CS_M13
CRITICAL SYSTEMS

(*Attempt* **2** *questions out of 3*)

Question 1.

(a) Determine the advantages and disadvantages of event tree analysis (ETA).

[3 marks]

(b) Describe two guide words used in HAZOP in all areas of critical systems and two guide words, which are mainly used for computer based systems. Give possible interpretations for those guide words and possible effects, if we apply them to the wire, which connects the red light of a traffic light with the relay switching it on and off.

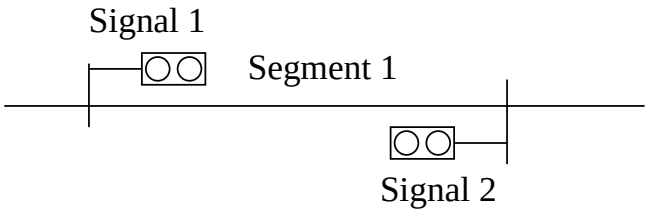
[8 marks]

(c) Give four reasons, why it is usually impossible to guarantee that a critical system is completely free from faults.

[6 marks]

(d) What is a race condition? Why are race conditions a particular problem in critical systems?

Consider the following example of a railway interlocking system, in which the access to a track segment from the left and right side is controlled by signals "Signal 1" and "Signal 2", respectively:



Assume a centralised control program, which controls the two signals and maintains a state variable, which determines whether the segment is occupied or free. Further assume that this control program is accessed simultaneously by two different railway control systems, located at different stations. Show how race conditions could result in two trains getting at the same time access to Segment 1, if insufficient care is taken when implementing the program.

[8 marks]

Question 2.

(a) Describe briefly what is meant by static and by dynamic redundancy. Compare both approaches. In the case of the computer system of the space shuttle, a third approach for achieving redundancy is used. What is this approach called? Describe it briefly.

[6 marks]

(b) Describe three fault detection mechanisms which can be used in order to detect crashes of a processor, how they detect such a crash, and the limitations of each of these mechanisms.

[9 marks]

(c) Even the most sophisticated fault tolerant architecture will not be able to provide complete fault-coverage against single-point failures of hardware. Why is this the case?

[3 marks]

(d) In the example of an AND-gate, there are 6 possible single-stuck-at faults. Describe these faults and the behaviour of the gate in the presence of each of them. How many of these errors can one distinguish by testing the input-output behaviour of the gate?

[7 marks]

Question 3.

(a) What was the original motivation for developing the programming language Ada? Explain how this influenced its design so that Ada is particularly suitable for critical systems.

[3 marks]

(b) When designing the SPARK Ada system, it was decided not to write a completely new language, but instead to base it on Ada. What was the reason for this decision?

[3 marks]

(c) Why does SPARK Ada not allow recursive functions?

[3 marks]

In questions (d), (e) and (f) consider the following SPARK Ada procedure:

```
procedure Test(X,Y: in out Float)
--# derives X from X,Y & Y from X;
--# pre X > 0.0;
--# post X > 0.0 and Y > 0.0;
is
begin
   Y := X;
   X := X+ Y;
end Test;
```

(d) Data flow analysis will report one error in the specification of the procedure (i.e. the line starting with the word “procedure”). Which one? You have only to determine the nature of this error, not the exact error message as given by SPARK Ada. Correct this error by modifying the specification of the procedure.

[4 marks]

(e) Information flow analysis will discover one more mistake in the “derives” clause of the program. Which one? Correct this error as well. Again, you have only to determine the nature of the error, not the exact error message as given by SPARK Ada.

[4 marks]

(f) Derive verification conditions from the program. Your answer doesn’t have to use exactly the same syntax as used by SPARK Ada.

[8 marks]