Xday, XX XXX 2009.

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 UK Health and Safety Executive provide guidance for companies on their responsibilities under the Control of Major Accident Hazards Regulations 1999 (COMAH). This documentation includes the following statements on the decommissioning of safety related applications:

"*General measures that should be adopted for a common approach to decommissioning include:*

- *Establish communication with plant personnel to ensure surrounding plant areas are prepared for decommissioning activity;*
- *Undertake removal of hazardous substance via a cleaning procedure to ensure plant item is clean and empty with particular consideration where there may be dead-legs where material may be trapped;*
- *Consideration of the disposal of items which may be contaminated by absorption of hazardous substances and chemical change;*
- *Mechanically isolate plant item from other surrounding plant items by physical disconnection or fitting of blanks;*
- *Electrically isolate plant item from power sources by physical disconnection".*

Briefly explain why this guidance does not explicitly refer to the role that software systems might play in the decommissioning of Major Accident Hazards.

[5 marks]

b) The COMAH guidance encourages the use of HAZOPS as a means of assessing the risks associated with the decommissioning of safety-related applications. This technique uses process flow diagrams to identify the intentions behind different components. For example, a pump may be intended to deliver coolant to a reactor. Keywords, such as "NO OR NOT", "REVERSE", "MORE", "OTHER THAN", "LESS", "SOONER THAN", "AS WELL AS", "LATER THAN", "PART OF", are then used to identify the effects of deviations in these intentions.

How might this approach be extended from the decommissioning of safety-critical applications to support the analysis of safety requirements for the decommissioning of programmable systems in COMAH processes?

[5 marks]

c) The Health and Safety Executive have recently published the guidance that they give their inspectors on how to assess the Process Safety Management Systems and Safety Cases that companies must develop when they seek approval to operate safety-critical systems. One of the most important sections of this document is a footnote, which states that "*Note: a particular problem found by HSE's inspectors has been of HAZOP actions remaining unresolved or uncompleted".* Explain why this problem might also affect the use of HAZOPS in the decommissioning of safety-critical software. What steps might you take in order to ensure that the actions identified in a HAZOPS study are addressed in an appropriate manner?

[10 marks]

2.

a) The UK Civil Aviation Authority has published CAP 722 on Unmanned Aircraft System (UAS) Operations in UK Airspace – Guidance this includes the requirement that "*any UAS outside a UK Danger Area will not increase the risk to existing users and will not deny airspace to them*". In particular, CAP 722 makes it explicit that Unmanned Aircraft Systems must provide "*a level of safety and security equivalent to that of manned aviation*".

Briefly explain the challenges that must be addressed before any operator or manufacturer could demonstrate that they have met an equivalent level of safety to manned operations.

[5 marks]

b) One way of achieving the integration of UAS' into controlled airspace is through the development of Detection, Sense and Avoid (DSA) systems that enable the UAS to identify and then avert a potential collision with another air vehicle. The US Standards group ASTM has issued a standard for DSA technology (F2411-04 DSA Collision Avoidance), which may become the basis for future certification requirements within the Federal Aviation Administration. The ASTM standard requires that a UAS detect any airborne object within a range of + or - 15 degrees elevation and + or -110 degrees azimuth. The UAS must also be able to act on this information so that collision is avoided by at least 500 ft.

Explain the problems that manufacturers face in verifying that on-board software is capable of meeting the DSA requirements within ASTM standard F2411-04.

[5 marks]

c) Describe the ways in which 'white box' and 'black box' testing might be combined during the certification of DSA software in Unmanned Aircraft Systems. How might data from previous accidents involving both manned and unmanned aircraft be used to direct the application of these techniques?

[10 marks]

3.

a) ‘Resilience Engineering’ has recently criticized the use probabilistic risk assessments (PRA) and probabilistic safety assessments (PSA); PRA and PSA focus too much on a small number of previous failures and, therefore, neglect the many different ways in which organizations respond in a flexible way in order to maintain safe and successful operation.

Briefly explain whether or not you believe the concepts of resilience engineering can usefully be applied to support the software engineering of complex safety-critical systems.

[6 marks]

b) In order for Resilience Engineering to be successful, it has been argued that companies must be provided with:

1. The means of measuring and monitoring the resilience of organizations in particular operating environments;
2. Tools and methods to help improve the level of resilience identified through the application of measurement techniques identified in point 1;
3. Techniques to predict short and long-term effects of the changes introduced by the use of tools and methods developed in point 2.

How might these requirements for resilience engineering be applied to study the safety related processes of a company involved in the development of safety-related software?

[4 marks]

c) In a recent study of safety within NASA, David Woods identified five different ways of assessing the resilience of an organization:

1. *“Preparedness/Anticipation: is the organization proactive in picking up on evidence of developing problems versus only reacting after problems become significant?*
2. *Opacity/Observability—does the organization monitor safety boundaries and recognize how close it is to ‘the edge’ in terms of degraded defences and barriers? To what extent is information about safety concerns widely distributed throughout the organization at all levels versus closely held by a few individuals?*
3. *Flexibility/Stiffness—how does the organization adapt to change, disruptions, and opportunities?*
4. *Revise/Fixated—how does the organization update its model of vulnerabilities and the effectiveness of countermeasures over time?”*

Identify ways in which these dimensions characterize the causes of previous accidents and explain how they might be used to support the software engineering of future systems.

[10 marks]

4. Previous initiatives to improve safety culture have focused too much on the operator and too little on the Board of Directors. Discuss.

   (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]