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

System Specification Using TLA$^+$
Winter Term 2023/24
Issued: 11.11.2023

Assignment 2

Deadline: Friday **17.11.2023** 23:55

Notes:

- Solve the assignment **on your own** — no groups allowed.
- Hand-written solutions will not be accepted, except for graphs and diagrams.
- If you hand in non-pdf files or multiple files, name your submission as `stla23_02_SURNAME.zip`, replacing `SURNAME` with your surname. Otherwise `stla23_02_SURNAME.pdf`. Also include your full name in the submitted PDF.
- Submit your solution via **Ilias**.

Exercise 2.1 A sending hour-clock — 16 Points

a) Write a specification of an hour-clock that sends the time to the environment over a channel `chan`. The specification should make use of the definitions from the `Channel` and `HourClock` modules by incorporating them with an `EXTENDS` statement. You find them attached to the assignment. Write two versions of the specification.

Version 1: The clock can tick any time.

Version 2: The clock cannot tick between sending a value on `chan` and the receipt of that value by the environment.

Include type invariants and use TLC to check them. **(8 points)**

b) Use TLC to check that the Version 1 specification implements the `Channel` specification with `Data` replaced by `1..12`. That is, every behavior allowed by your specification satisfies the specification `Spec` of module `Channel`, with `Data` replaced by the set `1..12`. Use TLC to check that Version 2 implements the specification `HourClockChannel` which is attached to the Assignment. **(4 points)**

c) Write specifications that hides the clock in the specifications of part **a)**. Explain informally why the resulting specification is equivalent to:

- The `Channel` specification with `Data` replaced by 1..12, for Version 1.
- The `HourClockChannel` specification, for Version 2.

(4 points)

Provide the output of TLC for all checks and hand in all relevant files (tla, cfg, pdf for the explanations...).

Exercise 2.2 A resettable hour-clock — 4 Points

Write a specification of a resettable hour-clock that communicates with a user over a channel `chan`. The user can send the clock an hour value. When the clock receives the value `v`, it resets `hr` to `v`. The clock can also advance hr as usual. The specification should make use of the definitions from the `Channel` and `HourClock` modules by incorporating them with an `EXTENDS` statement. You find them attached to the assignment. Hand in the tla file.

Total: 20 Points