

CS5103 Project II

For this project, you will use NuSMV to verify that a small software system satisfies certain desired properties specified in LTL. You will work in groups. The project has two deliverables, including a comprehensive report as well as the NuSMV code. The report will document the design of the system, the verification results you have obtained, and the experience you have gained.

Possible systems that you can choose to verify include

1. An elevator control system (See enclosed description)
2. A traffic light control system (See enclosed description)
3. A non-trivial software or hardware system related to your research.

Due date: May 8, 2014. Every group will demonstrate the project on May 8, 3:15 – 5:45pm.

I. An elevator control system

You will specify the behavior of a software system to be installed to control a simple elevator system. The elevator services a three-floor building. Inside the elevator there are request buttons, one for each floor. If the user inside the elevator presses a button, the elevator will visit the corresponding floor and open its doors.

- button1: tell the elevator to go to floor 1
- button2: tell the elevator to go to floor 2
- button3: tell the elevator to go to floor 3

Floor 1 and floor 3 each has a request button that a user presses to command the elevator to come to that floor and to open its doors. Floor 2 has two request buttons to indicate which direction (up or down) the user will want to be taken once they are inside the elevator.

- upF1: request at floor 1
- upF2: going-up request at floor 2
- downF2: going-down request at floor 2
- downF3: request at floor 3

If the elevator's doors open, they should stay open for five time units. The elevator has two buttons to open and close the doors. When any of these buttons is pressed, the button will light up until the request is responded.

- buttonOpen: request to open the door
- buttonClose: request to close the door

When any of these buttons is pressed, the button will light up until the request is responded. You should not make any assumptions about how much time it takes the elevator to move between floors.

At the very least, you should make sure that the following properties hold in your system.

1. Requests to be delivered to a particular floor are eventually serviced
2. The elevator never moves with its doors open

II. A traffic light control system

You will specify the software that will control the traffic lights at an intersection of two-way street running north and south intersects a two-way street running east and west. The goals are to design the system so that collisions are avoided and no traffic waits at a red light forever. There are four sensors for detecting whether cars are approaching the intersection from the four directions.

- at_n: cars approach the intersection from the north, ready to enter the intersection
- at_s: cars approach the intersection from the south, ready to enter the intersection
- at_w: cars approach the intersection from the west, ready to enter the intersection
- at_e: cars approach the intersection from the east, ready to enter the intersection,

The traffic-light control system generates four outputs with Boolean values that indicate whether a green light should be given to traffic in each of the four respective directions.

- n_light green light for traffic from the north
- s_light green light for traffic from the south
- w_light green light for traffic from the west
- e_light green light for traffic from the east

You might need to introduce more variables to help you develop a NuSMV model to specify the behavior of the traffic light control system.

At the very least, you should make sure that the following properties hold in your system.

1. Cars from any direction will eventually be given green lights
2. The lights in cross directions are never green at same time