Rigorous Methods for Software Engineering (**F21RS**):

(2023-2024)

Specification of Coursework 2

A SPIN Design Modelling and Verification Exercise

THIS IS AN INDIVIDUAL PROJECT

While discussion with fellow students as to the general nature of this project is acceptable, it is critically important that the solution you adopt as well as the associated code and report are completely your own work. The re-use of other peoples code (other than the code provided as part of this coursework) is not permitted and if identified will be treated as a disciplinary matter. Information on plagiarism can be found via

`https://www.hw.ac.uk/students/studies/examinations/plagiarism.htm`

Contents

1 Introduction

This coursework focuses on ensuring the safety of vehicles at a road junction. Background on the problem is given in section **??**. Your task is to design a distributed traffic light system that will make the network safe. As well as modelling your design in Promela you are required to formally verify safety and liveness properties of your design. The modelling and verification tasks are described in §3 and §4 respectively. Finally, in §5 the deliverables that are expected of you are described. Note that this coursework counts for 20% of your overall course mark.

2 System-Level Description

Road traffic signals are used to reduce the risk of accidents at road junctions. Figure 1 shows a junction where two roads cross. The role of the traffic signals is to prevent vehicles traveling North-South colliding with vehicles traveling West-East. Specifically, **Picture A** shows the situation where vehicles are allowed to travel West-East while the North-South traffic are signalled to stop. Conversely, **Picture B** shows the situation where vehicles are allowed to travel North-South while the West-East traffic is signalled to stop. Critically, **Picture C** shows the situation that the signalling must be designed to prevent, i.e. vehicles being signalled to proceed North-South and West-East at the same time.

3 Modelling and Verification Tasks

Your task is to model in Promela the traffic control signalling system (TCSS) outlined above. Specifically, you are required to undertake the following modelling and verification tasks:

T1: Develop a model of the TCSS that involves 5 processes (i.e. protypes) – 4 traffic light processes and 1 central control process. The central control process should communicate to the 4 traffic light processes, i.e. the control process should instruct each traffic light what aspect (i.e. danger or proceed) it should be displayed. Note that a traffic light process should not communicate with any other traffic light process. Your model should satisfy the properties defined in tasks [T2-T4].

T2: Formulate an invariant as a monitor process that expresses the safety constraint: *North-South and West-East traffic should never be signalled to proceed at the same time.*

T3: Formulate an invariant as a LTL property that expresses the safety constraint: *North-South and West-East traffic should never be signalled to proceed at the same time.*

T4: Formulate a LTL response property that states that it is always true that whenever a traffic light displays a proceed aspect then eventually it will display a danger aspect.

4 Deliverables

Based upon the above tasks you are required to produce the following deliverables:

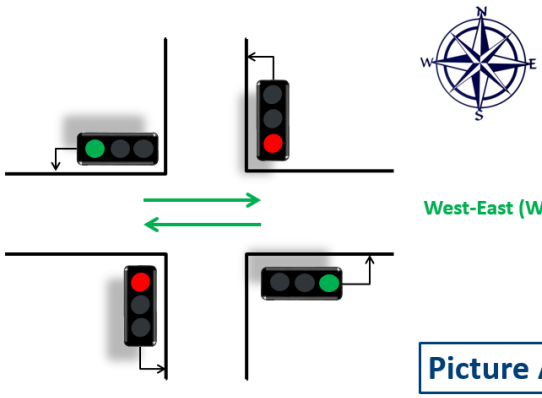
D1: A statement of any assumptions you have made about the requirements, and how they have impacted on your modelling decisions. *[2-marks]*

D2: State machine description of your central control process. *[4-marks]*

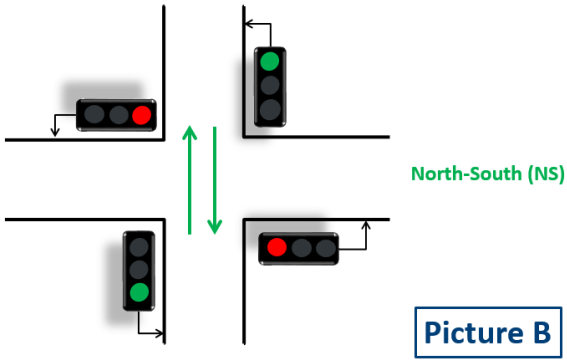
D3: Your Promela source code. Ensure that your code well formatted and readable. *[12-marks]*

D4: Screen shots of **iSpin** showing the successful verification runs. Clearly state which verification parameters have be set for each verification *[5-marks]*

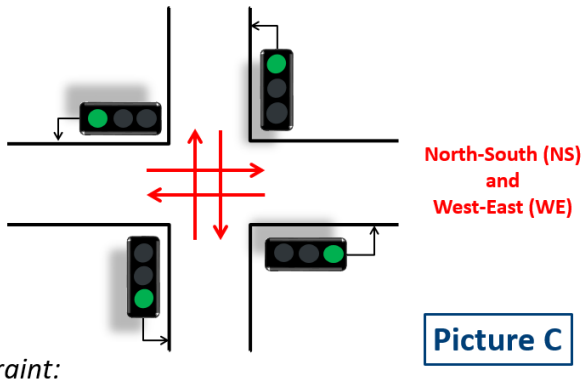
D5: With reference to an example Promela program, describe the notion of a **race condition**. Your answer should explain why the presence of a race condition can have an negative impact on a software system, particularly within the context of system critical systems. In addition, describe a mechanism that would eliminate the race



- West-East bound traffic are signalled to proceed
- North-South bound traffic are signalled to stop



- West and East bound traffic are signalled to stop
- North and South bound traffic are signalled to proceed



Safety Constraint:

North-South and West-East traffic should never be signalled to proceed at the same time.

Figure 1: Traffic Control Signals at a Road Junction

condition from your given Promela program. You should aim for no more than 500 words (excluding code). *[5-marks]*

There will be 2-marks allocated according to the clarity, quality and accessibility of your report. Note that this coursework counts for 20% of your overall course mark.
[30 marks in total]

5 Submission Requirements and Deadline

- The deadline for this coursework is **Monday 28 November 2022 (week 12): 3.30pm for Edinburgh registered students and 11.59pm for Dubai registered students.** As noted above, as well as your report, you should also provide a standalone copy of your Promela source code. You should use the following source code file naming convention: `<surname>-<username>-F21RS.pml`. For example, `smith-as42-F21RS.pml`.
- **Note that this is an individual project which means that your submission MUST be your own work.**
- **This coursework counts for 20% of the overall course mark.**
- **The University Policy on the Submission of Coursework can be found via the following link:**

`https://www.hw.ac.uk/services/docs/learning-teaching/policies/submissionofcoursework-policy.pdf`