Xday, XX XXX 2014.

9.30 am - 11.15am ***(check this!)***

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) Briefly explain the relevance of verification and validation to the maintenance of safety critical software.

[6 marks]

b) The UK Railways & Other Guided Transport Systems (Safety) Regulations 2006: Guide To The Application Of Safety Verification published by Her Majesty's Railway Inspectorate states that:

> "Safety Integrity Levels (SIL) are measures of the safety of a given process. Specifically, to what extent can the end user expect the process in question to perform safely, and in the case of a failure, fail in a safe manner? Usually applies to electronic systems particularly software and firmware architecture". (UK HMRI, 2007)

Briefly explain how you would both validate the assignment of a SIL to a specific process AND how you might verify that the SIL has been achieved?

[6 marks]

c) The UK 2006 Regulations, cited above, expect that safety verification will be performed on behalf of a train operator by a 'competent person', defined as:

> "a person with sufficient practical and theoretical knowledge as well as experience of the particular task, plant, machine, procedure, equipment (etc) involved to enable them to thoroughly examine and identify any defects or weaknesses during examinations, and to assess their importance in relation to the safety, function and continued use of the plant, machine, procedure, (etc again) and to be aware of their own particular limitations with regard to the task to be undertaken." (UK HMRI, 2007)

What problems arise when trying to identify a 'competent person' to be responsible for the verification of safety-critical software?

[8 marks]

2.

a) Traceability is a core concept in DO-178C, Software Considerations in Airborne Systems and Equipment Certification. It must be possible to trace from high to low level requirements. It must also be possible to trace requirements to code. Traceability applies more widely across the lifecycle. It is important to show that all major software components have been tested; this implies links between test results and source code. The amount of time and money invested in traceability is linked to the software level which is determined by the effects of a failure on the system.

Briefly summarise the problems of demonstrating traceability across complex safety-critical software.

[5 marks]

b) DO-178C supports the use of model-based development; where abstractions including state-diagrams can be used to construct a high-level design that is then automatically transformed into executable code. This enables traceability between the high-level requirements expressed in the abstract representation and the implementation that can be automatically generated by appropriate tool support, for instance using Simulink's Code Inspector.

Identify five potential risks that might arise during the use of model-based development for safety-critical software engineering?

[5 marks]

c) At the very highest levels of integrity, DO-178C requires Modified condition/decision coverage (MDCD) testing. This assumes that you must test each decision in a program (Boolean expression) to examine every outcome. Each condition must also be shown to independently affect the outcome of the decision.

Briefly explain why MCDC testing is both costly and time consuming.

[10 marks]

3.

a) Why is it important to avoid a culture of ‘blame’ in the aftermath of a major accident or incident?

[5 marks]

b) The UK HSE defines Human Error to be an action or decision that was not intended. Identify five different causes of intended violations that commonly occur during the operation of safety-critical systems.

[5 marks]

c) The HSE guidance on ‘Reducing error and influencing behaviour’ (2007) identifies fatigue as a key factor in human error leading to major accidents and incidents.

Write a brief technical report explaining to senior management the risks that fatigue creates for the users of safety-critical software. Expand your answer to recommend a number of measures to combat the effects of fatigue and identify Key Performance Indicators (KPIs) that might be used to assess the effectiveness of these measures.

[10 marks]

4.

The Boeing 777 uses a Fly-By-Wire flight control system. High levels of reliability are achieved using triple redundancy across all major hardware including the computing, power, hydraulic communication systems. The Primary Flight Computer (PFC) uses triple modular redundancy and N-version diversity; there are three channels; each contains three dissimilar computation lanes.

Write a technical report explaining the technical strengths and weaknesses of this approach. Explain how an appropriate safety-management system can ensure potential weaknesses are identified and resolved in the design of future aircraft, including updates to the 777.

[20 marks]