KF6009
Model-based design and verification
Course Work 2018-19

Module tutor: David Kendall

1 Assessment submission and feedback

Date of hand out to students:
16 November 2018

Mechanism to be used to disseminate to students:
eLP

Date and Time of Submission by Student:
23.59 on 17 January 2019

Mechanism for Submission of Work by Student:
The items should be submitted via eLP using the links as follows:

- Report: `Assessment->Report`.
- ZIP archive: `Assessment->ZIP archive`.

Date by which Work, Feedback and Marks will be returned to Students:
14 February 2019

Mechanism(s) for return of assignment work, feedback and marks to students:
email with meeting by appointment on request.

2 Assignment brief

2.1 Scenario

Introduction

The University of San Serif (USS) is about to spend a large research grant, acquired under a Sustainable Energy programme, on the development of a steam-driven electricity generator. In order to ensure the safety of staff and students, they require a *Steam Boiler Management System* to be implemented. You are required to produce a design for this software and to use appropriate methods and tools to develop confidence that your design is satisfactory.

The System in Detail

A schematic diagram of the system is shown in figure 1.

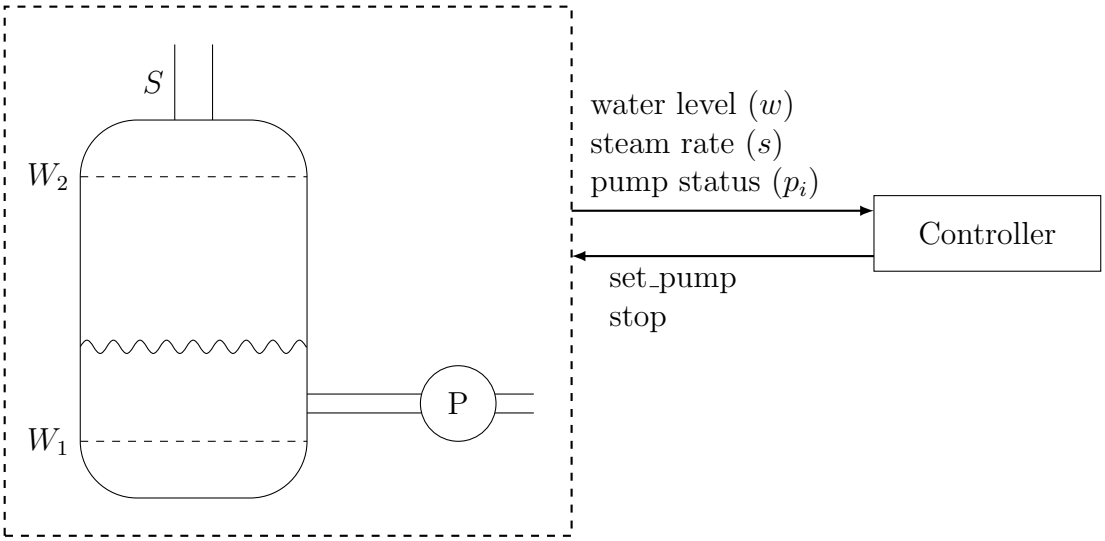

Figure 1: Steam boiler system

The physical plant consists of a steam boiler and a pumping system. Water is allowed into the boiler using the pumping system, where it is heated and evaporates to produce steam. The steam escapes from the top of the boiler and is used to power a generator. The heating system is novel and its design and operation remain a closely guarded secret. It is assumed that the

amount of heat, and so the amount of steam, is variable. The heater is not under the control of the system to be developed.

It is considered unsafe to operate the boiler if the water level is not maintained between specified minimum (W_1) and maximum (W_2) levels. The current water level (w) can be monitored using a sensor. So, we require $W_1 \leq w \leq W_2$ at all times. Similarly, the rate of flow of steam from the boiler must not exceed some specified maximum rate (S). The current steam rate (s) can be monitored using a sensor and we require $s \leq S$ at all times.

The water-level and steam-flow sensors are polled and each is expected to reply with its reading within 0.5 second. If no reply is received, another poll is issued. Polling repeats at 0.5 second intervals until a reply is received. If 5 polls are unanswered, the system is deemed to be faulty and shuts 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 no more than one pump is active at any time. Two pumps are provided in order to maintain system operation in the event of a pump failure. The status of each pump can be monitored and it is assumed that even a failed pump is capable of accurately reporting its status. We assume that a pump may be repaired during system operation and will resume operation in the OFF state.

The controller is a digital system that is able to monitor the plant using its sensors and control it by turning pumps on or off, or by stopping it. It is assumed that the controller is connected to an emergency stop button (not shown in Figure 1) which can be pressed by the plant supervisor in order to stop the system manually.

Aside: This specification is intentionally incomplete and may be vague and ambiguous. You will need to make assumptions to fill in the missing details, e.g. you may wish to make assumptions about the time taken to complete the system actions that you include in your model. You should document your assumptions carefully in your report.

2.2 What you should do

1. Model the system using *either* the **TLA+/Pluscal** modelling language *or* the **UPPAAL** modelling language. Decompose the system into two or more processes which communicate using messages.

2. Specify a set of properties that the system should satisfy. State the properties both informally and formally.

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

4. Compare and contrast the strengths and weaknesses of `TLA+/Pluscal` and `UPPAAL` for modelling and reasoning about this kind of system.

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

2.3 What you should hand in

You should hand in

1. a report (PDF required).

2. a ZIP archive of your model and specifications

Details of the expected contents are given below.

Report

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

1. Discussion of the design of your model. In particular, you should address the system decomposition and communication between components. Consider alternative approaches that you could have taken to the design and justify the approach that you adopted finally. *(15 marks)*

2. Discussion of the specification. State your chosen specification properties both informally and formally. Briefly justify your choice of properties and discuss the conclusions that can be drawn from the results of attempting to verify them with a model-checker. *(10 marks)*

3. Discussion of the *security* of the boiler control system and the role of model-checking in testing it.

   Focus in particular on the vulnerability of the system to an attack in which an intruder fools the boiler controller into believing that a pump is working correctly when, in fact, it has failed.

   A protocol intended to counter this threat is shown below.

$$B \rightarrow P : \{N_B, B\}_{K_P}$$
$$P \rightarrow B : \{N_B, N_P\}_{K_B}$$
$$B \rightarrow P : \{N_P\}_{K_P}$$

   where B represents the boiler controller and P represents the pump sensor and the other symbols have their usual security protocol meanings. The intention is that B and P should authenticate themselves by exchanging *nonces* encrypted with an appropriate public key.

   Your discussion should

   (a) explain the reasoning of B and P in this authentication protocol and critically evaluate its strengths and weaknesses with respect to this system. *(10 marks)*

   (b) outline a formal approach to test the security of this protocol using a model-checker. *(10 marks)*

4. Critical evaluation of the strengths and weaknesses of `TLA+/Pluscal` and `UPPAAL` for the design and verification of computer systems. *(15 marks)*

5. Critical evaluation of the decision of the developers to apply formal methods to the specification and design of this system. Focus in particular on the *economic justification* for the application of formal methods in this case. Your answer is expected to show evidence of wider reading. *(10 marks)*.

Archive of design/verification documents

Your ZIP archive should contain your formal design model and specifications for **ONE** of the following:

- For **TLA+/Pluscal**, this should be the file `boiler-model.tla`, containing your complete `TLA+/Pluscal` model and specifications (it should

be possible to load your model into the version of the `TLA+ toolbox` available in the CIS labs, and to use this tool to check the model). You may also include any snapshots of verifications that you have performed.

- For **UPPAAL**, this should be `boiler-model.xml` and `boiler-model.q` (it should be possible to load your model into the version of the `UPPAAL` tool available in the CIS labs, and to use this tool to check your model).

(30 marks)

3 Further information

Learning Outcomes assessed in this assessment: This assignment assesses all module learning outcomes, as indicated below:

1. 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.
2. Construct and evaluate formal models of a variety of computer systems.
3. Compose formal specifications of system properties and analyse system models with respect to them.
4. Identify, apply and evaluate appropriate software tools to support the construction and analysis of formal system models and properties.
5. 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.

Assessment Criteria/Mark Scheme: The coursework consists of

1. a report (70%)
2. a ZIP archive of design documents and verification snapshots (30%)

More detailed marks allocation is provided in the assignment brief.

Referencing Style: Harvard

Expected size of the submission: Your report should be about 9 to 10 A4 pages in length, excluding appendices (assuming 10pt and normal margins). There is no fixed penalty for exceeding this limit but unnecessary verbosity, irrelevance and 'padding' make it difficult for the marker to identify relevant material and may lead to some loss of marks.

Assignment weighting: 100%

Academic Integrity Statement: You must adhere to the university regulations on academic conduct. Formal inquiry proceedings will be instigated if there is any suspicion of plagiarism or any other form of misconduct in your work. Refer to the University's Assessment Regulations for Northumbria Awards if you are unclear as to the meaning of these terms. The latest copy is available on the University website.