Xday, XX XXX 2008.

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) The DO-178B definition of COTS is “Commercially available software sold by vendors through public catalogue listings. COTS software is not intended to be customized or enhanced. Contract negotiated software developed for a specific application is not COTS software”

Describe the problems that the use of COTS creates for the verification and validation of safety-critical software.

[5 marks]

b) COTS operating systems pose a number of further problems in the certification of safety-critical systems because it can be difficult to make arguments about the safety of a novel application based on the successful use of the operating system with another application.

Explain why arguments about experience in previous applications cannot easily be used to support the certification of COTS operating systems.

[5 marks]

c) Lynuxworks have recently developed a hard real-time operating system that they argue can be certified to DO-178B level A in a number of different applications. It uses both space and time partitioning to support multithreaded and multi-process systems in safety-critical environments and can be run on both Pentium and PowerPC platforms. It exploits many of the concepts familiar in other flavors of the UNIX operating system. In addition, it provides the notion of a Virtual Machine with partitions which are intended to prevent one process from interfering with another.

Describe how you would create an argument to convince regulators that a particular application did not suffer from interference in time or space between multiple concurrent processes and threads.

[10 marks]

2.

a) The HAZOPS technique typically begins with a form of functional block analysis which breaks complex systems down into their component parts. What problems might arise in applying HAZOPS to analyze the safety of software systems?

[4 marks]

a) HAZOPS proceeds by applying guidewords to the functional models of a complex system. The intention is to identify the impact of potential deviations from the intended design. Many applications of the technique are based around a general collection of guidewords such as "NO OR NOT", "REVERSE", "MORE", "OTHER THAN", "LESS", "SOONER THAN", "AS WELL AS", "LATER THAN", "PART OF".

Explain whether or not this list would be sufficient to conduct a HAZOPS for a complex software system and, if the list is insufficient then identify further THREE guidewords that might specifically support HAZOPS for programmable electronic systems.

[6 marks]

b) HAZOPS studies can be documented in a tabular form using the following headings:

Deviation	Cause	Consquence	Safeguards	Action

A deviation typically refers to an element of the functional decomposition and one of the guide words. For instance, a sensor reading may be processed by the software 'LATER THAN' a specified deadline. Once a system has been deployed, experience of using software in an operational context can be used to guide subsequent HAZOPS studies. In particular, any deviations that have been observed during operation can be analyzed to identify causes, consequences and so on.

Briefly explain why the post operational application of HAZOPS to software systems requires a very high level management commitment to the monitoring, documentation and audit of a software application.

[10 marks]

3.

a) Lloyds Register of Shipping have coordinated studies into the impact that Electromagnetic Compatibility (EMC) can have upon the functional safety of maritime systems. They argue it is essential that designers and operators "account for the effects of EMC in the marine industry" using hazard and risk assessment techniques that are appropriate for particular EMC environments. The main sources of interference above decks are the ship's radio transmitters.

Describe the technical problems that can arise when trying to demonstrate EMC for computational systems in maritime applications.

[5 marks]

b) Lloyds Register is a classification society. These are private companies that are authorised to inspect ships and issue safety certificates for States where ships are registered. A European directive (94/57/EC) describes requirements that classification societies must meet in order for them to be recognized by a Member State under European legislation.

What problems can arise when recruiting well qualified staff to work for certification societies and similar organizations that work as independent safety assessors?

[5 marks]

c) The UK Maritime and Coastguard Agency inspects a proportion of vessels in UK ports. During 2006-7, 4.9% of the foreign ships inspected in the UK were detained. A mean of 4.5 deficiencies were found during each inspection. Some states are named on an international 'black list' which reflects particular concerns over their safety management. The 8.4% detention rate for ships from these states was over twice the rate for non-targeted flags. A total of 19 ships classed by members of the International Association of Class Societies (IACS) were detained where the Classification Society was found to be held responsible for the detention. The detention rate for IACS ships was 1.2%. Ships classed with Classification Societies which are not members of IACS were over 6 times more likely to be held responsible for a detention than IACS societies.

Imagine you have been asked to act as a consultant to one of the states on the international 'black list', write a technical report describing how you would go about improving the safety record of vessels that operated under the flag of that state. (Hint: you may refer to elements of your answer to part b)

[10 marks]

4. Safety can be described as an emergent property that cannot easily be determined before complex applications have been deployed in their eventual context of use. State whether or not you agree with this view. Develop your answer with examples and explain the implications that emergency views of safety have for the resilience engineering of complex systems.

[20 marks]