

Critical Systems Engineering 2000

Weeks: 3 and 4

Course topic: Dependable Systems Specification

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 and Chapter 21 (Section 21.2).

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. Why is it the case that dependability specifications must sometimes be described in terms of forbidden behaviour?
2. What are the arguments for and against the use of formal specification techniques when specifying critical systems?
3. What must be taken into account when producing a system reliability specification?
4. Explain why reliability should be specified quantitatively?
5. Describe the 4 metrics that may be used to specify reliability?
6. Explain why ROCOF is an inappropriate metric for specifying the reliability of a telephone exchange system
7. Why must time units be considered when specifying reliability?
8. Briefly describe the process of reliability specification
9. Explain why POFOD is an appropriate metric to specify the reliability of the insulin delivery system? What metrics would be inappropriate for use in the context? Why?
10. Why should safety requirements be specified separately?
11. Describe the key stages in the safety life cycle
12. What is the role of hazard analysis in developing a safety specification?
13. Explain how fault trees are used in hazard analysis
14. Explain how safety requirements are generated from a hazard analysis
15. Describe the stages in the process of developing a security specification