UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2001

MEng Honours Degree in Information Systems Engineering Part IV
MEng Honours Degrees in Computing Part IV
MSc 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 Associateship of the City and Guilds of London Institute

PAPER C439=I4.26

SAFETY-CRITICAL SYSTEMS

Friday 11 May 2001, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1a Briefly describe the safety analyses HAZOPS, FTA, and FMECA. State their outputs and explain the relationships between themselves and with the system and component models for the system under design.

b Figure 1 shows a part of the specification for a milk processing plant. A particular hazard associated with the part of the system shown in the diagram is the manway in the input tank being left open during cleaning. Recall that the cleaning fluid is dilute hydrochloric acid.

Draw a fault tree for this hazard in the case that the main control system fails to react to close down the cleaning fluid input route and use it to calculate the probability of the top event. Assume the valves on the route are controlled by independent control channels and that the rate at which such a valve fails open (= energised) is 10^{-3} per hour, and that sensors fail energised at the same rate. Assume that one cleaning operation is carried out every five hours and takes thirty minutes and that the controller failure rate is 10^{-2} per demand.

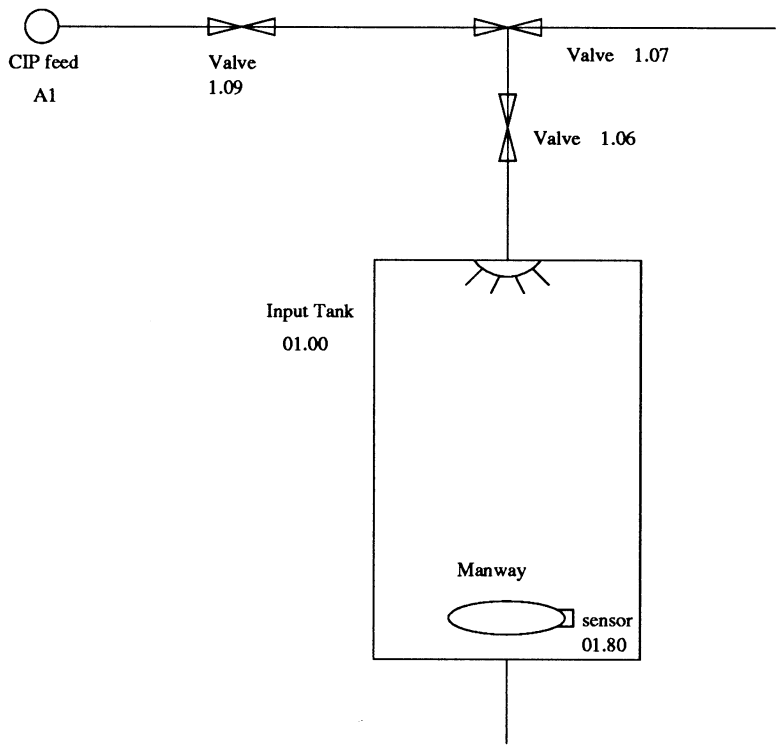

Figure 1: Input Tank in Milk Plant

c Use tables 1 and 2 to assess the risk level of this hazard. Assume that exposure to sufficient quantities of the acid might kill. State a safety invariant corresponding to this hazard and suggest a way in which the risk level you calculated might be reduced.

(The three parts carry, respectively, 30%, 45% and 25% of the marks).

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 1: Risk Classification (from Def-Stan 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 (from Def-Stan 00-56)

2a Draw a diagram illustrating Triple Modular Redundancy and explain how it works. How many simultaneous faults in the modules can such a setup tolerate? What kinds of faults can TMR tolerate and not tolerate? If TMR is generalised to N-modular Redundancy, how many simultaneous faults in the modules can be tolerated?

b State the formula for the reliability of a system of components placed in series, in terms of the reliability of the individual components, where $R(t)$ is the reliability of the system and $R_i(t)$ is the reliability of component i.

A series system containing 100 components is required to have a reliability of at least 0.999. Assuming that each of the components is equally reliable, what minimum reliability would they require to achieve the specified system performance? Please comment.

c Consider a TMR unit. Ignoring the reliability of the voter (assume it is completely reliable), give an expression for the reliability, $R(t)$, of the TMR unit in terms of the reliability of the individual redundant modules,$R_1(t)$, $R_2(t)$,$R_3(t)$. Justify your derivation. Assuming that $R_1(t) = R_2(t) = R_3(t)$, simplify the expression; then generalise to a system in which there are N redundant modules of which M must function correctly to prevent system failure.

Finally, calculate the reliability of a 3 out of 5 redundant module system if the five identical modules each have a reliability of 0.95 and once again you can ignore the reliability of the voter.

(The three parts carry, respectively, 30%, 30%, and 40% of the marks).

3a Explain briefly how an operation can be thought of as a predicate transformer and how it is characterised by its weakest precondition.

b Give the weakest precondition with respect to a predicate R for the following three generalised substitutions:

i) an assignment, x:=E,

ii) a preconditioned substitution, PRE P THEN S END,

iii) a non-deterministic choice, S [] T.

c Evaluate: [PRE x>5 THEN ((x:=x+1) [] (x:=x+2))](x<10)

d The condition [S]true characterizes the fact that S terminates. Give similar conditions for:

i) S aborts,

ii) S is feasible, and

iii) S is miraculous.

e The predicate of a substitution, prd(S), is defined as ¬[S]¬(x'=x). Explain with help of an example why the two negations appear in the definition.

(The five parts of the question carry respectively: 10%, 20%, 20%, 20% and 30% of the marks.)

4a Describe briefly the advantages and disadvantages of proof compared with testing for ensuring the correctness of software.

b Describe the principal features of each of the three provers in the B-Toolkit. What are the three outcomes that may arise when using the interprover?

c Explain how the invariant is used in the design of software for safety critical systems in the B method.

What needs to be shown to demonstrate that a given invariant is in fact an invariant property of a specification?

d Explain how reduction of non-determinism and reduction of non-definedness support the view of a specification as a contract.

Describe the main features of algorithm refinement and data refinement.

Explain how structured specifications are used together with compositional refinement to support layered design in the B method.

(The four parts of the question carry respectively 10%, 30%, 20%, and 40% of the marks.)