Xday, XX XXX 2010

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 development of the European Geostationary Navigation Overlay Service (EGNOS) and Galileo systems will revolutionise the critical infrastructures of many European states. The encrypted Galileo Public Regulated Service (PRS) and Safety of Life Service (SoL) provide reliable services to a range of end-users including the police and military as well as transport applications, such as air-traffic management. However, there are significant safety concerns. For example, the additional accuracy offered by overlay architectures has supported the development of EGNOS Controlled Rail Applications in which the opening and closing of railway crossings is driven by a precise knowledge of the location of each train in the system. The intention is to minimise the delays to rail and road traffic. Rather than closing the gates for as long as it takes for the slowest train to pass the junction, they can be closed as soon as the EGNOS application reports that the train has moved on. In other words, the provision of accurate satellite based positioning systems enables the gradual erosion of previous safety margins by increased performance and reduced breaking.

Briefly explain how you would use safety integrity levels to guide the development of safety-critical applications such as the EGNOS Controlled Rail Application.

[5 marks]

b) In the past, there was relatively little on-board information processing by satellites. Instead they acted as a form of router – forwarding data to the ground based processors for further analysis. This is changing and owners are becoming increasingly interested in the use of redundancy to harden satellites to processor failures. Briefly identify at least three different ways in which redundancy might be used to address the problem of on-board processor failures.

[5 marks]

c) Global Navigation Satellite Systems, such as Galileo, have three major components:

a. A ground control system responsible for maintaining the operation of the satellite;
b. Communications ground stations that send and receive data to the satellite.
c. The satellite itself that is controlled by the ground control system and which provides data to, and receives data from, the communications ground control system.

A company is hoping to develop and market a variant of the EGNOS Controlled Rail System. Even though you might have reservations about this approach, you have been asked to write a report explaining how one might use estimates of failure probabilities to derive numeric risk assessment for the failure of software modules in these three components.

[10 marks]

2.

a) A recent report published by a group of 7 nuclear regulators, including the UK Health and Safety Executive, summarized the problems of software development for nuclear reactors in the following way:

> "It is widely accepted that the assessment of software cannot be limited to verification and testing of the end product, i.e. the computer code. Other factors such as the quality of the processes and methods for specifying, designing and coding have an important impact on the implementation. Existing standards provide limited guidance on the regulatory and safety assessment of these factors. An undesirable consequence of this situation is that the licensing approaches taken by nuclear safety authorities and by technical support organizations are determined independently and with only limited informal technical coordination and information exchanges. It is notable that several software implementations of nuclear safety systems have been marred by costly delays caused by difficulties in coordinating the development and the qualification process".

Briefly explain why regulators find it so difficult to develop appropriate means of certifying safety-critical software for use within the nuclear industry.

[5 marks]

b) The same report recommended that:

"Before a system is taken into operation, the licensee should submit written proposals to the Regulatory Authority on the methods to be employed (change control, configuration management, maintenance, data entry etc.) to ensure that the required level of integrity of the safety system will be maintained throughout its operational life".

Explain the importance of traceability and configuration management in the life-cycle of safety-critical software.

[5 marks]

c) The 7 European nuclear regulatory agencies identified a number of benefits that can be derived from the use of mathematics and formal methods in the specification and analysis of complex, software systems. However, they also enumerated a number of concerns:

> "…when used inappropriately, formal methods may be dangerous as:
>
> - their lack of legibility may lead to difficulties in understanding and verification, especially for plant specific application software which must be understood by different branches of engineering,
> - no method is universal, and the impossibility of expressing some types of requirements important to safety (e. g. non functional requirements or aspects of real time behavior) may lead to incompleteness or inconsistencies,
> - they might be used by insufficiently trained personnel or without support of adequate tools. In addition, the training effort required by the use of a formal method can be disproportionate to the benefits that can be expected".

Write a brief technical report explaining to the managers of a reactor operating company how these limitations might be addressed to support the use of formal techniques in software development.

[10 marks]

3.

a) Human Factors distinguishes between "skill-based" performance, "rule-based" performance, and "knowledge-based" performance. Skills are routine behaviors that we perform almost without thinking. Rule based performance involve more conscious thought as we seek to apply procedures that we have been taught. Knowledge based performance often requires wider forms of inference and general knowledge when we cannot find an applicable procedure.

Briefly explain why these three concepts are important for the design of safety-critical systems with reference to one of the accidents or incidents that you have studied during this course.

[6 marks]

b) Slips and lapses are errors of skill based behaviour. In contrast, mistakes are associated with rule or knowledge based performance. Distinguish between these different forms of human error and explain what measures you might take to reduce the frequency of each type of error in the design of the safety-critical system mentioned in your answer to part a).

[6 marks]

c) Performance shaping factors (PSFs) can have a major impact on the frequency of human error in complex, safety-critical systems. Write a brief report describing how PSFs might affect the occurrence of slips, lapses and mistakes. You should then explain how testing might be conducted to assess the impact of PSFs on the operation of safety-critical user interfaces.

[8 marks]

4. The Haddon-Cave review into the loss of Nimrod MR2 Aircraft XV230 advocated the development of ‘risk cases’ that are to be maintained throughout the life of a safety critical system. The QC argued that ‘a paradigm shift is required away from the current verbose, voluminous and unwieldy collections of text, documents and GSN diagrams to Risk Cases which comprise succinct, focused and meaningful hazard analysis which stimulate thought and action’.

   Write a brief technical report that describes how the Haddon-Cave recommendations might affect the development of complex safety-critical systems that integrate software components.

[20 marks]