SOEN 331: Introduction to Formal Methods for Software Engineering Assignment 2 on EFSMs

Ali Jannatpour

February 18, 2020

Contents

1 General Information

Date posted: Tuesday February 18th, 2020.

Date due: Tuesday March 3rd, 2020, by 23:59.

Weight: 7.5% of the overall grade (2.5% as bonus).

2 Introduction

Your assignment is to work in teams of 3-4 and produce a formal specification and a state diagram for a driverless car system. Each team should designate a leader who will submit the assignment electronically.

3 Ground rules

This an assessment exercise. You may not seek any assistance while expecting to receive credit. **You must work strictly within your team and seek no assistance for this project (from the instructor, the teaching assistants, fellow classmates and other teams or external help).** Failure to do so will result in penalties or no credit.

4 Your Assignment

Consider a driver-less car system. A self-driving car (sometimes called an autonomous car or driverless car) is a vehicle that is capable of sensing its environment and moving safely with little or no human input. The description of the system is given in the following. In this assignment you produce a formal specification, a state diagram, as well as a declarative representation for a driverless car system. Subsequently, you will extend the declarative representation of the system by providing some rules to demonstrate the behavior of the system (see section 6).

4.1 Description of the system

The description of the system is stated in the following. While various states of the system is provided in the text, you may use additional / pseudo states to design the system using an EFSM. The top level states of the system are as follows:

1. The system is initially in the idle state. The system is activated when the driver starts the car. In this state the engine is idle and the car is ready to drive. This state may also be referred to as the parked mode.

2. While being in the parked mode, the driver may use the navigation system to set the destination.

3. While being in the parked mode, the driver would issue a drive signal and provided the engine is idle, the system will go to manual driving mode.

4. From the parked mode, the driver has also the option to initial a cruise signal, by which the system goes to the cruise mode. This mode, however, requires the destination being set already. If the destination is not set, the system beeps and stays in the manual mode.

5. While driving, in case the destination is set, the driver may choose to switch to cruise mode or switch back from cruise mode to manual mode.

6. In the manual mode, if the car is stopped, the driver may put the car in the marked mode.

7. While in the cruise mode, upon unforseen events the system may go to panic mode, during which the car stops immediately and the hazard signal is turned on.

8. During the cruise mode, if the car is arrived at the destination, the system automatically goes to parked mode.

9. The driver may switch off the panic which brings the car in the parked mode and turns the hazards off.

10. At any time, during the cruise mode, the driver may issue a manual drive option, by which the system goes to manual driving mode.

11. When in parked mode, the driver may shut-off the engine, by which in turns off the system.

4.2 Manual mode

1. While manual driving, the driver may issue accelerate or reduce speed signals to make the engine run faster or slower.

2. The driver may also issue a break signal which causes the engine to go to 0-speed, immediately; in which case, it remains in the break mode unless the driver issues an accelerate signal.

4.3 Cruise mode

The Cruise mode may be activated by the driver upon issuing the cruise signal if the destination is set on the navigation system. While initially being in the cruising state, it may go to tailing or changing lane sates. The cruise mode deals with the following issues:

- Maintaining desired speed
- Avoiding obstacles
- Navigation

The cruise control system maintains the above frequently by frequently checking the statuses of the signals received form the sub-systems. The specifications of the three subsystems are given in the following.

4.3.1 Maintaining desired speed

The default speed is the default speed of the road, set automatically. The car maintains the speed within the desired range. The desired range is the default speed ±5%.

1. If the current speed is less than the minimal speed, it issues an accelerate signal to increase the speed.
2. If the current speed is above the maximal speed, it issues an reduce speed signal to decrease the speed.

4.3.2 Avoiding obstacles

During the cruise mode, the system also checks for obstacles (i.e. cars ahead). The car must maintain a minimum distance with the cars ahead. Upon detecting an obstacle, it measures the distance from the car ahead.

1. If the distance is above the threshold limit, it maintains the current speed.
2. Otherwise, it goes to tailing mode in which the speed must be reduced until the minimum distance is obtained.
3. In case the obstacle is not moving or perhaps the safe distance cannot be maintained, the system issues a change lane signal (changing one lane to the left). See section 4.3.4.

4.3.3 Navigation

The navigation system is a live sub-system that constantly monitors the traffic information and takes control of the routing. It is activated when the driver sets the destination. The frequency of the monitoring is every second, at which it MAY issue the following signals:

1. Turn left ahead: a signal indicating that the car must change lane and be in the left-most lane.
2. Turn right ahead: a signal indicating that the car must change lane and be in the right-most lane.
3. Turn left: upon which the car must turn left at the next intersection.
4. Turn right: upon which the car must turn right at the next intersection.

5. Destination ahead: car is approaching the destination and must take the rightmost lane.

6. Arrived at destination: upon which the car is reached at the destination and should be stopped.

4.3.4 Changing lane

Changing lanes may occur during the cruise mode for many reasons. It functions as follows:

1. This state uses a lane variable that indicates the target lane.

2. Changing lane is obtained by changing one lane at a time.

3. Whether taking the left lane or the right lane, the system checks if the lane is open.

4. If changing lane is possible, it changes the lane, otherwise, it remains on this state until the opportunity becomes available.

5. The above is repeated until the car is in the target lane, in which case it goes back the cruising state.

6. In case there is obstacle ahead and there is no possibility of changing lanes, the system panics; in which case, it issues a panic signal, causing the system to go to panic mode.

4.4 Panic mode

This mode is reserved for rare occasions that the system cannot resolve issues. Upon reaching this state, the car immediately stops and the hazard signal is turned on. The system also gives the drive the option to turn on the panic signal manually. While at panic state, the driver also has the option to turn off the panic signal, in which it brings the system into parked mode.

5 Guidelines

There are a few things to consider while preparing your assignment. The following guidelines will help you stay in the right track. They will also help you validate your formal specification.

- Start my creating the main state machine.
- Identify states, signals and/or events.
- Identify the transitions and guards.
- The hierarchy of the document suggests composite states and sub-states. Yet some may be merged.
- Once the elements of the state machines are identified, draw a sketch of the EFMS. Check for errors.
- Work on your model until all requirements are addressed.
- Once completed, compile the UML diagram into the formal specification.
- In the last stage, translate the formal language into a Prolog database. See section 6.2.

6 What to submit

You must write your specification using the LaTeX text formatting package. Similar to Assignment 1, you need to install a) the LaTeX package for your operating system, and b) some LaTeX editor. One recommended combination is `MiKTeX` with `Texmaker`. You will find necessary resources on the course website.

Use the template provided to prepare the formal specification and produce a **pdf** file named after the id of the person to submit, e.g. `123456.pdf`. See also section 6.2.

6.1 The specification document

Your submission must include a pdf document, created using LaTeX, which contains the formal specification of the system along with the UML diagram of your EFSM, embeded in the PDF.

Use the template that is provided. You may use a software of your choice to draw the UML diagram, i.e. Microsoft Visio, Rational Rose, or even use online tools (i.e. draw.io). You may convert the diagrams in encapsulated postscript (.eps).
Total marks: 5%.

6.2 Bonus Section

The following is considered as Bonus which counts for an additional 2.5%.

6.2.1 The Prolog Database and Queries

Create a declarative database (facts and rules) as a **.pl** file. Submit it with your pdf specification in a single **zip** file, named after the id of the person who will do the submission. Write the following queries to check the validity of your model:

Queries

1. Rule **"transition"** receives two states (at the same level of abstraction), and succeeds if there is transition between them. It will capture and display all ⟨**event, guard, action**⟩ triplets that are associated with the transition.

2. Rule **"interface"** succeeds by obtaining a collection of all unique ⟨**state, event**⟩ pairs in the entire system.

Run your rules and record your interaction. **Submit this record.**

Section Submission

Section S Please submit on Moodle. Your instructor will provide you with more details.

Section U Please submit your pdf file at the Electronic Assignment Submission portal

`(https://fis.encs.concordia.ca/eas)`

under Theory Assignment 2.