CS580
Homework 06:
Electronic brake safety.
Yie Sheng Chen 1303

Problem definition

A formal specification of the electronic brake system with usability and driver safety in mind is developed such that a electronic brake software can be proved correct.

This electronic emergency brake operates as follows: the driver presses and releases a button to control the emergency brake: the result is either (1) full engagement or disengagement of the e-brake (emergency brake) on all hour wheels or (2) smart application of additional braking power under certain conditions.

Solution overview:

The main idea is that e-brake can only be used when car is in low speed or parked. And when car is in high speed and user pressed e-brake button, instead of e-brake on all 4 wheels, only smart additional braking power is applied. And if user does not release e-brake button by pressing it again, once the car's speed is lowered, the overall smart e-brake system will switch its operation from "smart application of additional braking power" to "e-brake on all four wheels."

Assuming two state of the e-brake system, buttonP and carHiSpeed are automatically updated from the events: (1) the press of a button by driver and (2) the speed sensor reading crossing the high speed threshold. In other words, the software assumes the sensed state as system input and does not do event handling.

Such behavior is captured in the following formal spec.:

Formal spec.:

```
State of the system:
  buttonP : boolean //whether e-brake button is pressed
  sBrake : boolean // whether smart brake is active
  eBrake : boolean // whether e brake on all wheels is active
  carHiSpeed : boolean // whether car's speed is high
  gearParked : boolean // whether the car is parked

invariants:
  inv. carHiSpeed ^ buttonP -> sBrake ^ ¬eBrake
  inv. (¬carHiSpeed ^ buttonP) V gearParked -> ¬sBrake ^ eBrake
  inv. ¬buttonP -> ¬sBrake ^ ¬eBrake
```

explanation of the variables:

```
* controlled by user:
  * buttonP
  * gearParked
* sensed ; read from sensor:
  * carHiSpeed
```