Assignment Brief

Northumbria University NEWCASTLE

Programme	Computer Science
Module Code	KF6009
Module Title	Model Based Design and Verification
Distributed on	week begining 11 November
Submission Time and Date	To be submitted by 23:59 GMT on 17 January 2020
Word Limit	5000
Weighting	This coursework accounts for 100% of the total mark for this module
Submission of Assessment	**Electronic Management of Assessment (EMA):** Please note if your assignment is submitted electronically it will be submitted online via Turnitin by the given deadline. You will find a Turnitin link on the module's eLP site. It is your responsibility to ensure that your assignment arrives before the submission deadline stated above. See the University policy on late submission of work.

1 Instructions on Assignment

1.1 Scenario

1.1.1 Introduction

The University of Sans Serif is developing new energy generation systems. One critical component of many of these is a steam generator, the steam drives turbines for electricity generation. The heat is supplied by various experimental systems.

In order for safe operation a *boiler-management* system is required. You are required to produce a design for the software and to use appropriate methods and tools to show your design is satisfactory.

1.1.2 The System in Detail

A schematic diagram of the system is shown in figure 1

The physical *Plant* consists of a boiler and pumping system. Water is pumped into the boiler, where it is heated to produce steam. The steam is drawn off to drive a turbo-generator, before being condensed and returned to the feed tanks for the pumps.

The heating system is one of a number of novel systems, and is not under the control of the boiler management system.

It is unsafe to operate the boiler if the water level is not maintained between the specified minimum (W_1) and maximum (W_2) levels. The water level in the boiler (w) is monitored by a sensor. So it is required that $W_1 \leq w \leq W_2$ holds at all times. Similarly the rate of steam flowing from the boiler must not exceed the specified rate (S), the flow rate (s) is measured by a sensor. It is required that $s \leq S$ holds at all times.

The sensors are polled each sensor is expected to reply within 0.5 s. If no reply is received, the sensor is polled again, repeating at 0.5 s intervals until a reply is received. *If 5 polls are unanswered*, the system is deemed to be faulty and shut-down.

The pumping system (P) consists of two pumps (p_1 and p_2). Each supplies water at a constant rate. It is essential that only one pump is active at any time. Two pumps are used to provide a degree of fault-tolerance through redundancy. The status of the pumps can be monitored, and it assumed that even in a case of failure a pump can accurately report its status. It is also assumed that an inactive pump may be repaired and brought back into operation, a pump resumes operation in the OFF state.

The Controller is a digital system that is able to monitor the boiler plant using the sensors and control its operation by turning pumps on or off, or is capable of stopping operation. The controller is connected to an emergency stop button for manual shutdown.

Aside: The specification above is intentionally incomplete and may be vague and ambiguous. You will need to make additional assumptions to fill in missing details. For example, you may wish to make assumptions about the time taken to complete system actions that you include in your model. You may also want to model the environment (boiler-system) that the controller interacts with.
You should document your assumptions carefully in your report

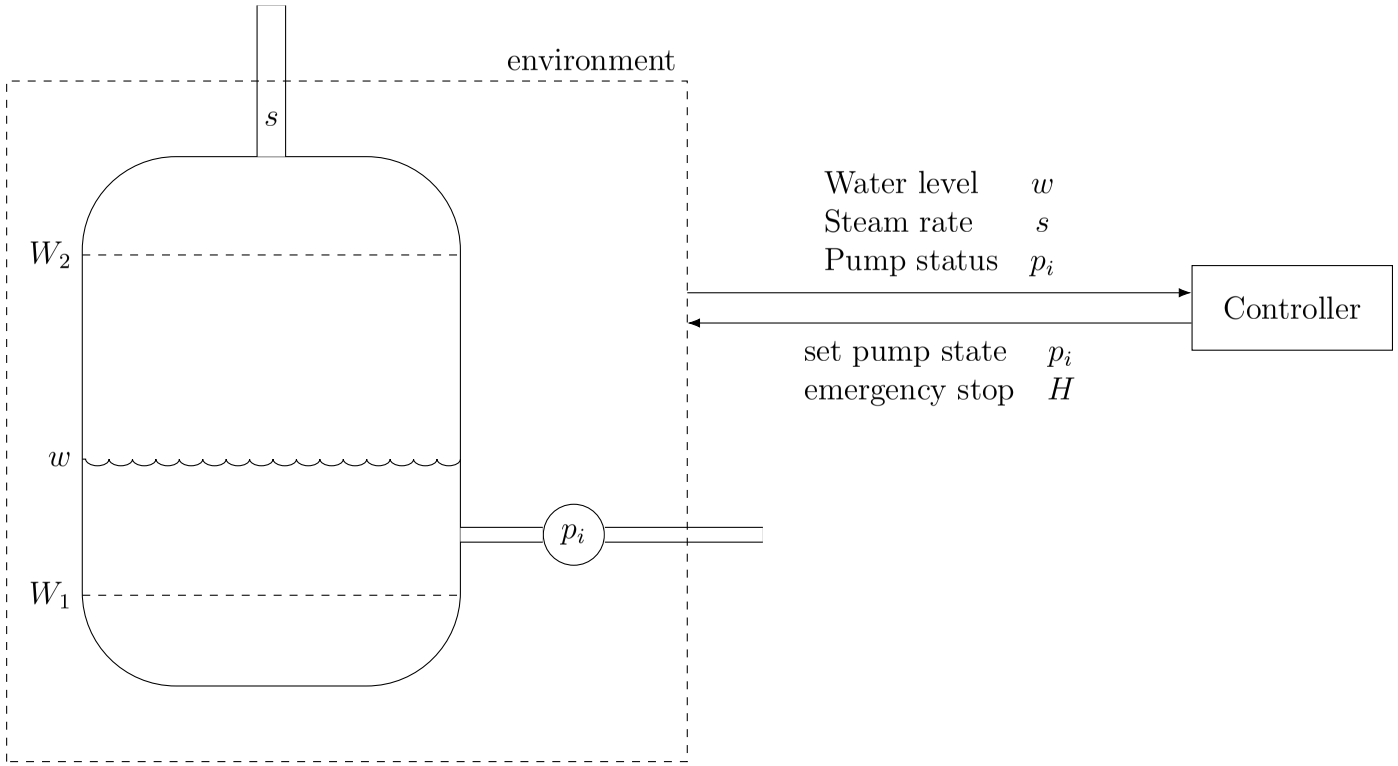

Figure 1: Schematic diagram for the steam generator

1.2 What you should do:–

1. *Model the system* using *either* the **TLA+/Pluscal** *or* the **Uppaal** modelling language. The system should exhibit *decomposition* into two or more sub-systems, which communicate using messages.

2. *Specify a set of properties* that the system should satisfy. Sate these formally and informally.

3. *Show the model satisfies these properties.* Show these hold for all operational cases (all modes of sensor operation).

4. What needs to be known/assumed about the behaviour of the *environment* of the *Open Model* of the controller .

5. Consider the role of formal methods in reasoning about aspects of the security of the system.

6. Compare and contrast the strengths and weaknesses of TLA+/Pluscal and Uppaal for modelling and reasoning about this kind of system.

7. Critically evaluate the economic case for the application of formal methods in the development of the system.

1.3 What you should hand in

You should submit (via blackboard)

1. A report (see 2.2), submit a PDF copy of your report. *70%* weight

2. A zip archive of your model and specifications containing *30%* weight

   TLA+ the model of you system `boiler-model.tla` and the supporting model, the directory `boiler-model.toolbox`

   Uppaal the model of your system, the files `boiler-model.xml` and `boiler-model.q`

   The models should be able to load into the versions of TLA+ or Uppaal as used in the module, and should include the properties verified.

2 Questions and marks

2.1 Specification and Model

Specification the set of properties that the system should satisfy. These include type and temporal invariants, reachability predicates, and other predicates. *10 marks*

Model The model of the boiler controller. This should show good decomposition into sub-systems, good communications and synchronisation as appropriate. You may make assumptions about the behaviour of external environment (heating and boiler dynamics) in order to produce a closed system model, that can be verified. Document the assumptions made about external systems. *20 marks*

2.2 Report

Your report should comprise numbered entries for each of the following:

1. Discussion of the specification. State your chosen specification properties both formally and an informal narrative. Justify your choice of properties and discuss the conclusions that can be drawn from the results of verifying them with a model-checker. *10 marks*

2. Discussion of the design of your model. In particular you should clearly address the *system decomposition* and *communication between components*. Consider alternative approaches that you could have taken, and justify the approach and assumptions you have made. *15 marks*

3. Discuss the *safety* and *security* of the boiler control system and the role of model-checking in in testing it. In Particular what are the critical safety factors that can be tested for by model checking. What are the limits of the safety case you can make with your model? What security risks are there and what role can model checking have in evaluating these? *20 marks*

4. Critical evaluation of the strengths and weaknesses of `TLA+/Pluscal` and `UPPAAL` for the design and verification of computer systems. Give an example of a system for which each is suited for. *15 marks*

5. A Critical evaluation of the use of formal methods in Software Engineering for the specification and design of systems. Focus in particular on the *economic justification* for the use of formal methods. Your answer is expected to show evidence of wider reading. *10 marks*

2.3 Referencing style

Harvard style referencing to be used.

A Further information

A.1 Learning outcomes assessed in the assessment

This assignment assesses all of the learning outcomes;

- Discuss the theoretical principles of various formal methods for the specification and design of computer software, and the algorithms and data-structures used in their supporting tools.
- Construct and evaluate formal models of a variety of computer systems.
- Compose formal specifications of system properties and analyse system-models with respect to these specifications.
- Identify, apply, and evaluate appropriate software tools to support the construction and analysis of formal system specifications and models.
- Evaluate the advantages and disadvantages of the application of various formal methods in the development of computer software, and justify their use where appropriate, having regard to professional, ethical, technical, and security issues.

A.2 Mapping to Programme Goals and Objectives

KU1. Demonstrate a systematic, critical understanding and detailed knowledge of computing facts, concepts, principles, theories, techniques and technologies

KU2. Demonstrate a detailed understanding of technical, professional, security, commercial and economic issues and risks surrounding the development, operation and maintenance of computing systems

KU3. Deploy knowledge and understanding of techniques and tools (some of which are at the forefront of the discipline) for the specification of requirements, analysis, design, implementation, testing and management of secure computing systems, thereby applying and critically evaluating a software engineering approach

KU4. Demonstrate a critical understanding of the professional, ethical, social and legal issues involved in the development and operation of computing systems

B Module Specific Assessment Criteria and Rubric

B.1 Specification and model

Specification *10 marks*

Looking for use of safety-properties $A\Box\varphi$ and $E\Box\varphi$, and use of liveliness properties $A\Diamond\varphi$, and $E\Diamond\varphi$. Captures safety requirements as stated in brief $A\Box(W_1 \leq w \wedge w \leq W_2)$, and $E\Box(s > S) \Rightarrow \mathit{Halt}$. There is a subtlety in the model that effects how explicit the first safety rule can be achieved. The students assumptions and design may require a weaker rule that still captures the intent.

9–10	Exceptional
8	Outstanding
7	Excellent: must capture explicitly the safety rules as stated in the brief
6	Good
5	Satisfactory: first safety rule can be relaxed if assumptions made in model exclude the exact version, safety rule given must capture this property as closely as possible,
4	Weak but satisfactory
0–3	Unsatisfactory: Poor or misapplied properties, does not capture major safety conditions

Model *20 marks*

Looking for level of decomposition, abstraction, and internal consistency throughout the model. Use of messages and synchronisation, and standard patterns for data transfer.

18–20	Exceptional:
16–17	Outstanding:
14–15	Excellent:
12–13	Good:
10–11	Satisfactory: minimum level where model must pass verification tests
8–9	Weak but satisfactory: model may not pass verification, the model may show the correct intention to capture the behaviour.
0–7	Unsatisfactory:

B.2 Report

Question 1 Design of specification. *10 marks*

Discussion on the selection and justification of the safety properties. Should show how the description in the brief translates into expressions of Temporal Logic. Additional properties may be specified along with their justification.

9–10	Exceptional:
8	Outstanding:
7	Excellent:
6	Good:
5	Satisfactory:
4	Weak but satisfactory:
0–3	Unsatisfactory:

Question 2 Design of model. *15 marks*

Discussion and justification of the model. What assumptions are made in modelling the boiler operation. How the model has been decomposed into their components and a discussion of the communicating requirements between components.

14–15	Exceptional:
12–13	Outstanding:
10–11	Excellent:
9	Good:
7–8	Satisfactory:
6	Weak but satisfactory:
0–5	Unsatisfactory:

Question 3 *20 marks*

18–20	Exceptional: Thorough discussion of safety and security of the boiler controller and the implications of failure. Clear and demonstrated understanding of the limitations of the model and factors outside the scope of the model, or outside the control of the system.
16–17	Outstanding:
14–15	Excellent:
12–13	Good: Shows understanding of the safety and security considerations, may not show much discussion beyond the system modelled.
10–11	Satisfactory:
8–9	Weak but satisfactory: Limited discussion of security or safety
0–7	Unsatisfactory:

Question 4 *15 marks*

12-15	Excellent evaluation of both TLA+ and Uppaal, well reasoned with good evidence (referenced if possible). Well argued role for each based on differences. Well thought out examples that fit the identified role for each system.
8-11	Good discussion and evaluation. Example uses not well justified based on arguments given.
6–7	Satisafactory evaluation of tools, missing example uses of each system.
1-5	Unsatisfactory evaluation of tools, no examples given.

Question 5 *10 marks*

8–10	Excellent, well referenced discussion of the case for using formal methods
6–7	Good case for use of formal-methods, references show some evidence of wider reading.
4–5	Satisfactory discussion of the case for model checking. References do not go beyond those presented in the module.
1–3	Unsatisfactory case for the use of formal methods

C Assessment Regulations

You are advised to read the guidance for students regarding assessment policies. They are available online here.

C.1 Late submission of work

Where coursework is submitted without approval, after the published hand-in deadline, the following penalties will apply.

For coursework submitted up to 1 working day (24 hours) after the published hand-in deadline without approval, **10% of the total marks available for the assessment (i.e.100%) shall be deducted** from the assessment mark.

Coursework submitted more than 1 working day (24 hours) after the published hand-in deadline without approval will be regarded as not having been completed. **A mark of zero will be awarded for the assessment and the module will be failed**, irrespective of the overall module mark.

The group work policy can be found here

These provisions apply to all assessments, including those assessed on a Pass/Fail basis.

The full policy can be found here.

C.2 Word limits and penalties

If the assignment is within +10% of the stated word limit no penalty will apply.

The word count is to be declared on the front page of your assignment and the assignment cover sheet. The word count does not include:

- figures and diagrams

Please note, in text citations [e.g. (Smith, 2011)] and direct secondary quotations [e.g. "dib-dab nonsense analysis" (Smith, 2011 p.123)] are INCLUDED in the word count.

Students must retain an electronic copy of this assignment (including ALL appendices) and it must be made available within 24hours of them requesting it be submitted.

The full Word Limit Policy is available here.

D Academic Misconduct

The Assessment Regulations for Taught Awards (ARTA) contain the **Regulations and procedures applying to cheating, plagiarism and other forms of academic misconduct**.

The full policy is available here

You are reminded that plagiarism, collusion and other forms of academic misconduct as referred to in the Academic Misconduct procedure of the assessment regulations are taken very seriously. Assignments in which evidence of plagiarism or other forms of academic misconduct is found may receive a mark of zero.