University of Glasgow

Wednesday 11 May 2016
9.30 am – 11.30 am
(Duration: 2 hours)

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

Safety-Critical Systems Development (H)

(Answer 3 out or 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) When the autonomous mode of a self-driving car disengages, the driver must assume direct control to ensure the safety of the vehicle. Google report that the number of disengagements of autonomous control in their fleet of test vehicles has dropped from 785 miles per disengagement in the fourth quarter of 2014 to 5318 miles per disengagement in the fourth quarter of 2015. What are the implications of this increase in reliability for the human factors of interaction with autonomous software controlled systems?

[4]

(b) Google's review of their tests on the roads of California has identified 69 reportable safe operation events. These included 13 where the test driver prevented the vehicle from making contact with another object. The remaining 56 were safety-significant because some aspect of the vehicle's behavior could have caused contact in other environments or situations including "proper perception of traffic lights, yielding properly to pedestrians and cyclists, and violations of traffic laws". Briefly describe the strengths and weaknesses of testing safety-critical systems in their final context of operation.

[6]

(c) Companies including Audi, Mercedes, Tesla, Bosch are all developing similar autonomous vehicles. It is possible to identify common ideas across many of these vehicles, integrating GPS, laser illuminating detection and ranging (LIDAR), radar, high-powered cameras and learning algorithms to 'sense and avoid' other objects in their environment.

Traditionally, artificial intelligence has been explicitly forbidden from higher Software Assurance Levels. Write a brief technical report for the senior management of a car company, explaining why regulators are reluctant to permit the use of AI in safety-critical applications and then summarizing the arguments that might be used to support the use of learning algorithms in self-driving cars.

[10]

2. (a) Briefly explain the key concepts behind resilience engineering.

[6]

(b) Identify the main challenges that can arise when introducing incident reporting into safety management systems for large-scale software engineering projects. Briefly explain how you would address these challenges.

[7]

(c) Write a brief technical report for software engineers, explaining why root cause analysis raises non-trivial problems during the analysis of degraded modes of operation or after major incidents involving complex, software systems.

[7]

3. (a) Briefly explain why we might need to use both qualitative and quantitative risk assessments during the development of complex safety-critical systems?

[4]

(b) Describe the role of safety integrity levels (SILs) within the IEC61508 standard and explain the differences between SILs and the Automotive Safety Integrity Levels within the ISO 26262 standard.

[6]

(c) What is 'regulatory lag'? Write a report for a senior government official explaining how you would address the problem of regulatory lag in software development within safety-critical autonomous systems that interact with members of the public.

[10]

4. Safety is a non-functional requirement.

Write a brief technical report to a Chief Executive Officer who only understands office-based software systems, explaining why non-functional requirements cause particular problems for the management of complex, software projects.

Identify at least three different measures that might be introduced into the software development lifecycle to help manage non-functional requirements from conception through to maintenance.

[20]