University of Konstanz
Chair for Software and Systems Engineering
Prof. Dr. Stefan Leue, Raffael Senn

Verification of Software and Systems
Summer Term 2024
Issued: 02.05.2024

Project Part I

Deadline: Sunday **09.06.2024** 23:55

Notes:

- Solve the Project in **a group of 2 to 3 students**.
- Write your report using a computer document editor, preferentially **LaTeX**. Hand-written solutions are only accepted for graphs and diagrams. The report must be submitted as a **PDF** file.
- Submit all required files (models, properties, report, etc.) as a single **ZIP** file via **Ilias**.
- Name your submission `voss24_project1_SURNAMES.zip`, replacing `SURNAMES` with the surnames all group members in alphabetical order. Also include the full names of all group members in all submitted files including the report.

Overview

In this part of the project, you are supposed to gain some practical experience with the state-of-the-art model checker Spin. Spin is a explicit state space model checker. Our choice of the system to be modeled is an Air Traffic Control (ATC) for a small airport.

System

The owner of a small airport for private airplanes wants to avoid crashes on his airfield. Thus, they ask you to model the air traffic control system of their airport. The airport has one runway, one taxiways and four gates. The air traffic is controlled by the tower that can issue four commands:

1. Cleared to land
   When given clearance to land the tower has authorized you to land on the runway. The phrase "cleared to land" gives you immediate use of that runway.
2. Cleared for take off
   When given clearance to take off the tower has authorized you to enter the runway and take off. The phrase "cleared for take off" gives you immediate use of that runway.
3. Cleared to taxi
   When told by ground control or tower that you are cleared to taxi, the controller has given you instruction to taxi along a taxiway centerlines according to taxiway markings.
4. Go around
   Pilots receiving this transmission should abandon their approach to landing. They may then make another approach to land.

Modeling

Model the airport in Promela. All relevant states of the system should be somehow represented. Write down additional **sensible** assumptions that you mak about the system. Your model should fulfill the following property:

a) There is never a situation where airplanes are stuck at the airport (No “deadlock” in the model).

Organizational Issues

Requirements

Modeling. Use Promela to model the system.

Verification. Use Spin to verify your model against the property. In case a property is violated, try to fix the problem by modifying your model, and then verify the property again on the modified model. Repeat this procedure until your model satisfies the property. If necessary, give the number of airplanes on the airport and in the air, for which the property still holds.

Report. During the project, write down the issues that you faced. What assumptions did you make? How does your model abstract the reality? What are the modelling drawbacks of Promela? What mistakes did you make? What are the verification results of your model? In case you obtain property violations, provide counterexamples and rationals on why the error has happened.

Groups

Participants must form groups of two to three persons. Details are discussed during tutorial.

Submissions

The required submissions for each group include

a) the plain source code of the model that you implement and

b) the verification report in PDF format.

Submissions must be uploaded to ILIAS.

The submission deadline is **June 9, 2024** *if not announced otherwise.*