SOEN331: Introduction to Formal Methods for Software Engineering
Assignment 2 on Extended Finite State Machines

Martin Marcos 40041398,

Samantha Guillemette 26609198,

Deepkumar Patel 40096716

February 29, 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

$Q = \{idle, parked\ mode, manual\ mode, cruise\ mode, marked\ mode, panic\ mode, exit\}$

$\Sigma_1 = \{start\ car, cruise\ signal, drive\ signal, switch, arrived, unforseen, panic, marked\ mode\ signal, panic$

$\Sigma_2 = \{system\ start, engine\ idle, beep, system\ off, stop\ car, hazard\ signals\ on, hazard\ signals\ off\}$

$q_0 : idle$

$V : nav\ system : \{set, not\ set, engine\ idle, car\ stopped\}$

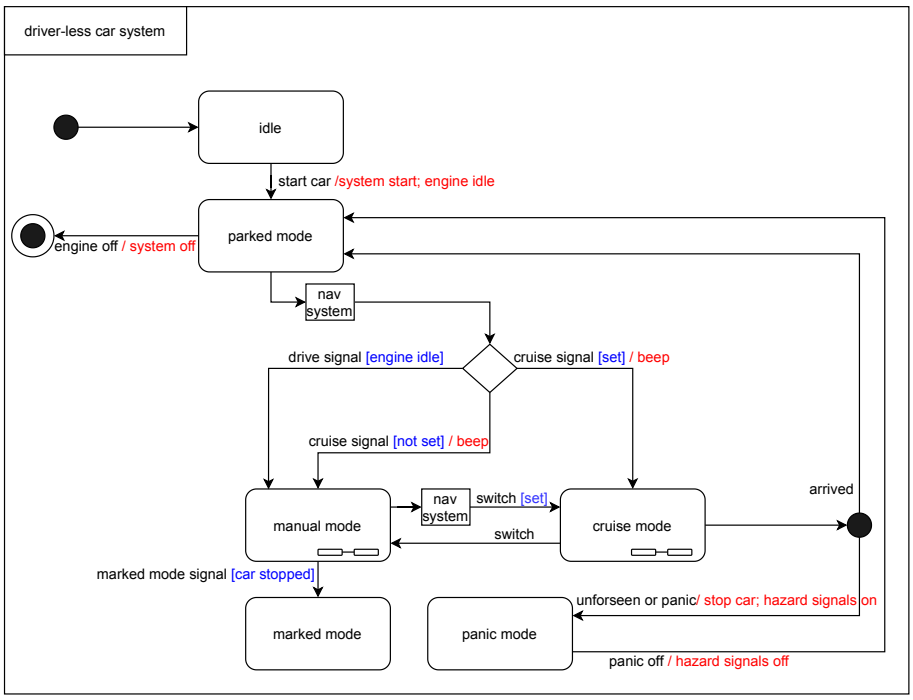
Λ: Transition specifications

1. $\rightarrow idle$
2. $idle \xrightarrow{\text{start/system start; engine idle}} parked\ mode$
3. $parked\ mode \xrightarrow{\text{engine off/system off}} exit$
4. $parked\ mode \xrightarrow{\text{cruise signal[not set]/beep}} manual\ mode$
5. $parked\ mode \xrightarrow{\text{cruise signal[set]/beep}} cruise\ mode$

6. *parked mode* $\xrightarrow{\text{drive signal[engine idle]}}$ *manual mode*
7. *manual mode* $\xrightarrow{\text{switch[set]}}$ *cruise mode*
8. *cruise mode* $\xrightarrow{\text{switch}}$ *manual mode*
9. *cruise mode* $\xrightarrow{\text{arrived}}$ *parked mode*
9. *cruise mode* $\xrightarrow{\text{unforseen or panic/stop car; hazard signals on}}$ *panic mode*
10. *manual mode* $\xrightarrow{\text{marked mode signal[car stopped]}}$ *marked mode*
11. *panic mode* $\xrightarrow{\text{panic off/hazard signals off}}$ *parked mode*

The UML state diagram is shown in Figure 1

2 UML state diagrams



assuming engine idle != car stopped. because while the car is parked and on,
I can still press the gas pedal and make the engine run while the car is still stop/immobile

assuming there is a marked mode signal, otherwise the moment the car is stopped in manual mode, it would automatically go to marked mode, but in the requirments it is implied that the driver can chose to go to marked mode or not during manual mode

assuming while having unforseen event in cruise mode,
the car does not immediately stop/hit the breaks that might cause an accident, but gradually stops

Figure 1: Main System.