**THE BCS PROFESSIONAL EXAMINATION**
**Professional Graduate Diploma**

**April 2001**

**EXAMINERS' REPORT**

**Safety Critical and Real Time Software**

## QUESTION ONE

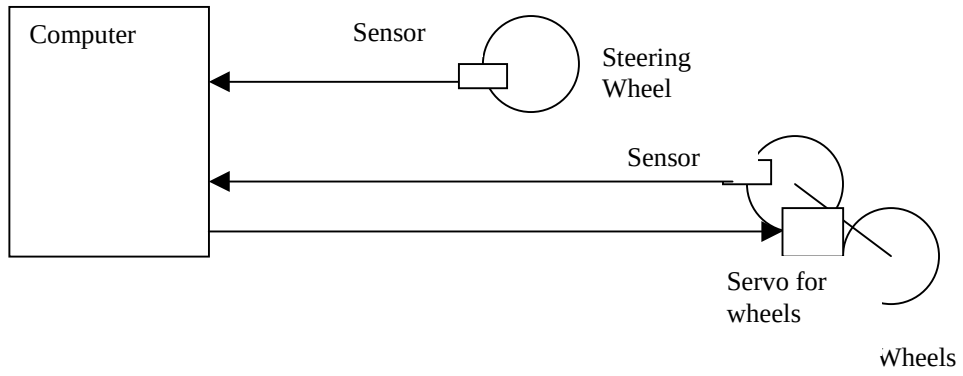
**A car manufacturer is considering introducing a *steer-by-wire* system that uses a computer system to control a servo that changes the direction of the wheels to ensure that they agree with the position of the steering wheel.**

**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 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)**



**Answer Pointers**

**a)** Here the student should mention FMEA and FTA (other possible methods would be FMECA and ETA) they might also mention HAZOP with some proviso that it is not really applicable to the subsystem. The answer should say something about the direction of the analysis, i.e. from failures to consequence or possible consequences back to failures.

**b)**

**c)** I'd expect to see some discussion of determining the severity and likely frequency of failures associated with the system and some discussion of how this approach needs modification when we are considering widely deployed systems where it is possible for many failures of the same kind to occur in different copies of the system.

**d)** I'd expect to see the student criticise this on the grounds that it may be hard to establish correct real-time behaviour because the interrupts make it hard to ensure deadlines are met. I'd expect the student would advocate some kind of polling of the sensors and scheduling of processed in the controller.

**Marks Breakdown**

| | | |
|---|---|---|
| **a)** | Correctly identifying methods | (Up to 3 marks) |
| | Discussion | (3 marks) |
| **b)** | Correct use of symbols and layout | (4 marks) |
| | Plausible fault tree for the given fault | (4 marks) |
| **c)** | Mention of severity | (2 marks) |
| | Mention of frequency | (2 marks) |
| | Discussion on how the system changes the way we see risk analysis | (2 marks) |
| **d)** | Criticism of interrupts | (3 marks) |
| | An alternative that ensures temporal predictability | (2 marks) |

**QUESTION TWO**

**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. (4 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?**

**Answer Pointers**

**a)** The main effects are on availability and reliability.

**b)** TMR will not detect Byzantine failure. We need quadruple redundancy and the use of something like the oral messages protocol to reach agreement and detect a Byzantine failure.

**c)** Arguments for are that diversity will reduce the likelihood of common mode failure. Arguments against are e.g. Butler and Finelli on non-independence of failure in software and Knight and Leveson experiments.

**d)** I'd expect the student to point out that basing everything on testing is probably prohibitively expensive. This suggests we need a safety case that takes deductive (proof or static analysis) evidence and process arguments into account.

**e)** Consider:

i. Restricted programming language/coding style
ii. Extensive defect testing
iii. Specific language constructions e.g. recovery blocks
iv. Reviews, pair programming
v. Reuse
vi. Static analysis, formal proof

**Marks Breakdown**

| | | |
|---|---|---|
| **a)** | Each mention of availability and reliability | (2 marks) |
| **b)** | Byzantine failure | (2 marks) |
| | Suitable architecture | (3 marks) |
| **c)** | Pro-argument | (2 marks) |
| | Con-arguments | (3 marks) |
| **d)** | Observation that testing is not enough | (2 marks) |
| | Description of deductive and process arguments | (3 marks) |

**e)** Award full marks for any answer involving at least three of these approaches, interpolate for one or two of the approaches.

**QUESTION THREE**

**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)**

**Answer Pointers**

**a)** Consider the following issues in Java:

1. Java includes many features explicitly excluded by some of the standards (e.g. recursion, dynamically allocated store, exceptions)
2. Timings in Java are not predictable (because of garbage collection)
3. There are no suitable qualified development tools for Java to satisfy the need for tools to be at the same level of certification as the software they are used to develop
4. There are no suitable tools for the safety analysis of Java programs

**b)** The following testing methods all play an important role:

1. Random testing to some operational profile to provide reliability data.
2. Black box testing to detect defects with the specification
3. White box testing to ensure the code has been exercised and found to operate in some circumstances
4. Mutation testing to test the adequacy of the test set.

**c)** The following could be considered:

1. Availability of process documentation for certification
2. Traceability evidence is available
3. Configuration management is implemented

**Marks Breakdown**

**a)** Recommending against Java (2 marks)
Each of up to 3 of the above suggestions (2 marks)

**b)** Each of the suggested methods (3 marks up to 8)

**c)** Each mention of the suggested considerations (3 marks up to 5)

**d)** Observation that it is mandated for some level in some of the standards (2 marks)

Observation that formal methods evidence is useful in making a diverse safety case for a system (2 marks)

**QUESTION FOUR**

**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)**

**Answer Pointers**

**a)** Any of the standard examples such as joint holders of a bank account simultaneously withdrawing money or two people booking the same aircraft seat.

**b)** Because of their dependency on real time. It is difficult to reproduce the timing conditions that caused the fault so its difficult to investigate it and difficult to know that you have corrected it.

**c)** Define the set, test, wait and signal operations, making it clear that they are atomic operations.

**QUESTION FIVE**

**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)**

**Answer Pointers**

**a)** There are many definitions in the text books, e.g. "a single execution of a sequential program" or " the dynamic invocation of a program". Candidates were expected to give one satisfactory definition and then explain it in terms of the allocation of processor resources.

**b)** Scheduling (in this context) is the process of deciding which process to run next. (Answers that dealt with high-level scheduling were accepted). The objectives will depend on the environment in which it is intended to operate. Thus the objective "ensure every process gets its fair share of resources" depends on what you mean by fair share in a particular context. Candidates were expected to show an awareness of such issues.

**c)** As with part b) this depends on the environment and candidates were expected to answer it with that in mind.