THE BRITISH COMPUTER SOCIETY

THE BCS PROFESSIONAL EXAMINATION
Professional Graduate Diploma

SAFETY CRITICAL & REAL TIME SOFTWARE

8th May 2002, 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.*

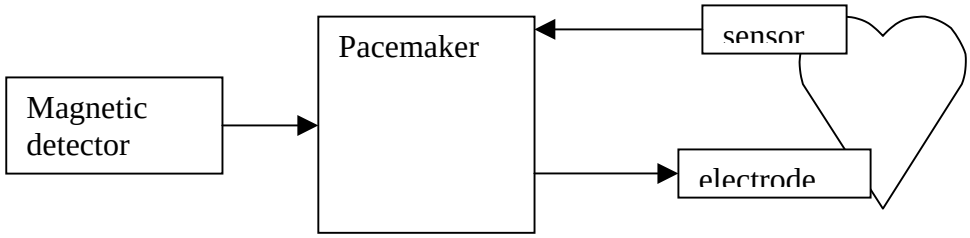
1. A manufacturer of medical devices is considering introducing a new design of *heart pacemaker*[1]. Most of the functionality of the pacemaker will be provided by software. The pacemaker operates in two modes: normal and maintenance. In *normal mode* the pacemaker regulates the pace of the heart. In *maintenance mode* the pacemaker interacts with the hospital control system to allow parameters to be set etc.. The change between modes is made when a magnetic pulse detector detects a particular pattern of magnetic fields of sufficient strength.

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 pacemaker system given below. The system detects the current rhythm of heart activity from a heart sensor and then regulates the pace of the heart via an electrode attached to the heart. The magnetic detector is responsible for detecting the need for mode changes. Draw a fault tree for this simple system where the top event is *heart is not paced properly*. **(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) The timing characteristics of the pacemaker are very important. Suggest an architecture for the software that could achieve millisecond precision in the timing of the pulses. Justify your answer. **(5 marks)**



2. *a)* Explain what is meant by deadlock and list the conditions that are necessary for it to occur. **(8 marks)**

b) Describe an algorithm for deadlock avoidance and discuss any advantages and disadvantages of using it. **(17 marks)**

---

[1] A heart pacemaker is an electronic device that is intended to regulate the rhythm of the heart in patients whose natural system has failed in some way. It does this by applying a small electric charge to the heart muscle in a repeated pattern.

3. A manufacturer of a software controlled component for use in telephony applications has developed a component that has a mean time to failure of 100 days and a mean time to repair of 1 day. Faults in the system can be detected completely reliably.

a) The manufacturer wants to deploy the component in a situation requiring high availability. The customer wants the system to be available 99.9% of the time. Suggest an architecture using this component that will achieve the required level of availability. Justify your answer. Clearly identify any assumptions you make about the availability or reliability of all components in the architecture. Are the assumptions realistic? **(9 marks)**

b) The manufacturer argues that diversity in the high availability system might be increased by having software developed by different teams in each of the components. What are the arguments for and against this? **(5 marks)**

c) What approaches would you suggest the manufacturer adopt in their software development process to ensure the software in the component achieves a mean time to failure of 100 days? **(5 marks)**

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

4. 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.

a) Write a short note explaining safety integrity levels (SILs) used in IEC 61508 and how we determine the SIL for a particular component in a system. In addition, provide a brief outline of the kinds of software process necessary to create components at the different SILs. **(10 marks)**

b) Write a short briefing note explaining the main points of similarity and difference between DO-178B and MoD 00-55 and how this might influence the approach to developing software under the different standards. **(6 marks)**

c) The company currently has a Capability Maturity Model level 4 process. Outline what would be necessary to move to a CMM level 5 process and the impact that would have on certifying products. **(4 marks)**

d) *"Formal methods make no direct contribution to the safety of systems designed using formal methods because the proofs always concern models of the system, not the running code."* What are the main points for and against this assertion? **(5 marks)**

5. *a)* Explain, with an example, why problems can arise when processes running asynchronously are sharing resources. **(5 marks)**

b) Describe THREE different programming language constructs that can be used to prevent these problems arising and discuss their effectiveness. **(12 marks)**

c) In an aircraft navigation system, there is a pool of data containing the aircraft's position: latitude, longitude and altitude. This pool of data is updated by a geographical positioning system and is read by the software that controls the aircraft's speed and direction. Using one of the constructs described in part *b)*, show how access to this pool of data might be controlled. You may assume that all the software in question is running on the processor. **(8 marks)**