
Integrated safety-requirements engineering

Using global concerns to drive requirements engineering in socio-technical systems

November 2004

©lan Sommerville 2004

Slide 1

Objectives

- To describe an approach to requirements engineering that may be used with safety critical information systems.
- To show how cross-cutting concerns can be used to identify requirements and requirements conflicts.
- To introduce a case study of a patient record system for mental health care.

November 2004

©lan Sommerville 2004

Slide 2

Integrated requirements engineering

- Safety requirements are business requirements so safety requirements engineering should not be a separate process but should be part of the system requirements engineering process
- Safety issues should be considered alongside other business requirements and trade offs made.
- Safety should not be compromised in these trade-offs but by changing other system requirements, the cost of achieving safety can be reduced.

November 2004

©Ian Sommerville 2004

Slide 3

Rationale

- Safety is not an isolated system property but must be considered in conjunction with other properties such as integrity and timeliness
- Requirements conflicts and trade-offs are harder to make when safety requirements are distinguished in some way
- Risks and hazards, especially for information systems, cannot be identified until you have some knowledge of the system requirements

November 2004

©Ian Sommerville 2004

Slide 4

Safety-critical information systems

- The safety-critical systems community has focused its attention on safety-critical control systems
- In those systems, the actual damage that is caused results from undesirable behaviour of the equipment that is being controlled
- Increasingly, however, socio-technical information systems are safety-critical in that system failure results in indirect risks to people
- Other systems (not necessarily equipment but also human systems) may rely on an information system for their correct functioning. Failure of these systems may then lead to damage

November 2004

©Ian Sommerville 2004

Slide 5

Examples

- **Design systems**
 - Failure of CAD systems that are used to design critical hardware and software may lead to the failure of the systems that have been designed
 - A story in the 1970s suggested that a number of plane crashes were a result of errors in a structural analysis program which resulted in structural weaknesses in the airframe
- **Records systems**
 - Incorrect information or unavailability of records systems may mean that users of these systems take actions that are potentially dangerous
 - If a maintenance record for an aircraft is incorrect, parts that have reached the end of their design life may not be replaced
- **Simulation systems**
 - Simulation systems that do not match the real environment may result in incorrect design decisions or misplaced confidence in the integrity of the system
 - In the Ariane 5 launcher failure in 1996, the launch simulator did not accurately reflect the actual launch conditions

November 2004

©Ian Sommerville 2004

Slide 6

Secondary risks

- In control systems, the risks (primary risks) are determined from the characteristics of the equipment that is being controlled
- This doesn't mean that risk assessment is easy but it does provide boundaries for the risk assessment and helps identify information sources
- In information systems, the risks are secondary risks - they result from the use of some other dependent system. For example, if a patient is allergic to some drug and this isn't recorded in their record, this may then result in a failure in the system for prescribing medication (ie an inappropriate medicine is prescribed)
- As there may be many systems that rely on an information system, identifying risks in the information system is consequently very difficult

November 2004

©Ian Sommerville 2004

Slide 7

Secondary risk example

- An electronic health record in a hospital may be used in:
 - Diagnostic processes
 - Anaesthetic processes
 - Treatment processes
 - Discharge processes
- A failure in that system associated with an individual record may be non-critical for some of these processes but critical for others

November 2004

©Ian Sommerville 2004

Slide 8

Hazard classes

- Data hazards, namely hazards that are associated with the data processed by the system, are the major type of hazard in information systems
- Control hazards, hazards that are associated with the software controlling the system are also significant

November 2004

©Ian Sommerville 2004

Slide 9

Data hazards

- Data hazards are hazards that are associated with the data in the system rather than the program itself.
- If data is unavailable or incorrect, then overall system failures may arise
 - Data missing
 - Data incorrect
 - Data inconsistent
 - Data unreadable

November 2004

©Ian Sommerville 2004

Slide 10

Control hazards

- Control hazards are hazards that result from the failure of the program controlling access to the patient data
 - System unavailability
 - Failure to read/write patient data
 - Failure to select the correct patient (and hence incorrect data accessed)
 - Failure to maintain data consistency

November 2004

©Ian Sommerville 2004

Slide 11

Goals and requirements

- High level system goals define what the system is supposed to do for the business or organisation operating that system
- The requirements for the system should therefore reflect the business goals and should not simply be driven by local or technical considerations.
- However, goals are much more abstract than requirements, so we need a mechanism to help develop requirements from the business goals.

November 2004

©Ian Sommerville 2004

Slide 12

Concerns

- Are issues that an organisation should pay attention to and that are **systemic** - they apply to the system as a whole
- They are cross-cutting issues that may affect all system stakeholders
- They have been designed as a mechanism to help bridge the gap between organisational goals and system requirements
- May exist at a number of levels so may be decomposed into more specific sub-concerns

November 2004

©Ian Sommerville 2004

Slide 13

Concerns

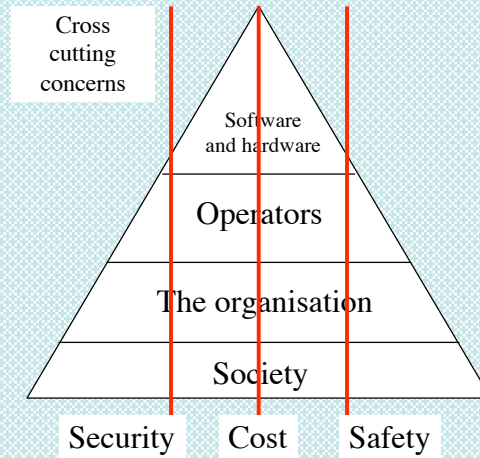
- Concerns are a general mechanism that we have devised that are used to reflect organisational goals. They also reflect constraints on the organisation that reflect the environment in which the organisation operates.
 - Accuracy - the system must provide accurate reports of the numbers of patients treated.
 - Regulation - the system must be developed in accordance with rules set out by some external regulator.
- Safety should be considered as an organisational goal and should be considered in conjunction with other organisational goals and business requirements, Safety is therefore normally an important concern.
- Concerns help focus the requirements engineering process and provide a basis for conflict analysis. We shall see more examples of concerns shortly.

November 2004

©Ian Sommerville 2004

Slide 14

Examples of concerns



November 2004

©lan Sommerville 2004

Slide 15

The MHCPMS

- This system (not its real name but a real system) is a generic medical information system that is configured for use in different regional health trusts
- MHCPMS stands for Mental Health Care Patient Management System
- It supports the management of patients suffering from mental health problems and provides information on their treatment to health service managers

November 2004

©lan Sommerville 2004

Slide 16

System goals

- To provide management information that allows health service managers to assess performance against local and government targets
- To provide medical staff with timely information to facilitate the treatment of patients
- To ensure safety of patients and staff
- To operate in accordance with laws, health service policies and local rules

November 2004

©Ian Sommerville 2004

Slide 17

Mental health care

- Patients do not always attend the same clinic but may attend in different hospitals and local health centres
- A shared information system is therefore a valuable mechanism for ensuring that medical professionals, who may be working at different sites, have up to date information on a patient's condition and treatment
- Patients may be confused and disorganised, miss appointments, deliberately or accidentally lose medication, forget instructions and make unreasonable demands on staff
- Information management is therefore a challenging problem for this system
- Mental health care is safety-critical as a small number of patients may be a danger to themselves and others

November 2004

©Ian Sommerville 2004

Slide 18

Concern identification

- The process of establishing concerns is probably best done in a series of meetings involving business managers and technical staff
- Brainstorming or a similar technique may be used
- Analysis of concerns between meetings is essential and someone should take an explicit action to do this
- Several meetings over a relatively short period of time are required for this stage

November 2004

©Ian Sommerville 2004

Slide 19

Concerns in the MHCPMS

- We have identified the principal concerns in the MHCPMS as:
 - Safety - the system should help reduce the number of occasions where patients cause harm to themselves and others
 - Privacy - patient privacy must be maintained according to the provisions of the Data Protection Act and local ethical guidelines
 - Information quality - the information maintained by the system must be accurate and up-to date
 - Operational costs - the operational costs of the system must be 'reasonable'

November 2004

©Ian Sommerville 2004

Slide 20

Key Points

- An increasing number of information systems of various kinds are safety critical systems
- Data hazards, such as missing data, are an important class of hazards in such systems
- Concerns are cross-cutting issues that reflect the business and dependability goals for the system
- In the MHCPMS, concerns are
 - Information quality
 - Safety
 - Privacy
 - Operational costs

November 2004

©Ian Sommerville 2004

Slide 21

Concerns in the MHCPMS

- We have identified the principal concerns in the MHCPMS as:
 - Safety - the system should help reduce the number of occasions where patients cause harm to themselves and others
 - Privacy - patient privacy must be maintained according to the provisions of the Data Protection Act and local ethical guidelines
 - Information quality - the information maintained by the system must be accurate and up-to date
 - Operational costs - the operational costs of the system must be 'reasonable'

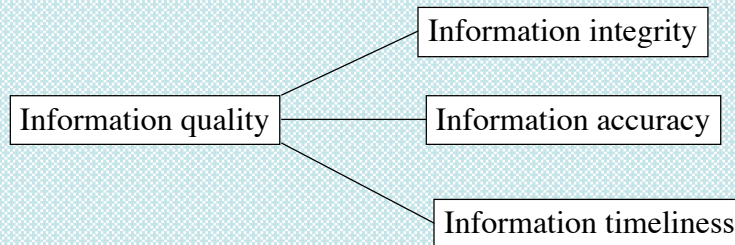
November 2004

©Ian Sommerville 2004

Slide 22

Concern decomposition

- High-level concerns have to be decomposed into sub-concerns:

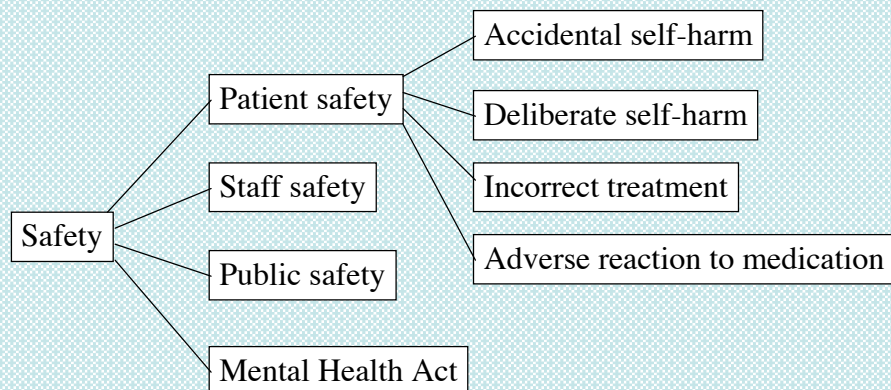


November 2004

©Ian Sommerville 2004

Slide 23

The safety concern



November 2004

©Ian Sommerville 2004

Slide 24

From concerns to questions

- A problem that I find with hazard analysis is the 'requirements gap'. You identify the hazards and possible root causes but there is no method for going from there to requirements
- To address this, we proposed that, after sub-concerns are identified, you should then explicitly identify questions and sub-questions associated with each concern
- Answers to these questions come from system stakeholders and help generate system requirements

November 2004

©Ian Sommerville 2004

Slide 25

Generic questions

- What information relates to the sub-concern being considered?
- Who requires the information and when do they require it?
- How is the information delivered?
- What constraints does the (sub) concern impose?
- What are the consequences of failing to deliver this information?

November 2004

©Ian Sommerville 2004

Slide 26

Deliberate self-harm sub-concern

- What information must be maintained:
 - Information about previous history of self-harm or threats of self-harm
 - Risk assessments by medical staff discussing likelihood of self-harm
- Who needs and information and when:
 - Medical staff during consultations
 - Relatives and carers when self-harm incidents are likely
- How is the information delivered:
 - Can be delivered to medical staff directly through the system.
 - Delivered to relatives and carers through a message from the clinic

November 2004

©Ian Sommerville 2004

Slide 27

Deliberate self-harm sub-concern

- What constraints does this sub-concern impose on the system:
 - No obvious constraints imposed
- What are the consequences of failing to deliver this information:
 - Failing to deliver information about self-harm at the right time may mean an incident of preventable self-harm occurs and the patient's safety is compromised

November 2004

©Ian Sommerville 2004

Slide 28

Concern-cross checking

- A generic problem in complex systems is requirements conflicts where different system requirements are mutually contradictory
- In my view, separating safety analysis in the RE process increases the likelihood of conflict and the costs of resolving that conflict
- Concerns partially address this problem as it allows cross-checking at a higher level of abstraction than the requirements themselves

November 2004

©Ian Sommerville 2004

Slide 29

Concern comparison

- Concerns should be compared in pairs to assess the likelihood of of potential conflicts
- Safety and information quality
 - Conflicts only likely if the requirements allow erroneous or out of date information to be maintained in the system
- Safety and privacy
 - Privacy may impose limits on what information can be shared and who can access that information.
 - Requirements on information sharing and access should be checked
- Safety and operational costs
 - Operational processes that require extensive staff time may be problematic

November 2004

©Ian Sommerville 2004

Slide 30

The privacy concern

- What information:
 - All information in the system that relates to identifiable individuals is covered by the Data Protection Act
- Who needs it:
 - All staff need to be aware of the requirements imposed by the Act
- How delivered:
 - There are no information delivery requirements
- Constraints
 - Personal information may only be disclosed to accredited information users
- Failure consequences:
 - Failure to address the concern could result in legal action against the Trust

November 2004

©Ian Sommerville 2004

Slide 31

A requirements conflict

- To reduce the likelihood of deliberate self-harm, the patient's relatives should be informed of incidents or threats of self-harm
- However, information may only be disclosed to accredited information users
- The privacy concern therefore conflicts with the safety concern

November 2004

©Ian Sommerville 2004

Slide 32

Requirements derivation

- Requirements are derived from the answers to the questions associated with concerns.
- However, there is not a simple 1:1 relationship between answers and requirements. The requirements engineer interprets answers to derive requirements
- By using answers to questions, the problem of stakeholders suggesting requirements that are too specific is reduced

November 2004

©lan Sommerville 2004

Slide 33

MHCPMS requirements

- The system shall provide fields in each patient record that allow details of incidents or threats of deliberate self-harm to be maintained
- The records of patients with a record of deliberate self-harm shall be highlighted to bring them to the attention of clinical system users
- The system shall only permit the transmission of personal patient information to accredited staff and to the patient themselves

November 2004

©lan Sommerville 2004

Slide 34

Concerns and safety analysis

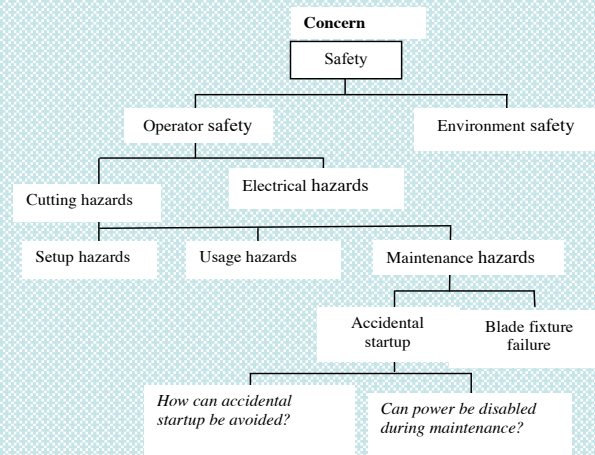
- Concerns are completely compatible with risk-based safety analysis as discussed in previous lectures.
- As we shall see later, each hazard or risk can be represented as a sub-concern.
- However, they provide a mechanism where safety can be integrated with other critical system requirements
- They help highlight trade-offs that may have to be made and conflicts that may arise

November 2004

©Ian Sommerville 2004

Slide 35

Concerns and hazard analysis



November 2004

©Ian Sommerville 2004

Slide 36

The DISCOS process

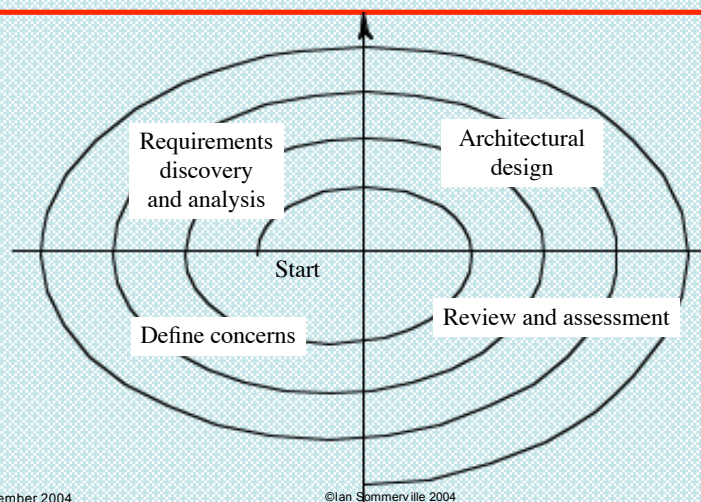
- The DISCOS approach is an approach that we have devised to integrate concerns with other requirements engineering activities
- It is intended (not exclusively) for critical systems requirements engineering
- DISCOS has been designed to be 'method independent'
- Any approach to requirements engineering (use cases, Robertson's VOLERE approach, scenarios, etc. may be used)

November 2004

©Ian Sommerville 2004

Slide 37

DISCOS spiral model



November 2004

©Ian Sommerville 2004

Slide 38

DISCOS activities

- Define concerns
 - Based on the business requirements for the system, establish the principal concerns that should drive the requirements engineering process
- Requirements discovery and analysis
 - Using the concerns as a driver, identify the system requirements
- Architectural design
 - Propose a hardware and software architecture for the system
- Review and assessment
 - Decide whether to continue the process, the effort and time required or whether to release the system requirements description

November 2004

©Ian Sommerville 2004

Slide 39

Key points

- Concerns are decomposed to sub-concerns and questions that then drive the requirements engineering process
- Concerns are a useful mechanism for identifying potential requirements conflicts. Pairwise comparison identifies areas where conflicts could arise
- The answers to concern questions are used to generate the system requirements
- The DISCOS method is a spiral model of requirements engineering for critical systems that integrates concerns, requirements and system architectural design

November 2004

©Ian Sommerville 2004

Slide 40