THE BRITISH COMPUTER SOCIETY

THE BCS PROFESSIONAL EXAMINATION
Professional Graduate Diploma

SAFETY CRITICAL AND REAL TIME SOFTWARE

20th April 2004, 10.00 a.m.-1.00 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 *proximity warning system* which sounds a warning if the car approaches too close to anything. The system operates in three modes:

- **Disabled:** the driver has turned off the system.
- **Parking:** both the front and rear sensors are operational and the system gives a warning when the car approaches within a few centimeters of an object.
- **Driving:** the system gives one audible warning when the car approaches too close to an object in front of it and different audible warning when an object approaches too close to the rear of the car. The distance at which these warnings activate depends on the speed of the car.

The system switches automatically to parking mode when the car is traveling slower than a preset speed.

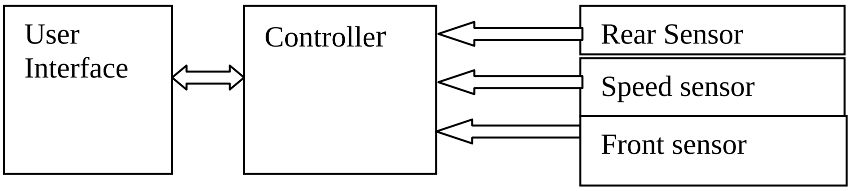
a) Describe what hazard analysis should be carried out before committing to the development of the project. In your answer be specific about what techniques you think are applicable and describe briefly what kind of information you would expect to derive from them. **(6 marks)**

b) What are the main hazards in the deployment of such a system? Provide at least two hazards and some justification that they are significant for the system. **(4 marks)**

c) Consider the simplified schematic for the system given below. Draw a fault tree for this simple system where the top event is *false warning provided*. **(8 marks)**

d) Outline the main risks in widely deploying a system of this kind over a large number of cars. Suggest ways of controlling these risks. **(4 marks)**

e) An engineer suggests that instead of providing a audible warning the system should apply the brakes if the car gets too close to the car in front. Is this a good or bad suggestion? Provide a justification for your answer**.** **(3 marks)**



2. A manufacturer of software-controlled telephone exchanges is developing a new system. In outline, the system will comprise three components:

- A supervisory component that detects incoming calls and initiates a new process to handle individual calls.
- A component to handle individual calls.
- A component to log activity and faults in order to provide input to the billing system and diagnostic information for engineers.

a) Explain the terms *reliability* and *availability*. The manufacturer wants to construct a system with high availability and reliability. Suggest target levels of availability and reliability for the system. Explain how meeting this overall requirement influences the required availability and reliability of the components described above. **(6 marks)**

b) Describe what methods a manufacturer might want to use to make a case that the required levels of availability and reliability have been achieved by each component. **(8 marks)**

c) Suppose that:
i) the overall system just fails to meet the required availability,
ii) the system has the capacity to self-detect failure with very high reliability, and
iii) the manufacturer wants to improve the availability without developing more software.
Suggest an approach the manufacturer might take to improve the availability of the system. Justify your answer. **(6 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? **(5 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 domestic robotics.

a) The company's first product is a medium-sized robot weighing approximately 50Kg that is intended to undertake household duties (cleaning, doing the laundry 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 2 process. Outline what would be necessary to move to a CMM level 3 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. Explain the problems that can arise when processes running asynchronously seek to communicate with each other through the use of shared memory. Illustrate your answer by analysing the following scenario:

A temporary traffic light system intended for use on roads with light traffic is controlled by software. The traffic lights themselves incorporate sensors that detect when a vehicle is coming towards them. A byte in memory contains F0 if a vehicle traveling from end A to end B is in the controlled section and 0F if a vehicle traveling from end B to end A is in the controlled section. If no vehicle has entered the controlled section for some preset length of time, the byte is set to FF. **(15 marks)**

Explain how you would use one of the standard types of synchronisation mechanism to avoid the problems inherent in this scenario. **(10 marks)**

5. Explain what is meant by deadlock in the context of real-time systems. What are the characteristic features of the system architecture that allow it to occur? **(10 marks)**

Critically discuss the possible approaches to deadlock avoidance. **(15 marks)**