UNIVERSITY OF SOUTHAMPTON COMP3011W1

SEMESTER 2 EXAMINATION 2013/2014

CRITICAL SYSTEMS

Duration: 120 mins

Answer THREE *out of* FOUR *questions.*

This examination is worth 70%. The coursework was worth 30%.
Show all your working in any calculated answers.
The handout "A Concise Summary of the Event-B Mathematical Toolkit" may be used in the exam. A foreign language translation dictionary (paper version) is permitted provided it contains no notes, additions or annotations.

Only University approved calculators may be used.

 Number of pages 13

Question 1

(a) Briefly describe a recent accident involving a safety-critical system. Describe some of the critical systems engineering lessons learnt from this accident.

(15 marks)

(b) Give two advantages and two disadvantages of using software in safety-critical control systems.

(4 marks)

(c) Fault trees and event trees are techniques in hazard analysis. Explain the difference between a fault tree and an event tree.

(4 marks)

(d) Construct an event tree for an emergency braking system for a moving machine. The brake system consists of a push-button, two independent air compressors and a pneumatic brake. Attach reasonable probabilities for correct operation to the components of the brake system and construct a probabilistic event tree.

You should clearly indicate the success outcomes on the tree and give the overall success probability of the system.

(10 marks)

Question 2

(a) Differentiate safety and reliability with the help of an illustrative example.

(6 marks)

(b) What is fault tolerance? Describe three techniques for achieving fault tolerance in computer systems. Describe a situation in which the use of a fault-tolerance technique is inappropriate and explain why it is inappropriate. *(9 marks)*

(c) Using the following table, explain the concept of Safety Integrity Level, including its use of 2 failure modes. Give the criterion for choosing between the 2 failure modes involved, and an example system in each mode.

SIL	High Demand Rate (Failure/hr)	Low Demand Rate (Prob of failure when required)
4	10^{-9} to 10^{-8}	10^{-5} to 10^{-4}
4	10^{-8} to 10^{-7}	10^{-4} to 10^{-3}
4	10^{-7} to 10^{-6}	10^{-3} to 10^{-2}
4	10^{-6} to 10^{-5}	10^{-2} to 10^{-1}

(8 marks)

(d) Assume a maximum tolerable risk fatality target of 10^{-5} pa, from a toxic spillage hazard. Assume there are 9 other similar hazards to be assessed from the same plant which will threaten the same group of people at the same time. Assume toxic spillage is fatal 1 in 10 times. A fault tree indicates that each of the processes will suffer an incident once in 50 years. Which type of SIL is indicated, and why ? Which SIL level is target ? Show your working, indicating failure rates and/or probabilities. *(10 marks)*

Question 3

(a) Explain what is meant by the formal process of *refinement*. List four different types of refinement, distinguishing between them.

(6 marks)

(b) The following is a partial abstract model of an email system. A *inbox* records a set of incoming messages(Msg) for each user($User$). A **send** event is provided to send message m from sender user su to receiver user ru:

VARIABLES
$inbox \in User \to \mathbb{P}\, Msg$
$subject \in Msg \to Data$
$sender \in Msg \to User$
$ccUsers \in Msg \nrightarrow \mathbb{P}_1\, User$
send =
any su, ru, m
where $su \in User \wedge ru \in User \wedge m \in Msg$
$\wedge\ su = sender(m)$
then $inbox(ru) := inbox(ru) \cup \{m\}$
end

Describe the exact meaning of each of the invariants by discussing their mathematical definitions. For the event, describe the working of its guard and action over the state variables.

(8 marks)

(c) Specify an event **receive** which will receive a message m for user ru, read the sending user su for the message, and remove the message from the inbox.

(6 marks)

(d) A refinement of the above model must now be specified. Each message has contents (*contents*) and is packaged (*Package*) with its destination user *destUser*. Packages are transmitted over a *middleware*,

modelled as a set of packages. Each user now has a send buffer (*sendbuf*) and a receive buffer (*receivebuf*) of packages.

Specify the concrete data structures, the typing invariant clauses, and a refinement of the **send** event of part (a).

Note that you should use the above italicized names as elements of your answer.

(10 marks)

(e) (i) The gluing invariant of this refinement states that every package arriving for user u in his receive buffer has contents matching some message in his inbox (in the abstract model). Specify this part of the gluing invariant.

(ii) The full gluing invariant places the same constraint on all packages in the middleware and in send buffers as well. Specify this part of the gluing invariant.

(12 marks)

Question 4 This question is concerned with certain aspects of modelling a car park. Parts (a-b) are concerned with controlling entry and exit of cars subject to maximum capacity. Parts (c, e-i) are concerned with the safe control of the entry/exit barriers. Each barrier operates in tandem with a zone sensor and a ticket machine. When a car is ready to exit, the barrier is opened and closed based on (i) whether there is a valid ticket in the machine and (ii) the reading of a zone sensor, which senses any obstruction (e.g. person or vehicle) in the near zone around the barrier.

(a) Draw a UML-B class diagram for the class **CarPark**.

- Add suitable class attributes (showing their types) to represent the number of cars in the car park and whether the car park is open or not
- Add class events *enter* and *leave* to represent cars going in and out of the car park
- Add a class invariant, which states that the number of cars in the car park must not exceed the capacity of that car park (Assume each car park has a maximum capacity defined via a constant attribute, CAPACITY.)

(5 marks)

(b) Give guards and actions as necessary to define the class events *enter* and *leave*. The events should respect the invariant as well as the property that cars may not enter the car park when it is closed.

(5 marks)

(c) Draw a UML-B state machine to model the 3 states of the class **ExitBarrier**, which are DOWN, WAITING and CLEAR (where WAITING means the barrier is up and waiting for the car to leave and CLEAR means the barrier is up and the car has gone). Add suitable transitions to the state machine (one of these should refine the *leave* event from the **CarPark** class).

(5 marks)

(d) SparkAda is a subset of the Ada programming language, used in critical systems. Describe how its language features make it suitable for use in critical systems.

(4 marks)

(e) For the car park barrier system, identify and distinguish between the controller and the environment components.

(1 marks)

(f) What are the safety requirements relating to the controller? (Think about what could go wrong and cause damage or injury, and what you need to ensure safe operation).

(3 marks)

(g) Write down an event with no parameters, a guard and an action that models the controller preparing a message to command the opening of the barrier, for allowing a vehicle to exit. Define and explain any new variables you need in the guard and the action.

(4 marks)

(h) Write down an event that models the controller sending a message to command the opening of the barrier for allowing a vehicle to exit. Define and explain any new variables you need in the guard and the action.

(2 marks)

(i) Write down the event of part (h) above, prepared for decomposition. It should be refined by adding a parameter to the event. Explain briefly why you need to do this.

(4 marks)