THE UNIVERSITY OF MELBOURNE

SWEN90010: HIGH INTEGRITY SOFTWARE ENGINEERING

Assignment 2

DUE DATE: 11:59PM, SUNDAY 22 APRIL, 2015

1   Introduction

This handout is the assignment 2 sheet. The assignment is worth 10% of your total mark.

The aim of this assignment is for students to apply safety engineering methods to a simplified safety-critical system. We will use the same system as in assignment 1: the ICD system.

You will work *in pairs* for the safety analysis part of this assignment. Safety analysis is most effectively done in groups, as the ideas presented by one individual trigger ideas in others. This is especially the case for exploratory hazard analysis.

As part of the assignment, you will be asked to apply the HAZOP method to the ICD system in order to identify a list of potential hazards, to propose some additional requirements for the ICD system in response to the identified hazards, and to briefly critique your submission to assignment 1 with respect to these requirements.

2   The system

The user requirements for the ICD system are outlined in the assignment 1 sheet. These requirements are *user* requirements, not system requirements. As such, they are incomplete and do not consider any safety issues. The safety analysis in this assignment should be performed on the user requirements and the system architecture presented in Figure 2 of assignment 1.

3   Your tasks

The tasks for the assignment are listed below:

1. Perform a preliminary hazard analysis on the entire ICD system using the Hazard and Operability Study (HAZOP) method, and document your findings in a hazard log.

   You should consider the safety of the entire system, including the hardware (heart rate monitor, impulse generator, connections between the heart and these devices, etc.), the software (the ICD component, user authorisation, and the `ClosedLoop` controller), and both the on and off modes. You should also consider the safety of any roles that are likely to interact with the system; that is, patients, cardiologists, and clinical assistants that can read and change settings.

   NOTE: You should consider this analysis as being performed on a real ICD system, not a simulator. That is, consider a real heart, not a software simulation of a heart, as used in assignment 1.

A template hazard log (`hazard-log-template.xls`) is available on the LMS. Your analysis should apply all guidewords on all design items, however, your hazard log should only document those that are thought to lead to a possible (and realistic) hazard.

2. Using the results from your HAZOP, update the requirements from assignment 1 to mitigate all hazards that you think need to be addressed. That is, provide new requirements that help to reduce the probability and/or impact of a hazardous event. List your requirements using the same headings as in the user requirements in assignment 1.

   Add a brief note to each new requirement identifying what hazard(s) the new requirements address.

   NOTE: Only list *new* requirements; there is no need to include the user requirements from assignment 1.

3. **Each student should do this for their own assignment 1 submission**: For your submission to assignment 1, identify which of the new requirements are NOT implemented in your submission to assignment 1.

   Submit *both* analyses in separate sections as part of the report.

   NOTE: You will *not* lose marks for not implementing safety-related behaviour in your assignment 1 solution. The purpose of this task is as an exercise in critiquing a system implementation against some safety behaviour, and will also feed into assignment 3.

4   Criteria

Criterion	Description	Marks
HAZOP application	The HAZOP has been applied systematically, correctly, and completely. All deviations from intent have been considered.	2 marks
Hazards	All major hazards have been identified and addressed.	3 marks
Causes, consequences, & risk classes	The identified causes, consequences and risk classes are all correct with respect to the hazard and the deviated behaviour.	2 marks
Requirements	The updated requirements mitigate all necessary hazards, and are correct, consistent, and complete.	2 marks
Analysis	The analysis of the assignment 1 submission is correct.	1 mark
Total		10 marks

5   Academic Misconduct

The University misconduct policy applies to this assignment. Students are encouraged to discuss the assignment topic, but all submitted work must represent the individual's understanding of the topic.

The subject staff take plagiarism very seriously. In the past, we have successfully prosecuted several students that have breached the university policy. Often this results in receiving 0 marks

for the assessment, and in some cases, has resulted in failure of the subject.

6   Submission

Submit the assignment using the Turnitin link on the subject LMS. Go to the SWEN90010 LMS page, select *Assignments* from the subject menu, and then select *View/Complete* from the *Assignment 2 submission* item. Following the instructions, upload a **PDF** file containing your solution.

Only *one* student from the pair should submit the solution, and the submission should clearly identify both authors.

Late submissions   Late submissions will attract a penalty of 1 mark for every day that they are late. If you have a reason that you require an extension, email Tim *well before the due date* to discuss this.

Please note that having assignments due around the same date for other subjects is not sufficient grounds to grant an extension. It is the responsibility of individual students to ensure that, if they have a cluster of assignments due at the same time, they start some of them early to avoid a bottleneck around the due date. The content required for this assignment was presented before the assignment was released, so an early start is possible (and encouraged).