THE BRITISH COMPUTER SOCIETY
Professional Graduate Diploma

SAFETY CRITICAL AND REAL TIME SOFTWARE

11th May 2001 – 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 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 committing with 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 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.

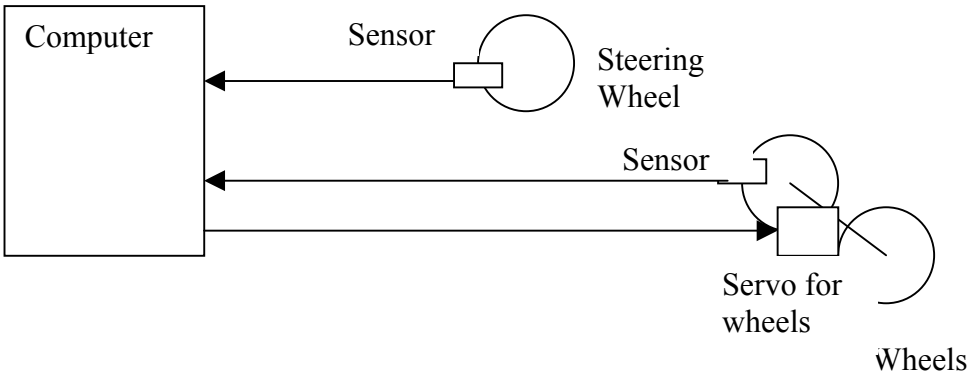
[8 marks]

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) When the system is in development the proposed solution is based on 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]



[Turn over

2. A manufacturer of an automatic train protection system (i.e. a system that stops the train if it passes a signal at danger) is proposing to use *triple modular redundancy* (TMR) in the system.

a) Explain why the manufacturer might choose this architecture for the system. Illustrate your answer by pointing out the effect of the architecture on key system attributes.

[5 marks]

b) Give an example of a fault that could not be detected reliably using such an architecture. Outline an architecture that could detect such faults reliably.

[5 marks]

c) The manufacturer is proposing to have different software teams develop the software for each of the three processors in the TMR system. Outline the arguments for and against this approach.

[5 marks]

d) In order to satisfy the regulator, the manufacturer must present evidence that the probability of failure on demand is less than 0.000001. Outline the different approaches that can be taken in providing such evidence and make clear the advantages and disadvantages of each approach.

[5 marks]

e) What approaches would you advocate to ensure the fault density in the software is as low as reasonably possible?

[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.

a) The development manager approaches you with a proposal to choose Java as the standard programming language for all the company's products. Write a short note giving the development manager advice on the decision in the light of the requirements of the various standards.

[8 marks]

b) The QA manager approaches you asking for advice on what kinds of testing will be required for the products. Produce a short report outlining the kinds of testing that will be required. For each kind of testing motivate its inclusion.

[8 marks]

c) The Technical Director would like to achieve Capability Maturity Model level 5 certification for their process. Produce a short note indicating how achieving this might contribute to the certification of products.

[5 marks]

d) Under what circumstances would you advocate the inclusion of formal methods in the development process for a product?

[4 marks]

4. This question concerns the problem of access control when cooperating processes running asynchronously are sharing resources.

a) Give an example to show how things can go wrong in such a situation if proper control is not exerted.

[5 marks]

b) Why are such problems difficult to detect and correct?

[5 marks]

c) Define the operations of an integer semaphore which allows no more than N processes to be in their critical section simultaneously.

[5 marks]

d) Suppose that there are two processes, STACKER and UNSTACKER, that are adding to and removing from (respectively) a stack. Show how to use integer semaphores to control the processes STACKER and UNSTACKER so that the stack never exceeds a given size and there is no attempt to remove an object from the stack when it is empty.

[10 marks]

5. In the context of real-time systems,

a) Explain what is meant by a process.

[5 marks]

b) Explain what is meant by scheduling and identify the objectives of a good scheduler.

[10 marks]

c) Discuss the advantages and disadvantages that might be associated with a scheduling strategy of "shortest process first".

[10 marks]