

2.1

a)

Der Benutzer versucht sich nochmals anzumelden, obwohl er schon angemeldet ist.

2.3

b)

Der Verifikationsversuch schlägt fehl wegen des Interleaving des Watchdogs. Der Fehler entsteht, wenn der Watchdog die Assertion überprüft, wenn Authentication den fail auf 3 erhöht hat, aber die currentState noch nicht auf 2 gesetzt wurde.

3

b)

Der Fehler beschreibt die Situationen wenn Autos von allen Richtungen kommen und es deswegen kein Auto gibt, welches fahren kann nach der oben genannten Regel.

4

a)

8191 konsekutive Ausführung von p.1 gefolgt von p.2 und q.1

b)

Ausgabe:

Verification result: error: max search depth too small
---

Da die Prozesse p und q unendlich laufende Do-Schleifen haben wird die Searchspace unendlich groß. Damit spin aber terminiert, wird eine maximale Tiefe angegeben. Wird der Fehler nicht innerhalb dieser Suchtiefe gefunden, gibt spin keine Fehlermeldung aus.

c)

spin bricht bei der Suche nach Gegenbeispielen ab, wenn die Suche ein bestimmte Tiefe erreicht wird. Die Tiefensuch würde dann bei einem Modell, die sehr(auch unendlich) lange Pfade hat, bei dem ersten Pfad, dessen Länge, die max. Tiefe überschreitet, die Suche abbrechen. Dies hat zur Folge, dass nicht alle Pfade, dessen Länge kleiner als die max. Tiefe

ist, abgesucht wird. Bei der Breitensuche werden alle Pfade abgetastet, welches der Grund dafür ist, dass spin das Gegenbeispiel finden konnte. Stellt man spin so ein, dass spin nicht bei dem ersten Gegenbeispiel die Suche abbricht, so meldet spin den folgenden Fehler:

error: max search depth too small

d)

Für die max. Tiefe von 8190 findet spin keinen Gegenbeispiel.

Für max. Tiefen  $> 8190$  finde spin immer das kürzeste Gegenbeispiel und je nach Tiefe auch andere Beispiele.