SCS Exam H 2015-16, Answer 3 Questions

1.

a) Briefly describe the benefits of a cold-redundant back-up system for a safety-critical application.

[4 marks]

b) What are the main problems that must be considered when applying cold-redundancy to software rather than hardware applications?

[6 marks]

c) Hot, Cold and Warm redundancy are also used in non-safety applications. For instance, Cisco uses these techniques to ensure that packets can still be forwarded even when hardware components fail. Explain in detail the different amounts of state information that must be held by primary and backup systems when using hot, cold and warm redundancy. (Hint: comment on their relative space and time efficiency).

[10 marks]

2.

a) Briefly identify the main components within a safety-management system and explain how they contribute to the safety of complex software.

[6 marks]

b) What technique would you use to identify and quantify the risks associated with **human error** within an interactive, safety-critical system? Briefly justify your decision and explain why you did not choose at least one other approach.

[7 marks]

c) What technique would you use to identify and quantify the risks associated with **software failure** within an interactive, safety-critical system? Briefly justify your decision and explain why you did not choose at least one other approach.

[7 marks]

3.

a) Briefly explain why we tend to use process rather than product based approaches to the validation and verification of safety-critical software.
[4 marks]

b) Explain the problems that can arise when attempting to validate and verify any maintenance tasks that have been conducted on legacy software components.

[6 marks]

c) A Nordtest review of PLC validation techniques argued that; "The complexity of such a validation task is further increased by the fact that a proper validation of the system must address not only the application software, but that as much as 5 different aspects must be considered:

- The PLC context, i.e. all external I/O interfaces, sensors, actuators and power supply.
- The PLC input/output hardware providing the interface between the context and the PLC processor.
- The PLC processing HW (e.g. CPU, memory, timers, interrupt, watchdog)
- The PLC operating system (OS) often called the kernel that provides the environment for the application soft- ware, as well as a certain amount of fault handling.
- The PLC application software, implementing the user specified functionality for:
  - Primary safety functionality
  - Derived functionality to handle context fault conditions".

Explain why each of these different aspects must be considered within the validation of a PLC within a safety-critical application.

[10 marks]

4. A number of researchers have identified the problems associated with responding to 'weak signals' in the design and operation of safety-critical systems. Briefly enumerate some of these problems and identify techniques that might be used to address these concerns.

[20 marks]