Safety-Critical Systems I
WiSe 2010/2011

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

Abgabedatum: 14.02.2011

Bonus-Aufgabenblatt

Durch Abgabe einer Lösung für dieses Bonus-Aufgabenblatt wird das Übungsblatt mit der schlechtesten Benotung nicht berücksichtigt.

Modellprüfung mit CSP und mit FDR: Spiegelplattentreiber

Als Grundlage für die folgenden Teilaufgaben dient die CSP-Spezifikation `mirdd.csp` für einen fehlertoleranten Spiegelplattentreiber.

Spezifiziert im Stil des Testautomaten `WATCHDOG` vier neue Watchdogs `WATCHDOG1`, ... `WATCHDOG4`, die das System SYS1 hinsichtlich der folgenden Korrektheitseigenschaften validieren:

- Wenn der Spiegelplattentreiber einen Schreibauftrag für ein bestimmtes Datum auf einen bestimmten Track erhält, dann schreibt er nichts anderes auf die physikalischen Platten.
- Wann immer sich eine der Platten `DISK0`, `DISK1` im Zustand der Wiedereingliederung befindet (d. h., *nach* Auftreten des `repaired.d`-Events und *vor* Auftreten des `restored`-Events), wird von dieser Platte nicht gelesen.
- Am Ende einer erfolgreichen Wiedereingliederung sind alle Tracks während dieser Wiedereingliederung kopiert worden (d.h. bei einem `restored`-Event, seit dem letzten `repaired.d`-Event davor).
- Das Gesamtsystem gibt für einen Track immer denjenigen Wert bei einem Read zurück, der zuletzt dort geschrieben worden war. Wurde dort noch nichts geschrieben, wird 0 zurückgegeben.

Der Watchdog soll bei einer entdeckten Sicherheitsverletzung einen Deadlock erzeugen, der dann mit FDR gefunden werden kann.