Failure may cause injury or death of human beings or substantial environmental harm.

Shopping cart is considered as a business critical system and it does not result in consequences of a safety critical system.

CSCM13
CRITICAL SYSTEMS
Exam January 2016

(*Attempt* **both** *questions*)

Question 1. *(Notion and areas of critical systems, programming languages for critical systems, hazard analysis, race conditions)*

Space satellite and aircraft.

Aircraft must be safe under high altitude and pressure with low temperature in the air.

ne briefly, what a safety critical system is. Why is the software controlling an e shopping cart usually not considered a safety critical system? To which type itical systems does it belong? **[3 marks]**

(b) Critical systems often operate under extreme environmental conditions. Give two examples of such systems and describe one example of an extreme environmental impact for each system. In what sense does one need to take this into account when developing such critical systems? **[4 marks]**

(c) One desirable property of programming languages for developing critical systems s that they guarantee bounded space. What is meant by this? Why is the guarantee f bounded space desirable? **[3 marks]**

Bound resource usage to ensure it will work under real-time environment

(d) Consider the emergency cooling system of a nuclear power station, consisting of two independent systems. Assume that in order to cool down the core in an emergency, it is sufficient that one of the two systems operates. Draw an event tree for this system. Take as events an emergency situation, where emergency cooling needs to be activated, and the failing or not failing of each of the two emergency cooling systems. Assume that the probability of an emergency requiring emergency cooling is p1, and that p2 and p3 are the probabilities of a failure of emergency cooling system 1 and 2, respectively. Determine the probability of each sequence of events in your event tree. What would be the probability that emergency cooling is required and both cooling systems fail? **[7 marks]**

(e) (i) Explain what is meant by a race condition. **[2 marks]**

(ii) Consider a railway interlocking system consisting of two signals, which control access from two directions to the same track segment.
Assume 3 variables, two for the two signals, which can be red or green, and one for determining the state of the track segment, which could be free or not-free. Free means that there is no train on it, and no signal gives access to it.
Assume each signal is controlled by a thread, and that both threads share the variable determining the state of the track segment.
Describe a scenario in which, if these threads are not designed carefully, race conditions could result in both signals being set to green. Therefore, trains coming from both directions might access the same track segment resulting in a collision. **[6 marks]**

Please turn over for Question 2

Question 2. *(Program verification using SPARK Ada)*

(a) When designing SPARK Ada it was decided that SPARK Ada should be a subset of the existing language Ada rather than creating an entirely new language. Give two reasons why this was a good decision. **[4 marks]**

All parts (b) - (f) of question 2 refer to the following partial SPARK Ada program, in which the question marks need to be filled in.

File test.ads:

```
pragma SPARK_MODE;

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

File test.adb:

```
pragma SPARK_MODE;

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

(b) Complete the signature of the procedure Test such that it passes SPARK Ada's data flow analysis. **[2 marks]**

(c) Complete the "Depends" clauses, so that the program passes SPARK Ada's information flow analysis. **[2 marks]**

(d) 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]**

(e) Which of the verification conditions are provable and which are not? Justify your answer. **[6 marks]**

(f) Modify your program so that it fulfils the verification conditions. Your modifications could affect any part of your code, including pre- and post-conditions. Each change you make should be necessary. **[4 marks]**