

Exercise 3

Modelling Safety-Critical Controllers

Aufgabe 1: Model-checking with FDR2

Perform a verification on the controller from the door locking mechanism example from the lecture slides (pp. 29–34). Copy the specifications from the physical model (EUC) and the controller, and define an appropriate watchdog process that triggers a deadlock as soon as a safety violation occurs. Then perform a deadlock analysis using FDR2.

Also show that your watchdog is capable of detecting these violations by modifying the controller accordingly.

Submit your solution to `florian(at)informatik.uni-bremen.de` and hand in a print-out in the session on Thursday, 9th of December.