Dana Dghaym
D.Dghaym@soton.ac.uk
Mohammad Divband Soorati
M.Divband-Soorati@soton.ac.uk
Thai Son Hoang
T.S.Hoang@soton.ac.uk
Luis-Daniel Ibanez Gonzalez
L.D.Ibanez-Gonzalez@soton.ac.uk

COMP1216. Software Modelling and Design (2022-23)

Coursework 2: Formal Modelling

Issue date:	15 March 2023
Submission deadline:	4pm, 12 May 2023

This coursework, to be undertaken in groups (the same group as Coursework 1), will contribute 15% towards the total for the unit. The assignment concerns the formal modelling of *an online auction system* from Coursework 1. It is intended to develop your skills in writing formal models using Event-B, to gain the experience of using the Rodin Platform and also re-enforce group working.

Please bear in mind the University Academic Integrity regulations: http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-regs.html

Due: **4pm Friday 12th May 2023** (*Electronic Hand in only*)

System Outline: An Online Auction Service

The outline of the system is as described in Coursework 1. For Coursework 2, you will model a similar system using Event-B according to the following requirements.

The set of requirements for an online auction service are as follows.

REQ 1	The online auction service allows users to submit items for auction and to bid for items that are being auctioned.

REQ 2	Users must be registered with the system in order to be able to submit items for auction and in order to place bids. Thus, a user can take both seller and bidder roles. The user's name, status, login id and password are recorded. User status records feedback given to the user by other users, and any penalty points the system has added.

REQ 3	The system should be able to manage multiple auctions.

REQ 4	A user (seller) with no more than two penalty points may submit an item for auction. The system creates a new auction and opens the auction to bids from other users (bidders). The system makes available the auction information the seller's feedback and penalties. An auction has only one seller. No user may be a bidder for an auction for which they are the seller.

REQ 5	When a seller submits an item for auction, they must provide a name for the item, start and end times for the auction and a reserve price for the item.

REQ 6	The seller may cancel their auction without penalty at any time until a bid no less than the reserve price is accepted. They may cancel after such a point and before auction closure but will then receive a penalty point. When an auction is cancelled all bidders are informed.

REQ 7	When a bidder makes a bid on an auction, the bid must be higher than the current highest bid for that auction.

REQ 8	When an auction duration has passed, that auction is closed.

REQ 9	For a defined period after auction cancellation or closure, bidders may provide feedback on the seller.

REQ 10	A closed auction succeeds if the highest bid is at least as high as the reserve price, otherwise it fails. When a closed auction succeeds, the winning (highest) bidder is informed.

REQ 11	A seller should be able to see the status of their auction at any stage after their auction has started.

Tasks (50 marks)

1. Create an Event-B model of the online auction system. We suggest you to use the system requirements, the class diagram, and state machine diagram from Coursework 1 to help with the development of the Event-B model. Make sure to

   • Identify appropriate Event-B sets and constants.

   • Identify appropriate Event-B variables and invariants. The invariants should clearly specify any constraints between state variables. You may lose marks by not having invariants to represent constraints on auctions.

   • Identify appropriate Event-B events. You should expect to have at least one event for each of the following use cases:

     – user registers with the system

     – user logs in

     – user logs out

     – create an auction,

     – start an auction

     – bid on an auction,

     – cancel an auction,

     – view the status of an auction,

     – close an auction,

     – gives feedback to the seller

     – view the history of all bids on an auction.

   • Where a use case has more than one outcome, you could have an event for each outcome. *It is not necessary to have an event for each step of a use case.*

2. Analyse your Event-B models using the Rodin tool including ProB animation.

3. You should consider using extension refinement to structure your Event-B model.

4. The current time may be represented by including a clock variable and an event that increases the clock.

Marking Scheme

There are a total of 50 marks for this coursework.

- 45 marks are for the accuracy of the Event-B model.

- 5 marks are for the quality of using extension refinement for structure your Event-B model.

Remarks

- Model developed without the Rodin platform (or cannot be imported into the Rodin platform) will receive a penalty of -10 marks.

- This means a paper-based solution without refinement will have a maximum of 35/50 marks.

Submission Instructions

Each group should submit the following documents

- a written report (PDF format, *one report per group*) clearly indicate your group number, member names and email IDs on the front page. Make sure your Event-B models are appropriately commented and are included in the report. A LaTeX template is provided for your convenience.

- An archive of your project from the Rodin tool containing your models.

Your report and Rodin archive should be submitted **electronically** using the automated hand-in facilities found on the ECS webpage at: https://handin.ecs.soton.ac.uk/.

If you feel there are any ambiguities in the requirements feel free to make your own interpretation, but make sure any interpretations you make are *clearly indicated in the report*. You should work *together as a group* to accomplish these tasks. It is the responsibility of each group to maintain contacts and arrange their own group meetings. Please inform us of any problems contacting your group members. You should avoid discussing your solutions with other groups.

NB: Group size is *five*. It may be necessary to run a few groups of four depending on the size of the class, or any students dropping out. In these cases the workload will be reduced accordingly.

- Group of 4:
  - You are *not required* to model the events corresponding to
    * user logs out
    * cancel an auction,

- Group of 3:
  - You are *not required* to model the events corresponding to
    * user logs out
    * cancel an auction,
    * view the status of an auction,
    * gives feedback to the seller