RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL
INFORMATIK XI
SOFTWARE FÜR
EINGEBETTETE
SYSTEME

Professor Dr.-Ing. Stefan Kowalewski
Dipl.-Inform. Bastian Schlich

Aachen, 22. Juni 2005
SWS: V2/Ü1, ECTS: 4

Übung für

Formale Methoden für eingebettete Systeme

SoSe 2005

Blatt 4: Model Checking mit SPIN

Aufgabe 1: Alarm für eine Prozessanlage

In dieser Übungsaufgabe soll die Steuerungssoftware für eine Alarmanzeige einer Prozessanlage überprüft werden. Die Software läuft auf einer SpeicherProgrammierbaren Steuerung (SPS). Das Modell der Software haben Sie schon in der Vorlesung kennen gelernt und mit dem Model Checker SMV überprüft. In dieser Aufgabe sollen Sie nun den Model Checker SPIN benutzen. In Abbildung 1 ist der Funktionsblock der Alarmanzeige dargestellt. Folgendes Programm läuft auf der SPS:

```
VAR_IN  Gefahr, Quittung, Reset  : Bool
VAR_OUT Rot, Gelb  : Bool := FALSE
LD    Gefahr
S     Rot
LD    Quittung
S     Gelb
R     Rot
LD    Reset
ANDN  Gefahr
R     Gelb
```

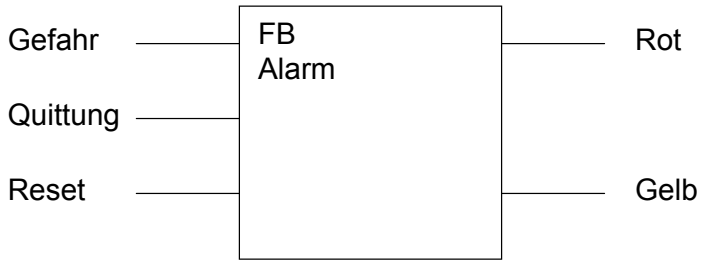

Abbildung 1: Funktionsblock Alarm

a) Modellieren Sie das Modell der Software in SPIN. Beachten sie dabei die Semantik der Programmiersprache Anweisungsliste (AWL) und das Verhalten einer SPS.

b) Überprüfen Sie, ob die folgenden Eigenschaften gelten. Übersetzten Sie dazu die Eigenschaften in eine LTL Formel.

- Bei Eintritt von Gefahr muss Rot angehen.
- Nach Quittung durch Bediener wird Rot ab- und Gelb eingeschaltet.
- Nach Bereinigen der Gefahr kann Gelb durch Reset gelöscht werden.

c) Bestehen die gefundenen Fehler auch in dem folgenden Programm? Beachten Sie dabei, dass `JMPC ENDE` dann zur Marke `ENDE:` springt, wenn die vorhergehende Auswertung true ergeben hat.

```
VAR_IN  Gefahr, Quittung, Reset  : Bool
VAR_OUT Rot, Gelb  : Bool := FALSE

LD    Gefahr
ANDN  Gelb
S     Rot
JMPC  ENDE

LD    Quittung
AND   Rot
S     Gelb
R     Rot
JMPC  ENDE

LD    Reset
ANDN  Gefahr
AND   Gelb
R     Gelb
JMPC  ENDE

ENDE:
```

d) Hat das zweite Programm andere Fehler? Wenn andere Fehler bestehen, schlagen Sie eine Lösung vor und verifizieren Sie diese.