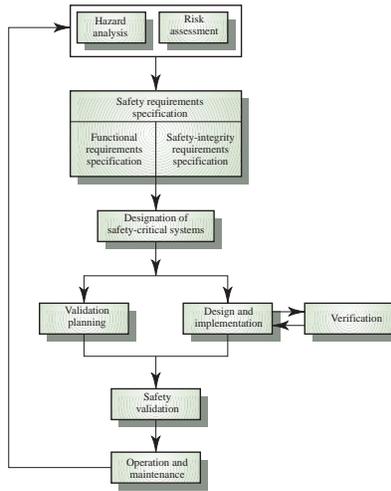
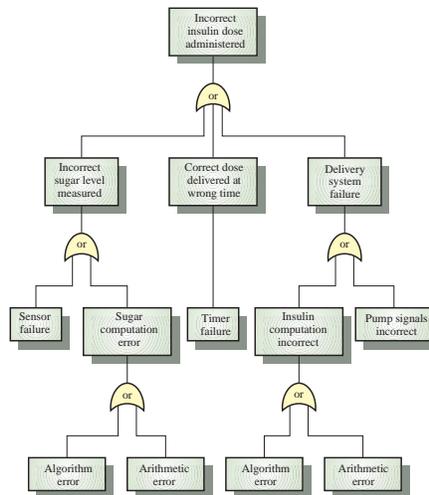


The safety life-cycle



©Ian Sommerville 1995 Software Engineering, 5th edition, Chapter 21 Slide 16

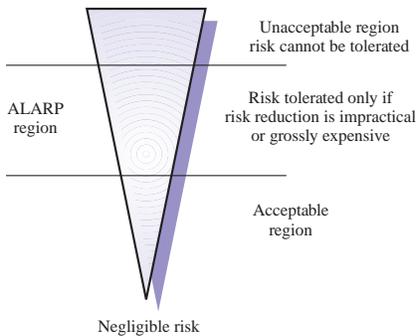
Insulin dose error



©Ian Sommerville 1995 Software Engineering, 5th edition, Chapter 21 Slide 24

Levels of risk

- u Width of triangle is proportional to the cost of dealing with the hazard



©Ian Sommerville 1995 Software Engineering, 5th edition, Chapter 21 Slide 26

Hazard log entry

Hazard Log, Page 4: Printed 21.12.90

System: Insulin Delivery System File: Insulin System/Safety/HLog
Safety Engineer: James Brown Log version: 1.3

Identified Hazard: Insulin overdose delivered to patient

Identified by: Jane Williams

Criticality Class: 1

Identified Risk: Moderate

Fault tree identified: YES Date: 10.11.90 Location: Hazard Log, Page 5

Fault tree creator: Jane Williams and Bill Smith

Fault tree checked: YES Date: 20.11.90 Checker: James Brown

System design safety requirements:

1. Incorporate self-testing software for sensor system, clock and delivery system. This should be executed at least once per minute and should cause an audible warning to be emitted if a fault is discovered. If a fault is discovered, no further insulin deliveries should be made until the system has been reset.
2. Incorporate a patient override facility so that the patient may modify the dose to be delivered by manual intervention. However, a limit should be set on the dose administered by the patient. This limit should be set by medical staff when the system is installed.
3. ...

©Ian Sommerville 1995 Software Engineering, 5th edition, Chapter 21 Slide 37

Informal safety proof

