P 10q1
RJA

Part Ia / IIg / Dip Software engineering I

2000

(1) One means of improving system reliability is to have three or more replicated systems and act on their majority output. Give two examples of failure that can be stopped by this mechanism, and two which cannot. At least one of each type should be illustrated by an ~~real~~ actual case history or application.

(12 marks)

An engineer attempts to (further) improve the reliability of such a system by multiversion programming – by having three separate systems coded by different teams and possibly in different languages. Discuss what might still go wrong

(8 marks)

(A) Examples stopped:

- Hardware failure, eg breakdown. Example: avionics
- Attack, eg by bad person physically loading a new copy of the operating system on to a server
- ...

Examples not stopped:

- Management failure, eg. London Ambulance Service
- Logical attack, eg malicious code

What still goes wrong with multiversion programming: management errors, specification errors, configuration errors, redundancy management errors, ...