THE UNIVERSITY
OF ADELAIDE
AUSTRALIA

Examination for
Bachelor of Agricultural Science, Bachelor of Architectural Studies,
Bachelor of Computer Science, Bachelor of Mathematical and Computer Science,
Bachelor of Business Information Technology, Bachelor of Engineering, and the Graduate Diploma in Computer Science

Semester Two, November 2005

3675, 6263 Software Engineering and Project COMPSCI 3006, 7015

Official Reading Time:	10 mins
Writing Time:	120 mins
Total Duration:	130 mins

Questions	Time	Marks
Answer all 6 questions	120 mins	120 marks
		120 Total

Instructions

- Begin each answer on a new page
- Examination material must not be removed from the examination room

Materials

- Open Book Examination
- 1 Blue book

DO NOT COMMENCE WRITING UNTIL INSTRUCTED TO DO SO

The questions in this exam paper relate to the following scenario.

The scenario

Your group has been contracted to write the software for a real minesweeping robot. The initial design for the robot has a magnetic mine sensor that can find metal mines. However half way through the development of the software the robot manufacturer asks you to change the system so that it can also support a new kind of mine sensor.

The new sensor works using Neutron Capture Gamma Ray Emission. You don't need to know anything about how this works, except for two things:

- The sensor provides a signal that is proportional to the amount of explosive under the sensor.
- The sensor uses a very dangerous radioactive source. This source is held in a lead box that has a remote controlled door in the floor. The door needs to be opened when the sensor is activated. To avoid the dangerous radiation, no person may be within 2 metres of the sensor when it is operating.

(The interested may like to know that such a detector is real, and research continues into building mine detecting robots using them.)

Most of this exam will explore the software engineering issues that stem from this scenario. More specific details will be given in the relevant questions.

Software Engineering Process Models

Question 1

(a) Two process models often encountered are the *waterfall* and *spiral* models. For each of these models describe the circumstances when each would be an appropriate choice.

[4 marks]

Suppose your project manager for the minesweeper software had heard rumors about the new sensor before the project started, and guessed that the team might be asked to support two sensors. With knowledge of the possibility of such an important change, he has chosen the *Spiral* model.

(b) Describe those features of the spiral process which allows your team to best handle the disruption and risks of the changed requirements.

[4 marks]

(c) Your company manager is much more familiar with the waterfall process. He will need convincing that the choice of spiral model instead of waterfall is a good idea. Provide two reasons why the waterfall model would be a bad choice.

[4 marks]

(d) In the specific context of this problem, suggest a process model that you would personally choose and provide an argument as to *why* this is an appropriate choice to best handle the requirements change.

[6 marks]

[Total for Question 1: 18 marks]

Tools

Question 2

(a) The new sensor for the robot is very expensive, and the older, cheaper, sensor is still useful in some minefields. So the robot manufacturer wants your group to support two versions of the robot software, one for each of the two sensor types.

Describe the techniques that you would employ to manage this change to the software source code. You should place particular emphasis on the manner in which the source code repository assists this task.

[4 marks]

(b) During unit testing of the code for the new sensor a bug is found that you realise is also likely to be in the code used in the older sensor. How would you handle this problem?

[2 marks]

(c) In the long term your company will be responsible for maintenance of the robot code. Describe the manner in which a bug discovered by a user of the robot system is handled. You should address the following in your answer:

- How software with the bug fixed is created.
- How you ensure that the bug does not reappear in later releases of the software.
- How you would handle a situation where the bug actually had reappeared in a later release.

[6 marks]

[Total for Question 2: 12 marks]

Task Management

Question 3

If a spiral model has been chosen (as in Question 1) we need to create a project time line that reflects this chosen process. It has been negotiated with the client that the project may take two years. This will include all phases of the project from initial requirements gathering through testing, certification with approriate regulatory authorities, and final delivery of a system ready to be used.

(a) Draw a timeline for the project using the spiral model.

Your timeline should clearly identify the actions that occur through time and wherever possible describe the actions in a manner specifically relevant to the robot project, and not just as generic actions.

You should take care to clearly show how the spiral model has been used to develop the timeline, and how the specific attributes of the sprial model guide the timeline.

[8 marks]

(b) If the new sensor requirement occurs one year after the project starts, draw a modified version of the lineline that shows how the new requirement is managed, and indicate those aspects of the spiral model that aid in managing this change.

[4 marks]

(c) This robot project will involve safety critical and dangerous components. As such the regulatory authorities will require that many safety and quality standards are met. Draw a timeline showing how the need to address standards is addressed in the project.

[4 marks]

[Total for Question 3: 16 marks]

Risks

Question 4

The robot system requires a license from the main safety authority before it can be sold or used. In order to be given such a license the safety authority take a robot and test it themselves. These tests take two weeks. Unfortunately, after running tests on the robot one of the software systems crashes. The safety authority decides the robot is not safe and refuse to grant an operating license. You will need to fix the fault and resubmit the robot for testing. This will clearly result in a serious delay.

(a) Write an appropriate entry, one that might appear in the SPMP, for this risk. The entry should cover the following:

- Risk description.
- Risk likelihood.
- Risk severity. (Justify you answer.)
- Actions in place to minimise likelihood of risk.
- Actions in place to minimise severity of risk.
- Actions to be taken if risk occurs.

[8 marks]

(g) Describe the changes you would expect to make to the project schedule in order to take account of this risk analysis.

[4 marks]

(h) Based upon your experience in the robot project in this subject suggest two problems that might occur in implementing the above risk management plan.

[4 marks]

[Total for Question 4: 16 marks]

Hazard Analysis

Question 5

The change to the robot's sensing component introduces new risks, especially to humans working near the robots. Indeed tests have shown that the radiation emitted by the sensing device can be dangerous to humans, particularly those in close proximity to the robot. Prolonged exposure to the radiation can cause severe injuries to humans and can be fatal in the extreme. With this in mind, you will conduct a hazard analysis, focussing on the changes to the system to identify new hazards, and to assess the risk associated with these hazards.

(a) Define a system level hazard associated with the change of sensing device that may lead to the accident described above. Define a corresponding safety requirement that mitigates against the hazard.

[2 marks]

(b) Give an accident sequence showing the sequence of events leading from the system hazard (the initiating event) through to the accident. Show all external coeffectors (intermediate events) that need to occur for the hazard to lead to the accident.

[4 marks]

(c) Based on the information from the accident sequence in (b), complete a risk assessment of the system hazard. Assign a severity and frequency to the accident (use either **high**, **medium** or **low** for severity and frequency). Briefly justify your answer.

Then based on the ALARP risk assessment system and using the classification matrix shown in Table 1, classify the risk associated with the hazard.

	SEVERITY		
LIKELIHOOD	high	medium	low
high	Intolerable	Intolerable	ALARP
medium	Intolerable	ALARP	ALARP
low	ALARP	ALARP	Acceptable

Table 1: Risk classification matrix

[4 marks]

(d) Develop a fault tree that shows the decomposition of the system hazard from (a) into component level hazards. The fault tree does not have to be complete, but it should consist of at least three levels (i.e. there should be at least one intermediate level between system and component hazards), and should identify at least three component hazards.

[10 marks]

[Total for Question 5: 20 marks]

Please go on to the next page...

Requirements and Testing

Question 6

With the addition of a dangerous radiation source to the robot the safety authority requires that a warning light is placed on the robot. The light must flash whenever the radiation source door is open, and acts to warn operators of the danger of radiation. The robot designer decides to turn the light on and off under program control, and asks the software team to add approriate functionality to the robot software design.

(a) Using the proforma, below, write *two* requirements that would be crucial in the implementation of the new warning light control software. These requirements should be additional to those that would exist in the original (non-radioactive) robot specification.

- Title
- Summary
- Rationale
- Specification
- Acceptance criteria
- Source

[12 marks]

You are now required to develop acceptance tests for the warning light.

(b) Describe two tests of the warning light:

- One using *black box* techniques,
- One using *white* or *glass box* techniques.

If you need to assume anything about the nature of the implementation of the warning light, you should briefly state those assumptions.

[12 marks]

(c) Describe a test that can be used to validate the *reliability* of the warning light.

[5 marks]

(d) In developing a test plan you identify the following steps:

- Analysis,
- Create test cases,
- Define results of tests,
- Execute tests,
- Check results.

However tests never go smoothly. Describe the process that your test regime would use to manage the test process with particular emphasis on how you will handle tests that fail. Use a flow diagram to illustrate your answer.

[5 marks]

Please go on to the next page...

(e) Your safety engineer is worried that the proposed warning light control design is a bad idea. After your study of the Therac-25 experience, suggest why these concerns might be valid. Suggest a better course.

- State what this flaw might be.
- Propose a safe alternative design.

[4 marks]

[Total for Question 6: 38 marks]

End of exam