UNI FR
UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Foundations of Dependable Systems
Department of Informatics
University of Fribourg, Switzerland

# Verification of Cyber-physical Systems : Exercise Sheet 2

Deadline : Monday 9th October 2017, 11 :55 pm

## Exercise 1 : Message Channels

Write a *Promela* model which contains the following :

1. A synchronous channel.
2. A looping sender process that can write, at each loop, a 0 or a 1 (non-deterministically) in the channel.
3. A looping receiver process, that reads the channel and counts the number of 0's and 1's and stores the value in `counter0` and `counter1`, respectively.

Use *iSpin* to run a simulation of your model to see if it meets your expectation.

## Exercise 2 : Modelling the Wolf, Sheep and Cabbage problem

The aim of the exercise is to model a well-known logical problem with *Promela* language, and see if *Spin* can solve it for us. The problem is the following :

> A farmer wants to cross a river (starting from the left side) with a wolf, a sheep and a cabbage.
> However, he can take only one item at a time on his boat. Besides, he cannot leave the sheep alone with the cabbage, nor the wolf alone with the sheep on either shore.

Your task is to model this problem in *Promela*, so that *Spin* can find a correct path to the solution. The correct final situation should be represented by an assertion violation (because *Spin* will do its best to find such a violation, and the trail created will be the shortest path to the solution).

Hints :

- Use *mtypes* to specify the various actors (wolf, sheep and cabbage).
- An execution should non-deterministically choose between any possible action (i.e. choose between carrying a wolf, a sheep or a cabbage if there are present, or nothing).
- The final solution should be modelled as an assertion violation.
- Bad situations (e.g. wolf and sheep alone) should block the execution of the branch, so that *Spin* does not go any further in the simulation of that branch.
- You can use arrays to represent the items present on each shore.
- You can use channels to transfer the items from one shore to the other.

Run your model in *Spin*. It should detect an error (meaning a solution).

Switch to simulation mode to navigate through the correct solution and write it down (in English, not *Promela*).

Submit your commented `.pml` files on *Ilias* and also paste it in your PDF submission.