Xday, XX XXX 2012.

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) Several major car manufacturers have recently been forced to recall their vehicles following software related failures involving Anti-lock braking systems (ABS) and cruise control applications.

Briefly explain why it is so hard for companies to guarantee the safety of their software before it is released onto the market.

[5 marks]

b) Earlier this year, a warning was issued in the United States about a complex software problem that led to a vehicle recall:

> XXXX IS RECALLING CERTAIN MODEL TRUCKS MANUFACTURED FROM OCTOBER 25, 2010, THROUGH NOVEMBER 20, 2010. THESE VEHICLES WERE INSPECTED USING INTEGRATED DIAGNOSTIC SYSTEM (IDS) THAT HAD A CUSTOM SOFTWARE ROUTINE TO READ THE SUSPECT BODY CONTROL MODULE (BCM) SERIAL NUMBER. BASED ON THE SERIAL NUMBER THE BCM WAS EITHER NOT AFFECTED OR REPLACED. THE CUSTOM SOFTWARE ROUTINE WAS NOT READING THE CORRECT SET OF CHARACTERS, AND WAS NOT ABLE TO IDENTIFY A BCM THAT REQUIRED REPLACEMENT AFFECTED BCMS MAY HAVE THE POTENTIAL FOR AN INTERNAL SHORT (THAT COULD RESULT IN A VEHICLE FIRE).

Briefly explain how a risk-based approach to safety-critical software development might have been used to identify the risks associated with the failure of the IDS.

[5 marks]

c) Last year, the media raised concerns that a major vehicle manufacturer had a software problem with their ABS. Groups within NASA were commissioned to determine whether or not such a problem existed. They were unable to replicate the reported errors and instead chose to focus on driver error and problems with the floor mats inside the vehicle.

Why is it so hard to identify the causes of intermittent software failures? Your answer should refer both to the likelihood of failure and also the risk exposure for mass-market applications.

[10 marks]

2.

a) The IEC 61508 standard focuses on the hazards that are associated with equipment under control (EUC). Briefly explain how this assessment is used to derive the Safety Integrity Level (SIL) of software within a safety-critical application.

[5 marks]

b) A number of criticisms have been raised about the application of SILs within international standards. These include the following:

- It is difficult to harmonize the use of SILs within and between industries;
- It is difficult to ensure the consistent use of SILs across different international standards;
- The use of SILs often drives the application of process rather than product based metrics;
- SILs are typically derived from expert judgments and reliability estimates that are difficult to validate.

Write a brief technical report for a software development company explaining what steps they might take to address some of these criticisms within their own engineering practices.

[10 marks]

c) In the UK, Health and Safety legislation is drafted to ensure risks are As Low As Reasonably Practicable (ALARP). The US equivalent is known as the As Low As Reasonably Achievable (ALARA) principle. Other countries use Minimum Endogenous Mortality (MEM) to guide risk-based decision making. MEM requires that organizations do not introduce hazards, which will 'significantly increase' the death rate beyond that expected from disease, congenital mortality etc.

Summarize the problems that arise when these approaches are used to guide the engineering of safety-critical software.

[5 marks]

3.

a) In November 2010, Space Exploration Technologies (Space X) was granted the first Federal Aviation Administration license allowing the reentry to Earth of a privately developed spacecraft. The FAA conducted a review of 1) the public safety issues; 2) the environmental impact; 3) the potential payloads; 4) national security and foreign policy concerns, and 5) insurance.

Identify the technical and managerial problems that can arise when assessing the adequacy of a commercial organization's ability to meet each of the five requirements considered in the FAA's review.

[5 marks]

b) The FAA certification described in part a) was required before tests could be conducted to determine whether or not it was safe for Space X's Dragon capsule to carry crew to the International Space Station (ISS).

Summarize the problems that arise when government agencies must assess the adequacy of tests that are conducted by commercial agencies meeting service oriented safety software requirements rather than delivering a product, such as a capsule or launch vehicle.

[5 marks]

c) The first flight of the Dragon to the ISS was scheduled for January 2012. This was delayed because the control software had to be delivered to NASA so that the algorithms could be validated. NASA's Commercial Orbital Transportation Services teams also needed copies of the code so that they could use Monte Carlo techniques in software verification.

Explain how program delays impose particular pressures for 'white box' verification and the validation of complex, safety-critical software systems. Identify techniques that can be used to reduce the impact of these pressures.

[10 marks]

4. Brazil, the Russian Federation, India and China have become known as the 'BRIC' nations. They are characterized by emerging and fast growing economies. However, their safety record arguably lags behind other nations'.

   You have been asked to write a brief technical report presenting a strategy for the introduction of software systems safety concerns into the development practices of a company that develops safety-critical software in a BRIC nation.

   (Hint: you should illustrate your answer by referring to previous accidents. Reference should also be made to the application of risk assessment techniques and to the study of human factors in safety critical systems).

   [20 marks]