CS_M13
CRITICAL SYSTEMS
Exam January 2015

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

Question 1. *(Accidents, metrics, race conditions)*

(a) You are an expert on critical systems and your friend reports that s/he recently had two occasions where s/he narrowly escaped a car accident. You want to give your friend some advice to make sure that this does not happen again. For this you carry out an analysis of what happened, using techniques you learned about dealing with critical systems. What are the steps in your analysis? What should be the objective of each step of your analysis?

[5 marks]

Availability is the probability of the system to function correctly at any given time.

Reliability is over a period of time.

Fire alarm must be available while nuclear plant monitor must be reliable.

(b) Availability and reliability are two different notions. What is the difference between the two? Give an example of a critical system where availability is more important than reliability, and an example of another critical system where reliability is more important than availability.

[6 marks]

(c) People get upset when they learn that a certain technology, such as a nuclear power station, results in a certain number of deaths per year of operation, even though the numbers are very low (e.g. 1 death per 1000 years).

(i) What notion is measured by "number of deaths per year of operation"?

[2 marks]

(ii) Why is it usually not possible to obtain a number of 0 deaths per year of operation?

[3 marks]

(iii) There is a reason to be critical about the estimated number of deaths stated. What could be a reason that the actual number is substantially higher than what is estimated?

[3 marks]

(d) Consider a program for controlling a medical radiation therapy machine. It has two threads: one interacts with the input device, waits continuously for input of the dose of the next treatment, and once it has received some input stores the result in a shared variable. The second thread waits for when a value is stored in this shared variable. It then checks whether the value is below a certain threshold, and then controls the treatment of a patient, until it is finished. Because of the physical adjustments to be made, it takes a while before the treatment is actually carried out. Explain how, if not carefully implemented, race conditions may lead to a patient being overdosed.

[6 marks]

Please turn over for Question 2

Question 2. *(Hazard analysis, verification vs validation, programming languages for critical systems, Ada, basic concepts of SPARK Ada)*

(a) Apply 3 different guide words of HAZOP to a traffic light and use them to identify 3 different possible problems causing hazards associated with it.

[6 marks]

(b) Object-oriented programs generate objects dynamically on the heap. Why is this a problem when using object-oriented languages for critical systems?

[3 marks]

(c) You want to define a new sublanguage of Ada for use in critical systems, which uses some innovative program annotations to support verification.

(i) Why do you decide to define a sublanguage of Ada instead of defining an entirely new language?

[3 marks]

(ii) What constructs of Ada could you use so that you obtain a sublanguage of Ada which compiles with ordinary Ada compilers?

[4 marks]

(d) Even a program in SPARK Ada, which fulfils all verification conditions, might, when executed, not function correctly. Explain why this could happen by referring to the notions "verification" and "validation".

[4 marks]

(e) The following instruction in standard Ada could possibly lead to a programming error, which is avoided in SPARK Ada.

$$\mathrm{X} := \mathrm{F}(\mathrm{Y}) + \mathrm{G}(\mathrm{Y});$$

What is the programming error which might occur? What does SPARK Ada do in order to prevent this error?

[5 marks]

Please turn over for Question 3

Question 3. *(Program verification using SPARK Ada)*

(a) Pre- and post-conditions in a SPARK Ada program are considered as a contract. Explain what is meant by this statement.

[4 marks]

(b) Parts (i) - (iv) refer to the following partial SPARK Ada program, in which the question marks need to be filled in.

```
procedure Test (X : ?? Integer; Y : ?? Integer)
with Depends  =>  ??,
     Pre      =>  (X > 0),
     Post     =>  (Y > 0);

procedure Test (X : ?? Integer; Y : ?? Integer) is
begin
  if X > 0
  then Y := 5;
  else Y := -1;
  end if;
end Test;
```

(i) Complete the signature of the procedure Test such that it passes SPARK Ada's data flow analysis.

[4 marks]

(ii) Complete the "Depends" clauses, so that the program passes SPARK Ada's information flow analysis.

[4 marks]

(iii) Derive verification conditions from the program. You can ignore any conditions regarding that integers need to be between the minimum and maximum integer value. Your output does not need to coincide exactly with the output of SPARK Ada.

[7 marks]

(iv) Which of the verification conditions are provable and which are not? Justify your answer.

[6 marks]