Safety-Critical Systems I
WiSe 2010/2011

AG Betriebssysteme FB3
Prof. Dr. Jan Peleska, Florian Lapschies

Submission date: 2011-01-20

Exercise sheet 5

Motivated by our previous door/laser locking mechanism examples the working example of this exercise sheet is the laboratory lock depicted in figure 1:

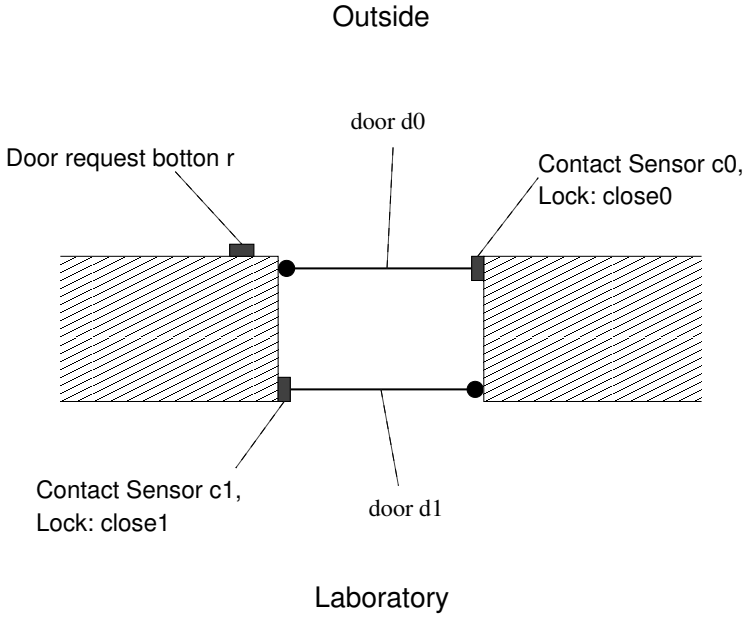

Figure 1: EUC: Door System

A laboratory room has a single entrance, a lock composed of two consecutive doors. Inside of the laboratory experiments are conducted that are potentially hazardous to humans. Each door d_0 and d_1 can be locked separately by an electro–mangnetic door lock. Applying electrical current to one of these door locks activates a magnet that lifts a metal bolt and thereby locks that door. If the current is released the door is unlocked. This setting has the advantage that no scientist is trapped inside the laboratory during a power outage. Notice, that the experiments conducted in that room require electrical power and immediately turn harmless in such a case. The locks are controlled by a single hardware controller that has the following inputs: An input r coming from a door–request button outside of the laboratory which is set iff the button is pressed. Contact sensors c_0 and c_1 that are set iff the door d_0 and d_1 are closed, respectively. By setting the outputs $close_0$ and $close_1$ the controller can lock the doors d_0 and d_1, respectively.

The door locking system should behave in the following way:

- For safety reasons only one scientist is allowed to be in the laboratory at a time.
- Both doors may never be unlocked or be open simultaneously.
- A scientist who wants to enter the laboratory has to press the door–request button. The controller then unlocks d_0 if no other scientist is in the laboratory or is currently entering it.
- After the scientist has passed and then closed d_0, the controller locks d_0 and unlocks d_1.

- The scientist then passes d_1 into the laboratory and then closes d_1. As long as the scientist is in the laboratory, d_1 remains unlocked.
- When the scientist finished his work in the laboratory he leaves by passing and then closing d_1. The controller then locks d_1 and unlocks d_0.
- After the scientist finally passed and then closed d_0, d_0 is locked again until the next door–request.

In addition the following assumption can be made:

- Initially, all doors are closed and locked, no scientist is in the laboratory or is entering it.
- Only one non claustrophobic scientist fits between d_0 and d_1.
- Once a scientist opens a door he actually passes that door. After that he closes it properly. In other words, he does not reconsider passing that door or likes opening doors for fun.

1 Circuit Design

Design the digital circuit for the door controller composed of *flip-flops*, *and*-, *or*- and *negation*-circuits.

2 Fault Tree Analysis

Perform a fault tree analysis of the laboratory lock controlled by your circuit design.