Xday, XX XXX 2013.

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) Identify three different systems of governance that can be used to ensure the safety of the general public and identify ONE limitation for each of these different approaches.

[6 marks]

b) The Chair of the UK Health and Safety Executive recently confirmed that her organization has been required to make a minimum of 35% savings; this is the same percentage reduction in costs expected for the Department of Work and Pensions as a whole. What impact might such cuts to regulatory agencies have upon companies that develop safety-critical software across a range of industries?

[5 marks]

c) THE UK Health and Safety Executive have published guidance on the Control of Major Hazards for processes involving programmable systems. One section of the guidance focusses on alarm systems that alert operators to plant conditions, such as deviation from normal operating limits which require timely intervention:

> "Alarm systems are not normally safety related, but do have a role in enabling operators to reduce the demand on the safety related systems, thus improving overall plant safety. However, where a risk reduction of better than 10-1 failures on demand is claimed then the alarm system, including the operator, is a safety related system which requires a suitable safety integrity level (SIL 1 or SIL 2 as defined by BS IEC61508)… For all alarms, regardless of their safety designation, attention is required to ensure that under abnormal condition such as severe disturbance, onset of hazard, or emergency situations, the alarm system remains effective given the limitations of human response. The extent to which the alarm system survives common cause failures, such as a power loss, should also be adequately defined".

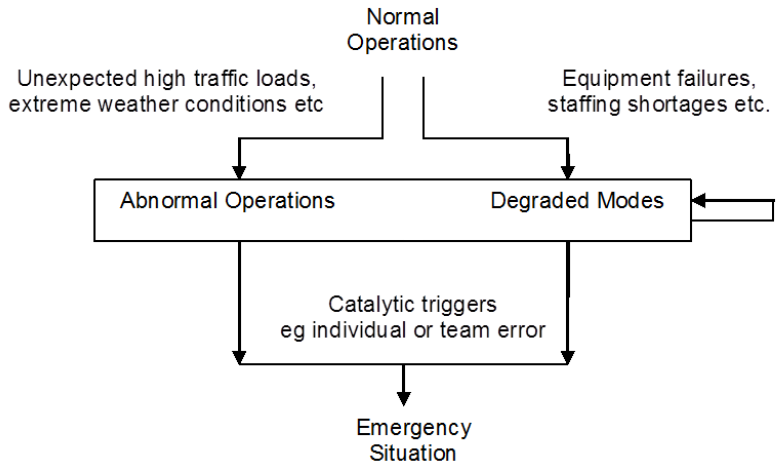
Write a brief technical report describing the problems that arise during the validation and verification of software in alarm systems for safety-critical applications.

[10 marks]

[Cont.]

2.

a) The following diagram has been adapted from UK Rail industry guidance on degraded modes of operation. Use the components of the model to analyse any of the accidents or incidents that have been discussed during the course.



[5 marks]

b) Redundancy is often cited as a powerful means of maintaining safety under degraded modes of operation. Briefly describe the following forms of redundancy:

- Data redundancy
- Temporal redundancy
- Single and Multi-version redundancy
- Hot and cold redundancy
- Triple modular redundancy

[5 marks]

c) Identify at least five limitations with the use of software redundancy as a means of ensuring the safety of complex systems.

[10 marks]

[Cont.]

3.

a) Briefly explain the differences between transient, intermittent, partial and total failures. Which of these different failure modes can be caused by electromagnetic interference with software systems?

[5 marks]

b) The European Electromagnetic Compatibility (EMC) 2004/108/EC came into force on 20 July 2007; products must not generate electromagnetic pollution. Equipment must also be resilient to interference. 2004/108/EC does not state the maximum levels of emissions or resilience. In practice, however, companies must develop tests across five different areas:

- Radiated emissions - Checks to ensure that the product does not emit unwanted radio signals;
- Conducted emissions - Checks to ensure the product does not send out unwanted signals along its supply connections and connections to any other apparatus;
- Radiated susceptibility - Checks that the product can withstand a typical level of radiated electromagnetic pollution;
- Conducted susceptibility - Checks that the product can withstand a typical level of noise on the power and other connections.
- Electrostatic discharge - Checks that the product is immune to a reasonable amount of static electricity.

Explain how safety cases can be used to record the relationship between evidence and the arguments that might be used to convince a national regulatory authority that a particular product meets the requirements of 2004/108/EC.

[5 marks]

c) There are a host of other directives that deal with EMC. These include 93/42/EC on Medical Devices and 95/54/EC on automotive applications. Under European Law, the areas addressed by these more specific directives are excluded from the provisions of 2004/108/EC.

You have been hired by a company developing a new family of safety-rated processors. Write a brief technical report for company management explaining the technical challenges that these different directives create when trying to sell hardware across different European industries. Your report should also identify ways to address the problems that different industry directives create.

[10 marks]

[Cont.]

4. NASA Software Safety Standard (NASA-STD-8719.13B) states that:

"Software shall be classified as safety-critical if it meets at least one of the following criteria:

a. Resides in a safety-critical system (as determined by a hazard analysis) AND at least one of the following apply:
   i. Causes or contributes to a hazard.
   ii. Provides control or mitigation for hazards.
   iii. Controls safety-critical functions.
   iv. Processes safety-critical commands or data (see note 4-1 below).
   v. Detects and reports, or takes corrective action, if the system reaches a specific hazardous state.
   vi. Mitigates damage if a hazard occurs.
   vii. Resides on the same system (processor) as safety-critical software (see note 4-2 below).
b. Processes data or analyzes trends that lead directly to safety decisions (e.g., determining when to turn power off to a wind tunnel to prevent system destruction).
c. Provides full or partial verification or validation of safety-critical systems, including hardware or software subsystems.

a) Use the previous paragraph to contrast the approach to safety-critical software engineering embedded within NASA's STD-8719.13B with key concepts in IEC61508.

[10 marks]

b) NASA-STD-8719.13B is being revised – extend your answer to part a) to suggest ways in which the concept of safety integrity levels in IEC61508 might be integrated into future revisions of the NASA Software Safety Standard.

[10 marks]

[/End]