Formal Specification and Design of Software
Winter Term 2022/23

# Task Descriptions for Exercise

Ao.Univ.-Prof. DI Dr. Bernhard Aichernig

7.11.2022

Form a group of two and develop a set of TLA+ specification with several refinements. For each refinement a separate specification, like in the lecture, shall be developed. Verify each refinement. There may be ambiguities and even inconsistencies. Take a decision and resolve them in your spec! Do not exchange your specifications with other groups! We will discuss the different decisions in the final presentations.

## 1 Car Alarm System

### 1.1 Requirements

The topic of the exercise is a controller of a car alarm system with the following requirements:

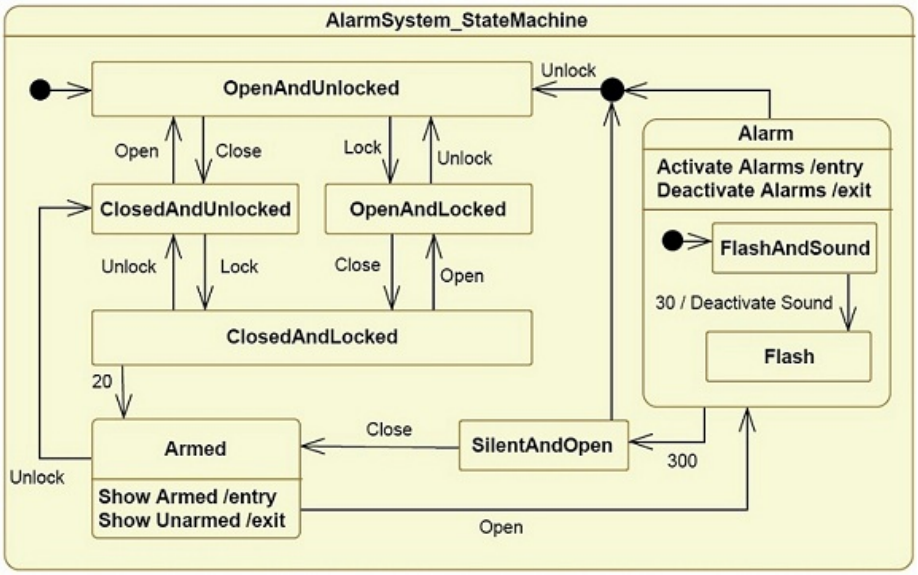
**Requirement 1** Arming. The system is armed 20 seconds after the vehicle is locked and the bonnet, luggage compartment, and all doors are closed.

**Requirement 2** Alarm. The alarm sounds for 30 seconds if an unauthorised person opens the door, the luggage compartment, or the bonnet. The hazard flasher lights will flash for five minutes.

**Requirement 3** Deactivation. The anti-theft alarm system can be deactivated at any time, even when the alarm is sounding, by unlocking the vehicle from outside.

### 1.2 State Machine

For a better understanding, we provide a state machine according to the requirements:




**Hint:** In a first refinement it is better to abstact from the timing behaviour and model the timeouts as non-deterministic actions. In later refinements, the method described by Lamport [1] can be used.

## 1.3 Refinement with Pincode

The requirements above shall be extended as follows:

**Requirement 4:** For unlocking, the car key sends a four-digit pincode. This pin is compared to an internally stored code. If the sent code fails to match for three times, then the alarm is triggered. This only happens when the car alarm system is armed.

**Requirement 5:** It shall be possible to set a new pincode (*setPinCode*). Here, the car must be unlocked and the old and new pincode must be provided. Again, the provision of a wrong pincode for three times triggers the alarm. Otherwise, the system acknowledges the successful update with the message *newPinSet*.

## 1.4 Refinement of the Doors

**Requirement 6:** There may be 2 or 4 passenger doors plus the luggage compartment door. The doors are considered to be closed, when all passenger doors are closed.

**Requirement 7:** The luggage compartment can be unlocked separately. Here, the car alarm system will not be deactivated.

### 1.5 Refinement of Keys

**Requirement 8:** There exists a set of keys, each with its own pincode initialized.

**Requirement 9:** There is a maximum number of keys.

**Requirement 10:** The car opens automatically when the key is within a certain distance and closes when the key is outside this distance.

**Requirement 11:** The feature in Requirement 10 can be disabled.

### 1.6 Optional Refinements

Invent your own requirements and refine the model accordingly.

## References

[1] Leslie Lamport. Real-time model checking is really simple. In Dominique Borrione and Wolfgang J. Paul, editors, *Correct Hardware Design and Verification Methods, 13th IFIP WG 10.5 Advanced Research Working Conference, CHARME 2005, Saarbrücken, Germany, October 3-6, 2005, Proceedings*, volume 3725 of *Lecture Notes in Computer Science*, pages 162–175. Springer, 2005.