CS_M13
CRITICAL SYSTEMS
(*Attempt* **2** *questions out of 3*)

Question 1.

(a) Define briefly, what a safety critical system is. Why is the system controlling the shopping cart of an online book shop not a safety critical system?

[3 marks]

(b) Define what is meant by risk. Assume two different technologies for producing a chemical product. It is estimated, that when using the first technology, every 10,000 years there is a major accident, which kills people in the surrounding area, and causes the death of approximately 10,000 people. With the second technology, every 100 years there will be an accident, which affects only people working in the factory, and causes the death of approximately 10 people. Compare the risk of the two technologies. Which of the two technologies has the higher risk? Explain your results.

[7 marks]

(c) Give a fault tree analysis of the system of brakes of a bicycle. You can assume that the system consists of two independent brakes, and that under normal circumstances, the failure of one brake will not cause an accident. Start with the failure of both brakes. Consider as causes for the failure of an individual brake that the cable connecting the handle with the brake is broken or that the brake shoe (the rubber part in contact with the wheel) has fallen off. Your fault tree analysis should contain at least one or-gate and one and-gate.

[5 marks]

(d) Consider a program for managing accounts of customers of an Internet bank via a webinterface. Apply HAZOP to this program in order to identify potential problems of this program. You should use 3 guide words used in all areas of critical systems and 2 guide words used mainly in the context of computer based systems. Identify for each keyword one possible problem. The problems identified need not be critical.

[10 marks]

Question 2.

(a) Define the notion of an accident. When a soldier kills one of his enemies in a war, this is usually not considered as an accident. Why?

[4 marks]

(b) Define what is meant by a race condition. Race conditions are often overlooked when formally verifying critical systems. Why?

[5 marks]

(c) The company RailCorrect has developed a new railway control system, the correctness of which has been fully verified using automated and interactive theorem proving techniques. When they start testing the system, it turns out that from time to time trains seem to vanish from the screen. Since the system is fully verified, it is clear that the software fulfills the specification. Which part of the development process for this software went wrong?

[4 marks]

(d) The research group of the Metropolitan University of Mumbles has developed a new language in which fully verified programs can be written. This new language, which has been used by approximately 100 users, has been bought by a large software company. This company has tested it thoroughly in their research laboratories. It is now suggested that this language be used for writing the software for the cooling system of a nuclear power station. Why do you think this is not a good idea?

[4 marks]

(e) The group for critical systems of Gower university is developing an automated wheel chair, which is controlled by speech. This wheel chair has two sensors, one on the left side and one on the right side, which detect whether the wheel chair has contact with a wall. The wheel chair moves so slowly, that it is always possible to stop it immediately. In order to simplify the situation we can assume that the wheel chair is used in a relatively big circular room, and that problems of having doors or other obstacles can be ignored. The specification reads as follows:

- If no sensor gives a signal, the wheel chair can move in any direction under the control of other routines.
- If the left sensor gives a signal, the control system of the wheel chair should prevent the wheel-chair from moving towards the left.
- If the right sensor gives a signal, the control system of the wheel chair should prevent the wheel-chair from moving towards the right.

This specification is incomplete, because there is a fourth possibility which isn't treated here. Identify the fourth possibility and the circumstances, under which it might occur. Correct the specification by treating this missing case.

[8 marks]

Question 3.

(a) In SPARK Ada, several restrictions were imposed on the original language of Ada in order to guarantee that a SPARK Ada program requires only bounded space. Why were such restrictions imposed on SPARK Ada? Identify two different restrictions imposed on Ada in order to achieve bounded space.

[7 marks]

In subquestions (b) – (d), consider the following procedure in SPARK Ada. Some parts of the code are left out and have to be filled in when answering (b) and (c).

```
procedure Myprocedure (X: ?? Float; Y: ?? Float; Z: ?? Float)
--# derives ??;
--# pre X = 0.0;
--# post Z = 0.0;
is
  begin
    Y:= X;
    Z:= Y;
  end Myprocedure;
```

(b) Determine which of the parameters `X, Y, Z` are input, output and input/output parameters. Justify your answer. Fill in the corresponding gaps in the procedure.

[6 marks]

(c) Determine the dependencies between the variables and fill in the derives clause in the program above. You are not allowed to use the wild-card $*$. Jusify your answer.

[6 marks]

(d) Determine the verification condition which can be derived from this program. Your answer doesn't have to be verbally identical to what is actually created by SPARK Ada. Does this procedure fulfil the verification conditions?

[6 marks]