SCS Exam M 2015-2016, Answer 3 Questions

1.

a) Identify the main components of risk analysis.

[5 Marks]

b) The US Department of Defence MIL-HDBK-217F on Electronic Reliability Prediction helps suppliers calculate the mean time between failure for electronic systems. It provides models for different electronic, electrical and electro-mechanical components to predict failure rates. These calculations consider environmental conditions, quality levels and stress conditions as well as the impact of non-operating periods on equipment reliability. Briefly explain why each of these factors is considered within 217F.

[5 Marks]

c) Building on your answer for part b) of this question, explain how you could go about calculation the mean time between failures for systems that include software components.

[10 Marks]

2.

a) Briefly explain why many safety-critical applications do not use conventional approaches to multi-processing.

[5 Marks]

b) The real time operating systems used in many safety-critical applications exploit on-chip memory management units (MMU) to ensure that individual threads run in hardware-protected address spaces. The MMU will translate any attempt to access physical addresses so that they are mapped to the region associated with a thread. The MMU will also flag attempts to access illegal logical addresses. Explain the benefits that MMUs provide for safety-critical systems.
[5 Marks]

c) The Linux operating system is gradually being introduced into a wider range of safety-critical applications, including flight control for SpaceX's Falcon, Dragon, and Grasshopper vehicles, SpaceX ground stations also run Linux. What are the main concerns about using Linux in safety-related environments?

[10 Marks]

3.

a) Briefly outline the problems that can arise when maintaining or extending the application of legacy code in safety-critical systems.

[5 Marks]

b) Why can virtualization sometimes be used to extend the life of legacy code on new families of processors. What are the concerns about this approach?

[5 Marks]

c) The FAA recently issued a circular on 'tool qualification guidance' that has been adapted by the European Aviation Safety Agency – this 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 analysis of the main challenges that arise during the safety certification and approval of software for autonomous systems.

[20 Marks]