UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1998

MEng Honours Degrees in Computing Part IV
MSci Honours Degree in Mathematics and Computer Science Part IV
MSc Degree in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the
Diploma of Membership of Imperial College
Associateship of the Royal College of Science
Associateship of the City and Guilds of London Institute

PAPER 4.39

SAFETY-CRITICAL SYSTEMS

Tuesday, May 12th 1998, 10.00 - 12.00

Answer THREE questions

For admin. only: paper contains 4 questions

1

a Describe the techniques of qualitative and quantitative analysis on fault trees, and describe the information which these techniques produce.

b Consider the following fault tree (Figure 1). Give the minimal cut sets for this tree, and calculate the rate of occurrence of event **A** and of the top event **E1**. Note that a rate of

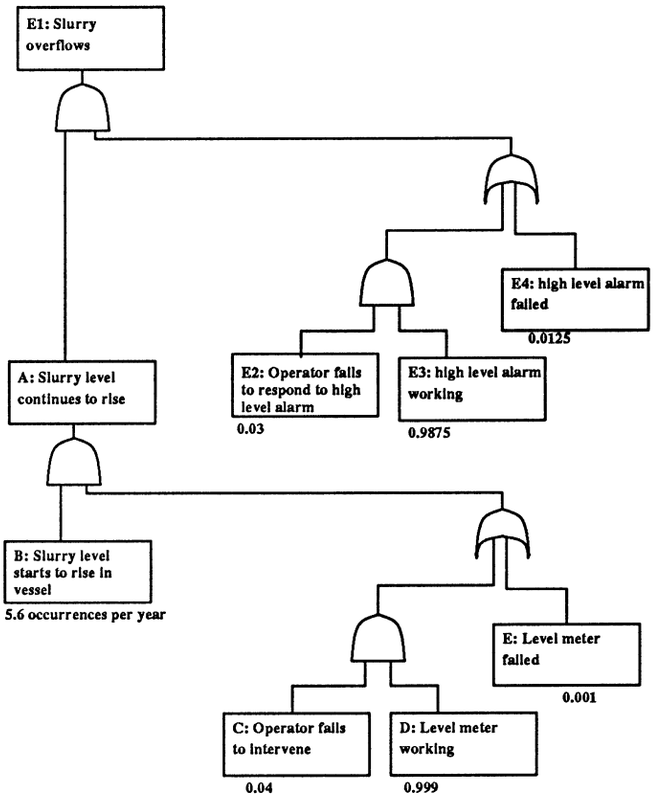

Figure 1: "Slurry overflows" fault tree

occurrence (**x** occ/year) can be multiplied by a probability **y** to give a rate of occurrence $\mathbf{x} * \mathbf{y}$ occ/year.

c What leaf event should be considered first as a means of reducing this rate, and why?

The three parts of this question carry 30%, 50% and 20% of the marks, respectively

2 The following problem concerns the control of a chemical reaction (Figure 2).

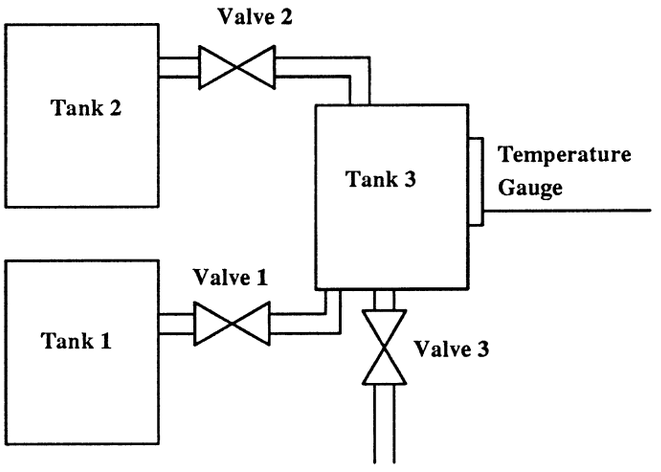

Figure 2: Components of System

Product is transferred from tank 1 to tank 3 via valve 1 until the temperature gauge TG in tank 3 reaches (ie, becomes $\geq$) level **min_temp**. At this point valve 1 should be closed and valve 2 opened, introducing an additional reactant. If TG goes below **min_temp** again, then valve 2 should be closed and the process terminates. If TG reaches **max_temp**, then valve 2 should be closed and valve 3 opened, emptying the contents into a dousing chamber. Once the temperature goes below **max_temp** again, valve 3 can be closed.

The initial state is that valve 1 is open, TG is $<$ **min_temp**, and the other valves are closed. The following safety invariants are required:

1. valves 1 and 2 must not both be open at the same time
2. TG $\geq$ **min_temp** implies that valve 1 is closed
3. TG $\geq$ **max_temp** implies valve 3 is open

a Specify a controller **MACHINE** for this system, including formalisations of these safety invariants, and reactions to events **min_reached**, **max_reached**, **goes_below_min**, **goes_below_max**.

You may assume the following types are declared in a **ReactionTypes** component: **ValveState** = {**open**, **closed**} and **Temp** = {**below_min**, **above_min**, **above_max**}, and that there are separate components **Valve1**, **Valve2**, **Valve3** with variables **v1state** : **ValveState**, etc, and operations **open_v1**, **close_v1**, etc.

b Argue rigorously to show that the first safety invariant is valid in this controller.

The two parts of the question carry respectively 60% and 40% of the marks

Turn over ...

3 The following description is used in parts **b, c** and **d** of this question:

In a particular automated railway control and protection system, the hazard **H** of loss of communication between the train and trackside monitors can lead to the following accident sequences:

1. if (independent) events **E1** and **E2** occur, an accident (excessive braking force) of critical severity will occur
2. if event **E3** occurs, the catastrophic accident of train collision will occur
3. if (independent) events **E4** and **E5** occur, an accident of critical severity will occur.

The probabilities of the accident chain events are: **E1** : 10^{-1}, **E2** : 10^{-1}, **E3** : 10^{-3}, **E4** : 10^{-1}, **E5** : 10^{-2}.

a What is meant by the *risk* of a hazardous situation?

b Calculate the maximum permissible frequency of occurrence of hazard **H** of the railway control system described above, if the risk level is to be at most class **B**.

c Calculate the maximum permissible frequency of occurrence of **H** if the risk level is to be at most class **C**. Use Tables 1 and 2, taken from 00-56, for these calculations.

Frequency	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	D	D	D
Incredible	C	D	D	D

Table 1: Risk Classification (00-56)

Probability	**Numeric Equivalent**	**Per Year**
Frequent	10000×10^{-6}/operating hour	100
Probable	100×10^{-6}/operating hour	1
Occasional	1×10^{-6}/operating hour	1 in 100y
Remote	0.01×10^{-6}/operating hour	1 in 10^4y
Improbable	0.0001×10^{-6}/operating hour	1 in 10^6y
Incredible	0.000001×10^{-6}/operating hour	1 in 10^8y

Table 2: Hazard Probability Ranges (00-56)

d What is the minimum SIL of the communication system between the train and trackside monitors, on the basis of this hazard?

e List, in order of general preference, 5 risk-reduction techniques.

The parts of this question carry, respectively, 10%, 25%, 25%, 10% and 30% of the marks

4 A machine **C** has the form:

```
MACHINE C
SEES B
INCLUDES A
VARIABLES c1
OPERATIONS
  opC1 = ...;

  opC2 = ...
END
```

where **A** has operations **opA1** and **opA2** and variables **a1** and **a2**, and **B** has operation **opB** and variables **b1**, **b2**.

a Which variables can be referred to in the invariant of **C**?

b Which variables can be referred to within the operations of **C**?

c Which variables can be directly assigned to in **C**?

d Which operations can be invoked within the definitions of the operations of **C**?

e The incomplete controller specification given in Figure 1 of the supplemental material is intended to control a level-crossing gate on a single-track railway. Sensor **S1** detects a train sufficient time before it can reach the crossing so that the gate can be closed as the train passes the gate. Sensor **S2** detects that the train has passed the crossing. The gate can be in one of four states (Figure 3).

Give definitions of operations **train_arrives_at_S2** and **train_passed_S2** in order that the safety invariant

$$\textbf{number\_of\_trains} \geq 1 \Rightarrow \textbf{gstate} \in \{\textbf{closed}, \textbf{closing}\}$$

is maintained by the controller. **number_of_trains** represents the number of trains which have reached **S1** but not yet reached **S2**.

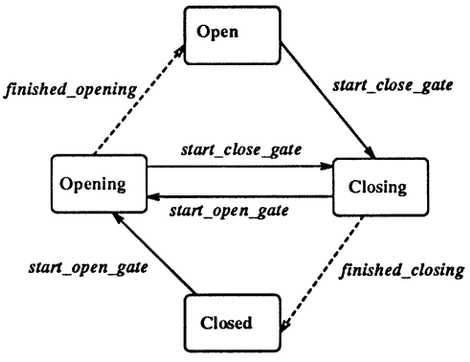

Figure 3: States of Gate

The five parts of this question carry, respectively, 15%, 15%, 15%, 15% and 40% of the marks

End of paper.

```
MACHINE Controller
SEES Bool_TYPE
SETS GState = {closed, opening, open, closing}
VARIABLES gstate, s1, s2, number_of_trains
INVARIANT gstate: GState &
  s1: BOOL & s2: BOOL &
  number_of_trains: NAT &

  (number_of_trains >= 1  =>  gstate: {closed, closing})
INITIALISATION gstate := open || s1 := FALSE ||
  s2 := FALSE || number_of_trains := 0
OPERATIONS
  train_arrives_at_S1 =
    PRE s1 = FALSE
    THEN
      s1 := TRUE ||
      number_of_trains := number_of_trains + 1 ||
      IF not(gstate = closed)
      THEN gstate := closing
      END
    END;

  train_passed_S1 =
    PRE s1 = TRUE
    THEN s1 := FALSE
    END;

  gate_completes_closing =
    PRE gstate = closing
    THEN gstate := closed
    END;

  train_arrives_at_S2 = ...;

  train_passed_S2 = ...;

  gate_completes_opening =
    PRE gstate = opening
    THEN gstate := open
    END
END
```

Figure 1: Controller Specification (Partial)