Critical Systems Validation

Objectives

- To explain how system reliability can be measured and how reliability growth models can be used for reliability prediction
- To describe safety arguments and how these are used
- To discuss the problems of safety assurance
- To introduce safety cases and how these are used in safety validation

Topics covered

- Reliability validation
- Safety assurance
- Security assessment
- Safety and dependability cases

Validation of critical systems

- The verification and validation costs for critical systems involves additional validation processes and analysis than for non-critical systems:
  - The costs and consequences of failure are high so it is cheaper to find and remove faults than to pay for system failure;
  - You may have to make a formal case to customers or to a regulator that the system meets its dependability requirements. This dependability case may require specific V & V activities to be carried out.

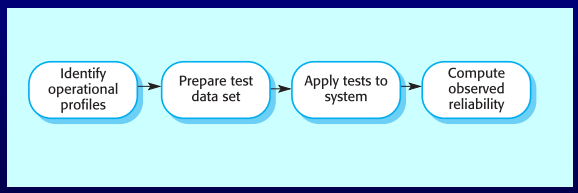
Validation costs

- Because of the additional activities involved, the validation costs for critical systems are usually significantly higher than for non-critical systems.
- Normally, V & V costs take up more than 50% of the total system development costs.

Reliability validation

- Reliability validation involves exercising the program to assess whether or not it has reached the required level of reliability.
- This cannot normally be included as part of a normal defect testing process because data for defect testing is (usually) atypical of actual usage data.
- Reliability measurement therefore requires a specially designed data set that replicates the pattern of inputs to be processed by the system.

The reliability measurement process



Reliability validation activities

- Establish the operational profile for the system.
- Construct test data reflecting the operational profile.
- Test the system and observe the number of failures and the times of these failures.
- Compute the reliability after a statistically significant number of failures have been observed.

Statistical testing

- Testing software for reliability rather than fault detection.
- Measuring the number of errors allows the reliability of the software to be predicted. Note that, for statistical reasons, more errors than are allowed for in the reliability specification must be induced.
- An acceptable level of reliability should be specified and the software tested and amended until that level of reliability is reached.

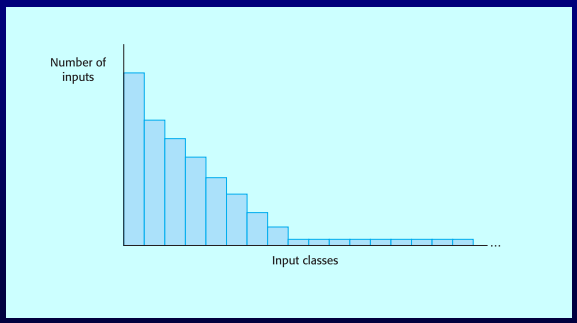
Reliability measurement problems

- Operational profile uncertainty
  - The operational profile may not be an accurate reflection of the real use of the system.
- High costs of test data generation
  - Costs can be very high if the test data for the system cannot be generated automatically.
- Statistical uncertainty
  - You need a statistically significant number of failures to compute the reliability but highly reliable systems will rarely fail.

Operational profiles

- An operational profile is a set of test data whose frequency matches the actual frequency of these inputs from 'normal' usage of the system. A close match with actual usage is necessary otherwise the measured reliability will not be reflected in the actual usage of the system.
- It can be generated from real data collected from an existing system or (more often) depends on assumptions made about the pattern of usage of a system.

An operational profile



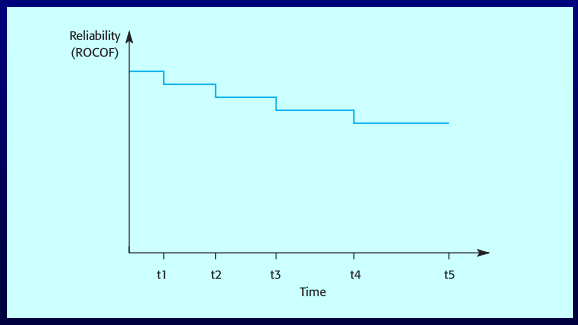
Operational profile generation

- Should be generated automatically whenever possible.
- Automatic profile generation is difficult for interactive systems.
- May be straightforward for ‘normal’ inputs but it is difficult to predict ‘unlikely’ inputs and to create test data for them.

Reliability prediction

- A reliability growth model is a mathematical model of the system reliability change as it is tested and faults are removed.
- It is used as a means of reliability prediction by extrapolating from current data
  - Simplifies test planning and customer negotiations.
  - You can predict when testing will be completed and demonstrate to customers whether or not the reliability growth will ever be achieved.
- Prediction depends on the use of statistical testing to measure the reliability of a system version.

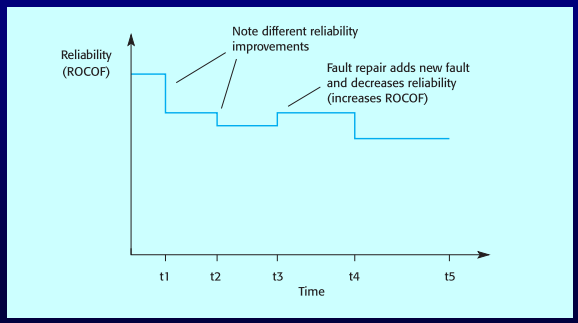
Equal-step reliability growth



Observed reliability growth

- The equal-step growth model is simple but it does not normally reflect reality.
- Reliability does not necessarily increase with change as the change can introduce new faults.
- The rate of reliability growth tends to slow down with time as frequently occurring faults are discovered and removed from the software.
- A random-growth model where reliability changes fluctuate may be a more accurate reflection of real changes to reliability.

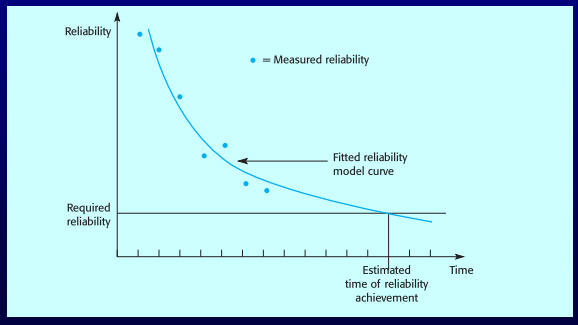
Random-step reliability growth



Growth model selection

- Many different reliability growth models have been proposed.
- There is no universally applicable growth model.
- Reliability should be measured and observed data should be fitted to several models.
- The best-fit model can then be used for reliability prediction.

Reliability prediction



Safety assurance

- Safety assurance and reliability measurement are quite different:
  - Within the limits of measurement error, you know whether or not a required level of reliability has been achieved;
  - However, quantitative measurement of safety is impossible. Safety assurance is concerned with establishing a confidence level in the system.

Safety confidence

- Confidence in the safety of a system can vary from very low to very high.
- Confidence is developed through:
  - Past experience with the company developing the software;
  - The use of dependable processes and process activities geared to safety;
  - Extensive V & V including both static and dynamic validation techniques.

Safety reviews

- Review for correct intended function.
- Review for maintainable, understandable structure.
- Review to verify algorithm and data structure design against specification.
- Review to check code consistency with algorithm and data structure design.
- Review adequacy of system testing.

Review guidance

- Make software as simple as possible.
- Use simple techniques for software development avoiding error-prone constructs such as pointers and recursion.
- Use information hiding to localise the effect of any data corruption.
- Make appropriate use of fault-tolerant techniques but do not be seduced into thinking that fault-tolerant software is necessarily safe.

Safety arguments

- Safety arguments are intended to show that the system cannot reach in unsafe state.
- These are weaker than correctness arguments which must show that the system code conforms to its specification.
- They are generally based on proof by contradiction
  - Assume that an unsafe state can be reached;
  - Show that this is contradicted by the program code.
- A graphical model of the safety argument may be developed.

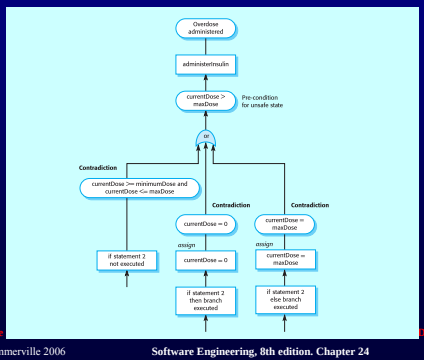
Construction of a safety argument

- Establish the safe exit conditions for a component or a program.
- Starting from the END of the code, work backwards until you have identified all paths that lead to the exit of the code.
- Assume that the exit condition is false.
- Show that, for each path leading to the exit that the assignments made in that path contradict the assumption of an unsafe exit from the component.

Insulin delivery code

```
currentDose = computeInsulin () ;
// Safety check - adjust currentDose if necessary
// if statement 1
if (previousDose == 0)
{
      if (currentDose > 16)
            currentDose = 16 ;
}
else
      if (currentDose > (previousDose * 2) )
            currentDose = previousDose * 2 ;
// if statement 2
if ( currentDose < minimumDose )
            currentDose = 0 ;
else if ( currentDose > maxDose )
            currentDose = maxDose ;
administerInsulin (currentDose) ;
```


Safety argument model



Program paths

- Neither branch of if-statement 2 is executed
  - Can only happen if CurrentDose is >= minimumDose and <= maxDose.
- then branch of if-statement 2 is executed
  - currentDose = 0.
- else branch of if-statement 2 is executed
  - currentDose = maxDose.
- In all cases, the post conditions contradict the unsafe condition that the dose administered is greater than maxDose.

Process assurance

- Process assurance involves defining a dependable process and ensuring that this process is followed during the system development.
- As discussed in Chapter 20, the use of a safe process is a mechanism for reducing the chances that errors are introduced into a system.
  - Accidents are rare events so testing may not find all problems;
  - Safety requirements are sometimes 'shall not' requirements so cannot be demonstrated through testing.

Safety related process activities

- Creation of a hazard logging and monitoring system.
- Appointment of project safety engineers.
- Extensive use of safety reviews.
- Creation of a safety certification system.
- Detailed configuration management (see Chapter 29).

Hazard analysis

- Hazard analysis involves identifying hazards and their root causes.
- There should be clear traceability from identified hazards through their analysis to the actions taken during the process to ensure that these hazards have been covered.
- A hazard log may be used to track hazards throughout the process.

Hazard log entry

Hazard Log **Page 4: Printed 20.02.2**

System: Insulin Pump System *File:* InsulinPump/Safety/HazardLog
Safety Engineer: James Brown *Log version:* 1/3

Identified Hazard	Insulin overdose delivered to patient				
Identified by	Jane Williams				
Criticality class	1				
Identified risk	High				
Fault tree identified	YES	*Date*	24.01.99	*Location*	Hazard Log, Page 5
Fault tree creators	Jane Williams and Bill Smith				
Fault tree checked	YES	*Date*	28.01.99	*Checker*	James Brown

System safety design requirements

1. The system shall include self-testing software that will test the sensor system, the clock and the insulin delivery system.
2. The self-checking software shall be executed once per minute
3. In the event of the self-checking software discovering a fault in any of the system components, an audible warning shall be issued and the pump display should indicate the name of the component where the fault has been discovered. The delivery of insulin should be suspended.
4. The system shall incorporate an override system that allows the system user to modify the computed dose of insulin that is to be delivered by the system.
5. The amount of override should be limited to be no greater than a pre-set value that is set when the system is configured by medical staff.

Run-time safety checking

- During program execution, safety checks can be incorporated as assertions to check that the program is executing within a safe operating 'envelope'.
- Assertions can be included as comments (or using an assert statement in some languages). Code can be generated automatically to check these assertions.

Insulin administration with assertions

```
static void administerInsulin ( ) throws SafetyException {

        int maxIncrements = InsulinPump.maxDose / 8 ;
        int increments = InsulinPump.currentDose / 8 ;

        // assert currentDose <= InsulinPump.maxDose

        if (InsulinPump.currentDose > InsulinPump.maxDose)
            throw new SafetyException (Pump.doseHigh);
        else
            for (int i=1; i<= increments; i++)
            {
                generateSignal () ;
                if (i > maxIncrements)
                    throw new SafetyException ( Pump.incorrectIncrements);
            } // for loop

    } //administerInsulin
```


Security assessment

- Security assessment has something in common with safety assessment.
- It is intended to demonstrate that the system cannot enter some state (an unsafe or an insecure state) rather than to demonstrate that the system can do something.
- However, there are differences
  - Safety problems are accidental; security problems are deliberate;
  - Security problems are more generic - many systems suffer from the same problems; Safety problems are mostly related to the application domain

Security validation

- Experience-based validation
  - The system is reviewed and analysed against the types of attack that are known to the validation team.
- Tool-based validation
  - Various security tools such as password checkers are used to analyse the system in operation.
- Tiger teams
  - A team is established whose goal is to breach the security of the system by simulating attacks on the system.
- Formal verification
  - The system is verified against a formal security specification.

Security checklist

1. Do all files that are created in the application have appropriate access permissions? The wrong access permissions may lead to these files being accessed by unauthorised users.
2. Does the system automatically terminate user sessions after a period of inactivity? Sessions that are left active may allow unauthorised access through an unattended computer.
3. If the system is written in a programming language without array bound checking, are there situations where buffer overflow may be exploited? Buffer overflow may allow attackers to send code strings to the system and then execute them.
4. If passwords are set, does the system check that password are ÕstrongÕ Strong passwords consist of mixed letters, numbers and punctuation and are not normal dictionary entries. They are more difficult to break than simple passwords.

Safety and dependability cases

- Safety and dependability cases are structured documents that set out detailed arguments and evidence that a required level of safety or dependability has been achieved.
- They are normally required by regulators before a system can be certified for operational use.

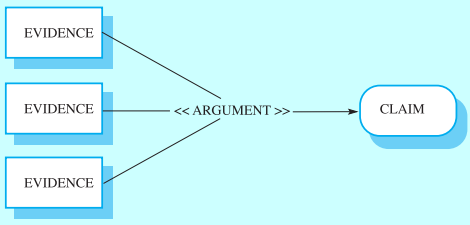
The system safety case

- It is now normal practice for a formal safety case to be required for all safety-critical computer-based systems e.g. railway signalling, air traffic control, etc.
- A safety case is:
  - A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.
- Arguments in a safety or dependability case can be based on formal proof, design rationale, safety proofs, etc. Process factors may also be included.

Components of a safety case

Component	Description
System description	An overview of the system and a description of its critical components.
Safety requirements	The safety requirements abstracted from the system requirements specification.
Hazard and risk analysis	Documents describing the hazards and risks that have been identified and the measures taken to reduce risk.
Design analysis	A set of structured arguments that justify why the design is safe.
Verification and validation	A description of the V & V procedures used and, where appropriate, the test plans for the system. Results of system V &V.
Review reports	Records of all design and safety reviews.
Team competences	Evidence of the competence of all of the team involved in safety-related systems development and validation.
Process QA	Records of the quality assurance processes carried out during system development.
Change management processes	Records of all changes proposed, actions taken and, where appropriate, justification of the safety of these changes.
Associated safety cases	References to other safety cases that may impact on this safety case.

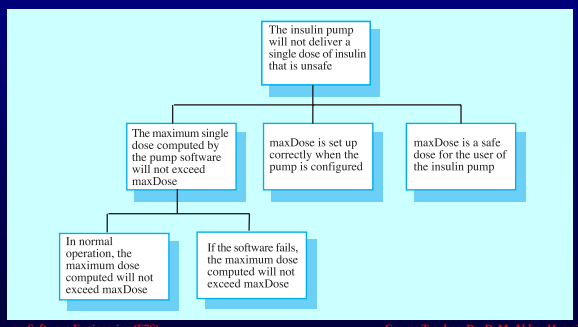
Argument structure



Insulin pump argument

Claim:	The maximum single dose computed by the insulin pump will not exceed maxDose.
Evidence:	Safety argument for insulin pump as shown in Figure 24.7
Evidence:	Test data sets for insulin pump
Evidence:	Static analysis report for insulin pump software
Argument:	The safety argument presented shows that the maximum dose of insulin that can be computed is equal to maxDose. In 400 tests, the value of Dose was correctly computed and never exceeded maxDose. The static analysis of the control software revealed no anomalies. Overall, it is reasonable to assume that the claim is justified.

Claim hierarchy



Key points

- Reliability measurement relies on exercising the system using an operational profile - a simulated input set which matches the actual usage of the system.
- Reliability growth modelling is concerned with modelling how the reliability of a software system improves as it is tested and faults are removed.
- Safety arguments or proofs are a way of demonstrating that a hazardous condition can never occur.

Key points

- It is important to have a dependable process for safety-critical systems development. The process should include hazard identification and monitoring activities.
- Security validation may involve experience-based analysis, tool-based analysis or the use of ‘tiger teams’ to attack the system.
- Safety cases collect together the evidence that a system is safe.