

SOEN331: Introduction to Formal Methods
for Software Engineering

Assignment 2 on Extended Finite State Machines

Gordon Pham-Nguyen, Ian Philips, Tabesh Haidary, Jeffrey Li

March 6, 2020

1 Driver-less car system formal specification

The EFSM of the driver-less car system is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$$Q = \{Idle (Parked), Manual Mode, Cruise Mode, Panic Mode\}$$

$$\Sigma_1 = \{State engine, shut off engine, drive signal, parked signal, cruise signal, manual signal, car arrived at destination, panic mode off, unforeseen event or panic signal\}$$

$$\Sigma_2 = \{beep, stop car, turn on, hazard lights, turn off hazard lights\}$$

$$q_0 : Idle (Parked)$$

$$V : \{\}$$

Λ : Transition specifications

1. $\rightarrow Idle (Parked)$
2. $Idle (Parked) \xrightarrow{\text{cruise signal [destination is set]}} Cruise Mode$
3. $Idle (Parked) \xrightarrow{\text{drive signal}} Manual Mode$
4. $Manual Mode \xrightarrow{\text{cruise signal [destination is set]}} Cruise Mode$
5. $Cruise Mode \xrightarrow{\text{car arrived at destination}} Idle (Parked)$
6. $Idle (Parked) \xrightarrow{\text{cruise signal [destination is not set] / beep}} Idle (Parked)$
7. $Manual Mode \xrightarrow{\text{parked signal [car is stopped]}} Idle (Parked)$
8. $Cruise Mode \xrightarrow{\text{unforeseen event or panic signal / stop car ; turn on hazard lights}} Panic Mode$
9. $Panic Mode \xrightarrow{\text{panic mode off / turn off hazard lights}} Idle (Parked)$
10. $Manual Mode \xrightarrow{\text{cruise signal [destination is not set] / beep}} Manual Mode$
11. $Cruise Mode \xrightarrow{\text{manual signal}} Manual Mode$
12. $Idle (Parked) \xrightarrow{\text{shut off engine}} Exit$

The EFSM of the car system in manual mode is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$$Q = \{Manual\ Mode, Break\ Mode\}$$

$$\Sigma_1 = \{accelerate\ engine, reduce\ signal, break\ signal, accelerate\ signal\}$$

$$\Sigma_2 = \{faster\ engine, slower\ engine, 0 - speed\}$$

$$q_0 : Manual\ Driving$$

$$V : \{\}$$

Λ : Transition specifications

1. $\rightarrow Manual\ Driving$
2. $Manual\ Driving \xrightarrow{accelerate\ signal/faster\ engine} Manual\ Driving$
3. $Manual\ Driving \xrightarrow{reduce\ signal/slower\ engine} Manual\ Driving$
4. $Manual\ Driving \xrightarrow{break\ signal/0-speed} Break\ Mode$
5. $Break\ Mode \xrightarrow{accelerate\ signal} Manual\ Mode$

The EFSM of the car system in cruising mode is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$$Q = \{Cruising, Tailing, Changing Lane\}$$

$$\Sigma_1 = \{Car\ detected\ ahead, after\ 1\ second, any\ change\ lane\ signal, target\ lane\ signal, panic\ signal\}$$

$$\Sigma_2 = \{reduce\ speed, maintain\ current\ speed, change\ to\ left\ lane\ signal, panic\ signal\}$$

$$q_0 : Cruising$$

$$V : \{\}$$

Λ : Transition specifications

1. $\rightarrow Cruising$
2. $Cruising \xrightarrow{\text{Car detected ahead [distance under threshold]/ reduce speed}} Tailing$
3. $Tailing \xrightarrow{\text{after 1 second [distance under threshold]/ reduce speed}} Tailing$
4. $Tailing \xrightarrow{\text{after 1 second [obstacle not moving or safe distance cannot be maintained]/change to left lane signal}} Changing Lane$
5. $Tailing \xrightarrow{\text{after 1 second [distance is above or at threshold]/ maintain current speed}} Cruising$
6. $Cruising \xrightarrow{\text{any lane change signal}} Changing Lane$
7. $Changing Lane \xrightarrow{\text{target lane signal}} Cruising$
8. $Changing Lane \xrightarrow{\text{panic signal/panic signal}} Cruising$

The EFSM of the car system in navigating mode is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$$Q = \{Navigating\}$$

$$\Sigma_1 = \{After\ 1\ second\}$$

$$\Sigma_2 = \{accelerate\ signal, increase\ speed, reduce\ speed\ signal, decrease\ speed, \\ car\ arrived\ at\ destination\ signal, turn\ right\ at\ next\ intersection, turn\ left\ at\ next\ intersection, \\ change\ to\ right - most\ lane\ signal, change\ to\ left - most\ lane\ signal\}$$

$$q_0 : Navigating$$

$$V : \{\}$$

Λ : Transition specifications

1. $\rightarrow Navigating$

2. $Navigating \xrightarrow{\text{after 1 second [left turn ahead]/ change to left-most lane signal}} Navigating$

3. $Navigating \xrightarrow{\text{after 1 second [right turn ahead]/ change to right-most lane signal}} Navigating$

4. $Navigating \xrightarrow{\text{after 1 second [Destination ahead]/ change to right-most lane signal}} Navigating$

5. $Navigating \xrightarrow{\text{after 1 second [turn left]/ turn left at next intersection}} Navigating$

6. $Navigating \xrightarrow{\text{after 1 second [turn right]/ turn right at next intersection}} Navigating$

7. $Navigating \xrightarrow{\text{after 1 second [arrived at destination]/ car arrived at destination signal}} Navigating$

8. $Navigating \xrightarrow{\text{after 1 second [current speed more than road speed + 5%]/ reduce speed signal; decrease speed}} Navigating$

9. $Navigating \xrightarrow{\text{after 1 second [current speed more than road speed - 5%]/ accelerate signal; increase speed}} Navigating$

The EFSM of the car system in lane changing mode is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$$Q = \{MergingLane\}$$

$$\Sigma_1 = \{After\ 1\ second\}$$

$$\Sigma_2 = \{target\ lane\ signal, obstacle\ ahead\ or\ cannot\ change\ lane, panic\ signal, change\ to\ right\ lane, change\ to\ left\ lane, change\ right\ lane\ signal, change\ left\ lane\ signal\}$$

$$q_0 : MergingLane$$

$$V : \{Lanes\}$$

Λ : Transition specifications

1. $\rightarrow MergingLane$

2. $MergingLane \xrightarrow{\text{after 1 second } [Lanes == 0] / \text{target lane signal}} MergingLane$

3. $MergingLane \xrightarrow{\text{after 1 second } [obstacle\ ahead\ or\ cannot\ change\ lane] / \text{panic signal}} MergingLane$

4. $MergingLane \xrightarrow{\text{after 1 second } [Lanes > 0 \wedge \text{right lane is open}] / (\text{change to right lane ; } Lanes- -)} MergingLane$

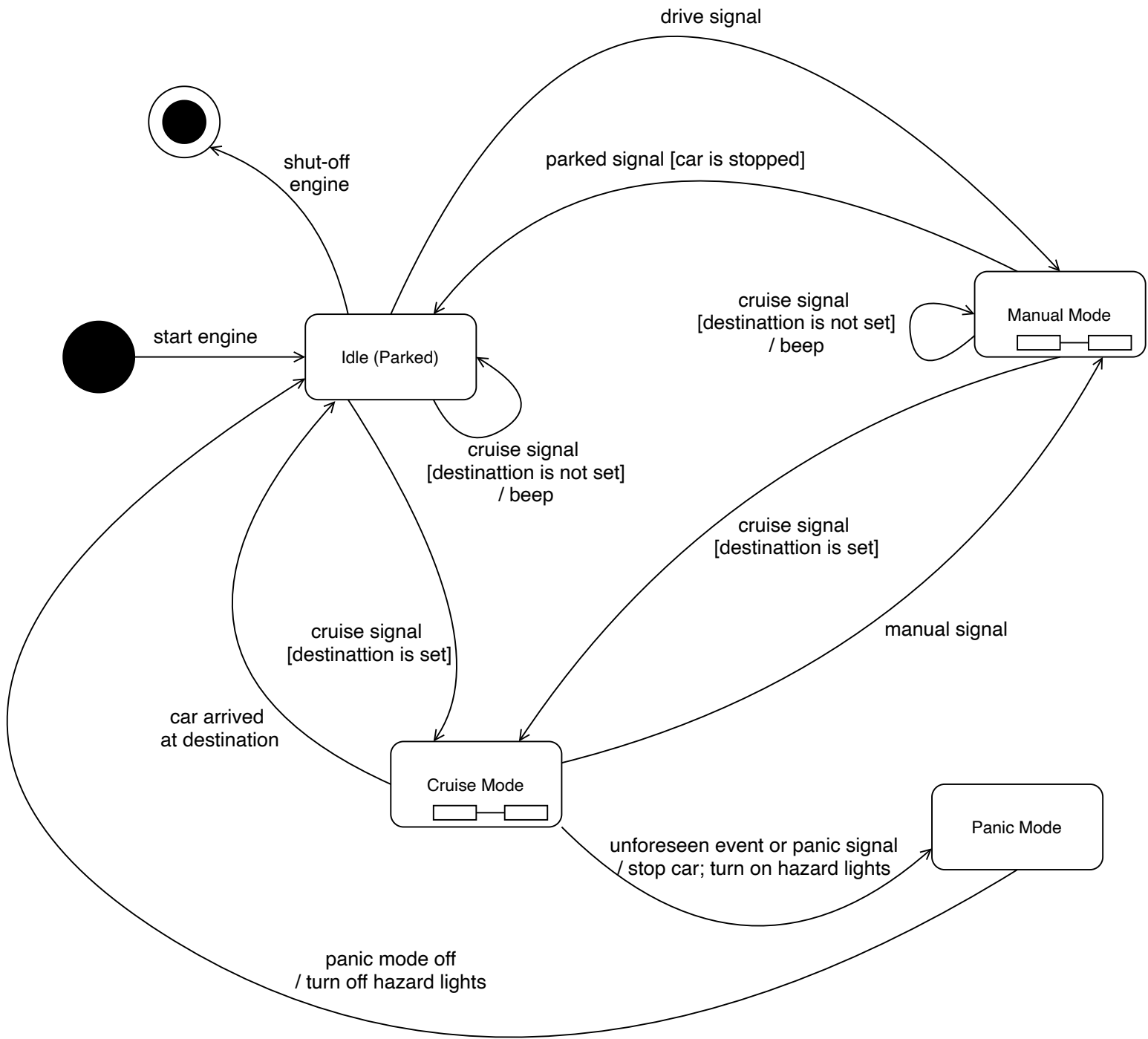
5. $MergingLane \xrightarrow{\text{after 1 second } [Lanes > 0 \wedge \text{right lane is not open}] / \text{change right lane signal}} MergingLane$

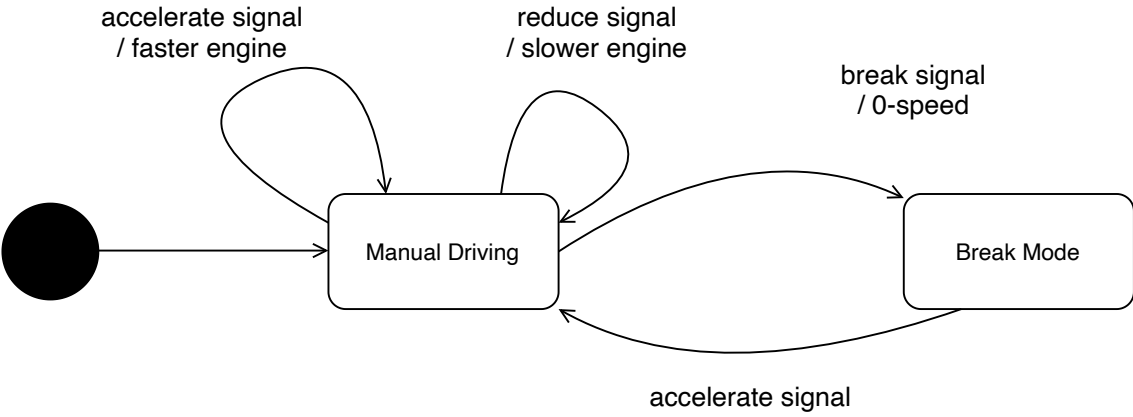
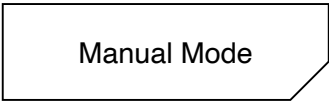
6. $MergingLane \xrightarrow{\text{after 1 second } [Lanes < 0 \wedge \text{left lane is open}] / (\text{change to left lane ; } Lanes++)} MergingLane$

7. $MergingLane \xrightarrow{\text{after 1 second } [Lanes < 0 \wedge \text{left lane is not open}] / \text{change left lane signal}} MergingLane$

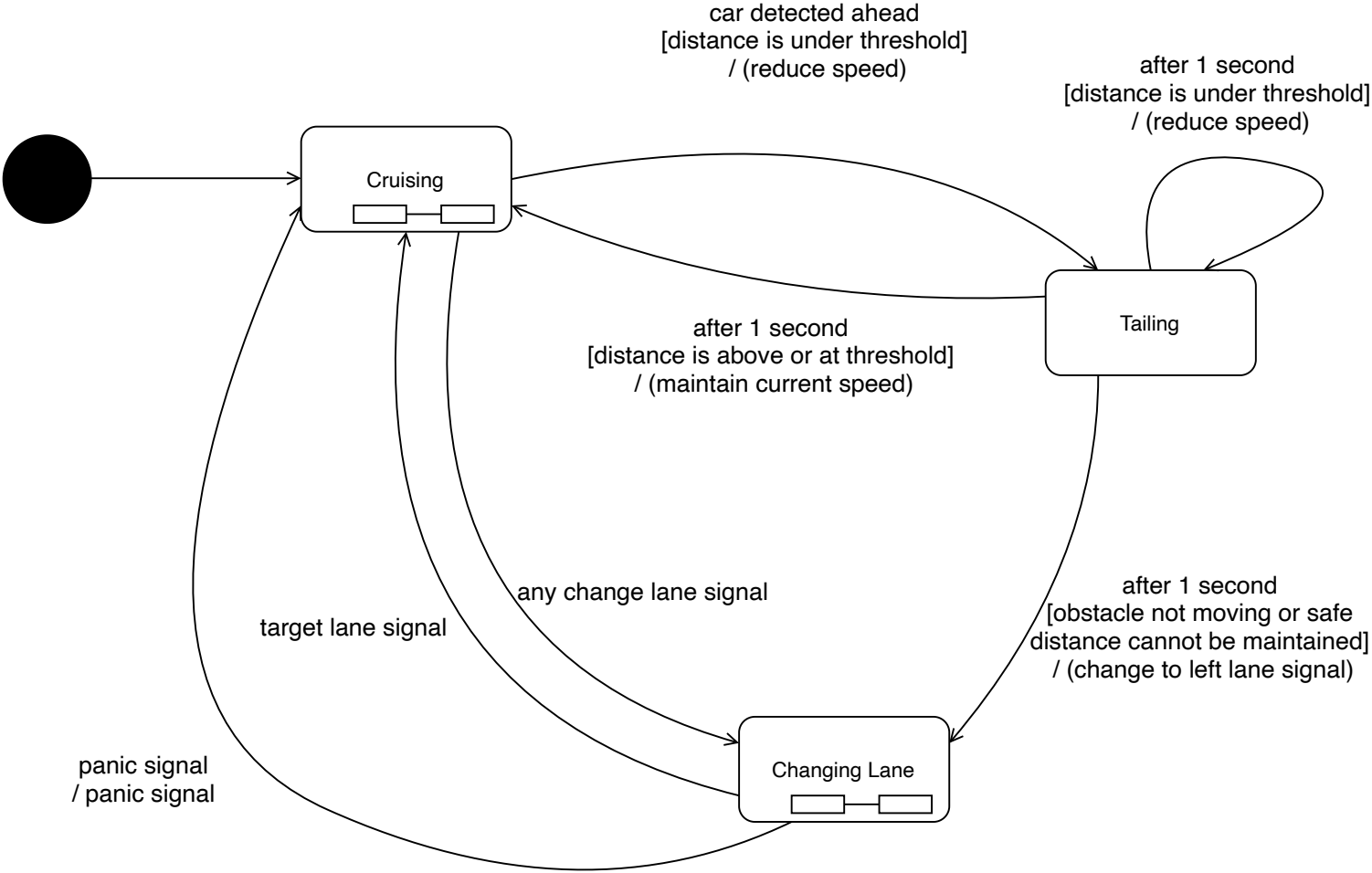
2 UML state diagrams

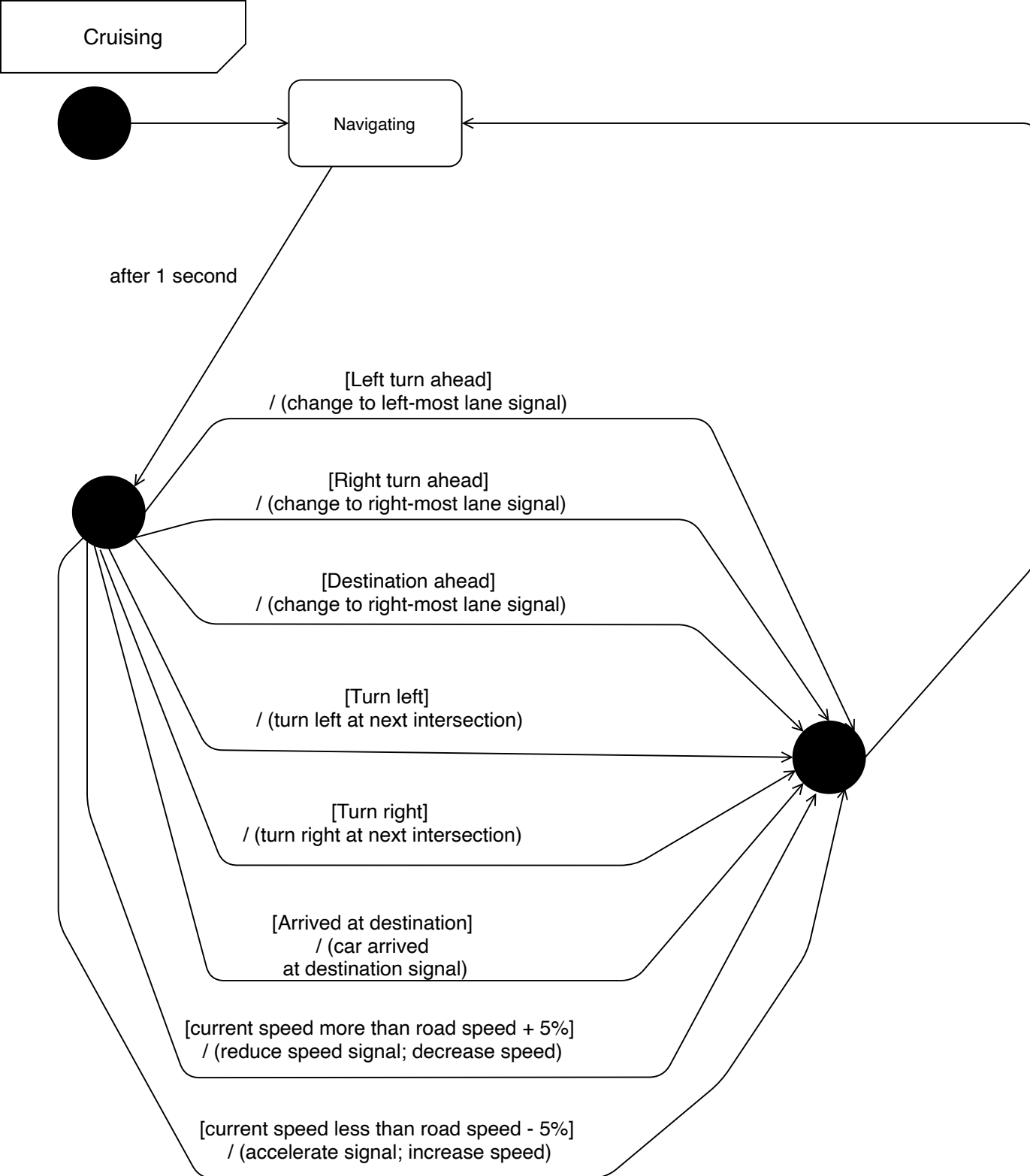
Driver-less car system





Cruise Mode





Changing Lane

