Faculty of Computing, Engineering & Media (CEM)
Coursework Brief 2023/24

Module name:	Rigorous Systems		
Module code:	CTEC3902		
Title of the Assessment:	Coursework		
This coursework item is: ***(delete as appropriate)***	Summative		
This summative coursework will be marked anonymously: ***(delete as appropriate)***	Yes		
The learning outcomes that are assessed by this coursework are: 1. Reason with a document written in a formal specification language 2. Use a formal notation to develop, analyse and critically review a (small-scale) system specification 3. Animate a specification using an appropriate practical tool and discuss the results			
This coursework is: ***(delete as appropriate)***	Individual		
If other or mixed ... explain here:			
This coursework constitutes 100 % **of the overall module mark.**			
Date Set: 20/02/2024			
Date & Time Due (the deadline):	**13/05/2024 at 12.00 noon**		
In accordance with the University Assessment and Feedback Policy, your marked coursework and feedback will be available to you on:			
You should normally receive feedback on your coursework **no later than 15 University working days after the formal hand-in date,** provided that you have met the submission deadline If for any reason this is not forthcoming by the due date your module leader will let you know why and when it can be expected. The Associate Professor Student Experience (CEMstudentexperience@dmu.ac.uk) should be informed of any issues relating to the return of marked coursework and feedback.			
When completed you are required to submit your coursework via: 1. Submit your work on the assignment link.			
Late submission of coursework policy: Late submissions will be processed in accordance with current University regulations. ***Please check the regulations carefully to determine what late submission period is allowed for your programme.***			

Academic Offences and Bad Academic Practices:

Please ensure you read the section entitled "Academic Offences and Bad Academic Practice" in the module handbook or the relevant sections in this link: BaseCamp Link: Overview: Assessment and Good Academic Practices

Tasks to be undertaken:

Exercise 1, 2, 3, 4 and 5

Deliverables to be submitted for assessment:

A zip file named <your P-number>.zip containing:

- Your developed Tempura specifications
- An electronic copy (pdf file) of your report (max 8 pages)

How the work will be marked:

See marking scheme for each exercise

Module leader/tutor name:	Vasileios Germanos
Contact details:	Email: Vasileios.germanos@dmu.ac.uk

Should you need any further information or advice please email cemadvicecentre@dmu.ac.uk

Section A

Theoretical Part

Exercise 1. (45 marks total)

Assessment Indicators:

- **Correctness**
- **Conciseness**

Give an English and pictorial description of the interval that corresponds to each of the following Interval Temporal Logic formulae.

a) $\neg P \ \wedge \ (fin\ P) \ \wedge \ skip^3$ **(6 marks)**

b) $skip^2 \wedge A = 2 \wedge (A\ gets\ -A)$ **(7 marks)**

c) $(skip \ \wedge \ fin(A = 0))\ ;\ (B = 1 \ \wedge \ skip)$ **(7 marks)**

d) $(P \ \wedge \ empty)\ ;\ skip\ ;\ skip^2$ **(8 marks)**

e) $A = 1 \ \wedge \ (A\ gets\ A \ + \ 2) \ \wedge \ halt(A = 7)$ **(8 marks)**

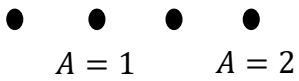
f) $len(4) \wedge (Q\ ;\ (skip \Rightarrow \bigcirc \neg \mathrm{Q})\ *)$ **(9 marks)**

Exercise 2. (15 marks total)
Assessment Indicators:

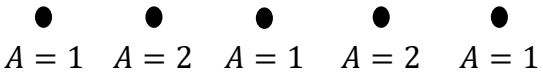
- **Correctness**
- **Elegance (clarity and conciseness)**

Give for each of the following intervals the corresponding Interval Temporal Logic formula.

a) **(6 marks)**



b) **(9 marks)**



Exercise 3. (10 marks total)
Assessment Indicators:

- **Correctness**

Give the formal semantics of the following Propositional Interval Temporal Logic formula.

$$(P \wedge skip); skip$$ **(10 marks)**

Section B

Practical Part

Exercise 4. (5 marks total)
Assessment Indicators:

- **Clear English**
- **Correctness**
- **Elegance (clarity and conciseness)**

Give an English description of the interval that corresponds to the following Tempura formula.

```
/* run */ define test1()={
  exists I: {halt(I=18) and I=-2 and
             chopstar(skip and I:=I+2) and
             always output(I)
  }
}.
```

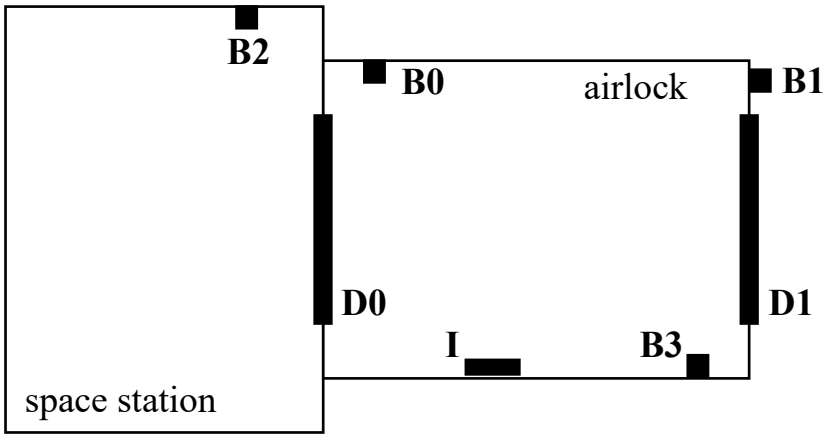
(5 marks)

Exercise 5. (25 marks total)
Assessment Indicators:

- **Ability to translate informal textual system description into formal description**
- **Ability to justify system design decisions**
- **Ability to analyse a formal system specification**

The following is a description of an airlock system HAL for entering and exiting a space station. HAL consists of sensors, actuators, and a control system. The following sensors and actuators are present:

- Doors D0 and D1.
- Buttons B0, B1, B2, and B3.
- Infrared sensor I.



The procedure for entering the space station is as follows.

- Press button B1, if it is safe then door D1 will open, and one can enter the airlock via door D1.
- Door D1 will close immediately when button B3 is pressed or after 5 seconds when sensor I detects that a person is present in the airlock.
- Press button B0, if it is safe then door D0 will open, and one can exit the airlock via door D0.
- Door D0 will close immediately when button B2 is pressed or after 10 seconds when I sensor detects that a person is not present in the airlock.

The procedure for exiting the space station is as follows.

- Press button B2, the door opens, and one can enter the airlock via door D0.
- Door D0 will close immediately when button B0 is pressed or after 7 seconds when sensor I detects a person present in the airlock.
- Press button B3, if it is safe then door D1 will open, and one can exit the airlock via door D1.
- Door D1 will close immediately when button B1 is pressed or after 6 seconds when sensor I detects that a person is not present in the airlock.

Be aware of the following constraints.

- The space station has 3 scientists. At any point in time at least 1 astronaut should be in the space station.
- There is only space for 1 person in the airlock.
- If both doors D0 and D1 are open, then air will escape from the space station, this needs to be always avoided.
- It is possible that more than one button is pressed at the same time, for example, an astronaut in the space station wanting to enter the airlock via door D0 and an astronaut wanting to enter the airlock via door D1. You need to resolve this type of conflict by giving priority to a particular button press. Note: an astronaut in the airlock cannot simultaneously press buttons B0 and B3.

The control system HAL determines whether doors Di are open or closed depending on the state of the infrared sensor and the buttons Bj.

a) Give a Tempura specification of HAL. A template solution is available on Blackboard. Use the following scenarios to illustrate your answer with output from your Tempura program:

    i) A short visit at space station: An astronaut enters the airlock via D1 using the above entering procedure for a short visit at the space station and comes back after 10 minutes and re-exits the space station via the airlock using the exiting procedure.

The following marking scheme will be used:

Environment: User/Sensors	
Tempura + 1 scenario English	: 06-08 : 00-02
Controller: HAL	
Tempura + 1 scenario English	: 06-08 : 00-02
Integration	
Tempura English	: 02-04 : 00-02

(20 marks)

b) The system that you have specified needs to satisfy certain safety conditions.
Give one example of a safety condition that your system should satisfy and formulate it in ITL/Tempura.

(5 marks)