Universität Bremen

Systeme hoher Sicherheit und Qualität WiSe 26/27

Serge Autexier
Christoph Lüth

3. Übungsblatt

Ausgabe: 28.10.26
Abgabe: 04.11.26

3.1 *Safety und Liveness (Hyper-)Properties*

Welcher Kategorie (Safety Property, Safety Hyperproperty, Liveness Property, Liveness Hyperproperty) ordnen Sie folgende Eigenschaften von Systemen zu:

(1) Die zentralen Sicherheitshinweise lassen sich auf der Steuerungskonsole der automatischen Fertigungsstraße einsehen.

(2) Der am Roboterarm befestigte Bohrer überschreitet die Höchsttemperatur von 600°C nicht.

(3) Solange der Reaktor nicht vollständig heruntergefahren ist bleibt das Kühlsystems uneingeschränkt aktiv.

(4) Je nach Zusammensetzung des Brennstoffes werden zwischen 1 und 1,5 Tonnen/Stunde in Wärmeenergie umgewandelt.

(5) Nach Betätigung des Notknopfes muss die Maschine zum Stillstand kommen.

3.2 *Wäsche Waschen*

Wir wollen eine Waschmaschine bauen (Abbildung 1). Die Waschmaschine soll zu jedem Zeitpunkt folgendes können:

- Die Tür öffnen und schließen;
- Das Wasser einlassen und abpumpen;
- Den Waschgang durchführen (30, 60, oder 90 Grad);
- Den Vorwaschgang durchführen;
- Schleudern.

Die Waschmaschine wird sehr einfach konstruiert (um Kosten zu sparen), deshalb kann beispielsweise die Tür jederzeit geöffnet werden (das ist vielleicht keine gute Idee, soll aber modelliert werden). Auch sonst sind konstruktiv keine Abhängigkeiten der Operationen vorhanden.

1. Modellieren Sie die Waschmaschine als endlichen Zustandsautomaten. Was sind die Zustände, was sind die möglichen Zustandsübergänge?
2. Vermutlich sollte man während des Waschens nicht die Tür öffnen, und vorzugsweise sollte auch während des Waschens Wasser in der Maschine sein. Formulieren Sie solche und ähnliche Eigenschaften als *(Hyper-)Properties*. Geben Sie an, ob es sich um Safety oder Liveness (Hyper-)Property handelt, und finden Sie je eine von jeder Sorte (soweit möglich).



Quelle: Frank C. Müller, via Wikimedia Commons

Abbildung 1: Waschmaschine (Symbolbild).