Xday, XX May 2006.

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) On 14th August 2003, the company responsible for ensuring the reliability of electricity supply in part of the northern USA suffered a failure in its Real-Time Contingency Analysis (RTCA) software. This program monitored the current state of the power network and then simulated what would happen if failures occurred. The following extract from the official report into the 'blackout' identifies a number of key factors in the failure:

> "about 12:15, the RTCA produced a solution outside the bounds of acceptable error. This was traced to an outage of the Bloomington-Denois Creek 230-kV line, although it was out of service, its status was not updated. Line status information is transmitted by the data network and is intended to be automatically linked to the RTCA software. This requires coordinated data naming as well as instructions that link the data to the tools. The automatic linkage of this line's status had not yet been established. To troubleshoot this problem the analyst had turned off the automatic trigger that runs the RTCA every five minutes. After fixing the problem he forgot to re-enable it. Thinking the system had been successfully restored, the analyst went to lunch" (US-Canadian Presidential Report, 2003).

Explain the importance of data integrity as a cause of this failure.

[5 marks]

b) While the RTCA system was disabled, a second and unrelated software 'failure' affected Emergency Management System (EMS) software. The RTCA program, mentioned above, was used to predict the consequences of a failure in the electricity network. In contrast, the EMS software was used to warn companies when there actually was a failure in the electricity network. The EMS application ran on several servers, any one of which could host all of the EMS functions. However, the normal configuration was to have one server remaining as a "hot-standby". The primary server hosting the EMS failed, due either to "the stalling of the alarm application" or a data overflow on remote terminals that relied on EMS data. As intended, the alarm system application and all other EMS software running on the first server transferred to the back-up server. However, the alarm application "moved intact onto the backup while still stalled and ineffective". The backup server failed 13 minutes later.

Identify the particular strengths and weaknesses of software redundancy that are illustrated by this case study.

[5 marks]

c) The EMS server failures mentioned in part b) slowed the refresh rate on the operators' displays. EMS data was often nested in windows providing more general network information and so the EMS delays affected the operators' ability to refresh more general system information. These problems were compounded because the IT staff did not inform the operators that the EMS servers had failed.

Using the information provided in parts a), b) and c), explain the role that human factors played in both the immediate and longer-term (latent) causes of this safety-critical failure.

[10 marks]

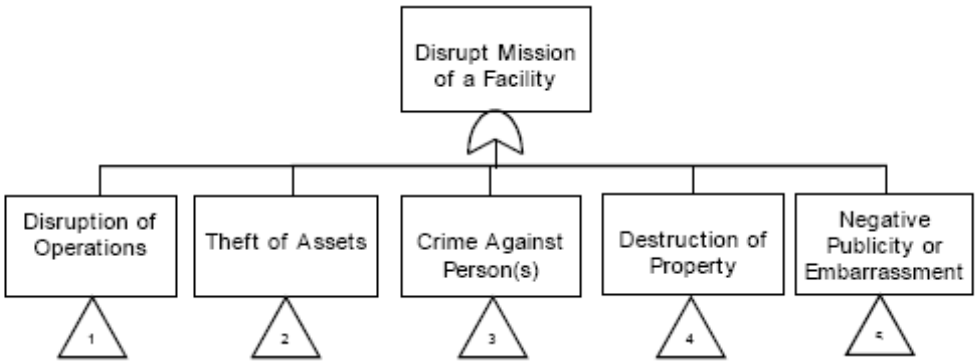
[Cont.]

2.

a) Briefly explain the different relationships that exist between the terms ‘reliability’, ‘safety’ and ‘security’. (Hint: is a secure system necessarily safe?)

[4 marks]

b) Risk based techniques have been advocated for secure applications. For example, the following diagram shows the US government’s Sandia Labs use of fault trees for risk assessment of security threats.



Briefly explain why this risk-based approach to the security of an application might make it more difficult to assess potential safety hazards.

[6 marks]

c) The same US government project that proposed the use of security fault trees has also recently promoted the development of the following risk equation:

$$R = P\_A * (1-P\_E) * C$$

Where R is the risk associated with adversary attack, P_A is the likelihood of the attack, P_E is the likelihood that the security system is effective against the attack, (1 – P_E) is the likelihood that the adversary attack is successful or the likelihood that security system is not effective against the attack and C represents the consequence of the loss from the attack. Using arguments derived from the assessment of safety-critical systems, comment on whether this simple formula is likely to provide important insights into the reliability of complex, security critical software.

[10 marks]

[Cont.]

a) The US Federal Motor Carrier Safety Administration has recently developed guidelines for the design and operation of Lane Departure Warning Systems (LDWS). These monitor the position of a vehicle and warn a driver if the vehicle is about to deviate outside their lane on the road. Currently these LDWS are forward looking, vision-based systems that use software to interpret video images to estimate vehicle state (lateral position, lateral velocity, heading, etc.) and roadway alignment (lane width, road curvature, etc.). The algorithms warn the driver of a lane departure when the vehicle is traveling above a certain speed and the vehicle's indicators are not in use. The LDWS software will also notify the driver when lane markings are inadequate for detection, or if the system malfunctions.

Briefly explain how a truck company might use black box testing to assess the reliability of a number of COTS LDWS applications.

[5 marks]

b) The Federal Motor Carrier Safety Administration describes a generic architecture for LDWS hardware. This includes an electronic control unit that accepts data from a lane boundary sensor through a J1708 or J1939 vehicle network. The control unit monitors the turn signal status and engine power. The output of the system is a status indicator and, when necessary, a warning, which appears on the driver-vehicle interface. Briefly explain how this proposed architecture might aid white box testing of the LDWS software by a system manufacturer.

[5 marks]

c) Celoxica are market leaders in the development of Lane Departure Warning Systems. They have pioneered the use of Electronic System Level (ESL) design. ESL increases the level of abstraction used in circuit design. Rather than building circuits using individual gates or circuit blocks, algorithms are characterized in C-based programming language. These are then implemented in silicon architectures that include software microprocessors, reconfigurable Field Programmable Gate Arrays and heterogeneous System on Chips. Briefly describe the strengths and weaknesses that arise from the use of innovative hardware and software co-design techniques for safety-critical systems.

[10 marks]

4. At present there is little agreement about how to determine whether a software engineer is competent to work on a safety-critical system. Write a brief technical report explaining how you would set up a national scheme so that the public could be confident programmers were competent to work on safety-critical software. Explain the benefits of your proposal by referring to any of the incidents and accidents that we have discussed during the Safety-Critical Systems course.

[20 marks]

[end]