SVP / THP2 WiSe 14	Praktikum 2 (Prüfungsvorleistung)	Prof. Dr. B. Buth 17.10.2014

1 Refinement - Traces und Failures

1.1 Verifikation mit Refinement

Gegeben seien die folgende CSP-Prozessdefinitionen (machine-readable CSP):

```
1  max = 3
2  nametype Data = {1..2}
3  channel push, pop: Data
4  STACK1 = push?d -> pop!d -> STACK1
5  STACK3(<>) = push?d -> STACK3(<d>)
6  STACK3(<h>^s) =
7     pop!h -> STACK3(s)
8     []
9    (#s < (max-1)) & push?d -> STACK3(<d>^<h>^s)
```

Welche der folgenden Zusicherungen gelten, welche nicht?
Geben Sie für geltende Bedingungen mindestens eine informelle Begründung, für nicht geltende Bedingungen eine Begründung oder ein Gegenbeispiel mit Erläuterung an:

a) `assert STACK1 [T= STACK3(<>)`

b) `assert STACK3(<>) [T= STACK1`

c) `assert STACK1 [F= STACK3(<>)`

d) `assert STACK3(<>) [F= STACK1`

Vorgehen:

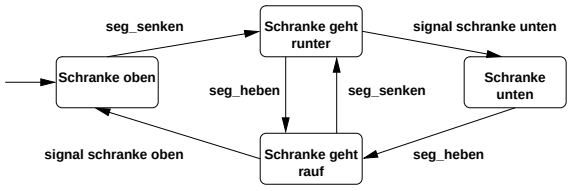
a) Besprechen Sie die Spezifikation im Team und in der Praktikumsgruppe

b) Erläutern Sie die Ergebnisse der Prüfungen im Praktikumstermin

2 CSP Spezifikation

2.1 Schrankenanlage

Spezifizieren Sie in CSP ein Prozess-System, das einen Schrankenübergang eines Eisenbahnnetzes modelliert. Der Schrankenübergang besteht aus einem gesicherten Gleisabschnitt, einer zweispurigen Straße und einer Schrankensteuerung mit je zwei Schrankensegmenten für die linke und die rechte Straßenseiten. Der gesicherte Gleisabschnitt kann nur aus einer Richtung befahren werden (vereinfachte Annahme) und wird durch ein Signal für kommende Züge bewacht; das Signal steht auf rot, wenn ein Zug nicht in den Abschnitt einfahren kann, ansonsten auf grün. Die Durchfahrt eines Zuges wird durch zwei weitere Ereignisse für den Eintritt und den Austritt aus dem gesicherten Abschnitt beobachtet.
Ein einzelnes Schrankensegment bewegt sich entsprechend dem folgenden Automaten:



Ein erfolgreiches Durchfahren des Schrankenabschnitts erfolgt in den folgenden Schritten:

- Wenn ein Zug sich dem Übergang nähert (Ereignis zug_kommt), ist das Signal rot. Der Zug sendet eine Durchfahrtsanfrage (df_anfrage) an die Schrankensteuerung.

- Wenn die Schrankensteuerung eine Durchfahrtsanfrage erhält, werden zunächst die rechten Schrankensegmente aus Fahrtrichtung der Fahrspuren gesenkt.
- Erst wenn die rechten Segmente der Schranken unten sind (Signal seg_unten), werden auch die linken Segmente gesenkt.
- Wenn alle vier Segmente unten sind, wird das Durchfahrtssignal für den anfragenden Zug auf grün geschaltet und der Zug erhält die Durchfahrtfreigabe (df_freigabe)
- Bei Einfahrt eines Zuges in den geschützten Gleisabschnitt wird zunächst das Eintrittsereignis (zug_rein) ausgelöst, bei Verlassen des Abschnitts das Austrittsereignis (zug_raus).In der Abstraktion können wir davon ausgehen, dass der Zug diese Ereignisse an die Steuerung sendet.
- Nach dem Eintrittsereignis wird das Signal wieder auf rot gesetzt.
- Wenn nach einem Eintrittsereignis das Austrittsereignis aufgetreten ist, wird das Durchfahrtsignal wieder auf rot gesetzt und anschließend alle Schrankensegmemente gleichzeitig geöffnet.
- Ein nachfolgender Zug kann das Öffnen der Schranke unterbrechen und die Schranke sich wieder schließen lassen - allerdings nur, wenn der vorausfahrende Zug den gesicherten Abschnitt verlassen hat.

Spezifizieren Sie CSP Prozesse für

- die Schrankensegmente entsprechend dem obigen Automaten: SEGMENT (...) =
- die Steuerung: STEUER (...) =
- das Signal: SIGNAL (...) =
- Züge: ZUG (id) =
- den Gesamtprozess des Schrankenübergangs mit 2 Zügen

und verwenden Sie dabei die folgenden Datentypen und Kanäle:

```
nametype ZId = {0,1,2,3}
nametype SegId = {l1,l2,r1,r2} ;; links 1 und 2, rechts 1 und 2
nametype SigStates = {r, g} ;; Signalzustand rot, grün
nametype SegState = {unten, oben, senken, heben };; Segmentzustand
channel zug_kommt, zug_rein, zug_raus: ZID
channel df_anfrage, df_freigabe: ZID ;; Durchfahrt Anfrage und Freigabe
channel seg_senken, seg_heben, seg_unten, seg_oben: SegId
```

Modellieren Sie das Prozesssystem und entwickeln Sie Prüfungen für die folgenden Eigenschaften:

- Züge fahren nur wenn die Schranken alle unten sind
- Kein Zug wird dauerhaft blockiert.

Präsentieren und diskutieren Sie die Modellierung und die Prüfungen sowie deren Ergebnisse im Praktikumstermin.
Anmerkung: das Spezifikationsskelett findet sich in der Datei `schranken-skelett.csp`

Bearbeitungszeitraum: Praktikumstermin 2

Die Bearbeitung der Aufgaben soll in den Teams von 3-4 Personen erfolgen, Diskussion in der gesamten Praktikumsgruppe
Abgabe der csp-Datei von 2.1 per email mit Betreff

`[SVP] Praktikum2, Aufgabe 2`