PRIFYSGOL CYMRU; UNIVERSITY OF WALES

DEGREE EXAMINATIONS MAY/JUNE 2002

SWANSEA

Computer Science

CS 411 Critical Systems

Attempt 2 questions out of 3

Time allowed: 2 hours

Students are permitted to use the dictionaries provided by the University

Students are NOT permitted to use calculators

CS_411
CRITICAL SYSTEMS

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

Question 1.

(a) Define briefly, what a critical system is.

[**3 marks**]

(b) Assume you want to create a safe gun using FMEA. What do you achieve by this, and what are the limitations of this method with respect to hazard analysis.

[**4 marks**]

(c) Assume two cars. One requires maintenance every 6 months for 1 day, the other every 12 months for 3 days. Otherwise both cars should function correctly. Which one is more available and which one is more reliable? Explain your result.

[**6 marks**]

(d) Define an event tree for the a fire alarm system consisting of a smoke detector connected to a relay, which activates a siren. The event tree should begin with the event corresponding to smoke created by a fire. The final event to be considered is whether an alarm is activated or not. The faults you should consider are the failure of the smoke detector, of the relay and of the siren.

[**6 marks**]

(e) Assume that in the situation of (d) the three components smoke detector, relay, siren each fail with a probability of 0.1%. Assign probabilities to the branches of your event tree and determine the probability of a the siren not sounding in the case of smoke caused by a fire. Since the probability of success is always high, you can approximate its contributions to the probability of an event sequence resulting in a failure by 1.

[**6 marks**]

Question 2.

(a) Why do more refined type theories allow us to achieve higher correctness of programs in safety critical systems?

[**4 marks**]

(b) Describe 3 general areas of applications, in which dependent types could be of use.

[**4 marks**]

(c) Consider the layout of a railway line with one track and two signals (showing either red or green) at each end of it, which control access to that line. Describe (informally or formally) the set of physical states and the set of control states (chosen by the railway controller) of that system. No control state should correspond to a physical state which might result in an accident, but every accident free physical state should correspond to a control state.

[**7 marks**]

(d) Define in the situation of (c) (informally or formally) how control states correspond to physical states.

[**3 marks**]

(e) What steps do you have to do in case of the system introduced in (c), in order to guarantee that the controller cannot make a mistake? (You can neglect the time it takes for trains to pass from one end of the line to the other, assume that a train can and will always stop if the signal is red and assume that trains never change direction on this line).

[**7 marks**]

Question 3.

(a) Define the set N of natural numbers in Agda. Introduce addition of two natural numbers in Agda.

[**5 marks**]

(b) Introduce in Agda, depending on natural numbers n, m, the set $\mathrm{Eq}(n, m)$ expressing that n and m are equal. Show that this equality is symmetric, eg. that $\mathrm{Eq}(n, m)$ implies $\mathrm{Eq}(m, n)$.

[**6 marks**]

(c) Define in Agda, depending on $n : \mathrm{N}$, the set $\mathrm{Vec}\ n$ of vectors of natural numbers of length n.

[**7 marks**]

(d) Define in Agda, depending on $n : \mathrm{N}$ and $A, B : \mathrm{Vec}\ n$, the sum of A, B. Here the sum of A and B is the vector of length n, the ith element of which is the sum of the ith element of A and of the ith element of B.

[**7 marks**]