THE BRITISH COMPUTER SOCIETY

THE BCS PROFESSIONAL EXAMINATION
Professional Graduate Diploma

SAFETY CRITICAL AND REAL TIME SOFTWARE

14th May 2003, 2.30 p.m.-5.30 p.m.
Answer THREE questions out of FIVE. All questions carry equal marks.
Time: THREE hours.

*The marks given in brackets are **indicative** of the weight given to each part of the question.*

1. A manufacturer of medical devices is considering introducing a new design of *infusion pump*[1]. Most of the control functionality of the pump will be provided by software. The pump operates in three modes: *administrative, normal* and *demand*. In summary:

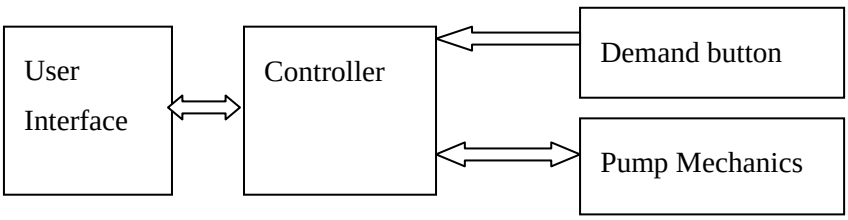
- In *administrative mode* the dose amounts and intervals are set and the maximum dose in any three-hour period.
- In *normal mode* the pump administers the set dose at the specified interval, provided the maximum dose is not exceeded.
- In *demand mode* a dose is delivered if the patient presses the demand button by the bedside provided the dose will not exceed the maximum.

a) Describe what hazard analysis should be carried out before committing to the development of the project. In your answer be specific about what techniques you think are applicable and describe briefly what kind of information you would expect to derive from them. **(6 marks)**

b) Consider the simplified schematic for the pump given below. Draw a fault tree for this simple system where the top event is *maximum dose exceeded*. **(8 marks)**

c) Outline the main risks in widely deploying a system of this kind over a large number of hospitals. For the risks you identify suggest ways to control them. **(6 marks)**

d) It is important that the maximum dose is not exceeded at any time. A hospital environment is difficult to control and the pump and controller may experience unscheduled power outages. Suggest a robust architecture to ensure the specified dose is not exceeded. **(5 marks)**



[1] An *infusion pump* is a medical device that is intended to deliver medication to a patient in a controlled manner. For example, if a patient is in pain an infusion pump can be used to deliver controlled doses of painkiller at regular intervals. Such pumps can also deliver medication on demand from the patient provided the requested medication is inside limits set by the clinician. Frequently repeated demands by the patient will eventually be refused by the system to avoid overdose.

2. A manufacturer of a software-controlled component for use in telephony applications is developing a component that has a requirement for 99.999% availability. The component will comprise a few thousand lines of source code.

a) Describe how the manufacturer might go about constructing the component in order to make a credible claim that the requirement has been achieved. **(10 marks)**

b) Unfortunately, after the component has been developed the estimated availability is 99.99%. The manufacturer does not want to re-develop the component, but is prepared to develop additional software to help achieve the requirement. What software would you advise the manufacturer to develop? **(6 marks)**

c) In testing the component has never failed in the first day of operation. The component is intended to provide a short-lived service (taking a few seconds to complete). In these circumstances what approaches might be used to increase the availability of the component? **(3 marks)**

d) "*Because design faults are responsible for software failures the use of statistical approaches to measure availability or reliability is invalid."* What are the main points for and against this assertion? **(6 marks)**

3. A large, highly diversified, company has retained you to act as a consultant on software process and certification issues. The company must certify products to different standards, at the highest levels, depending on the intended market for the product. These include DO-178B, IEC 61508 and MoD 00-55. You have been hired to assist in opening up a new business area in medical systems.

a) The company's first product is an implantable device intended for use on very seriously ill patients. One group proposes using IEC 61508 as the main standard to inform the development process for the software in the new device. Write a short briefing note advising on the soundness of this proposal. **(6 marks)**

b) The company is also proposing to develop software for large scale imaging devices that involve large amounts of software and incorporate Commercial Off-The-Shelf (COTS) software. Some of the software is high-criticality (e.g. image processing systems).

i) Write a briefing note advising which of the above three standards is most appropriate to the development of the proposed systems. **(6 marks)**

ii) Explain why *partitioning* arguments are particularly important in justifying the safety of such systems. **(4 marks)**

c) The company currently has a Capability Maturity Model level 3 process. Outline what would be necessary to move to a CMM level 4 process and the impact that would have on certifying products. **(4 marks)**

d) "*Formal methods are not applicable to large-scale systems because the cost per line of code is very high."* What are the main points for and against this assertion? **(5 marks)**

4. Answer each of the following:

a) Explain the difference between static and dynamic redundancy in the context of hardware architectures for safety related systems. Give diagrams that illustrate a triple-redundant architecture of each type and contrast their properties, illustrating your answer with examples of applications for which each type would be suited. **(8 marks)**

b) Explain the meaning of *common mode failure* in the context of redundant architectures. Identify potential common-mode failure points in relation to the architectures you supplied in answer to part *a)* of this question. **(5 marks)**

c) Explain how software redundancy may be used to increase the reliability of a safety-related computer system. In your answer you should describe, and consider the roles of, n-version programming, recovery blocks, temporal redundancy, and information redundancy. **(12 marks)**

5. An on-line booking system allows multiple enquiries and updates to be carried out simultaneously on a database.

a) Briefly explain the problems that might arise in this system if concurrency is not managed correctly. **(7 marks)**

b) Outline how the system might be implemented using semaphores to manage concurrency. **(6 marks)**

c) Outline an alternative implementation using a monitor to control concurrency. **(6 marks)**

d) State, with reasons, which of the two implementations you consider preferable. **(6 marks)**