Xday, XX May 2004.

9.30 am - 11.15am

University of Glasgow

DEGREES OF BEng, BSc, MA, MA (SOCIAL SCIENCES).

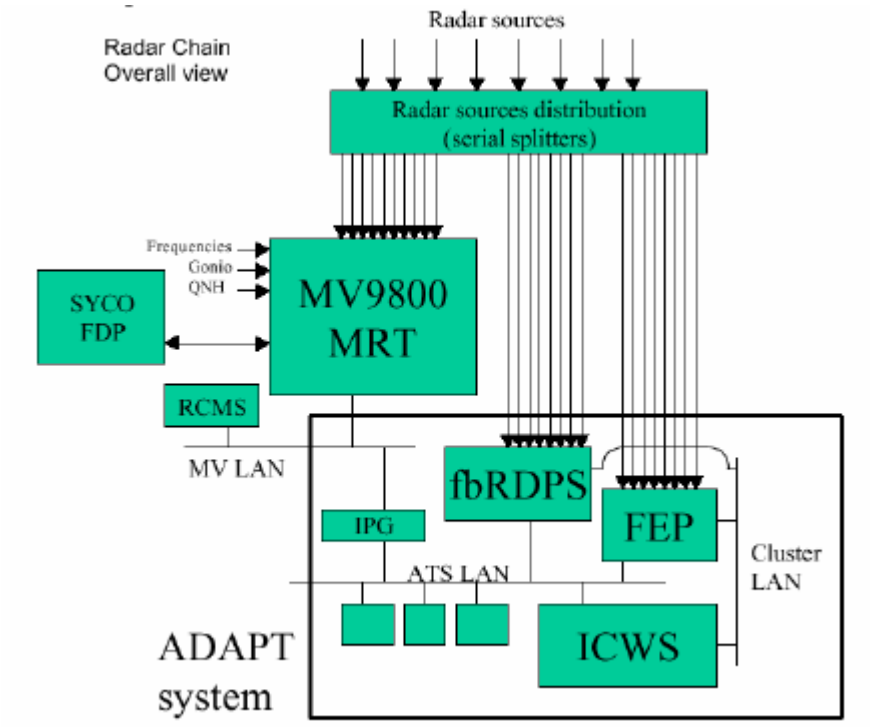
COMPUTING SCIENCE - SINGLE AND COMBINED HONOURS
ELECTRONIC AND SOFTWARE ENGINEERING - HONOURS
SOFTWARE ENGINEERING - HONOURS

SAFETY-CRITICAL SYSTEMS DEVELOPMENT

Answer 3 of the 4 questions.

1.

a) The following image shows part of the network schema for the Zurich Air Traffic Control system that was involved in the recent Überlingen mid-air collision.



The German BFU investigation into the collision describes the network as follows. "The radar data processing system consists of three main Thomson MV9800 computers. One MV computer generally is in "hot operation", the second is on "hot standby" and the third is used for test purposes and software development. This one is on "cold standby". The MV9800 processes the incoming signals and correlates them automatically with the flight plan data supplied by the flight data processing system (SYCO). The MV9800 is controlled and monitored by the RCMS (Remote Control & Monitoring System). The radar images correlated in the MV computer are sent via the IPG-IPS Interface Gateway to the monitors at the controllers' workstations (ICWS – Integrated-Controller-Workstation). Legal Recording records the radar raw data and the output of the radar data processed by the MV9800".

Briefly describe the way in which hot and cold standbys were used to increase the reliability of the Zurich Air Traffic monitoring system before the Überlingen accident.

[3 marks]

b) At the time of the accident, maintenance was being conducted on the system. In normal operation, the controller workstation (ICWS) uses flight plan data (FDP in the above diagram,) and direct radar information so that the controller can see the intended route for each of the aircraft. Flight plans describe the route that an aircraft is supposed to follow. However, the maintenance activity affected the flight plan system. Each controller had to manually work out the flight plan associated with each radar target on his or her screen. Using any of the techniques that we have looked at on this course, briefly conduct a high-level risk assessment for such maintenance activities and the potential impact on the controller.

[7 marks]

c) The Überlingen accident occurred at night when two controllers should have been on-duty. Traffic was light so one controller went to rest in another room. The remaining Air Traffic Control Officer had to move between two workstations several meters apart. He had to guide an A320 to land at Friedrichshaven

airport and coordinate the movements of a TU-154 and a B757. The maintenance work prevented his computer systems from generating a visual warning (Short Term Conflict Alert) for the TU154 and the B757. The controller apparently also failed to hear the aural warning that was generated. He eventually noticed the problem and asked the TU154 crew to descend. The TU154 crew were told by their on-board computer system (TCAS - Traffic alert Collision and Avoidance System) to climb but they instead followed the controller's instructions. The controller thought they had resolved the problem and moved to the other workstation to help the A320. Meanwhile, the B757 descended into the TU154 following instructions from TCAS. (Hint: The TCAS software communicates between each plane to coordinate the instructions to each crew. The TU154 was told to climb by TCAS and the B757 to descend. However, international regulations allow controller's to over-ride TCAS if they think they can avoid a collision.)

Briefly explain the role that the controller's situation awareness might have played in the causes of this accident. Comment on whether or not you feel that this was a 'systemic' failure.

[10 marks]

2.

a) The FIA are the governing body of Formula One racing. Their regulations require that "All software must be registered with the FIA, who check all the programmable systems on the cars prior to each event to ensure that the correct software versions are being used". Briefly explain the problems of using 'white box' testing to support the safety regulation of a competitive sport such as Formula One racing.

[5 marks]

b) The process of checking that a car's software conforms to the Formula One guidelines causes a number of problems. There are many changes to algorithms during the racing season and the software contains commercially sensitive information. In recent years, the FIA have offered teams two choices.

> **Option 1:** The software can be checked, line-by-line at the start of the season. A copy of the machine code is then kept by the FIA so that it can be compared at any time during a Grand Prix.
>
> **Option 2:** The software is not inspected at the start of the season. The FIA can demand an upload of all software at any time for a 'full check' if deemed necessary.

In recent seasons, each team has been asked to choose option 1 or option 2 at the start of the season. Most have chosen Option 2. Compare and contrast the strengths and weaknesses of each approach as a means of ensuring driver safety in motor sport.

[7 marks]

c) A recent summary of this scrutineering process argued that for any car control systems, the software is inspected to ensure that "ALL the code is accessed". It went on to argue that "System software is inspected to ensure that uploading, de-compiling and comparison software do not eliminate or modify the control software in any way. Especially important are checks to ensure that it is not possible to download an illegal program into RAM which is overwritten and lost when the system is switched off and then on again" (Peter Wright – Formula One Technical Guide, Scrutineering). Briefly explain the technical difficulties of performing these kinds of checks for complex, safety-critical systems.

[8 marks]

[Cont.]

3.

a) Two devices can be defined to be electromagnetically (EM) compatible when the electromagnetic disturbances produced by one device are not powerful enough to affect the operation of another, or when that equipment is protected enough from EM disturbances to continue working. Briefly explain why it can be difficult to use this definition to ensure that any particular device is safe from the hazards of electromagnetic radiation.

[3 marks]

b) The European EM compatibility directive requires computer and light industrial equipment to function in electromagnetic fields up to 3V/m. Computers and equipment in heavier industry must operate in EM fields up to 10V/m. Environmental conditions also affect performance. For example, systems that integrate many different items of equipment are more susceptible to electromagnetic problems than might be predicted by examining each of their components. Briefly explain how you would demonstrate that a proposed system design would be safe against the hazards of electromagnetic radiation.

[7 marks]

c) A recent report by the Institution of Electrical Engineers argued that it is increasingly difficult to keep potential sources of radiation, including mobile phones and Wireless LANs, away from sensitive safety-critical devices. The summary at the end of the report identified redundancy as a potential solution. Briefly explain the problems of using redundancy and diversity as protection against electromagnetic radiation.

[10 marks]

4. Explain the strengths and weaknesses of the ALARP ('as low as reasonably practicable') approach to design, as embodied within the Health and Safety legislation of various countries.

[20 marks]

[end]