Formal Methods in Software Engineering

989902

Homework No: 1

- **Goal:** Integrating formal methods to the design phase of software life-cycle development using the tool GROOVE
- **Deadline:** 99.02.12, 11:59 pm. Homeworks submitted after the deadline and before 99.02.15, 11:59 pm will have 30% deduction. Homeworks submitted after 99.02.15, 11:59 pm will have 50% deduction.
- **Deliverables:** Only one RAR file entitled "Your family - Your student no - HW01.rar" that contains a "read-me.docx" file and a folder named "groove-cruise-control-model". In the read-me file, you should report the details of your designed model. In the folder, you should put the groove model. The model should work correctly and produce the specified outputs using the tool GROOVE.
- **Submission**: The asked deliverables are to be submitted on LMS
- **Considerations:** Ask if you have any questions in "Q/A Forum" on LMS.

In this assignment, you will formally design a *cruise control* using the tool GROOVE[1]. Assume a car domain consisting of the four applications *anti-lock braking*, *cruise control*, *stability control*, and *fingerprint security* as illustrated in Fig. 4.2.

The domain modeling phase for each application will produce a model for each entity of interest for that application and its relationship to different functional and nonfunctional requirements of that application. For each object in each application in the model, a component is designed. The behavior of each component is specified by an extended finite state machine. Below we illustrate these steps for the *cruise control* system.

[1] https://sourceforge.net/projects/groove/files/

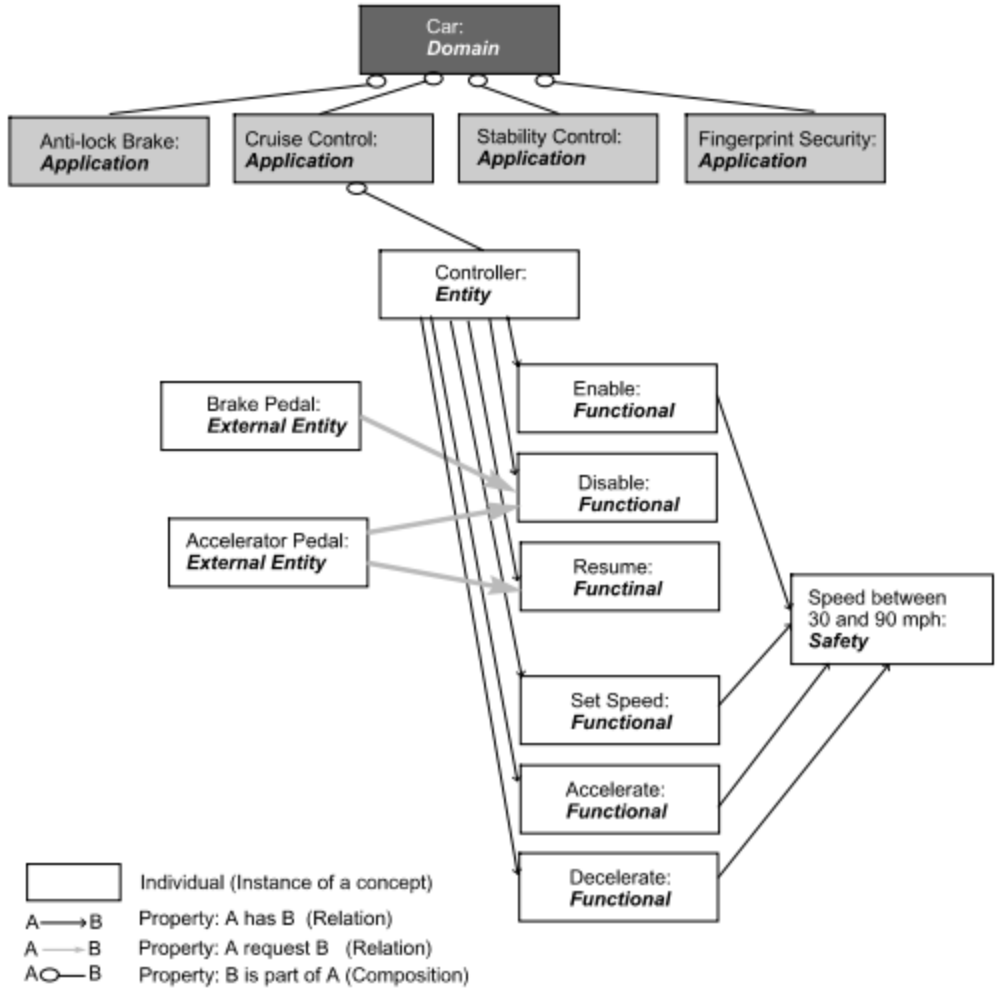

Fig. 4.2 Car ontology example focusing on the cruise control system

Cruise Control System (CCS)

The cruise control system (CCS) in a car is a multi-function computer system which automatically manages the speed of the car. It consists of four parts: Accelerator pedal (AP), Brake pedal (BP), Dashboard (DB), and Controller (CO). By stepping on to the AP the vehicle goes faster, and by releasing the pedal the vehicle slows down. So, AP has two states, which are named idle and goFaster as in Fig. 7.7(a). The transition specifications are:

- idle $\xrightarrow{\text{accelerate}}$ goFaster
- goFaster $\xrightarrow{\text{accelerate}}$ goFaster
- goFaster $\xrightarrow{\text{releasePedal}}$ idle

BP has two states corresponding to 'brake is not applied' and 'brake is applied' as in Fig. 7.7(b). Its transition specifications are similar to that of AP.

DB is the interface to interact with CCS. It has four buttons with the following functionalities.

- On and Off : The on button gets the car ready to accept a cruising control command. The off button turns the cruise control off.
- Set-Accel: The Set-Accel has a dual function. If the car is at the enabling state, which means the On button has been pushed, then the cruising control will start and CCS will fix and maintain the speed that the car is currently driving. If the car is in cruise control state and the Set-Accel button is hit, then holding down the Set-Accel button will make the car accelerate faster.
- Resume-Decel: If the car driver hits the brake pedal while in cruising state, CCS will be at disable state. Hitting the Resume-Decel button at the disable state will command the car to accelerate back to the most recent speed setting. If the car is in cruise control state and the Resume-Decel button is hit, then holding down the Resume-Decel button will make the car decelerate.

The transition specifications of DB are given below.

- idle $\xrightarrow{\text{on}}$ turnOn
- idle $\xrightarrow{\text{off}}$ turnOff
- turnOn $\xrightarrow{\epsilon}$ idle
- turnOn $\xrightarrow{\varepsilon}$ idle
- idle $\xrightarrow{\text{setAccel}}$ turnSA
- idle $\xrightarrow{\text{resumeDecel}}$ turnRD
- turnSA $\xrightarrow{\varepsilon}$ idle
- turnRD $\xrightarrow{\varepsilon}$ idle
- turnSA $\xrightarrow{\text{setAccel}}$ turnSA
- turnRD $\xrightarrow{\text{resumeDecel}}$ turnRD

The complete behavior of DB is shown in Fig. 7.7(c). When CCS in the car is activated through DB the controller, CO manages the correct behavior of CCS. When the accelerator pedal is pressed, CCS is disabled and the speed increases. When the accelerator is released, the CCS resumes at its last set speed. If at any point of time during acceleration the CCS speed is set, CCS replaces the old set speed with the new speed. The controller CO has the following safety features:

- CCS is automatically disabled when the car speed is either below 45 kmph or above 160 kmph.

- CCS is automatically disabled when the Anti-Lock Brake system is activated.

Figure 7.7(d) shows the extended finite state machine of the controller for CCS. Note, the transition specifications, as shown in the figure, can be written down. The behavior of CCS is the combined behavior of the four state machines shown in Fig. 7.7.

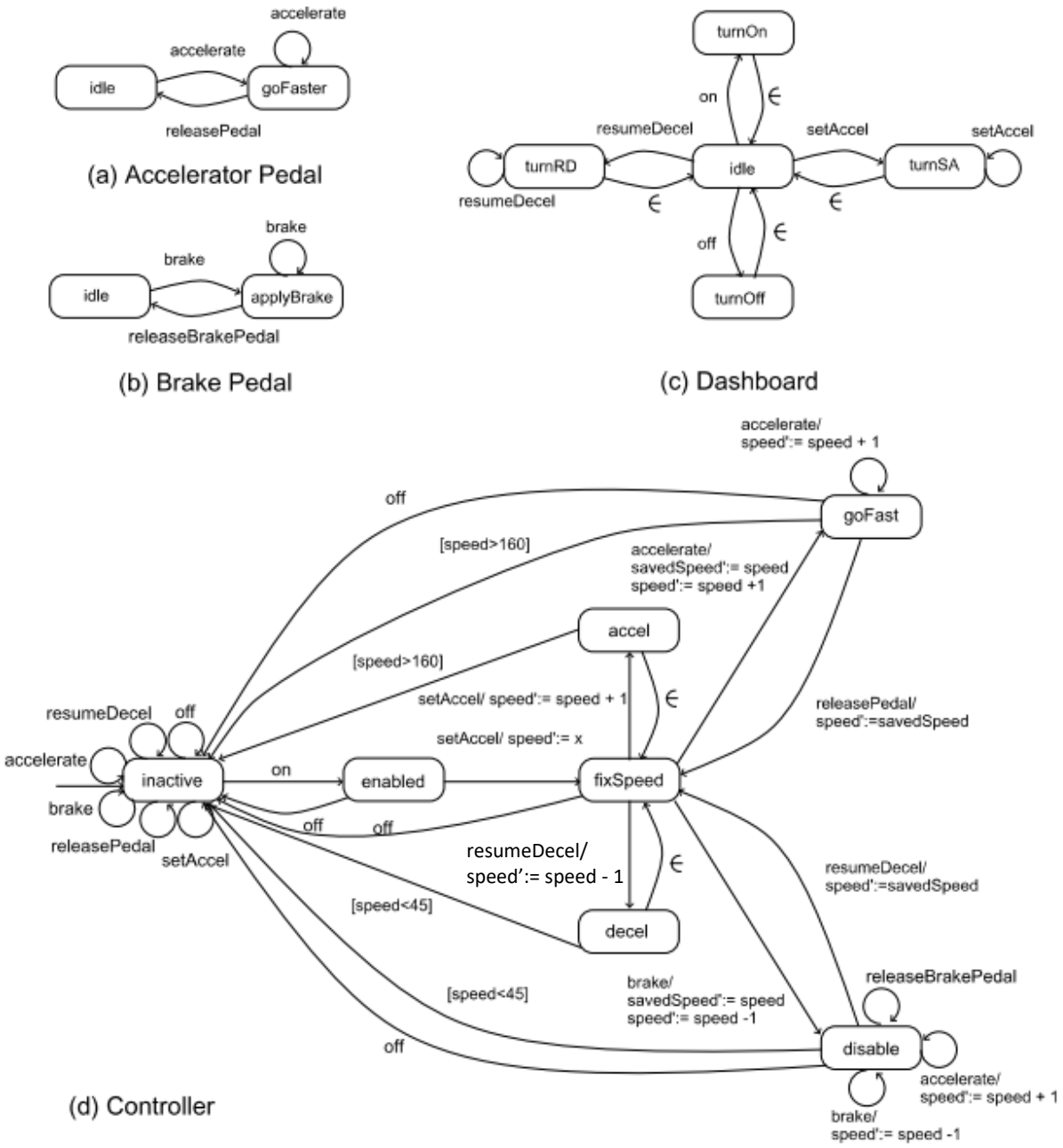

Fig. 7.7 Cruise control system