THE BRITISH COMPUTER SOCIETY

THE BCS PROFESSIONAL EXAMINATION
Professional Graduate Diploma

SAFETY CRITICAL AND REAL TIME SOFTWARE

19th April 2005, 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 car manufacturer is considering introducing a *steer-by-wire* system that uses a computer system to control a servo that changes the direction of the wheels to ensure that they agree with the position of the steering wheel.

a) Describe what hazard analysis should be carried out before embarking on 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 steer-by-wire system given below. The computer detects the required direction of turn from the steering wheel sensor and then controls the servo to ensure the direction of the wheels matches the required direction. Draw a fault tree for this simple system where the top event is *wheels point in the wrong direction.*

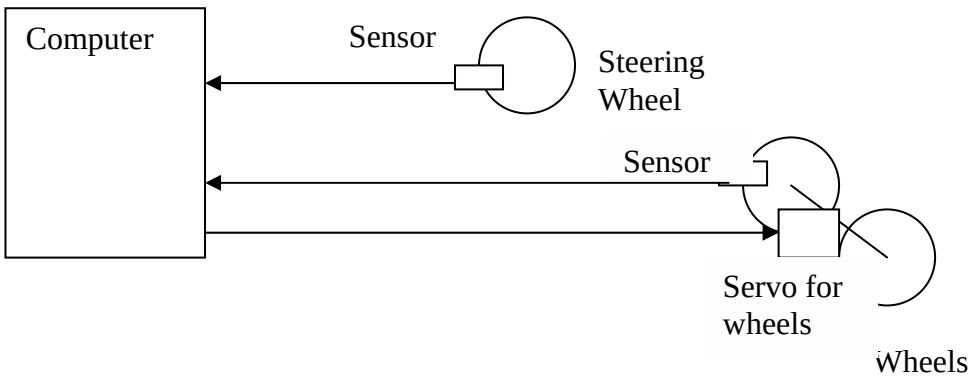
(8 marks)

c) Outline how you would go about carrying out a risk assessment for such a system. The car manufacturer is aiming to sell 50,000 copies of this car each year. How would this influence your approach to the assessment?

(6 marks)

d) The solution being considered uses an interrupt-driven system based on interrupts generated by the sensors when the positions they are monitoring change. Outline the strengths and weaknesses of this approach in this context and propose an alternative approach to the construction of the system.

(5 marks)



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 hospital robotics.

a) The company's first product is a medium-sized mobile robot weighing approximately 50Kg that is intended to undertake delivery duties around the hospital (delivering soiled linen to the laundry, delivering samples to the pathology laboratory, etc). One group proposes using IEC 61508 as the main standard to inform the development process for the software in the new robot. Write a short briefing note advising on the soundness of this proposal. **(6 marks)**

b) The company is worried that it may not get the product to market in time to beat its competitors so it has two teams working on the software in parallel:

i) One team is using formal methods to develop a small highly reliable system. Provide a briefing note for the manufacturer explaining which of the above three is the best standard to use for this team and how likely it is that this approach will lead to an acceptable product that reaches the market on time. **(5 marks)**

ii) A second team is developing the system by adapting a very large Commercial Off-The-Shelf (COTS) system. Provide a briefing note for the manufacturer explaining which of the above three is the best standard to use for this team and how likely it is that this approach will lead to an acceptable product that reaches the market on time. **(5 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) *"COTS components are not usable in safety-critical environments because we can never be confident of their properties."* What are the main points for and against this assertion? **(5 marks)**

4. *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.

(9 marks)

c) In a machine for delivering radiotherapy, there is an area of memory that holds the details about the dosage to be delivered to the patient. This is set by an operator using a keyboard, who can also correct the information if it has been entered wrongly. It is accessed by a process that displays the current setting on the operator's screen and by a process that controls the delivery of the dose. Using one of the constructs described in section (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 same processor. **(11 marks)**

5. Describe the main functions of a real time executive suitable for use in small real time systems.

(10 marks)

Outline a generic design for such an executive and indicate the main design decisions that have to be taken and the factors that affect them.

(15 marks)