

Critical Systems Engineering 2000

Week: 7 and 8

Course topic: Critical Systems Validation

Objective: To discuss the specification of dependable systems with a particular focus on reliability and safety specification.

Essential reading: “Software Engineering”, 5th edition. Chapter 18 (Sections 18.3 and 18.4) and Chapter 21 (Section 21.3).

Background reading: Software Reliability Handbook (ed P. Rook) Elsevier
Safety-critical Systems, M. Storey, Addison Wesley

Web resources: <http://info.comp.lancs.ac.uk/year3/notes/options/365/index.htm>

Self-test:

1. Discuss the role of formal methods in the validation of critical systems
2. Briefly describe the process of reliability validation
3. What are the main problems in validating system reliability
4. Explain why an operational profile can be difficult to define
5. What is a reliability growth model and how is it used to predict reliability?
6. Explain why the equal-step model of reliability growth is simplistic.
7. Why is there no such thing as a 'standard' reliability growth model?
8. Describe 4 design principles for safe software
9. What is a system safety case? Who uses a safety case?
10. Describe 4 types of safety review
11. Explain how hazards should be used to drive safety reviews
12. What is a safety proof and how are safety proofs normally developed?
13. Why is it easier to develop a proof of safety rather than a proof of correctness
14. How are safety assertions used to support the process of run-time safety checking?
Give examples from the insulin pump system.
15. Explain why the Ariane 5 launcher failure can be thought of as a failure of the validation process.