises, it does not develop into an incident or accident
 - Ensure that, if an accident happens, then the damage is minimised
 - Ensure that, if damage occurs, then the costs of recovery from the damage is minimised
- Where appropriate, generate requirements that ensure that there is a high-probability that these safety functions will be available

Risk classification for reduction

- Risks that may be addressed by ensuring that the machine operates within a safe envelope
- Risks that may be addressed by ensuring that the system is operating correctly
- Risks that may be addressed by specifying design constraints
- Risks that may be addressed by specifying the operational processes of the machine
- Risks that may be addressed by restricting the operating context of the system

November 2004

©Ian Sommerville 2004

Slide 23

Risk reduction

- Insulin overdose
 - Requirements to define a safe operating envelope
 - Requirements to ensure correct operation
- Insulin underdose
 - Requirements to define a safe operating envelope
 - Requirements to ensure correct operation
- Electrical interference with other medical devices
 - ‘Requirements’ to constrain the operating context
- Infection
 - Requirements that define the operational process
- Physical damage
 - Requirements that specify material used (design)
 - Requirements that define the operational process
- Allergic reaction
 - Requirements that specify material used (design)

November 2004

©Ian Sommerville 2004

Slide 24

Safe operating envelope

- A widely-used approach to ensure safety is to identify an operating envelope for the system where safety is highly probable and constrain the system operation to that envelope
- Safety requirements may define that envelope and how violations are detected and corrected

November 2004

©Ian Sommerville 2004

Slide 25

Safe operation of the insulin pump

- No dose of insulin shall exceed some given maximum dose that is defined when the machine is configured for a user (Max single dose)
- The maximum dose of insulin delivered in a 24 hour period shall be constrained to a maximum value (Max daily dose)
- No single dose delivered shall be more than 4 times the previous dose

November 2004

©Ian Sommerville 2004

Slide 26

Correct operation

- Requirements that specify how system failures should be detected and handled
- Requirements that specify design constraints that support fault tolerance and recovery
- Requirements that specify diagnostic and error messages to be generated in the event of a system failure

November 2004

©Ian Sommerville 2004

Slide 27

Dependability requirements

- The system shall include a hardware diagnostic facility that shall be executed at least 4 times per hour
- The system shall include an exception handler for all of the exceptions that are identified in Table 3. Actions to be taken in handling each exception are defined in Table 4
- The audible alarm shall be sounded when any hardware anomaly is discovered and a diagnostic message as defined in Table 5 should be displayed

November 2004

©Ian Sommerville 2004

Slide 28

Key points

- Risks to the system and its environment should be used to drive the process of deriving dependability requirements
- Risk mitigation strategies include risk avoidance, risk management and damage reduction
- Risks should be classified as unacceptable, ALARP or acceptable
- Safety requirements should be derived from an understanding of the root causes of risks
- Safety requirements may specify safe operating envelopes, system dependability, system design or operational processes