MARKING GUIDE

Software Engineering and Design – Paper 10 Question 12 (AFB) 2005

Imagine that you are the user interface designer responsible for a system that manages the shutdown of a nuclear power station.

(*a*) Comment on hazards, risks and reliability. [3 marks]
PAGE 83 & 84 OF LECTURE NOTES

(*b*) What special procedures should be taken during design? [3 marks]
PAGE 84, 85, 89 OF NOTES

(*c*) There is some debate among the team about whether the operator should be in the control loop. What options are there? [4 marks]
PAGE 81 & 82 OF NOTES

(*d*) In order to assess alternative options like these, then:
PAGES 62-67 OF NOTES

(*i*) How could you estimate the speed of operator action based on a draft interface layout? [4 marks]

(*ii*) How could you measure the speed of operator action using alternative prototypes? [4 marks]
PAGE 74 OF NOTES

(*iii*) How could you estimate the probability of operator error? [2 marks]
PAGE 80 OF NOTES

a) 1 MARK EACH

b) FOR EACH OF HAZARD ANALYSIS, FMEA & FAULT TREE ANALYSIS: 1 MARK FOR NAMING, 1 MARK FOR EXPLAINING (MAX 3)

c) 1 MARK FOR EACH CONTROL LOOP OPTION

di) 1 MARK FOR KLM, 1 MARK FOR SUMMATION, 1 MARK FOR LIST OF TIMES, 1 FOR COMPARISON

dii) 1 MARK FOR IDENTIFYING CONTROLLED EXPERIMENTS, 1 FOR SAMPLING AND 1 FOR COMPARISON OF MEANS 1 FOR SIGNIFICANCE TEST

PAPER 10 QUESTION 12 (SW ENG & DESIGN) – MODEL ANSWER

(A) HAZARDS IN A NUCLEAR POWER PLANT INCLUDE RADIOACTIVE MATERIALS, HIGH TEMPERATURES.

RISKS ARE THAT THE PLANT MIGHT CONTINUE OPERATING, OR THAT IN AN EMERGENCY, THE EMERGENCY SITUATION IS NOT RESOLVED

RELIABILITY OF THE MAIN PARTS OF THE SOFTWARE COULD BE EXPRESSED AS MEAN TIME TO FAILURE, BUT THE SPECIAL SHUTDOWN FUNCTIONS MIGHT BE REQUIRED TO OPERATE WITHOUT FAILURE IN A CERTAIN PROPORTION OF OCCASIONS (SAY [illegible] IN 10,000)

(B) HAZARD ANALYSIS COULD BE CONDUCTED FROM THE OUTSET, FOLLOWED BY FAULT TREE ANALYSIS TO DETERMINE POSSIBLE CAUSES OF ACCIDENTS. AT LATER STAGES OF DESIGN, FAILURE MODE EFFECTS ANALYSIS COULD BE USED TO ESTIMATE ERROR CONSEQUENCES, OR TO ANALYSE FAILURE OF ELECTRO-MECHANICAL COMPONENTS SUCH AS SWITCHES

(C) 1. OPERATOR CAN READ INSTRUMENTS DIRECTLY, AND CONTROL SYSTEM OPERATION, BOTH ADVISORY INFORMATION FROM COMPUTER

2. COMPUTER CAN READ SENSORS AND SET ACTUATORS, BASED ON GUIDANCE/POLICY DECISIONS BY OPERATOR

3. COMPUTER CAN INTERPRET SENSOR DATA FOR PRESENTATION TO OPERATOR, WHO CONTROLS PLANT DIRECTLY

4. OPERATOR MAKES CONTROL DECISIONS, WITH ACTIONS PASSED VIA COMPUTER

(D) i) SPEED OF OPERATOR ACTIONS CAN BE ESTIMATED USING GOMS OR THE KEYSTROKE-LEVEL MODEL, THIS WOULD REQUIRE SOME INFORMATION ABOUT TYPICAL TYPING/POINTING SPEED FOR INTENDED OPERATORS, WHICH CAN THEN BE AGGREGATED AS TIME REQUIRED FOR EACH ACTION, PLUS COMPUTER RESPONSE TIME, PLUS MENTAL PREPARATION TIME. THE ALTERNATIVE INTERFACES FOR EACH OF THE ACTIONS (C) CAN BE COMPARED ON THIS BASIS

(D) ii) IF YOU BUILT PROTOTYPES ACCORDING TO EACH OF THESE MODELS, YOU COULD THEN RUN A CONTROLLED EXPERIMENT IN WHICH USERS CARRY OUT THE STANDARD SEQUENCE. YOU SHOULD MAKE REPEATED MEASUREMENTS OF TRIALS, AND ALSO RUN THE EXPERIMENT WITH A SAMPLE OF DIFFERENT USERS. IF THE MEAN OPERATION TIME BETWEEN THE PROTOTYPES DIFFERS BY MORE THAN A CERTAIN NUMBER OF STANDARD DEVIATIONS (SAY 3), THEN YOU CAN CONCLUDE THAT THERE IS A STATISTICALLY SIGNIFICANT DIFFERENCE BETWEEN THE DESIGNS

(D) iii) YOU COULD MAKE A ROUGH ESTIMATE BASED ON EXPERIMENTAL STUDIES OF ERROR RATE UNDER PARTICULAR CONDITIONS OF STRESS, MOTIVATION AND FAMILIARITY. IN THE CASE OF AN EMERGENCY SITUATION, HIGH STRESS AND LOW FAMILIARITY MAY BE SOMEWHAT COUNTERED BY HIGH MOTIVATION.