Formal Approaches to Software Engineering

SET10112/SET10412

Coursework – Space!

Assessment Details: Follow after this cover sheet.

Learning Outcomes Covered:	LO1: Produce a design and specification for an application using a formal approach LO2: Plan and develop an application which conforms to the obligations defined in a formal design and specification LO4: Evaluate formal methods in comparison with other software development processes and development methodologies LO5: Integrate a formal approach into an existing software development process

Assessment Type:	Report
Overall module assessment	75% coursework, 25% test.
For this assessment:	75%
Assessment Limits:	10 pages
Submission Date:	Tuesday, 09 May 2023
Submission Time:	**1500**
Submission Method:	Via Moodle
Turnitin:	Single Attempt
Module leader:	**Peter Chapman**
Tutor with Direct Responsibility:	Peter Chapman

Standard Instructions to Students:

1. By submitting the report via Moodle (or otherwise), you are confirming that it is your own work.
    - Please note regulation Section B5.3.b regards component weighting.
2. You are advised to keep a copy of your assessment solutions.
3. Late submissions will be penalised following the University guidelines as follows:
    - **Up to 5 working days late the mark will be capped at 40%.**
    - **After 5 working days a mark of 0%.**

4. Extensions to the submission date may only be given by the Module Leader for exceptional circumstances. – by submitting appropriate request form - Extenuating circumstances (napier.ac.uk)

5. The University rules on Academic Integrity will apply to all submissions.

6. Feedback on submissions will normally be provided within three working weeks from the submission date.

Coursework - Space!

Peter Chapman & Andreas Steyven

SET10112/SET10412

Abstract. In this coursework, you will have to design a control system for a space station. You will then create Ada-SPARK specifications and bodies for your system, along with a justifications using a graphical representation of the safety case in Goal Structuring Notation. A report, containing your specification definitions and descriptions, must be produced that is no longer than 10-pages in the LNCS style template. These templates are made availabe for you on Moodle.

1 Overview

Outer space is hazardous to human health. Lots of effort, on the part of various space agencies, goes towards ensuring that humans can go to, and return from, space safely. In this coursework, you are going to design the control system for an orbiting space station. You need only use what you have learnt in this module.

You will develop a control system for a 3-person modular space station. This system will prevent certain actions when they are unsafe. For example, airlock doors should not be open at the same time; the space station should maintain orbit height (within a narrow range); and so on. In particular:

- It is not the case that both airlock doors are open at the same time.
- The space station should come neither too close to, nor get too far away from, Earth.
- New space station modules are added on a first-in-last-out basis.
- When a space walk is attempted by a crew member, the other two crew members must be monitoring from opposite ends of the station.

1.1 SPARK levels

Recall from the lectures and materials online that there are grades of SPARK implementation:

- **Stone level** - valid SPARK
- **Bronze level** - correct initialisation, data and information flow
- **Silver level** - absence of run-time errors
- **Gold level** - proof of key integrity properties
- **Platinum level** - full functional proof of requirements

Each level subsumes the level below it, in that, for example, one cannot achieve silver without achieving bronze. Normally, these levels are applicable at the program level, but you will be assessed at the subprogram level. For example, your "air lock" system may achieve bronze, but your altitude system may achieve gold.

2 Report

Your report *must* use Springer's Lecture Notes in Computer Science (LNCS) template. Templates for LaTeX and Word are provided on the Moodle page for the module. The page limit is **10 pages**. Deviation from either the template or the page limit will result in a penalty on your coursework. (For reference, this document is in LNCS format.) Your report should include the following sections:

1. *Introduction* - a high-level overview of the problem you have solved, including brief descriptions of your solution and any extensions to the problem. This section, if read alone, should give the reader a clear, if brief, picture of what you have done.
2. *Controller Structure* - a high-level view of your space-station control system. You should include a description of *why* your system is structured in that way (i.e. explain any global variables, types, etc. in your system.)
3. *Descriptions of procedures and functions* - a more detailed look at the individual components, including descriptions of parameters, constants, post-conditions, and pre-conditions.
4. *Proof of Consistency* - you should include descriptions of which parts of your system are formally verified, justifiying your decisions (with reference to the demonstration video). For anything that is particularly key to your specification (and in any case for at least one procedure or function) you should demonstrate *by hand* how the proof obligations are satisfied.
5. *Safety Plan for the above* - Create a safety plan for the system you developed above, which needs to include the following sub-set of what we would expect to find in a full case: a hazard and risk analysis; list any mitigations that you propose; and a failure analysis. Limit the hazard and risk analysis to any two of the four requirements given in the Overview section. There is no need to include mitigations in the overall system requirements and consider them in any of the sections above. Limit the Failure Analysis to the three most severe risks.
6. *Safety Case and Safety Manual* - create a safety case using the Goal Structuring Notation to document explicitly the elements and structure of your argument as well as the argument's relationship to the evidence. Use the evidence created in the sections above. Document any relevant information of your proposed system design in a Safety Manual.
7. *Conclusion* - this section should detail any shortcomings of your specification, including aspects you would like to have included but did not.

3 Submission

The assessment will be consist of two parts:

– the **pdf** version of your report. **Do not submit Word or TeX files**. The name of the pdf should be your student number. You **will not** submit your code to Moodle.

– the **video demo** of your working code, submitted with your report. The demo will allow the marker to determine which aspects have been implemented, and which SPARK level you have achieved on each aspect. Whilst the demo carries no marks, failure to complete it satisfactorily will result in a coursework mark of 0. The type of video file is limited to those which are natively supported by browsers. (i.e. .mov .mp4 .m4v .ogv .webm)

4 Mark Scheme

The coursework will be marked out of 100.

> **Any deviation from the template or page limit will limit your mark to** 65

The breakdown of marks will be as follows:

– *Solution Structure* **15 marks** - does your program demonstrate good software engineering design principles, such as re-usability?
– *Solution Coverage* **20 marks** - does your program fully address the space-station scenario? Are your subprograms appropriate, with appropriate variables, visibility etc.? Do the procedures and functions make sense in the context?
– *Solution Correctness* **20 marks** - which SPARK level have you achieved? Are any pre-conditions too strong, and if so, why? It is this section which the **demo** will primarily assess. The SPARK levels do not map on to a linear scale of marks.
– *Safety Plan and Documentation* **25 marks** - Correct and proper application of appropriate tools and methods to Hazard, Risk and Failure analysis. Coverage of all identified risks for hazard and risk analysis and coverage of residual risk to the required extend for the failure analysis. Scope and sense of proposed mitigations and are they linked to the hazards they are intended to mitigate. Safety Manual covering appropriate details with respect to your proposed solution.
– *Quality of the diagram* **10 marks** - GSN diagram quality: correct use of notation and completeness of the diagram with respect to your proposed solution. The diagram produced with a suitable software package and a readable screenshot included.
– *Quality of written report* **10 marks** - adherence to the template, quality of written English, quality of any displayed formulae, document flow (i.e. does your work read like several sections which have little in common, or like a coherent narrative?)