Xday, XX May 2004.

9.30 am - 11.15am

University of Glasgow

DEGREES OF BEng, BSc, MA, MA (SOCIAL SCIENCES).

COMPUTING SCIENCE - SINGLE AND COMBINED HONOURS
ELECTRONIC AND SOFTWARE ENGINEERING - HONOURS
SOFTWARE ENGINEERING - HONOURS

SAFETY-CRITICAL SYSTEMS DEVELOPMENT

Answer 3 of the 4 questions.

1.

a) What is Reliability Centred Maintenance?

[3 marks]

b) The European Union recently funded a project into a Reliability Centred Maintenance Approach for the Infrastructure and Logistics of Railway operations (RAIL). This project used risk assessment to guide the monitoring and correction of potential faults across European rail networks. As part of the RAIL project, the team developed a two-stage approach in which the first step was to identify the criticality of network components using the following table:

Factor	Description	Value 1	Value 2	Value 3	Value 4
Technology	Kind of technology on the line or section.	Mechanical	Electro-mechanical	Electric	Electronic
Traffic density	Number of circulations per day.	[1,20]	[21,60]	[61,200]	>200
Revenues	Income from exploitation of network.	Low	Medium	High	Very High
Availability	Number of hours that the line must be available per day.	Low	Medium	High	Very High
Exploitation	Number of passengers or dangerous freight.	Low	Medium	High	Very High
Maintainability	Maintenance process complexity.	Low	Medium	High	Very High
Costs	Costs associated with maintenance.	Low	Medium	High	Very High
Environmental risk	Risk of environmental damage generated by an installation failure.	Low	Medium	High	Very High
Safety risk	Risk of people damage generated by an installation failure.	Low	Medium	High	Very High

i. Briefly explain why this table relies almost entirely on qualitative criteria for criticality assessment.

[4 marks]

ii. Briefly explain why computational failures are only considered indirectly within this table.

[3 marks]

c) The second stage of the RAIL approach focuses on each of the high criticality network components identified using the table in part b of this question. Each of these components is then subjected to a Failure Modes Effect and Criticality Analysis (FMECA). The severity (R) of any failure is defined by the following equation:

$$R = (S+C+D)\frac{P}{MTBF}$$

.

Where S is a numerical measure of safety, C is a measure of costs, D is a measure of punctuality, P is the probability of the failure and MTBF is the mean time between each occurrence of that failure. Recall that there may be many ways, or modes, by which a failure can occur. Briefly comment on whether it is possible to use this formula to consider the severity of a failure where the loss of a programmable system is one of the potential failure modes.

[10 marks]

2.

a) The Boeing 777 is unusual in that the decision was taken early in development to write as much as possible for the software in Ada. Honeywell developed the primary flight controls and purchased DDC-I, Inc.'s Ada Compiler, using it as the front-end for Honeywell's symbolic debugger. The two companies worked together for eighteen months to build the compiler's debugger and the back-end, targeted to an AMD 29050 microprocessor. Briefly explain why so much care was taken to distinguish between the high level language, the compiler and the analysis tools, and the target processor.

[3 marks]

b) One of the other 777 subcontractors, Sundstrand, chose a compiler from Alsys. This generated code for an Intel 80186 microprocessor that relies upon the Certifiable Small Ada Run Time (CSMART) executive. Members of the development team argued that this enables them to reuse code. For example, the Gulfstream V business jet and the Comanche helicopter Sundstrand's library of common generic packages written for the 777. Briefly explain the importance of testing the CSMART executive to support such reuse.

[5 marks]

c) On the 777, three processors provide triply redundant computation for the primary flight control system. Each Primary Flight Computer (PFC) receives data from three control buses. Each PFC only transmits on its associated bus. Each PFC channel contains three dissimilar processor lanes that use different processors and were developed using different Ada compilers. Each lane contains its own power source and has its own terminals to communicate with the buses. Explain how this architecture contributes to the overall safety of the Boeing 777 aircraft.

[12 marks]

3.

a) A recent study by the US Food and Drugs Administration examined 3,140 medical device recalls. This revealed that 242 (7.7%) were attributable to software failures. Of these, 192 (79% of softeware related failures) were caused by software defects that were introduced when changes were made to the software after its initial production and distribution. The majority of these updates stemmed from ‘usability’ problems. The FDA concluded that ‘software validation and other related good software engineering practices … are a principal means of avoiding such defects and resultant recalls’. Briefly explain why regulators now typically rely on certifying the development process or ‘engineering practices’ rather than individual safety-critical systems.

[3 marks]

b) The Da Vinci system is the first fly-by-wire robotic aid to be approved for surgical applications by the Food and Drugs Administration. Briefly explain why conventional forms of black-box testing may not provide sufficient assurance of the safety of such an application.

[6 marks]

c) You have been appointed as a Safety Manager working in a company that produces a programmable ventilator. These devices are used to help anesthetize patients. You have just been sent a report from the Food and Drugs Administration that describes an incident involving one of your devices and the attempts of your colleagues to help the clinician using the device:

THE VENTILATOR ON THE ANESTHESIA FAILED WITH AN ERROR MESSAGE "GAS INLET VALVE FAILURE." PATIENT WAS VENTILATED BY HAND AS PREPARATIONS WERE MADE TO SWAP OUT THE ANESTHESIA MACHINE. the SERVICE REP WAS CONTACTED, HE TELEPHONED INTO OPERATING ROOM. HE WALKED ANESTHESIA ATTENDING THROUGH A SERVICE PROCEDURE TO "BLOW OUT" GAS INLET VALVE. VENTILATOR WORKED AFTER THIS AND FOR REMAINDER OF PROCEDURE. MACHINE WAS TAKEN OUT OF SERVICE AND VALVE IS BEING SENT BACK TO manufacturer. THERE ARE REPORTS OF OTHER RECENT SIMILAR INCIDENTS INVOLVING NEWLY INSTALLED ANESTHESIA MACHINES OF THE SAME MODEL

Using one of the incident analysis techniques introduced in this course, identify any lessons that might be learned from this incident report and explain how you would go about identifying any necessary corrective measures.

[11 marks]

4. To what extent is it acceptable to blame 'systemic failure' rather than operator or managerial 'error' as a cause of accidents involving programmable systems. Illustrate your answer with detailed references to two of the accidents that we have studied in this course.

[20 marks]

[end]