University of Glasgow

Wednesday XXX
XX-XX
(Duration: 2 hours)

DEGREES OF MSc, MSci, MEng, BEng, BSc,MA and MA (Social Sciences)

Safety Critical Systems Development (M)

(Answer 3 out of 4 questions)

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. (a) During the 1990s, the Motor Industry Software Reliability Association (MISRA) introduced a set of guidelines for the use of C in vehicle systems, which became known as MISRA-C. This aimed to provide the benefits of C including easy access to hardware, as well as memory and run-time efficiency while minimizing recognized problems such as limited run-time checking, opaque syntax and areas of the language that are implementation defined.

Briefly comment on the effectiveness of this approach as a means of improving the safety of automotive software.

[5 Marks]

(b) A new initiative has been created to develop Automotive Grade Linux (AGL). The initial focus is on In-Vehicle-Infotainment but is gradually being expanded to instrument clusters and telematics systems. At present the group developing AGL has not decided on a formal position with respect to the standard ISO 26262.

Why might this create concerns for the future use of AGL?

[5 Marks]

(c) The US National Highway Traffic Safety Administration defines five levels of automation: Level 0 (no automation); Level 1 (function-specific automation); Level 2 (combined-function automation); Level 3 (limited self-driving automation); Level 4 (full self-driving automation).

Explain the increasing problems that arise for the verification and validation of safety critical software as you move from level 0 to level 4 of this automation hierarchy.

[10 Marks]

2. (a) Top-down apportionment of risk can be used to set reliability targets for subsystems. For example, an overall reliability target was set for the Airbus A380 and then the risk apportionment was divided amongst individual sub-systems. Verification and validation activities were then used to ensure that those sub-systems could meet the target level of reliability before full manufacturing commenced.

Briefly describe the technical challenges that arise when using risk apportionment to guide the development of complex, safety-critical software.

[4 Marks]

(b) Scaling adjusts the risk apportionment of subsystems to reflect the relative scale of particular components compared to other subsystems. A number of factors can be considered when scaling the apportionment of risk, these include:

- physical size (area of plant or factory);
- size of workforce exposed to a hazard;
- throughput as an indicator of relative importance to company/process;
- inventory of hazardous materials or processes;
- potential impact on surrounding community.

Justify the use of each of these criteria for scaling the risk apportionment of subsystems.

[6 Marks]

(c) Standards such as IEC61508 associate higher levels of risk with incidents that might affect the general public rather than direct employees of an organization. Higher levels of risk are also associated with incidents that lead to multiple casualties from a single adverse event.

Explain why these distinctions are made and outline the impact that they can have for the development of safety-critical software in complex systems.

[10 Marks]

3.

(a) NASA GB 8719.13 Software Safety Guidebook contains the requirement that "Each NASA project, regardless of its level of safety-criticality, must perform an IV&V evaluation at the beginning of the project, and whenever the project changes significantly".

Briefly explain why it is important to plan for IV&V both at the start of a project and when there are significant project changes.

[4 Marks]

(b) NASA guidance GB 8719.13 also advocates a change management process that includes the use of cross-indexing to link software changes, requirements, code, component versions and testing.

Why is it important to support each of these forms of traceability? Explain how safety cases can be used to assess the impact that software changes have upon the overall safety of a complex system.

[6 Marks]

(c) The US Federal Aviation Administration (FAA) recently issued a circular on 'tool qualification guidance' that includes the following requirement:

"If your legacy system software was previously approved using ED-12 / DO-178 or ED-12A / DO-178A, and you intend to use a new or modified tool for modifications to the legacy system software, use the criteria of ED-12C / DO-178C, section 12.2, to determine if tool qualification is needed. If you need to qualify the tool, use the software level assigned by the system safety assessment for determining the required Tool Qualification Level (TQL), and use ED-215 / DO-330 for the applicable objectives, activities, guidance, and life cycle data. You may declare your qualified tool as having satisfied ED-215 / DO-330 and not the legacy system software as having satisfied ED-12C / DO-178C".

Write a brief technical report for a project manager explaining what this means for future software development projects involving legacy code.

4. Write a technical report for the senior management of a safety-critical software company explaining the problems that can arise when attempting to improve safety culture across the software supply chain.

Your answer should explain how some of the risk assessment techniques that have been presented in the course might be used to focus resources on those software suppliers, which have the greatest impact on **system safety**.

[20 Marks]