Prof. Dr. A. Podelski,
Dr. B. Westphal

Summer term 2019

**Softwaretechnik/Software Engineering**

http://swt.informatik.uni-freiburg.de/teaching/SS2019/swtvl

# Exercise Sheet 4

Early submission: Wednesday, 2019-06-26, 12:00    Regular submission: Thursday, 2018-06-27, 12:00

## Exercise 1 – Class and Object Diagrams (10/20 Points)

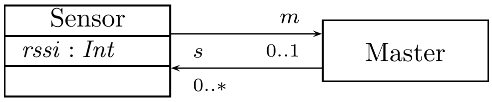


Figure 1: WFAS masters and slaves.

Recall the Wireless Fire Alarm System (WFAS) from Lecture 6. A cornerstone of the design is the idea that for each sensor,[1] there is a so-called master to monitor the sensor and take notifications (like indications of fire). If the system is operational (not in maintenance mode), each sensor must have a link to exactly one master, and the sensor-master links must be reciprocal, i.e. the master's link includes all sensors who have a link to this master.
Figure 1 shows an abstract model of this design idea.

(i) Provide the **abstract syntax** of the diagram. (5)

(ii) Clarify the intended usage of the data-structure as described in the introductory text to this exercise; use at least three *own* (i.e., not from the lecture, not from an exercise) non-trivial system states (over the Class Diagram from Figure 1 and structure $\mathscr{D}$ with $\mathscr{D}(Int) = \mathbb{Z}$ and $\mathscr{D}(\mathscr{C})$ of your choice) shown as Object Diagrams.

- One system state that models a typical configuration in operational mode. (1)
- One system state that models a corner-case configuration, i.e., which may be (dis)allowed by the wording above but which seems questionable from the WFAS context. (1)
- One system state that is not allowed in operational mode. (1)

*Hint: Note that the task asks for 'clarification', i.e., a set of system states alone is not a solution to this task. Rather assume that your submission is a review of the proposed structural model as requested by an imaginal 'boss'.*

(iii) For one of your Object Diagrams from Task (ii), provide the underlying system state in function notation. (2)

## Exercise 2 – Writing Class Diagrams (3/20 Points)

Technically, both sensors and masters (repeaters or central units) comprise a main controller (CPU, Memory, etc.) where the software that implements the system-monitoring and alarm protocols, and an independent transceiver module that sends or receives data and is accessible from the main controller via some industry standard bus system.
The transceiver can be on or in power-save mode, and in send or receive mode. Sensors and masters use different main controllers but the same variant of transceiver modules.

[1] Which keeps track of a received signal strength indicator (RSSI).

(i) Extend Figure 1 by classes and associations to also model transceiver modules and their relations as described above, assuming that 'Sensor' and 'Master' represent the main controller including everything else except the transceiver module. (2)

*Hint: Note that this is a modelling task in the sense that a Class Diagram alone is not a solution. Explain how to see that your proposed diagram is a model of (your understanding of) the description above.*

(ii) Provide the abstract syntax of your Class Diagram from Task (i) (1)

## Exercise 3 – Evaluating OCL Formulae (7/20 Points)

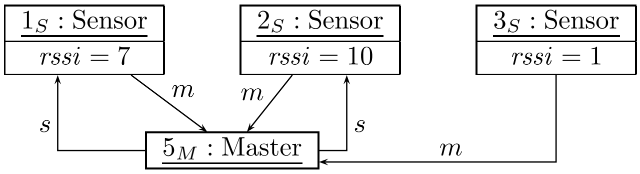


Figure 2: Complete object diagram.

Consider the system state $\sigma_1$ given by the complete Object Diagram in Figure 2.

(i) To which value does the Proto-OCL formula

$$F := \forall\, self \in allInstances_{\text{Master}} \bullet \forall\, n \in s(self) \bullet rssi(n) \geq 3 \wedge rssi(n) \leq 10$$

evaluate for $\sigma_1$? Prove your claim, i.e., compute $\mathcal{I}[\![F]\!](\sigma_1, \emptyset)$. (5)

(ii) Provide system states $\sigma_2$ and $\sigma_3$ such that for each truth value *true*, *false*, or $\perp$, there is an $i \in \{1, 2, 3\}$ such that $\mathcal{I}[\![F]\!](\sigma_i, \emptyset)$ evaluates to this truth value. Argue your claim. (2)

*Hint: A proof is not necessary for this task, yet proofs are possible ways to argue for claims.*

## Exercise 4 – Writing OCL Formulae (0/20 Points + 3-10 Bonus)

Use Proto-OCL to formalise **ONE OF** the following requirements on the WFAS software:

(i) The RSSI values of sensors ranges between 0 and 10. (3 Bonus)

(ii) Each sensor has a master. (5 Bonus)

(iii) Masters must not monitor more than 20 sensors. (5 Bonus)

(iv) If a master monitors a sensor (i.e. the sensor is included in this master's $s$ link), then this sensor has that master as master (via $m$). (10 Bonus)

Demonstrate that your solution is (at least) plausible:

- Give at least one example of a system state that you expect to satisfy your chosen requirements and at least one that you consider to violate the requirement (i.e., where your formalisation should evaluate to *false*) — together with the outcome you expect.
- Argue why your formula evaluates to the expected outcomes.

*Hint: You may use the function symbol '$size : 2^{\tau} \to \mathbb{Z}_\perp$' with*

$$size_{\mathcal{I}} : \mathcal{I}[\![2^{\tau}]\!] \to \mathcal{I}[\![\mathbb{Z}_\perp]\!]$$

$$size_{\mathcal{I}}(x) = \begin{cases} |x| & x \neq \perp \\ \perp & otherwise. \end{cases}$$