UNIVERSITY OF LONDON

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1999

MEng Honours Degrees in Computing Part IV
MEng Honours Degree in Information Systems Engineering 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 / I 4.26

SAFETY–CRITICAL SYSTEMS

Tuesday, May 4th 1999, 10.00 – 12.00

Answer THREE questions

For admin. only:
paper contains 4 questions

1

a Explain the role of Fault Tree Analysis in safety and hazard analysis.

b Consider the following hazard on the milk processing tank of Figure 1: failure to clean the tank, which can lead to bacterial contamination of raw milk and hence death of customers. Build a fault tree for this hazard, and calculate the rate of occurrence of the top node. The failure rates of Table 1 can be used for this calculation. Assume that there is one cleaning operation every 10 hours.

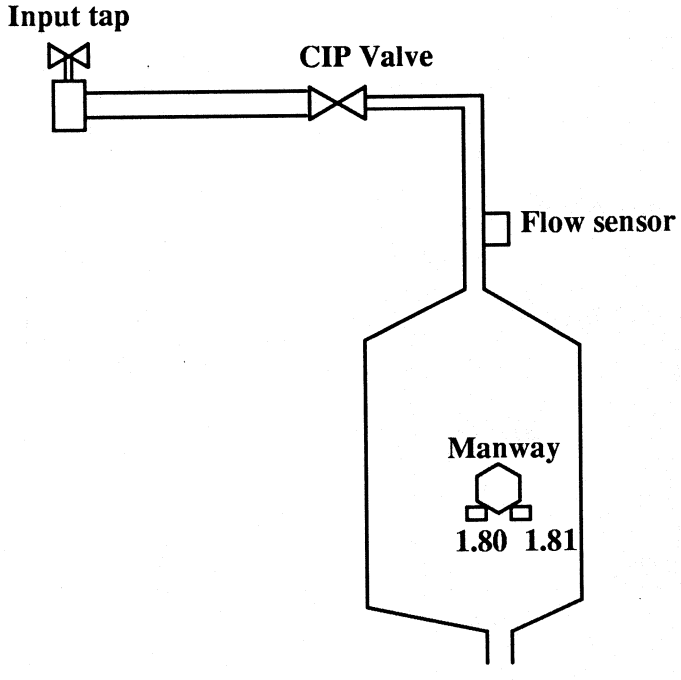

Figure 1: Input Tank in Milk Plant

Component	*Failure rate*
Input tap	10^{-2} per cleaning instance – human failure to turn on tap
CIP valve	10^{-3} per hour – failed closed
Flow sensor	10^{-3} per hour – failed in state signalling that there is a flow, even if there is none
Manway sensor 1.80	10^{-3} per hour failed sensing manway closed when open
Manway sensor 1.81	10^{-3} per hour failed sensing manway closed when open

Table 1: Failure Rate of Tank Devices

c Identify the risk class of this hazard, given that the severity is catastrophic. Tables 2 and 3 give the relevant frequency and risk categories from DEF-STAN 00-56.

d Calculate the maximum probability and probability class of the hazard state "Manway open undetected during cleaning", given that sensors 1.80 and 1.81 must both fail for the open state to be undetected.

The four parts of this question carry 25%, 50%, 15% and 10% of the marks, respectively.

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	C	D	D
Incredible	C	D	D	D

Table 2: 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 3: Hazard Probability Ranges (00-56)

[Turn over ...

2

a Explain what the 'bathtub curve' of component reliability is and how it helps simplify reliability analysis.

b Calculate the reliability of the composite network shown in Figure 2.

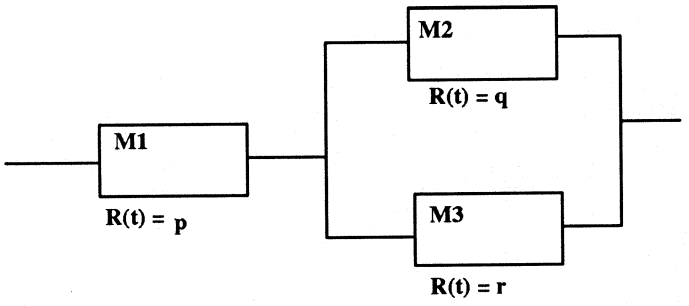

Figure 2: Series and Parallel Network

c Calculate the reliability of a TMR combination of three modules with reliability 0.6, and the reliability of a standby spare combination of two modules of reliability 0.6 and a fault detector with coverage 0.9.

d If a module **M** is constructed as a parallel combination of two identical modules with reliability **R**, what is the failure coverage of a comparitor which checks for failure in **M** by looking for differences in the outputs of the two component modules?

The four parts of this question carry 20%, 20%, 30% and 30% respectively of the marks.

3

a Is the following set of dependencies between B machines valid?

```
A USES C,  B INCLUDES C,
D EXTENDS A, B
```

Explain your answer.

b In this situation, can **A** invoke the operations of **C**? Explain your answer.

c Write a B machine for **Motor** from the state machine given in Figure 3. The variable for the motor state should be called **mstate**. In part **d** you can assume that there is a similar machine for the brake, with variable **bstate**.

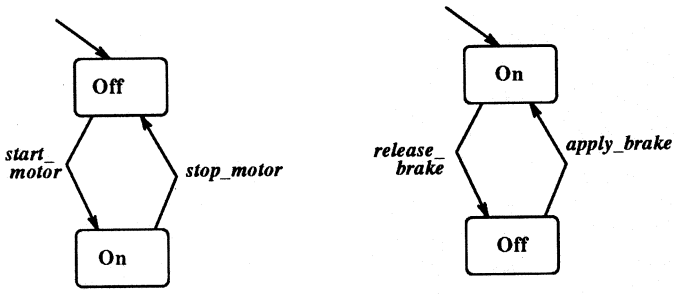

Figure 3: Statecharts of Motor and Brake

d These components are used as actuators in a train control system, which responds to a command to **switch_on** by starting the motor and releasing the brake, provided the train doors are locked (**dstate** = **locked**). It responds to a command to switch off by setting the motor off and applying the brake. Define operations for **switch_on** and **switch_off**.

e Formalise the safety invariant that the door is locked whenever the motor is on.

The five parts of this question carry 15%, 15%, 30%, 30% and 10% of the marks, respectively.

[Turn over ...

4 The system shown in Figure 4 is a controller for a drill. The drill may be on or off (**tstate = on**, **tstate = off**) and lowered for use, or up (**position = down**, **position = up**). A plastic guard is intended to protect operators when the tool is operating, it may be in position (**gstate = present**) or out of position (**gstate = absent**). An alarm should sound (**astate = on**) if the guard is out of position when the tool is down or operating. The drill can only operate if it is down: pressing the 'on' button only activates the drill if it is down and the guard in place.

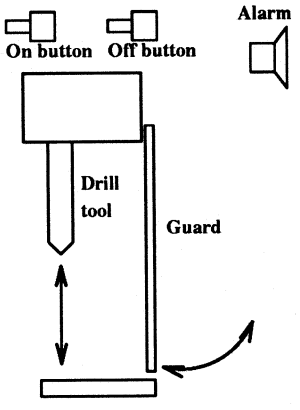

Figure 4: Drill Control System

a Add operations for the events **lower_tool**, **switch_on** and **raise_guard** to the following partial B specification:

```
MACHINE DrillControl
SETS State = {on, off};
  Position = {down, up};
  GState = {absent, present}
VARIABLES tstate, position, gstate, astate
INVARIANT tstate: State & position: Position &
  gstate: GState & astate: State
INITIALISATION
  tstate := off || astate := off || gstate := absent || position := up
OPERATIONS
  raise_tool = PRE position = down
               THEN
                 position := up ||
                 tstate := off ||
                 astate := off
               END;

  switch_off = tstate := off;

  lower_guard = PRE gstate = absent
                THEN
                  gstate := present ||
                  astate := off
                END;
  ...
END
```

b Express the safety and operational invariants given informally above as formal B invariants of **DrillControl**.

The two parts of this question carry 70% and 30% of the marks, respectively.

[End of paper