University of Glasgow

Wednesday XX XX 2017
XX.XX-XX.XX
(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) Briefly explain how perception, cognition and physiology influence the safety of complex, interactive software systems.

[4]

(b) The UK Office of Rail Regulation publishes guidance on Managing Rail Staff Fatigue. This stresses that fatigue increases the likelihood of errors and adversely affects performance, especially in tasks that require vigilance and monitoring; decision-making; awareness; fast reaction time; tracking ability; memory.

Briefly explain how software might be used to mitigate the impact of fatigue on each of these types of task.

[6]

(c) Automation is frequently cited as a way of mitigating the impact of human error, by reducing the operator's ability to intervene with safety-critical applications. Explain some of the problems that have been encountered when fully autonomous systems are integrated with more conventional applications.

(Hint: illustrate your answer using case studies that we have met on the course in the safety engineering of either autonomous cars or Unmanned Airborne Systems)

[10]

2. (a) What are non-functional requirements?

[6]

(b) Explain the problems that arise when integrating cyber security concerns into safety-related risk assessments.

[7]

(c) The US Food and Drugs Administration (FDA) recently issued a warning about the cyber-security of infusion pumps; these deliver drugs to a patient at a pre-programmed rate for fixed periods of time. Some infusion pumps can be programmed remotely through a health care facility's Ethernet or wireless network. An unauthorized user with malicious intent could access the pump remotely and modify the dosage it delivers, which could lead to over- or under-infusion of critical therapies.

Goal Structuring Notation (GSN) has been proposed as a means of integrating cyber-security concerns into the engineering of safety-critical systems.

Describe how this approach might be used to combine evidence about safety and security to improve our confidence in the software engineering of the infusion pumps examined by the FDA.

[7]

3. (a) How do safety kernels improve the reliability of critical software applications?

[4]

(b) Safety kernels are often resident in non-volatile ROM or in another form of protected memory. There is also often a requirement that the kernel is implemented so that it cannot be corrupted, delayed or substituted by any other program in the system.

Briefly explain the importance of each of these requirements for the implementation of safety kernels in high reliability software systems.

[6]

(c) Software testing is 'necessary but not sufficient' for the verification and validation of safety-critical systems. Justify this statement and explain how a range of other techniques can be used to ensure that software meets safety requirements in complex, safety-critical applications.

[10]

4. 'Incident analysis provides greater insights into future risks than accident investigations involving safety-critical software.'

State whether or not you agree with this statement and illustrate your answer with examples drawn from the course.

(Hint: do not attempt this question unless you have done some of the preparatory reading in this area)

[20]