Seminar Dicussion Questions on Reliability Types

Exercise 1.

You are a software engineering consultant to a team designing a networked traffic light system for a city centre. The design that is emerging is of a number of processor nodes controlling the lights in their vicinity, networked to a "master" control computer. Your role is to advise on reliability issues.

(a) The operational requirements of a real-time system can be classified as *fail-operational, fail-active, fail-safe,* and *high-availability.* Describe the characteristics of each of these four categories, and classify the traffic light system in one of these categories, giving your reasons.

(b) What particular reliability issues arise as a result of the fact that the system is *distributed*?

(c) You have been asked by the team leader to explain various options for designing the software to be fault-tolerant. Describe each of these techniques ...

- backward error recovery with recovery blocks
- exception handling
- N-version programming

(d) Consider the strengths and weaknesses of each of these and make a recommendation of one for the traffic light system.

Exercise 2

You are a software engineer in a team designing a control system for a network of electricity distribution substations. The consensus in the team is that each substation should have a control processor monitoring and controlling the plant in the substation, and these should be networked to a central control computer. Your role is to advise on reliability issues.

(a) Should the operational requirements this real-time system be classified as *fail-operational, fail-active, fail-safe,* or *high-availability*? Define these four categories, and give reasons for your choice.

(b) What particular reliability issues arise as a result of the fact that the system is *distributed*?

(c) Briefly describe a protocol which the distributed system can use so that processing nodes always agree on the ordering of events.

(d) Explain the following fault-tolerant software design techniques and recommend one for the control system.

- backward error recovery with recovery blocks
- exception handling
- N-version programming

Exercise 3

A car production line contains a number of conveyors and robotic tools controlled by networked processors which communicate data gathered by various sensors. This system requires certain level of *fault tolerance*, as a failure of any part of it will result in the production line clogging and possible damage to the cars.

(a) Explain the four levels of fault tolerance. Which is appropriate for the production line system?

(b) Various application software error-handling approaches are possible: *exception handling*; *backward error recovery* using *recovery blocks; and N-version programming*. Define these and discuss their suitability for the production line system.

(c) The system is distributed, employing several processors in different parts of the production line, communicating via a network. What particular reliability issues arise as a result of this fact?

Exercise 4

A building environmental (air temperature, humidity, CO_2 level) control system has a requirement for fault tolerance. Software engineering consultants to the design team suggested using ***recovery blocks*** to build fault-tolerance into the system software; the design team leader responded that ***exception handling*** is essentially the same, and they would use this approach instead.

(a) Clearly explain each of these two approaches, and evaluate the design team leader's comment by comparing and contrasting them.

(b) The operational requirements of a real-time system can be classified as *fail-operational, fail-active, fail-safe,* and *high-availability.* Describe the characteristics of each of these four categories, and classify the environmental control system in one of these categories, giving your reasons.

(c) Another approach is ***N-version programming***. Compare this with the previous two approaches: would this be a suitable alternative for the environmental control system?

(d) The system is distributed, employing several processors in different parts of the building, communicating via a network. What particular reliability issues arise as a result of this fact?