Xday, XX May 2006.

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) The Airbus A380 cabin air pressure control is a highly safety-critical system. It must ensure the comfort and well-being of passengers and crew across a range of altitudes and was developed to the DO-178B standard, 'level A'. At this level, the failure of any software is assumed to have potentially catastrophic consequences for flight operations.

Explain how risk assessments can be used to justify the assignment of 'level A' criticality to the A380 cabin air pressure control system.

[5 marks]

b) In order to meet the DO-178B 'level A' requirements, software testing must have complete coverage across the three different dimensions listed below:

- Statement Coverage; every statement in the program should be invoked at least once during testing.

- Decision Coverage; every entry and exit in the program should be tested at least once and each decision in the program should be examined at least once across all possible values.

- Modified Condition Decision Coverage; every entry and exit point in the program should be invoked at least once, every decision in the program should be tested for all possible outcomes at least once and each condition in a decision should be shown to independently affect the outcome.

Briefly explain the management techniques that must support the manual analysis of code to ensure coverage of 'level A' software verification under DO-178B. (Hint: consider the potential problems of conducting tests across each of these three dimensions and whether it is possible to satisfy all of these requirements in the general case).

[5 marks]

c) Part of the A380 cabin pressure control system has been developed using a code generator. This system enables developers to use more abstract, mathematically based languages using environments such as Matlab, Simulink and Stateflow to create the high-level design for a system. The code generator will then help to derive executable software based on these designs.

Explain why the use of code generators can reduce the burdens associated with the verification of 'level A' software in DO-178B and explain the potential dangers of using a code generator.

[10 marks]

2.

a) The US Army recently announced that it is likely to support a combination of the Linux operating system and Intel processors for its Future Combat System (FCS) program. FCS is intended to support the next-generation of manned and robotic air and ground systems connected by a fast, secure communications network. There are four layers identified in the high-level architecture: applications, services, transport and standards and it is estimated that the eventual system will integrate more than 35 millions lines of computer code.

Explain the potential benefits of using the Linux-Intel combination for the development of potentially safety-critical applications.

[4 marks]

b) One of the leading figures in the development of the Future Combat System (FCS) project, General Charles Cartwright, recently confessed that they were unsure about "how you put ground troops and robots together at the same time". In particular, it can be difficult to guarantee safety and liveness properties. For example, a safety property might require that an FCS vehicle never fires on friendly troops. A liveness property might require that information from friendly forces eventually arrives at the intended FCS vehicle.

Describe some of the technical difficulties in demonstrating safety and liveness properties for complex, safety-critical systems such as the FCS applications.

[6 marks]

c) A key component in the Future Combat System (FCS) software is the System-of-Systems Common Operating Environment (SOSCOE). This architecture uses commercial off-the-shelf hardware to produce:

> "…a nonproprietary, standards-based component architecture for real-time, near-real-time, and non-real-time applications. SOSCOE also contains administrative applications that provide capabilities including login service, startup, logoff, erase, memory zeroize, alert/emergency restart and monitoring/control. The SOSCOE framework allows for integration of critical interoperability services that translate Army, Joint, and coalition formats to native, internal FCS message formats using a common format translation service. Because all interoperability services use these common translation services, new external formats will have minimal impact on the FCS software baseline. The FCS software is supported by application-specific interoperability services that act as proxy agents for each Joint and Army system. Battle Command (BC) can access these interoperability services through application program interfaces that provide isolation between the domain applications, thereby facilitating ease of software modifications and upgrades.

(Acknowledgement: http://www.army.mil/fcs, last accessed 11th January 2007)

Identify the features of the System-of-Systems Common Operating Environment that have an implication for the safety of the Future Combat System (FCS). Explain any techniques that you would use to address the safety concerns that arise from your analysis.

[10 marks]

3.

a) During 2007, the European Space Agency (ESA) hopes to launch the Jules Verne spacecraft; this is the first of a proposed series of Autonomous Transfer Vehicles (ATVs). These ATVs are extremely large, approximately the size of a double-decker bus and will initially dock with the International Space Station. Because the autonomous design limits human intervention, there is redundancy in both the hardware and software. For example, the main Fault Tolerant Computer (FTC) that navigates the ATV mission is composed of three identical processing chains all executing the same code. In addition, a completely independent Monitoring and Safing Unit (MSU), incorporating two processing chains, monitors the performance of the FTC. If it detects an anomaly, it will first isolate the FTC and then execute a collision avoidance maneuver.

Explain why the MSU hardware and software must be independent from the FTC and why the MSU has been described as 'a satellite within a satellite'.

[5 marks]

b) The Autonomous Transfer Vehicle is of considerable strategic importance for the European Space Agency because there is a long term plan to use it in a modular approach to human space flight. This would involve the development of a Crew Transport Vehicle (CTV) which would add an accommodation module onto the existing ATV design. The software architecture would remain the same with the addition of an independent processor monitoring the accommodation capsule. However in order to support human spaceflight, the MSU emergency procedure would have to support more than the existing avoidance maneuvers.

Identify the new functions the MSU would have to support before trusting the lives of a crew to this architecture and identify any problems that you would envisage during the introduction of this new functionality. (Hint: you should make clear any assumptions about the MSU functionality in the ATV or CTV applications).

[5 marks]

c) Two different companies are involved in the validation of the existing MSU software. EADS is responsible for primary development under contract from the European Space Agency (ESA), while Rovsing of Denmark provide independent verification and validation of the code.

Imagine you are an employee of Rovsing, write a brief technical report for the project managers in the ESA explaining how you might use a combination of white and black box testing to increase confidence in the MSU software. (Hint: your answer should consider the limitations of independent testing in the context of such a complex mission)

[10 marks]

4. The legal systems in Scotland and in England and Wales provide for the common law offence of ‘manslaughter’ using the *mens rea* or ‘controlling mind’ principle. The prosecution must identify a responsible individual in order to establish guilt. In particular, the legal systems do not allow not allow for aggregation where the actions of a number of people over a period of time cumulatively provide the necessary evidence of a ‘guilty mind’ even when there is no individual who might exhibit this degree of culpability.

   Briefly explain the influence that these provisions have upon the operation and management of safety-critical technologies and state the reasons why you feel that *mens rea* should either be retained or removed.

   [20 marks]