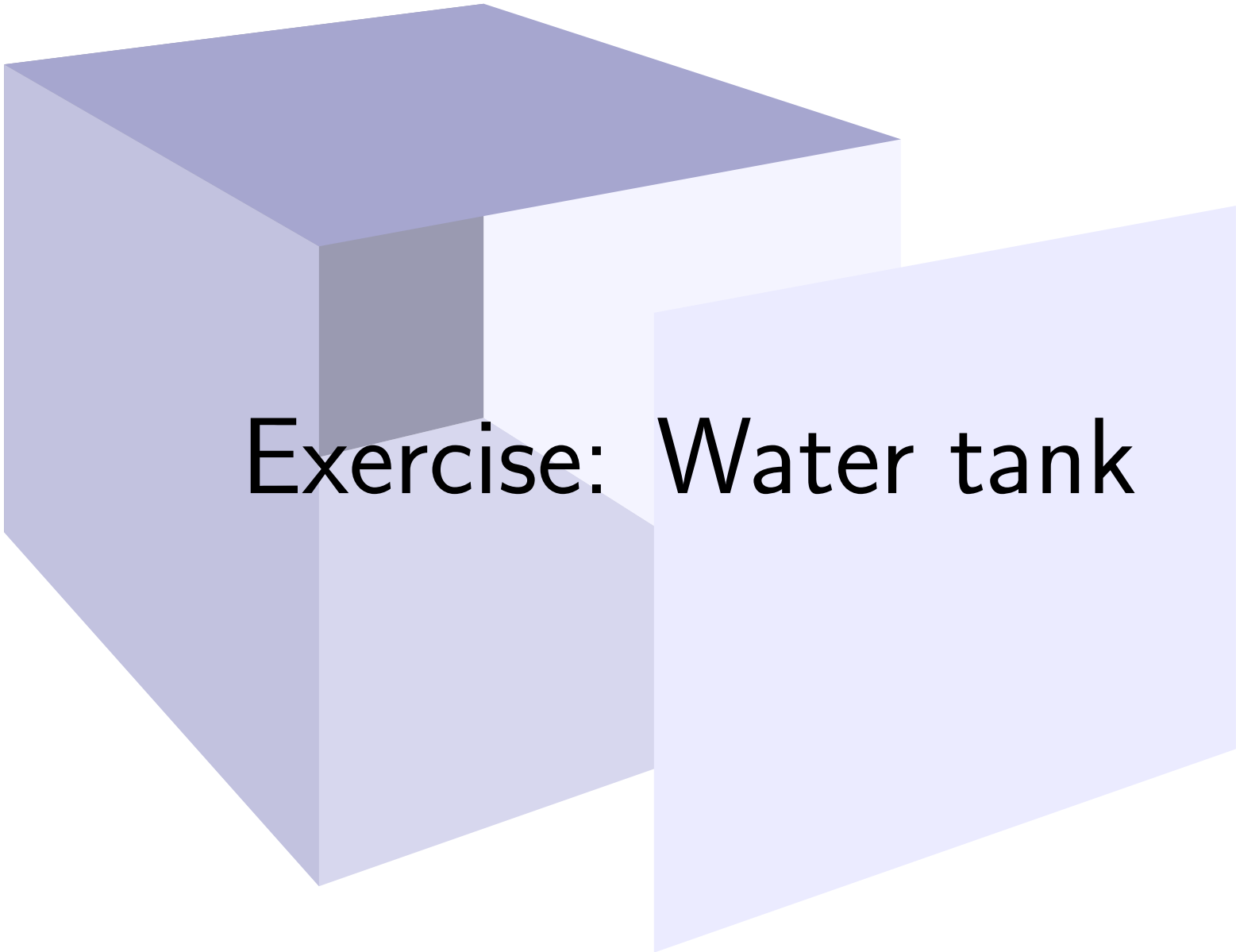
Practical Reactive Synthesis

Lecture at the
1st Summer School on Formal Methods for Cyber-Physical System

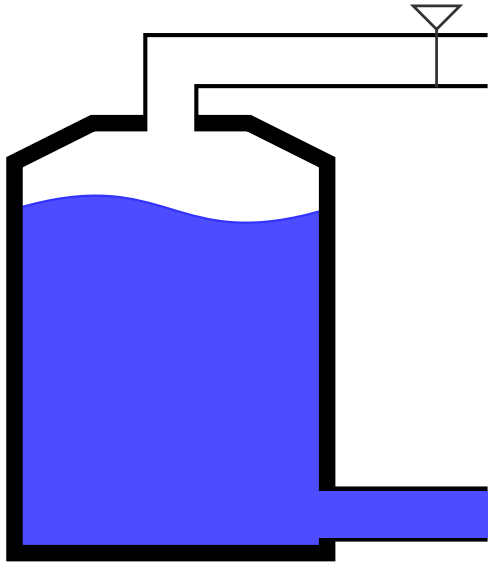
Rüdiger Ehlers, University of Bremen

September 2017



Exercise: Water tank

Water tank



Input /Output

In: `waterin` $\in \{0, \ldots, 5\}$, `waterout` $\in \{0, \ldots, 3\}$, `keeplow`

Out: `inValve`, `lowmode`, `waterlevel` $\in \{0, \ldots, 100\}$

Use the web interface of the `slugs` tool available at:

`http://webslugs.ruediger-ehlers.de`

Specification – Level 1

Assumptions

- Initially, no water flows in or out

Guarantees

- initially, the water level is 50
- initially, the inValve is closed
- The water level is always updated according to waterin and waterout

Starting point

```
[INPUT]
waterin:0...5
waterout:0...3
keeplow

[OUTPUT]
inValve
lowmode
waterlevel:0...100

[ENV_INIT]
waterin=0
waterout=0

[SYS_INIT]
waterlevel=50
!inValve

# Watertank Simulator Specification

[SYS_TRANS]
waterlevel'+waterout' = waterlevel+waterin'
```

Specification – Level 1(b)

Assumptions

- If the inValve is closed, the next `waterin` value is 0
- If the inValve is open, the next `waterin` value is at least 3

Specification – Level 2

Additional Guarantees

- infinitely often, the water level is smaller than 20
- infinitely often, the water level is larger than 80

Specification – Level 3

Additional Assumptions

- Infinitely often, water flows out
- Infinitely often, more than 3 units of water flow in (or the `inValve` is closed)

Specification – Level 4

Additional Assumptions

None!

Additional Guarantees

- Whenever the system declares to be in `lowmode`, the water level is smaller than 50.
- Whenever the system is in `lowmode`, the system stays in `lowmode` while `keeplow` is true
- Whenever the `keeplow` signal keeps being switched on, the system eventually enters `lowmode`.

Specification – Level 5

Additional Guarantees

- After the status of the valve changes, it has to stay the same for at least 3 steps.