2021/2022

Master of Science MAE1
Practical course

Study case - Design a Control System for Aircraft Traffic on Airport

Reference documents

Designation	Source
Rodin platform	*http://www.event-b.org/install.html*
Event-B book	*http://www.event-b.org/abook.html*

© photo V. Joncheray

As far as the requirements are concerned, they are classified by category according to labels as follows:
FUN : for functional requirements,
OPE : for operational requirements,
CON: for constraint requirements,
SAF : for safety requirements

Statement of work

The system to be designed is an automatic airport controller that aims at controlling the traffic of aircraft on the taxiway and the runway. This system also manages the authorization to access the runway for aircraft willing to takeoff or to land.

At a time, each runway can only be used by one plane taking off or landing.

The authorizations are permanent for a normal functioning period and given through a clearance delivered by the studied controller. Every plane heading to the runway has an authorization for takeoff or landing. The authorization is granted according to the aircraft identifier.

The capacity of the airport in relation to the number of planes on ground (taxiway and runway) is limited to 20 planes max. The airport consists of at least one runway.

As per the operational scenario, the system interacts with a few external elements. These external elements are the air traffic controller (human operator), the pilot and the plane. Each concerned plane is supposed to possess an authorization. This authorization allows it, under the control of the system, to access to the runway for takeoff or landing.

In summary, we've got this requirements table hereunder:

The system is to control planes on ground: taxiway and runway	FUN-1
The system controls the access to the runway for takeoff or landing	FUN-2
The number of planes on ground is limited to 20 max	CON-1
The airport has at least one runway	CON-2
Aircraft are permanently assigned the authorization to access the runway	OPE-1
A plane which is on one runway must be allowed to be there	OPE-2
A runway is not occupied by more than one aircraft at a time	SAF-1
A runway that is not usable for operation should not be assigned a clearance	SAF-2

Questions

1. What is the system of interest? Define it.
2. Give the purpose, mission and objectives of this system

Abstract model

This model only focuses on the evolution of the number of aircraft on ground. It considers few requirements, mainly events related to take-off and landing from airport viewpoint.

3. Which requirements are considered?
4. Model the abstract system by describing CONTEXT and MACHINE components.
5. Check that invariant preservation and deadlock freedom PO rules are discharged.
6. Simulate your model with ProB/Animation.

NB: Explain why we cannot discharge DLF rule when removing axiom “nb_max=20” .

First refinement

The airport has at least one runway. Each runway can be used by only one plane, taking off or landing, at a time. We consider the number of runways and the number of planes on runways going to take-off or running after landing. We also consider the number of planes on the taxiway.

7. Which requirements are considered?

8. Model the refined system by describing MACHINE component. Identify the “glue invariant” between this model and the abstract one.
9. Check that invariant preservation and deadlock freedom PO rules are discharged.
10. Find out the variant for the relative deadlock freedom PO rule. Explain it.

Second refinement

We now consider the main objects that constitute the environment of the system of interest:

- PLANES is a finite set that contains all the planes that might operate in the airport.

11. Write down the extended context by taking into account the new information. 11. Create a new machine that refines the previous one. Complete this machine to take into account the sets instead of the numbers. We consider 3 subsets of PLANES :

- pl_rt: planes on runway for take-off,
- pl_rl: planes on runway for landing,
- pl_t: planes on taxiway.

The glue invariants relate the new variables to the previous ones thanks to the cardinality function. The number of elements of a set is its cardinality, noted card(E), where E is a set.
You also need to include invariants on disjunction of sub-sets.

TakeOff, Land, Leav_rwy, Enter_rwy are refined events, which take into account sets rather than numbers.

12. Complete the first refinement model and check all invariant preservation and deadlock freedom PO rules are discharged.

NB: Do we need to add a variant? Why?

Third refinement

We now consider the objects that constitute the airport:

- RUNWAYS is a set that contains all the runways of the airport (it does not contain the taxiway).

We finally want to take into account the authorizations and clearances. Any plane can have an authorization for more than one runway. The permanent authorization called *aut*, which associates the two sets, PLANES and RUNWAYS. The authorization corresponds to the possibility for a plane to go to a specific runway (for example, if a runway is too short for a plane to take off from it, it will not have an authorization for this runway and will therefore never be granted a clearance for it either).
The clearance or the accepted demand for access the runways is called clearance. This clearance associates one plane to one runway, and one runway may be occupied by only one aircraft at a time.

We also consider two subsets of RUNWAYS :

- rwy_occ: the runways currently used for take-off or landing,
- rwy_nok: the runways currently not available for operation because they are under construction, or occupied by a vehicle, for instance.

All the other runways are suitable to be granted a clearance.

13. Write down the extended context by taking into account the new information.
14. Refine the previous machine to take into account the clearance (as a new variable) in the events. (Right-click on your previous machine and select “Refine”)

As for the invariant section, it includes the definition of the variables and additional invariants at least: any planes on runway have got an authorization.

4 new events are described:

- Accept_clearance: parametric event enables to associate a plane with a runway (as one action); the other action adds this runway to rwy_occ;
- Add_rwy_nok: parametric event enables to add a not cleared runway to rwy_nok;
- Free_rwy_occ: parametric event enables to remove a pair of (plane, runway) from the clearance list (as one action); the other action removes this runway from rwy_occ;
- Free_rwy_nok: parametric event enables to remove a runway from rwy_nok.

15. Check all invariant preservation.
16. Write the deadlock freedom PO theorem accordingly and explain why it is not discharged.