

Kapitel 7

Sicherheitseigenschaften

Prof. Dr. Rolf Hennicker

20.06.2013

7.1 Der Begriff der Sicherheitseigenschaft

Sicherheitseigenschaften (“safety properties”) drücken aus, dass während der Ausführung eines parallelen Programms “nichts Schlechtes“ passiert.

Sicherheitseigenschaften können formuliert werden durch:

1. Angabe der illegalen Abläufe: “Was nicht passieren darf!”
2. Angabe der legalen Abläufe: “Was passieren darf!” (aber deshalb noch nicht passieren muss)

Das Komplement der legalen Abläufe sind die illegalen Abläufe. Häufig ist es einfacher (und auch sicherer) die legalen Abläufe anzugeben. In FSP geschieht dies durch “Property-Prozesse“.

7.2 Property-Prozesse

Definition:

Ist P ein Prozessidentifikator und E ein Prozessausdruck, dann ist

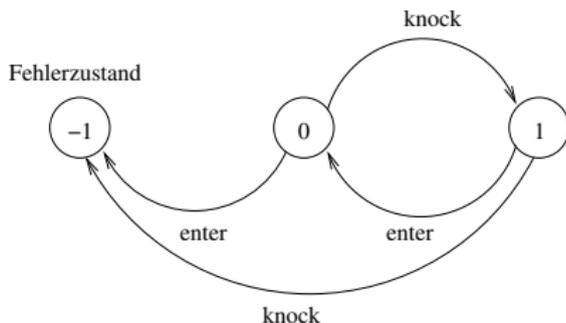
property $P = E$.

eine *Property-Prozessdeklaration*. Die Deklaration ist rekursiv, wenn P in dem Ausdruck E frei vorkommt, d.h. $P \in FV(E)$.

Beispiel:

property POLITE = (knock \rightarrow enter \rightarrow POLITE).

Im LTS eines Property-Prozesses werden die illegalen Abläufe offenbart.



Semantik von Property-Prozessen

Sei $T = (S, A, \Delta, q_0)$ ein LTS (wie bisher).

Die Property-Vervollständigung von T ist definiert durch:

$$\text{property}_{\text{LTS}}(T) =_{\text{def}} (S \cup \{\pi\}, A, \Delta', q_0)$$

wobei

- ▶ π ein (neuer) ausgezeichneter Fehlerzustand ist und
- ▶ $\Delta' = \Delta \cup \{(s, a, \pi) \mid s \in S, a \in A, \nexists s' \in S : (s, a, s') \in \Delta\}$.

Sei $\text{property } P = E$. eine Deklaration eines Property-Prozesses.

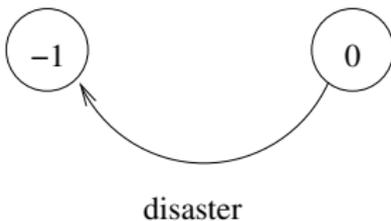
Dann ist

$$\text{Its}(P) =_{\text{def}} \begin{cases} \text{property}_{\text{LTS}}(\text{Its}(E)) & \text{falls } P \notin \text{FV}(E) \\ \text{property}_{\text{LTS}}(\text{Its}(\text{rec}(P=E))) & \text{sonst} \end{cases}$$

Bemerkungen:

1. Fehlerzustände können explizit in FSP-Prozessausdrücken repräsentiert werden durch den vordefinierten (konstanten) Prozess ERROR.
2. Es ist auch möglich zu spezifizieren, dass eine bestimmte Aktion niemals in einem Ablauf vorkommen darf, z.B.

property CALM = STOP + {disaster}.



7.3 Erfüllung von Sicherheitseigenschaften

Generelle Voraussetzung:

Property-Prozesse sind *deterministisch* (d.h. es gibt keinen Zustand, von dem ausgehend es mehr als eine Transition mit derselben Aktion gibt) und sie enthalten keine verborgenen Aktionen.

Legale Aktionsfolgen:

Sei P ein Property-Prozess und w eine endliche oder unendliche Aktionsfolge über dem Alphabet αP . w ist eine *legale Aktionsfolge bzgl. P* , wenn kein endlicher Anfang von w im LTS von P zum Fehlerzustand führt.

Ablaufeinschränkung:

Sei w eine endliche oder unendliche Aktionsfolge über einem Alphabet A und sei $B \subseteq A$. Entfernt man aus w alle Aktionen aus A , die nicht zu B gehören, so erhält man die *Einschränkung* von w auf B , bezeichnet mit $w|_B$.

Definition (Erfüllung von Sicherheitseigenschaften):

Sei P ein Property-Prozess und Q ein (gewöhnlicher) FSP-Prozess mit $\alpha P \subseteq \alpha Q$. Q *erfüllt* die Sicherheitseigenschaft P , geschrieben $Q \models P$, wenn für alle Abläufe w von Q die Einschränkung $w|_{\alpha P}$ eine legale Aktionsfolge bzgl. P ist.

Beispiele:

1. Sei

$$\text{VISITOR} = (\text{knock} \rightarrow \text{enter} \rightarrow \text{discuss} \rightarrow \text{VISITOR}).$$

VISITOR erfüllt die Sicherheitseigenschaft POLITE.

2. Sei

$$\text{WRONG_VISITOR} =$$

$$(\text{knock} \rightarrow \text{enter} \rightarrow \text{discuss} \rightarrow \text{enter} \rightarrow \text{WRONG_VISITOR}).$$

WRONG_VISITOR erfüllt die Sicherheitseigenschaft POLITE nicht.

3. Sei Q ein beliebiger FSP-Prozess mit $\text{disaster} \in \alpha(Q)$ und $\text{property CALM} = \text{STOP} + \{\text{disaster}\}$.

Q erfüllt CALM genau dann, wenn in keinem Ablauf von Q die Aktion "disaster" vorkommt.

7.4 Nachweis von Sicherheitseigenschaften

Vorbemerkung: Bei der parallelen Komposition von LTSsen werden alle Zustände der Form (s, π) identifiziert mit dem Fehlerzustand π .

Beispiel (WRONG_VISITOR):

(WRONG_VISITOR||POLITE) hat das LTS

Beispiel (VISITOR):

(VISITOR||POLITE) hat das LTS

Intuition:

Gegeben sei ein Prozess Q und ein Property-Prozess P mit $\alpha P \subseteq \alpha Q$. Sei w ein beliebiger Ablauf von Q . Durch die parallele Komposition von Q mit dem Property-Prozess P wird jede Aktion in w , die auch im Alphabet von P vorkommt, im LTS von P in eindeutiger Weise (da P deterministisch) begleitet (durch Aktionssynchronisation). Erreicht man auf diese Weise den Fehlerzustand, dann ist $w|_{\alpha P}$ ein illegaler Ablauf (bzgl. P) und umgekehrt.

Satz 1:

Sei P ein Property-Prozess und Q ein (gewöhnlicher) FSP-Prozess mit $\alpha P \subseteq \alpha Q$ und $\pi \notin \text{Its}(Q)$. $Q \models P$ **genau dann, wenn** in $\text{Its}(Q \parallel P)$ der Fehlerzustand nicht erreichbar ist.

Automatisches Checken von Sicherheitseigenschaften:

Durch Breitensuche im LTS von $(Q \parallel P)$ nach Erreichbarkeit des Fehlerzustands kann entschieden werden, ob ein Prozess Q eine Sicherheitseigenschaft P erfüllt oder nicht.

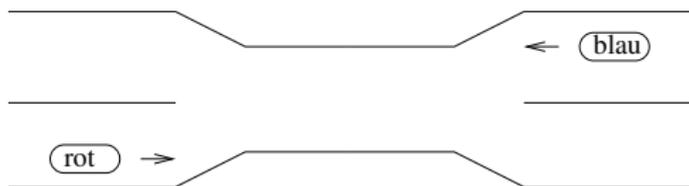
Bemerkung:

Seien P und Q wie in Satz 1. $Q \models P$ genau dann, wenn $(Q \parallel P) \sim Q$.

Entwicklungsmethodik für Programme mit Parallelität

1. Spezifikation der gewünschten Eigenschaften (Sicherheits- und Lebendigkeitseigenschaften) mit FSP.
2. Modellierung eines Entwurfs mit FSP.
3. Nachweis, dass das Entwurfsmodell deadlockfrei ist und die spezifizierten Eigenschaften erfüllt.
4. Java-Implementierung mit Threads und Monitoren gemäß des angegebenen Schemas zur Überführung von FSP-Entwurfsmodellen nach Java.

7.5 Beispiel: Einspurige Brücke



Sicherheitseigenschaft:

Rote und blaue Autos dürfen nicht gleichzeitig über die Brücke fahren.

Modellierung der Grundkonzepte (des Problembereichs):

```
const N = 3      // Anzahl Autos pro Seite
range ID = 1..N
```

CAR = (enter → exit → CAR).

|| CONVOY = [ID]:CAR.

|| CARS = (red:CONVOY || blue:CONVOY).

1. Spezifikation der Sicherheitseigenschaft:

$$\text{property ONEWAY} = (\text{red[ID].enter} \rightarrow \text{RED}[1] \\ | \text{blue[ID].enter} \rightarrow \text{BLUE}[1]),$$

$$\text{RED}[i:\text{ID}] = (\text{red[ID].enter} \rightarrow \text{RED}[i+1] \\ | \text{when } (i==1) \text{ red[ID].exit} \rightarrow \text{ONEWAY} \\ | \text{when } (i>1) \text{ red[ID].exit} \rightarrow \text{RED}[i-1]),$$

$$\text{BLUE}[i:\text{ID}] = (\text{blue[ID].enter} \rightarrow \text{BLUE}[i+1] \\ | \text{when } (i==1) \text{ blue[ID].exit} \rightarrow \text{ONEWAY} \\ | \text{when } (i>1) \text{ blue[ID].exit} \rightarrow \text{BLUE}[i-1]).$$

ONEWAY besagt, dass wenn immer ein rotes (bzw. blaues) Auto auf der Brücke ist, nur ein rotes (bzw. blaues) Auto auf die Brücke fahren darf.

Bemerkung:

ONEWAY modelliert eine Anforderung (bzgl. Sicherheit) und *keinen* Entwurf.

2. Modellierung eines Entwurfs:

Zur Kontrolle der Brücke wird ein Monitor verwendet.

range T = 0..N

BRIDGE = BRIDGE[0][0],

BRIDGE[nr:T][nb:T] =

(when (nb==0) red[ID].enter → BRIDGE[nr+1][nb]

| red[ID].exit → BRIDGE[nr-1][nb]

| when (nr==0) blue[ID].enter → BRIDGE[nr][nb+1]

| blue[ID].exit → BRIDGE[nr][nb-1]).

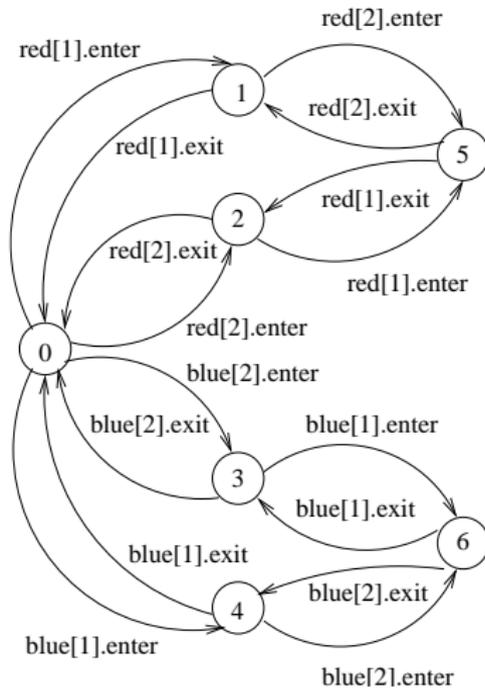
Modell des Gesamtsystems:

||SYS = (CARS || BRIDGE).

3. Nachweis der Sicherheitseigenschaft:

Wir betrachten das LTS von (SYS || ONEWAY) und checken, dass der Fehlerzustand nicht erreichbar ist.

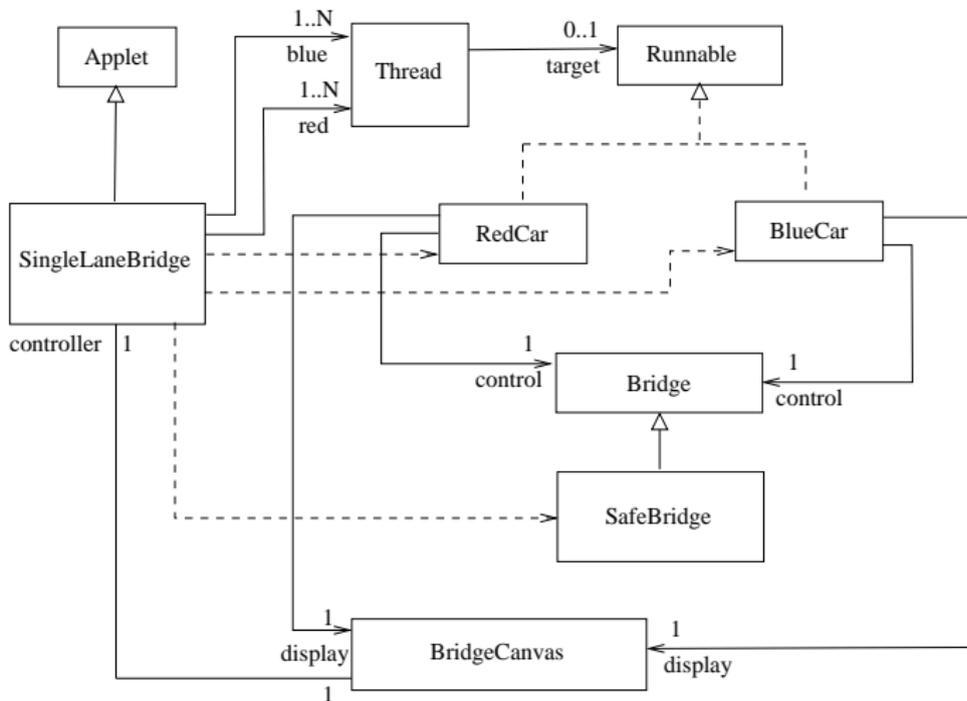
LTS von $SYS = (CARS \parallel BRIDGE)$ für $N=2$:



4. Implementierung in Java:

Aktive Objekte: rote und blaue Autos

Passives Objekt: Brücke



Java-Code (Auszug):

```
public class SingleLaneBridge extends Applet {
    BridgeCanvas display;
    int maxCar;
    ...
    Thread[] red; // roter Convoy
    Thread[] blue; // blauer Convoy
    ...
    public void start() {
        red = new Thread[maxCar];
        blue = new Thread[maxCar];
        Bridge b = new SafeBridge();
        ...
        for (int i=0; i<maxCar; i++) {
            red[i] = new Thread(new RedCar(b,display,i));
            blue[i] = new Thread(new BlueCar(b,display,i));
            red[i].start();
            blue[i].start();
        }
    }
}
```

```
class Bridge { // unsafe
    synchronized void redEnter() { }
    synchronized void redExit() { }
    synchronized void blueEnter(){ }
    synchronized void blueExit() { }
}

class SafeBridge extends Bridge {
    private int nred = 0; // red cars on bridge
    private int nblue = 0;

    synchronized void redEnter() throws InterruptedException {
        while (nblue>0) wait();
        nred++;
    }
    synchronized void redExit() {
        nred--;
        if (nred==0) notifyAll();
    }
    synchronized void blueEnter() throws InterruptedException {
        while (nred>0) wait();
        nblue++;
    }
    synchronized void blueExit() {
        nblue--;
        if (nblue==0) notifyAll();
    }
}
```

```
class RedCar implements Runnable {
    BridgeCanvas display;
    Bridge control;
    int id;

    RedCar(Bridge b, BridgeCanvas d, int id) {
        control = b;
        display = d;
        this.id = id;
    }

    public void run() {
        try {
            while (true) {
                while (!display.moveRed(id)); // not on bridge
                control.redEnter();
                while (display.moveRed(id)); // move over bridge
                control.redExit();
            }
        } catch (InterruptedException e) {}
    }
}
```