

# Critical Systems Engineering 2000

**Week:** 5 and 6

**Course topic:** Dependable Software Development

**Objective:** To discuss software development techniques that may be used when implementing critical systems with a particular focus on techniques for software fault tolerance.

**Essential reading:** “Software Engineering”, 5<sup>th</sup> edition. Chapter 19.

**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. Briefly describe two complementary approaches that may be used to support the development of dependable software
2. What preconditions are necessary for the development of fault-free software?
3. Explain why some programming language constructs are error-prone and briefly describe the problems with 4 error-prone constructs.
4. What is information hiding and why is it important in the development of critical systems?
5. Why is the process that is used important in critical systems development?
6. Briefly describe 4 process validation activities
7. What is a fault tolerant systems and what actions are necessary in such a system?
8. Describe two complementary approaches to achieving system fault tolerance
9. What is an exception and why are exception management facilities essential if a fault-tolerant system is to be developed?
10. Describe two approaches to fault detection and explain why both of these may be required.
11. What are the limitations of Java’s type model in supporting fault detection?
12. What is damage assessment? Describe three damage assessment techniques that may be used.
13. What is the difference between forward and backward error recovery?
14. Why do some systems have to be built around a fault-tolerant architecture?

15. Explain the differences between N-version programming and recovery block architectures for fault tolerance.
16. Why is design diversity important in the development of fault-tolerant systems?
17. How is design diversity achieved in the Airbus flight control system?
18. What do you understand by the concept of system survivability?
19. Briefly describe 4 steps in a method for survivability analysis and improvement.
20. Describe three strategies for improving the survivability of a system.