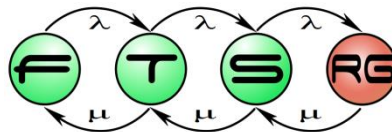


# Überprüfung der Modelle

**Budapest University of Technology and Economics**  
**Fault Tolerant Systems Research Group**



# Ariane 5 Trägerrakete

- Die leistungsfähigste europäische Trägerrakete



# Ariane 5 Trägerrakete

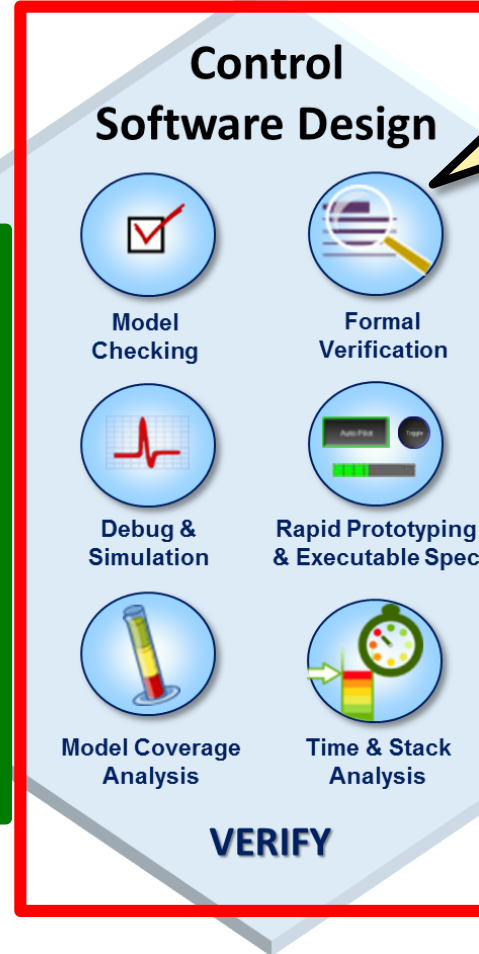
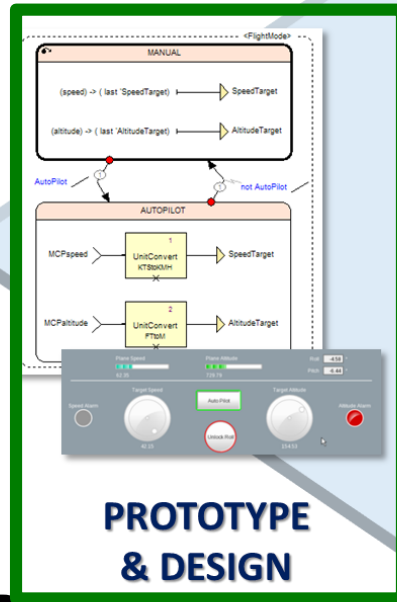
- Am 4. Juni 1996 hat die Rakete sich 37 Sekunden nach dem Start zerstört
  - die gelieferten vier Cluster-Satelliten sind auch zerstört worden
  - \$370 Millionen Verlust



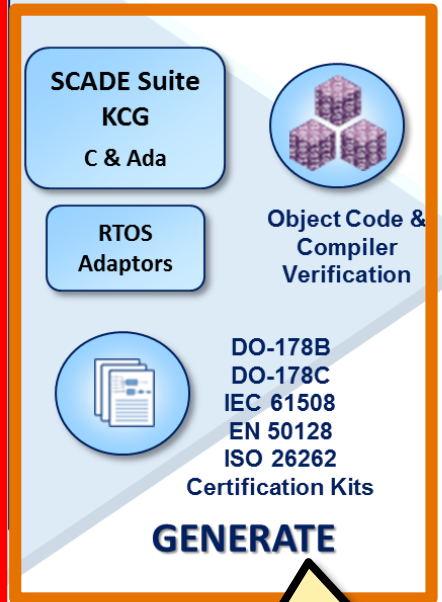
# Ariane 5 Trägerrakete

- Am 4. Juni 1996 hat die Rakete sich 37 Sekunden nach dem Start zerstört
  - die gelieferten vier Cluster-Satelliten sind auch zerstört worden
  - \$370 Millionen Verlust
- Einer der teuersten Softwarefehler der Welt
  - primäre Ursache:
    - erfolglose Konversion einer Zahl von 64 Bit zu 16 Bit
  - sekundäre Ursache:
    - Die Modulen wurden nie zusammen getestet**

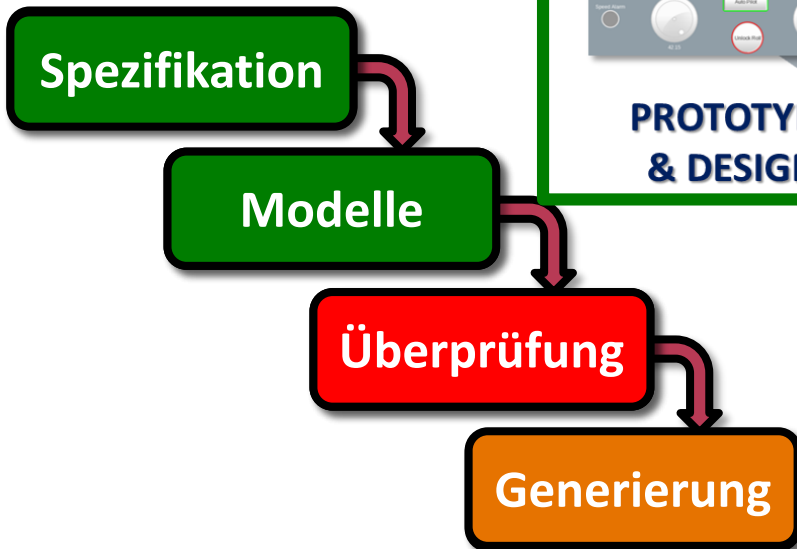
# Beispiel: Esterel SCADE



**Überprüfung der Modelle**



Flugzeuge, kritische ES, Automotive



Grundbegriffe

Stat. Überprüfung

Testen

Formale Verifikation

# INHALT

# Lebenszyklus der Modelle

Entwicklung  
von Modellen

Software-  
Entwicklung

Anforderungen,  
Spezifikation

Anforderungen,  
Spezifikation

Ausgangsmodelle

Entwurf

detailliertere  
Modelle

Implementation

Überprüfung

Testen

Wartung

Wartung

```
97 m_nFN = float.PositiveInfinity;
98 return;
99 }
100 m_nFN = (ro / (1-ro)) * (1- (ro*(float-1)
101 m_nFN = ro*ro / (2*(1-ro));
102 m_nFD = m_nFN/lambda;
103 m_nFW = m_nFN/lambda;
104 }
105 }
106 }
107 }
108 m_nFN = float.PositiveInfinity;
109 m_nFN = float.PositiveInfinity;
110 m_nFD = float.PositiveInfinity;
111 m_nFW = float.PositiveInfinity;
112 return;
113 }
114 m_nFN = (ro / (1-ro)) * (1- (ro*(float-1)
115 m_nFN = (lambda*lambda/(k*mu*mu) * ro*ro)
116 m_nFD = m_nFN / lambda;
117 m_nFW = ((float-1) / (2*k(float-1)) * ro /
118 }
119 }
120 }
121 }
122 }
123 }
124 }
125 }
126 }
127 }
128 }
129 }
130 }
131 }
132 }
133 }
134 }
135 }
136 }
137 }
138 }
139 }
140 }
141 }
142 }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 }
151 }
152 }
153 }
154 }
155 }
156 }
157 }
158 }
159 }
160 }
161 }
162 }
163 }
164 }
165 }
166 }
167 }
168 }
169 }
170 }
171 }
172 }
173 }
174 }
175 }
176 }
177 }
178 }
179 }
180 }
181 }
182 }
183 }
184 }
185 }
186 }
187 }
188 }
189 }
190 }
191 }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 }
200 }
201 }
202 }
203 }
204 }
205 }
206 }
207 }
208 }
209 }
210 }
211 }
212 }
213 }
214 }
215 }
216 }
217 }
218 }
219 }
220 }
221 }
222 }
223 }
224 }
225 }
226 }
227 }
228 }
229 }
230 }
231 }
232 }
233 }
234 }
235 }
236 }
237 }
238 }
239 }
240 }
241 }
242 }
243 }
244 }
245 }
246 }
247 }
248 }
249 }
250 }
251 }
252 }
253 }
254 }
255 }
256 }
257 }
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
```





# Automatische Kodengenerierung

Entwicklung  
von Modellen

Software-  
Entwicklung

Anforderungen,  
Spezifikation

Anforderungen,  
Spezifikation

Ausgangsmodelle

detailierte Modelle

Implementation

Testen

Überprüfung

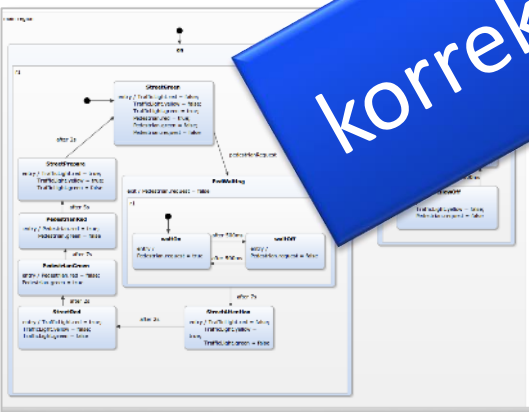
Wartung

Wartung

korrektes Modell, korrekterer Code

```
import java.util.Vector;
import java.util.Hashtable;
import java.awt.*;
import java.awt.event.*;

public class InternetClient implements Serializable
{
    private Socket socket;
    private ObjectInputStream objectIn;
    private ObjectOutputStream objectOut;
    // Creates a connection to the internet
    public InternetClient(int port, String message)
    {
        // Connection to
        // To read object
        // To write object
        // Int
        // Int
        // Mess
    }
}
```





Grundbegriffe

Stat. Überprüfung

Testen

Formale Verifikation

# GRUNDBEGRIFFE

# Modelle und Aufgaben

- **Synthese:**

*Entspricht das Modell  
der Spezifikation?*



- **Analyse:**

*Wie ist das Verhalten  
des Modelles?*



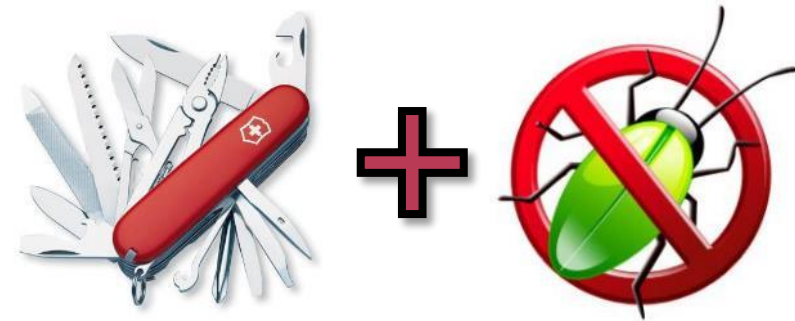
- **Steuerung:**

*Wie ist der gewünschte  
Zustand erreichbar?*



# Korrektheit

- Die **Korrektheit** ist die Fähigkeit des Modell oder Kode, dass es den gegenüber ihm gestellten Anforderungen entspricht.
  - **funktionale Korrektheit:** Das Entsprechen den funktionalen Anforderungen
  - Über Prüfung der nichtfunktionalen Anforderungen (siehe die Vorlesungen über Leistungsmodellierung)
- **Aspekte:**
  - Erfüllung der Aufgabe
  - Fehlerfreiheit, Sicherheit
  - Kein verbotenes Verhalten



# Klassifizierung der funktionalen Anforderungen

- **Erlaubtes Verhalten** (z.B. safety)
  - Welche Zustände darf das System (nicht) aufnehmen?
  - Was für Verhalten sind verboten?
  - Universelle Anforderungen
    - sollen immer wahr sein
- **Erwartetes Verhalten** (z.B. liveness)
  - Welche Zustände sollen erreichbar sein?
  - Welche Funktionen soll das System leisten können?
  - Existenzielle Anforderungen
    - sollen immer erreichbar sein

# Klassifizierung der funktionalen Anforderungen

## ■ Erlaubtes Verhalten (z.B. safety)

- Welche Zustände darf das System (nicht) aufnehmen?
- Was für Verhalten sind verboten?
- Universelle Anforderungen
  - sollen immer wahr sein

„Die Verkehrsampeln einer Kreuzung **dürfen nie** gleichzeitig grün sein.“

## ■ Erwartetes Verhalten (z.B. usability)

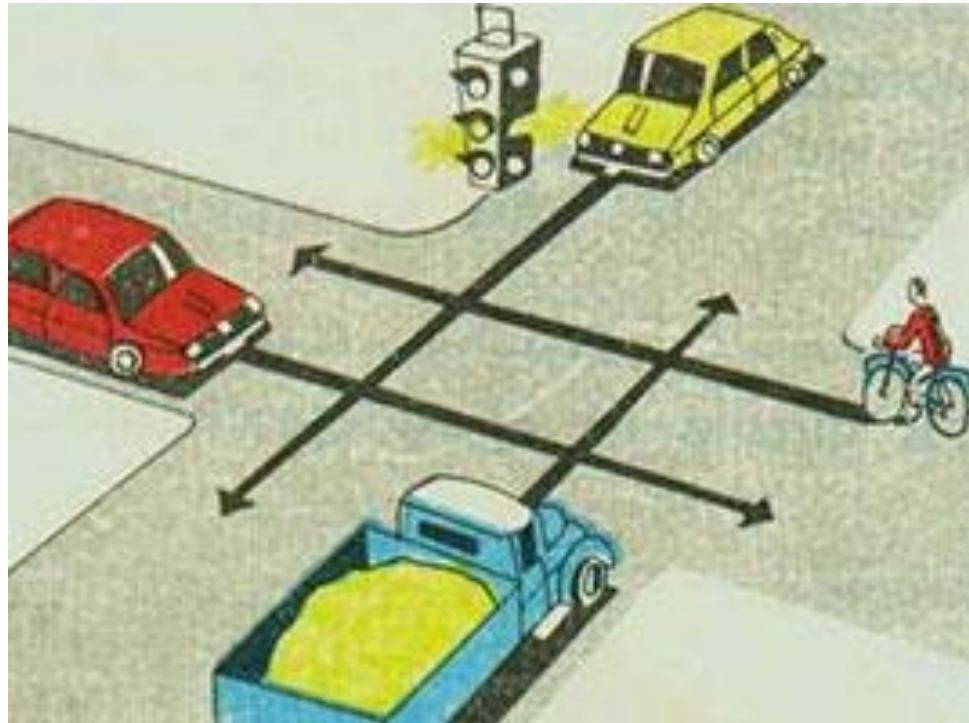
- Welche Zustände sollen erreichbar sein?
- Welche Funktionen soll das System leisten?
- Existenzielle Anforderungen
  - sollen immer erreichbar sein

„Die Verkehrsampel **soll immer fähig sein** auf grün zu wechseln.“

# Verklemmung (deadlock)

**Verklemmung:** Eine Zustandsmenge, aus der das System ohne äußeren Eingriff nicht weiterrreten kann.

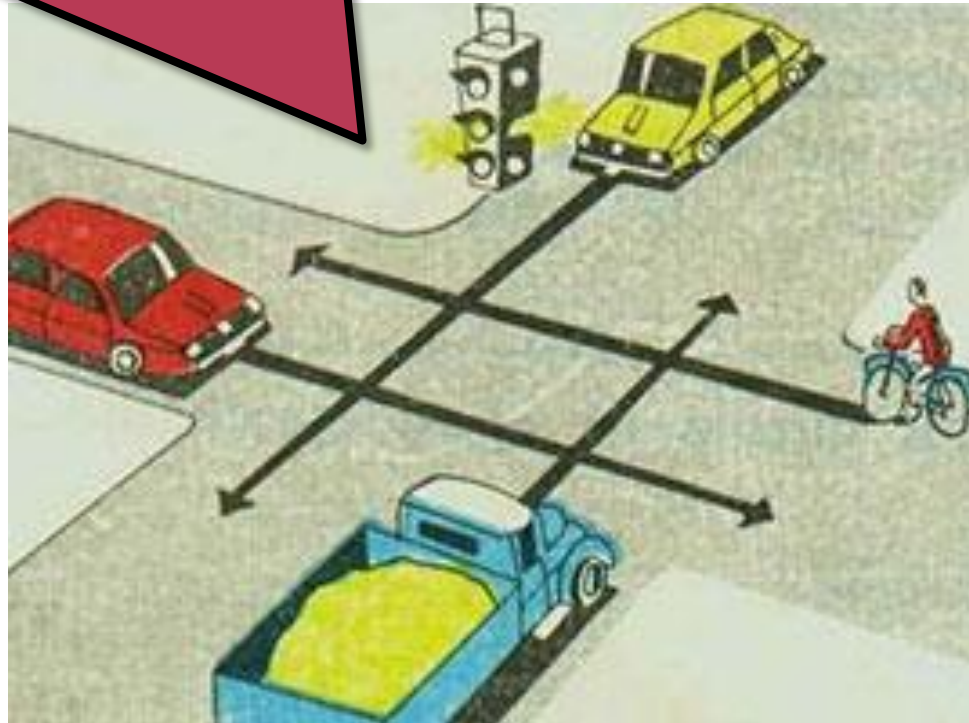
- z.B. aufeinander wartende Prozesse



# Verklemmung (deadlock)

„Fahrzeuge, die von rechts kommen, haben, sofern die folgenden Absätze nichts anderes bestimmen, den Vorrang; Schienenfahrzeuge jedoch auch dann, wenn sie von links kommen.“

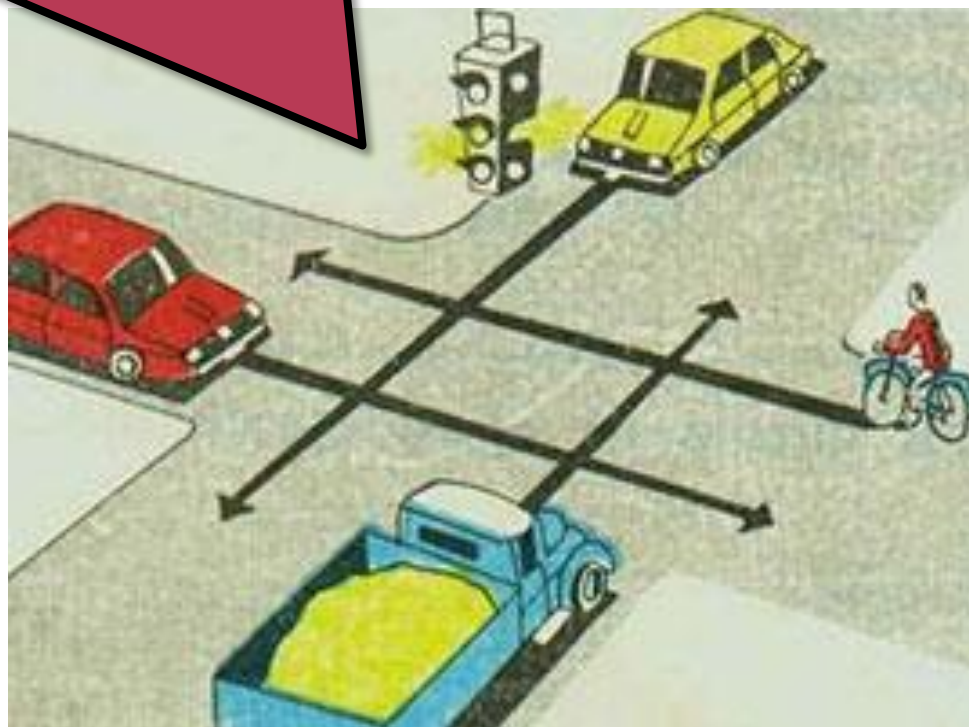
(Straßenverkehrsordnung §19 Abs. 1)





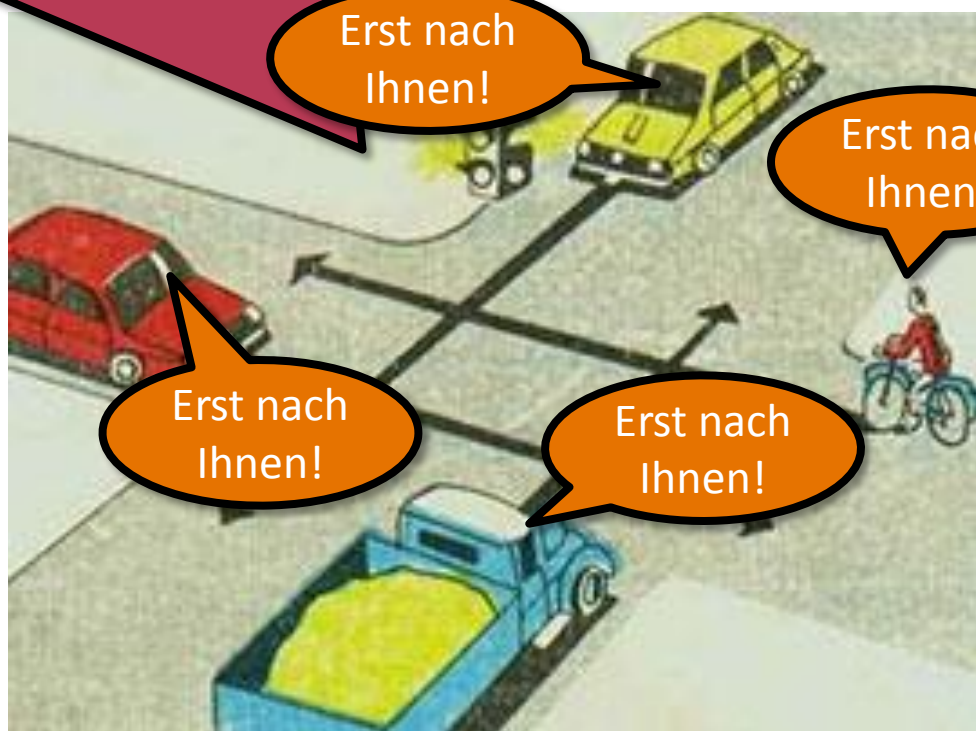
# Auflösung einer Verklemmung

„Wenn 4 Fahrzeuge in einer Kreuzung mit Rechtsvorrang gleichzeitig ankommen, soll irgendeiner der Fahrer auf seinen Vorrang verzichten. Ansonsten werden sie laut StVO ewig stehenbleiben.“  
(gyakorikerdesek.hu)



# Auflösung einer Verklemmung

„Wenn 4 Fahrzeuge in einer Kreuzung mit Rechtsvorrang gleichzeitig ankommen, soll irgendeiner der Fahrer auf seinen Vorrang verzichten. Ansonsten werden sie laut StVO ewig stehenbleiben.“  
(gyakorikerdesek.hu)



# Neue Verklemmung

„Wenn 4 Fahrzeuge in einer Kreuzung mit Rechtsvorrang gleichzeitig ankommen, soll irgendeiner der Fahrer auf seinen Vorrang verzichten. Ansonsten werden sie laut StVO ewig stehenbleiben.“  
(gyakorikerdesek.hu)

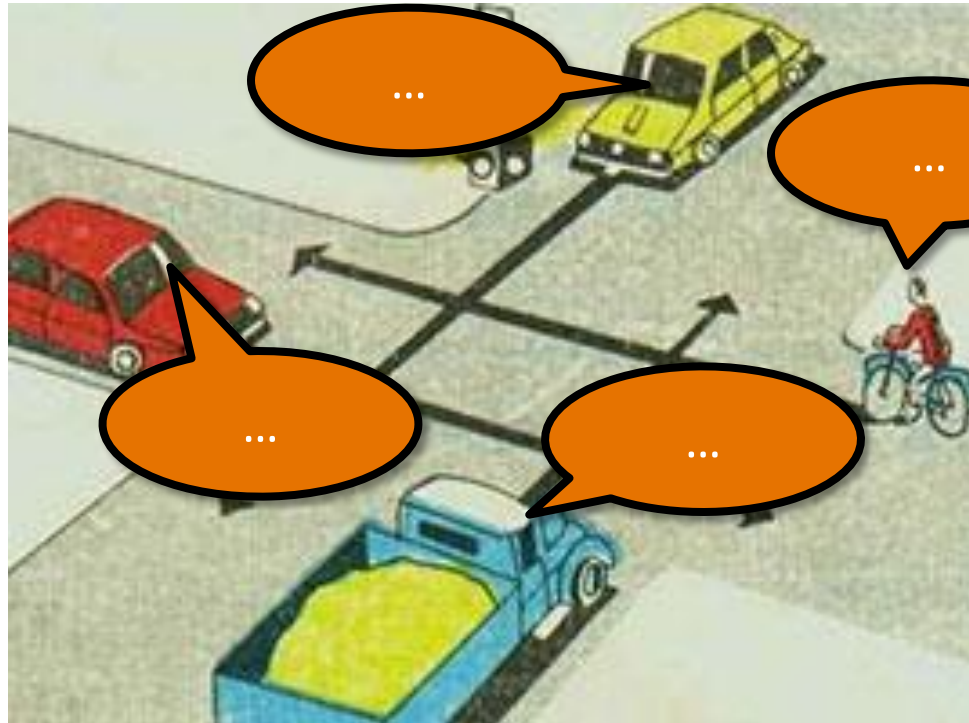


## Auflösung der Verklemmung der Auflösung:

- Asymmetrische Algorithmen
- Algorithmen mit Zufallsprinzip
  - Siehe den Backoff-Verfahren bei Ethernet-Netzwerken

# Endlosschleife (livelock)

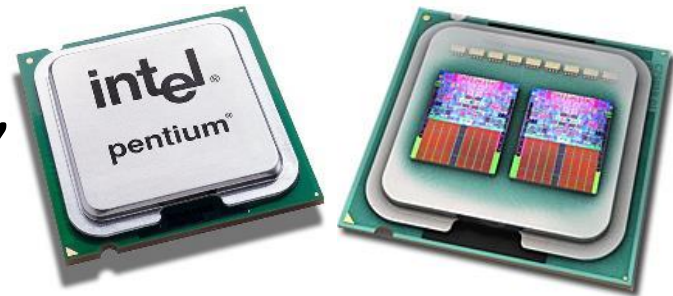
- Eine weitere **Zustandsmenge**, aus der das System ohne äußeren Eingriff nicht weiterrreten kann.
  - z.B. gerade wegen der Auflösung einer **Verklemmung**
  - Z.B. das Google-Auto mit dem Fixie



# Verklemmung (deadlock)

## ■ Häufiger Planungsfehler bei parallelen Systemen

- Manchmal ist es schwer zu vermeiden, aufzulösen
  - eine für gut gehaltene Lösung kann auch so ein Problem verursachen
- Durch Testen schwer zu entdecken, kann scheinbar zufällig sein
- „Krise der Multi-core Prozessoren“

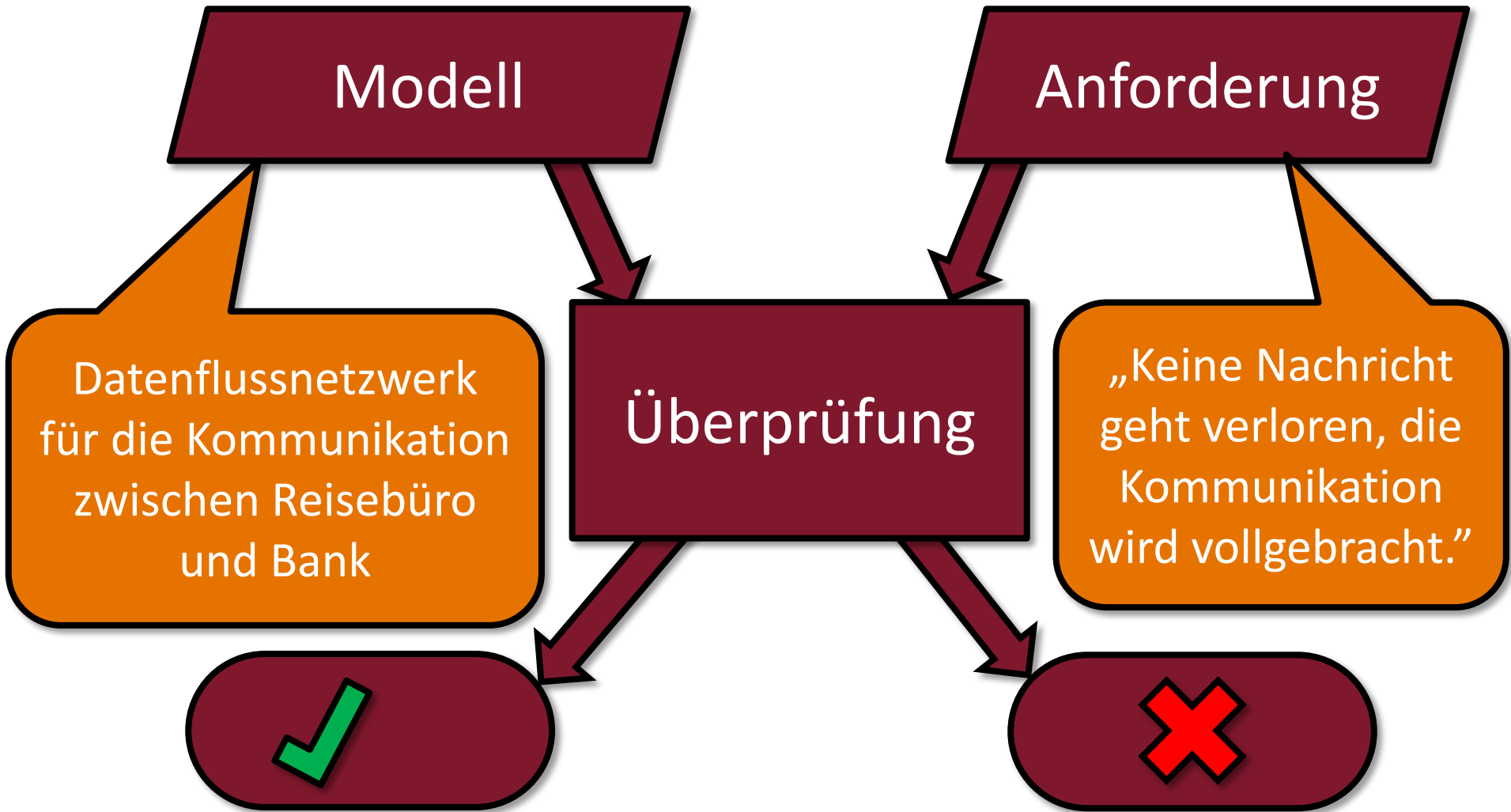


## ■ Beispiele

- Zwei Prozesse wollen Nachrichten austauschen, beide warten auf den anderen
- Zwei Prozesse brauchen zwei Ressourcen, jeder hat eine schon bekommen, jeder wartet auf die andere R.



# Überprüfung von Modellen



# Arten der Untersuchungen

## ■ Nach dem Zweck:

### ○ **Verifikation: Ist das System richtig gebaut?**

- Ist die Implementation entsprechend der Spezifikation?

### ○ **Validation: Ist das richtige System gebaut?**

- Erfüllt das System die Benutzeranforderungen?

## ■ Nach der Methode:

### ○ Statische Überprüfung

### ○ Dynamische Überprüfung

- stichprobenartig (Testen, Simulation)
- ausführlich/vollständig (Überprüfung der Modelle)

Grundbegriffe

Statische Überprüfung

Testen

Formale Verifikation



Grundbegriffe

Stat. Überprüfung

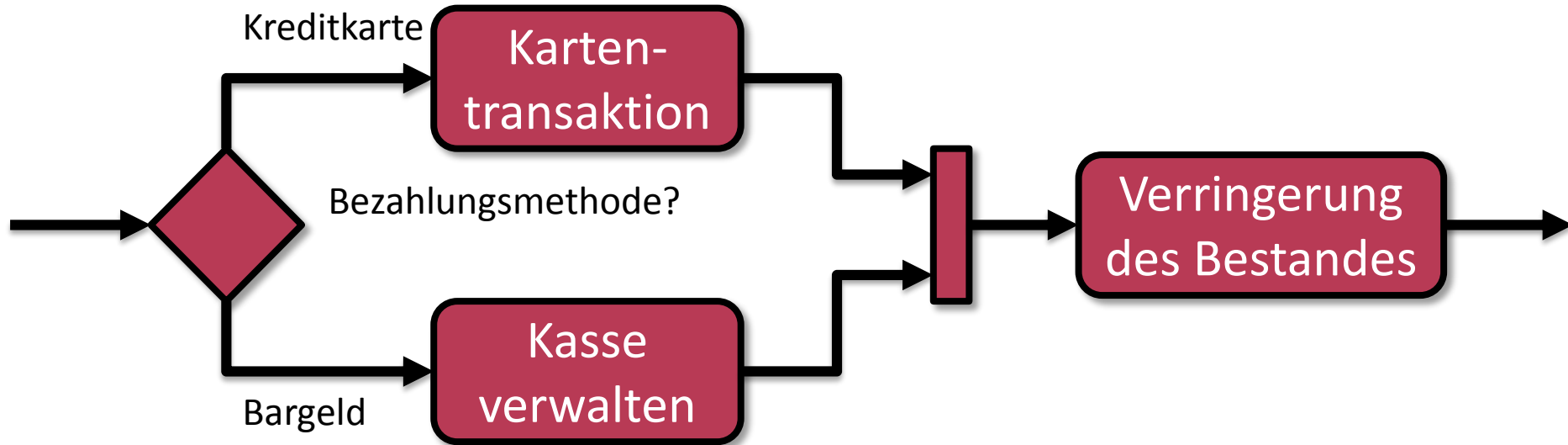
Testen

Formale Verifikation

# STATISCHE ÜBERPRÜFUNG

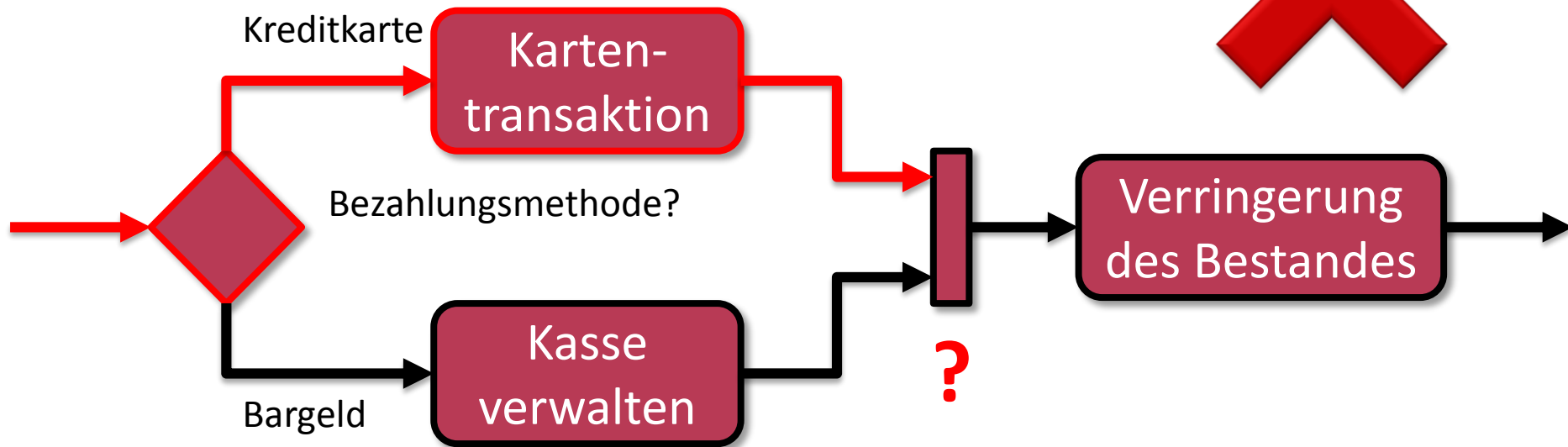
# Decision und Join

- Ist das untenstehende Modell richtig?



# Decision und Join

- Ist das untenstehende Modell richtig?

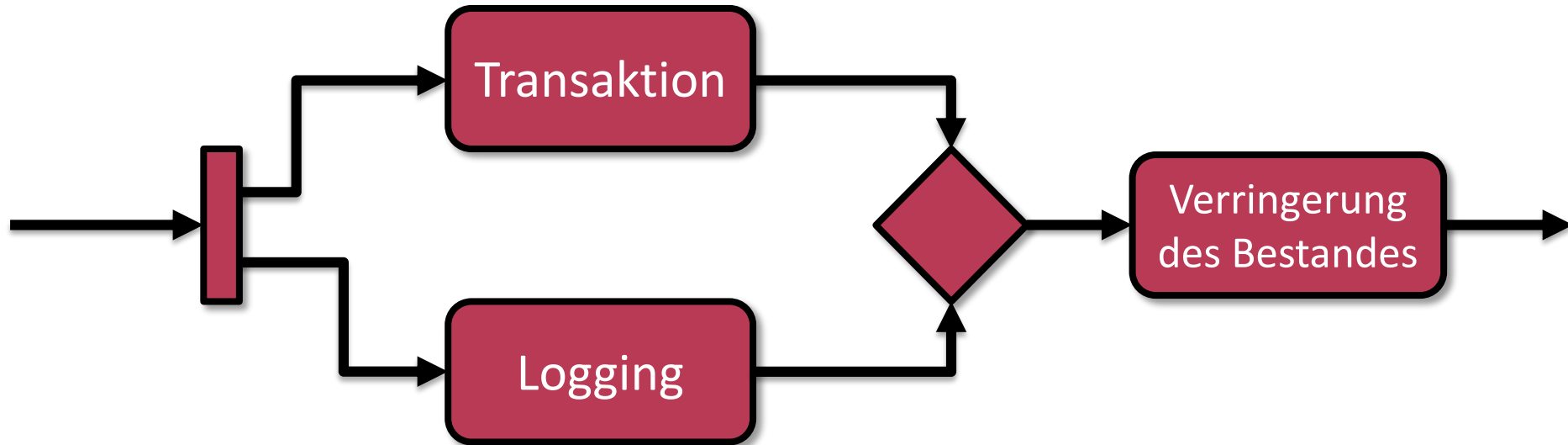


- Join: Eine Fortsetzung ist nur möglich, wenn an allen Eingängen ein Token angekommen ist

→ **VERKLEMMUNG (DEADLOCK)**

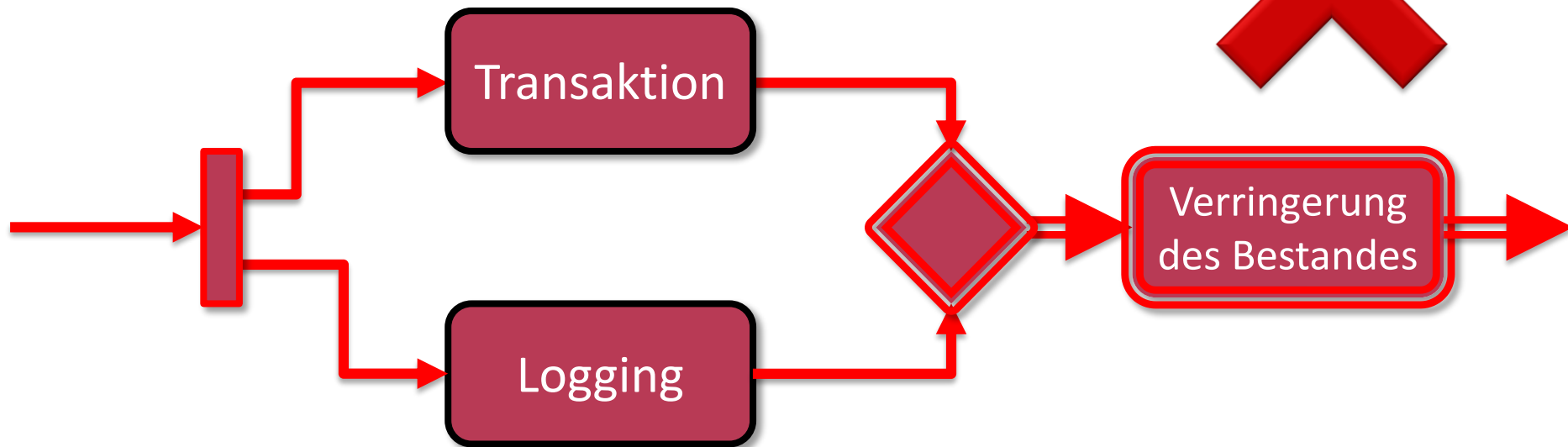
# Fork und Merge

- Ist das untenstehende Modell richtig?



# Fork und Merge

- Ist das untenstehende Modell richtig?



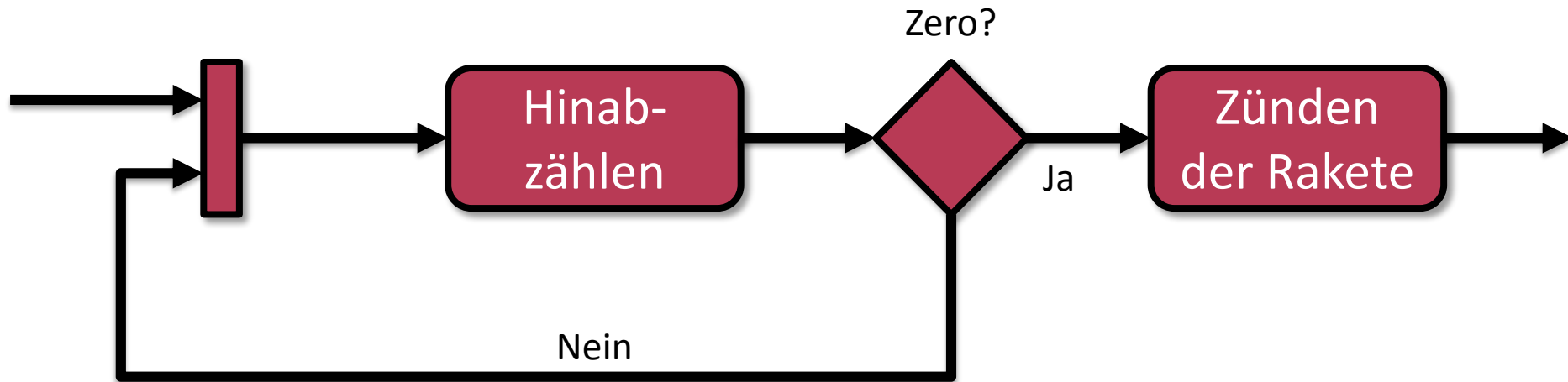
- Merge: Eine Fortsetzung ist möglich, sobald an einem Eingang ein Token angekommen ist

- Keine Synchronisation der Faden

→ **DOPPELTE „VERRINGERUNG DES BESTANDES“**

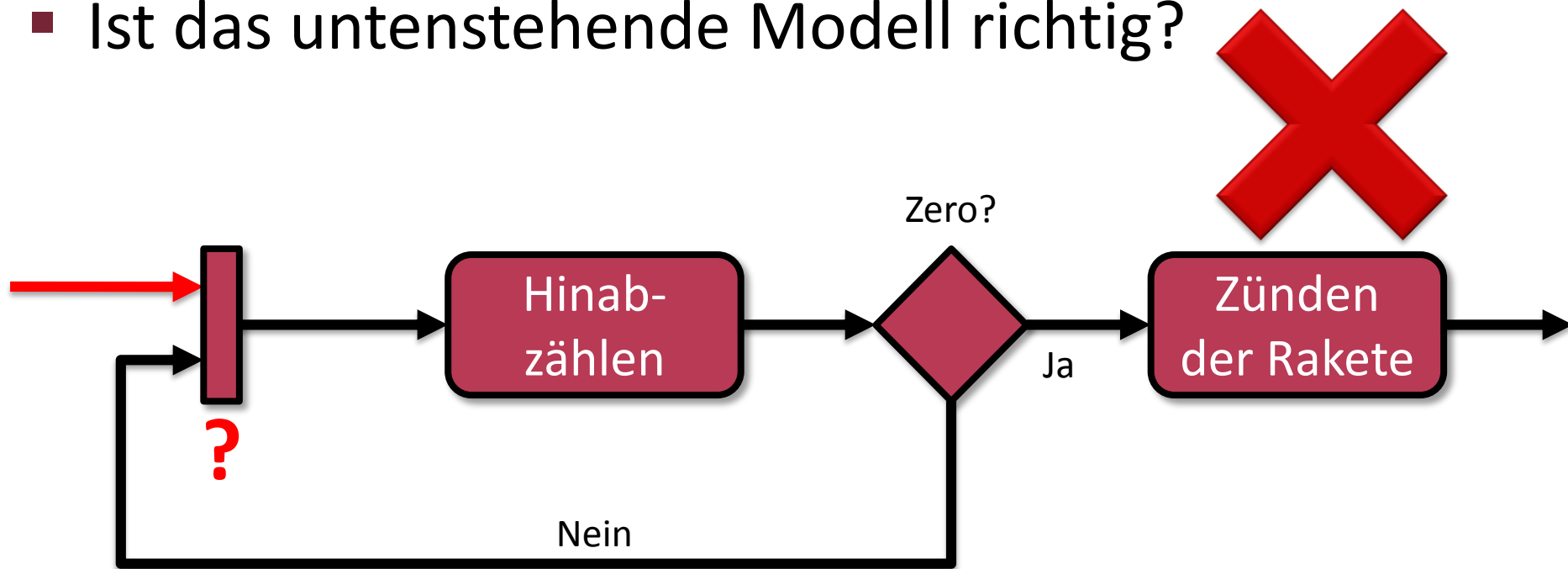
# Schleife 1.

- Ist das untenstehende Modell richtig?



# Schleife 1.

- Ist das untenstehende Modell richtig?



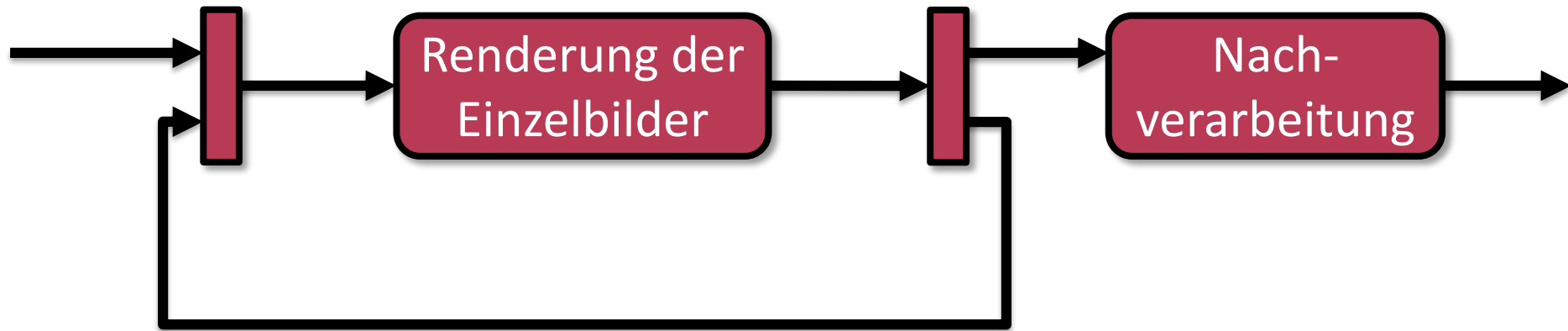
- Join: Eine Fortsetzung ist nur möglich, wenn an allen Eingängen ein Token angekommen ist

→ **VERKLEMMUNG (DEADLOCK)**



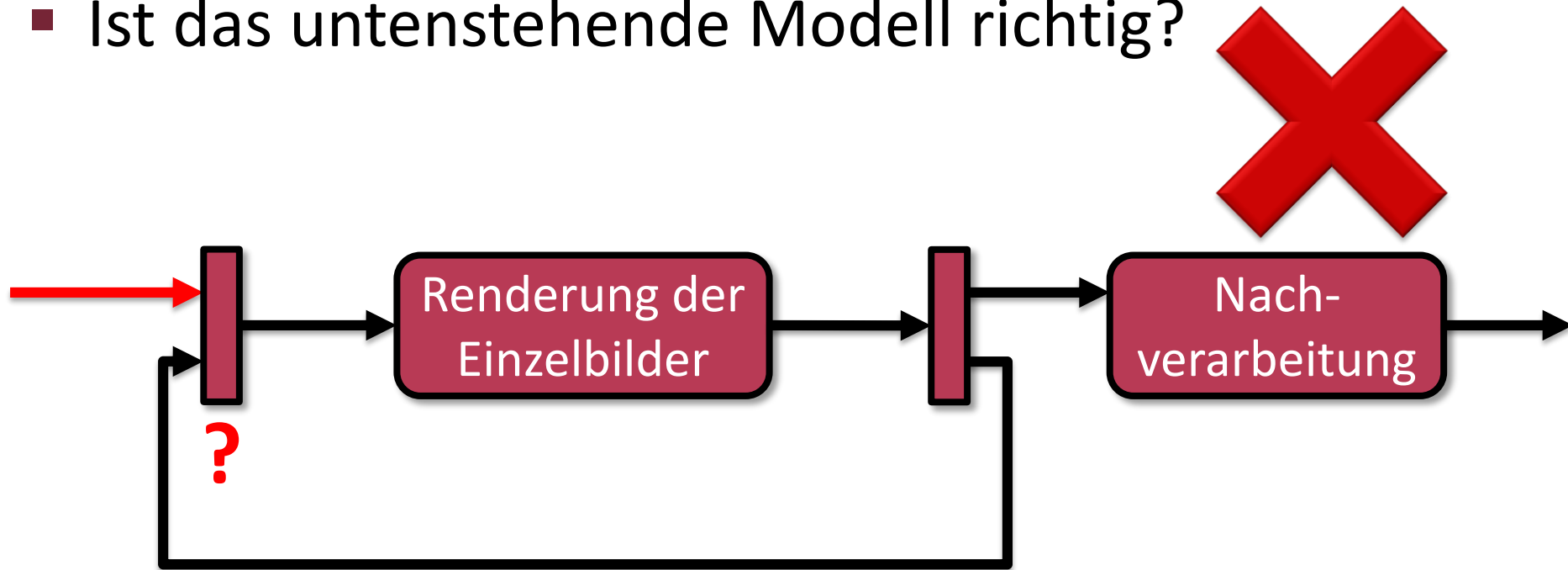
# Schleife 2.

- Ist das untenstehende Modell richtig?



# Schleife 2.

- Ist das untenstehende Modell richtig?

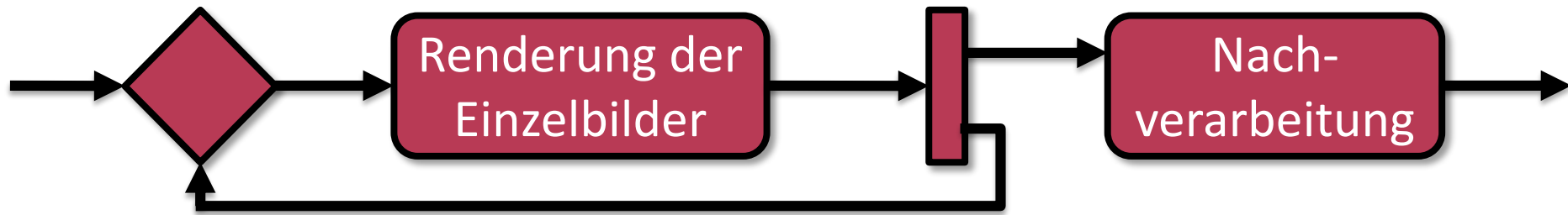


- Join: Eine Fortsetzung ist nur möglich, wenn an allen Eingängen ein Token angekommen ist

→ **VERKLEMMUNG (DEADLOCK)**

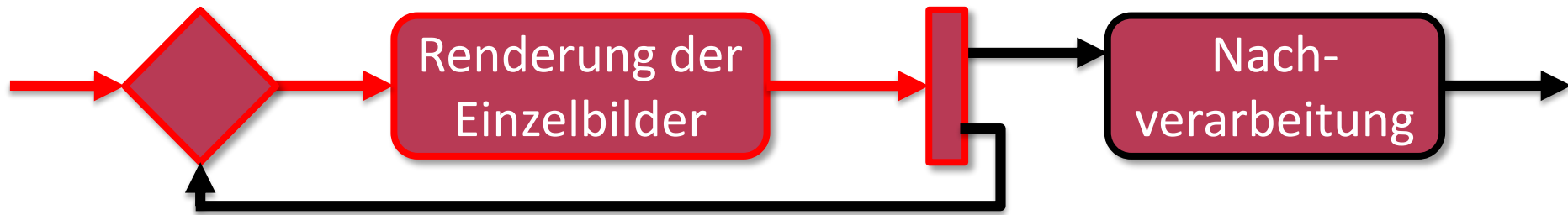
# Schleife 3.

- Ist das untenstehende Modell richtig?



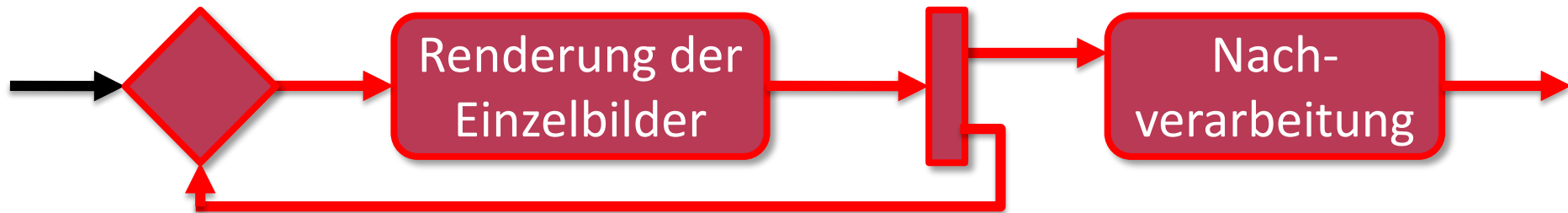
# Schleife 3.

- Ist das untenstehende Modell richtig?



# Schleife 3.

- Ist das untenstehende Modell richtig?

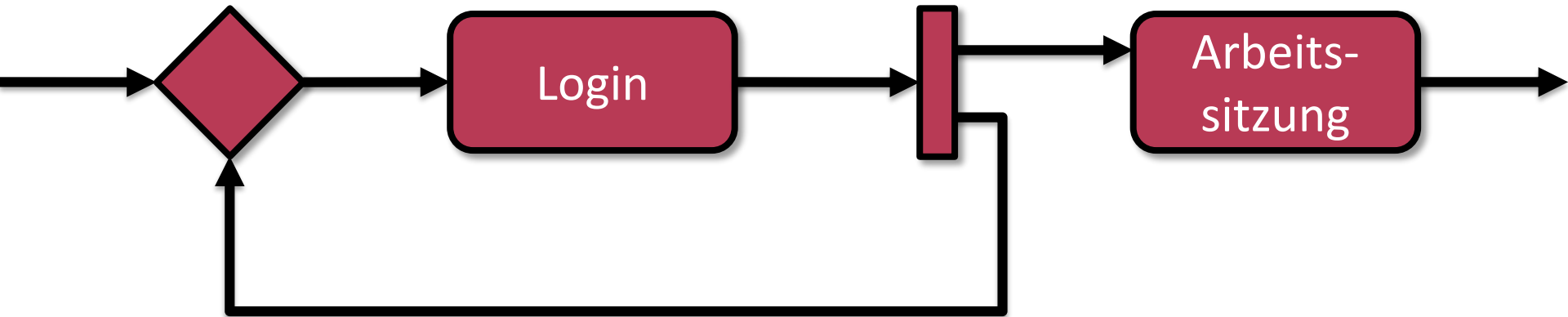


- Ein neues Bild in jeder Iteration
  - Nachverarbeitung jedes Bildes in neuem Faden (Wie viel mal?)

→ **GEFÄHRLICH**, WEIL ES UNENDLICH VIELE FADEN PRODUZIEREN KANN

# Ciklus 3.

- Ist das untenstehende Modell richtig?
  - Und jetzt?

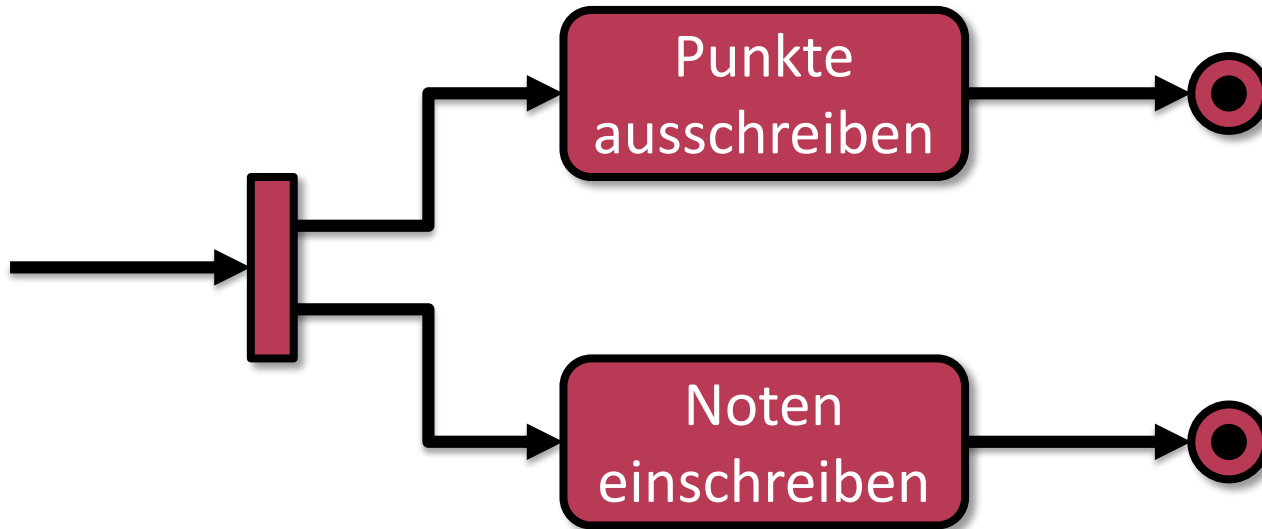


- Nach jedem Login ein weiteres Login ...
  - ...und eine Arbeitssitzung (working session) ...?

→ Die fehlerhafte Implementierung „produziert“ Threads

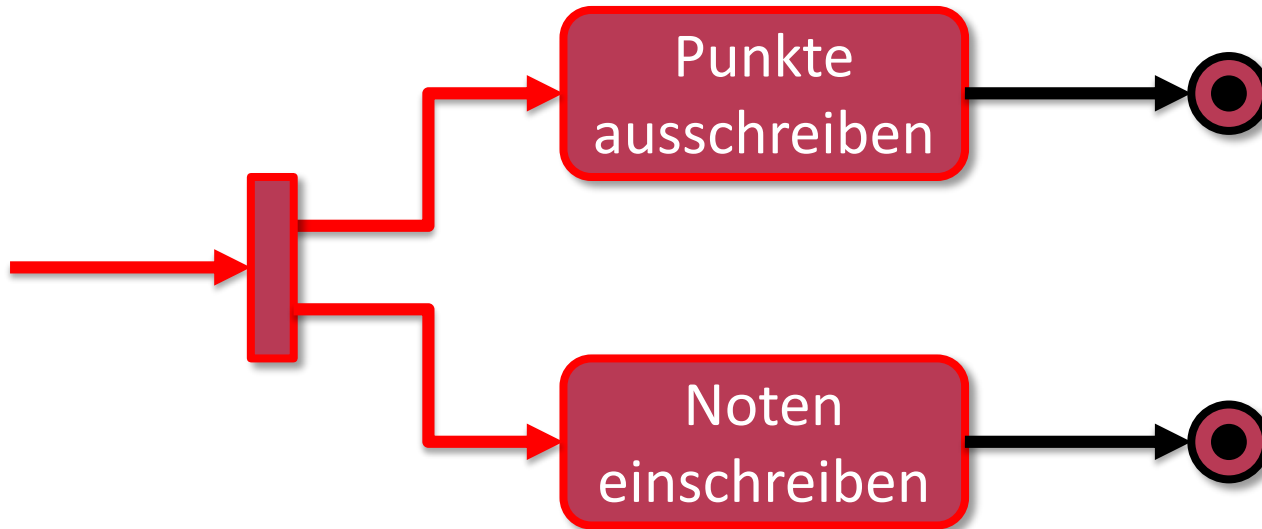
# Endknotenpunkte

- Ist das untenstehende Modell richtig?



# Endknotenpunkte

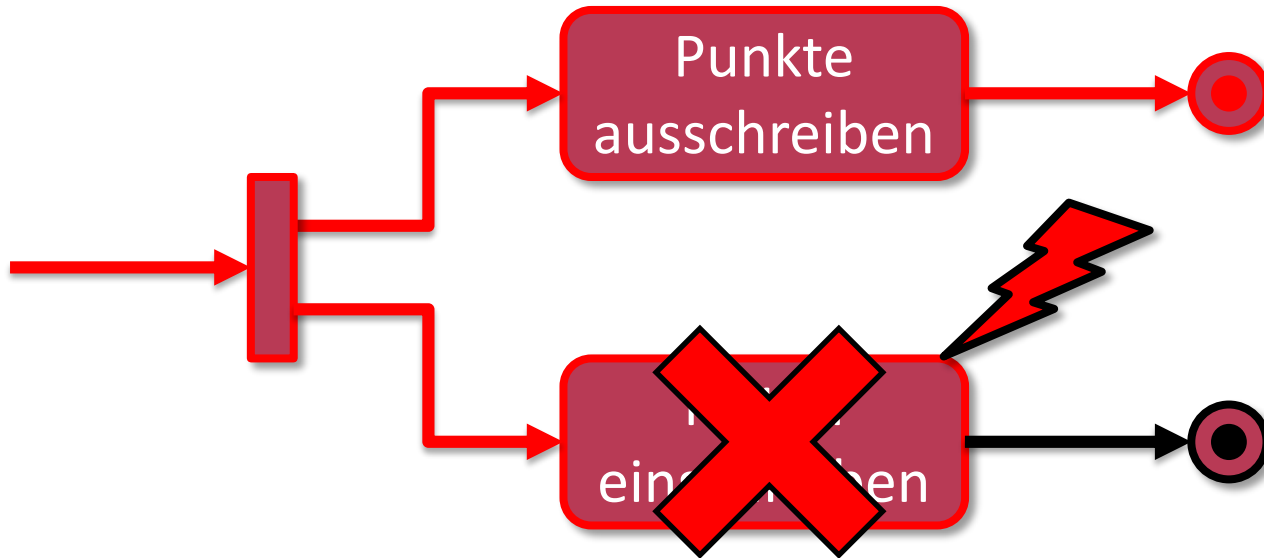
- Ist das untenstehende Modell richtig?





# Endknotenpunkte

- Ist das untenstehende Modell richtig?

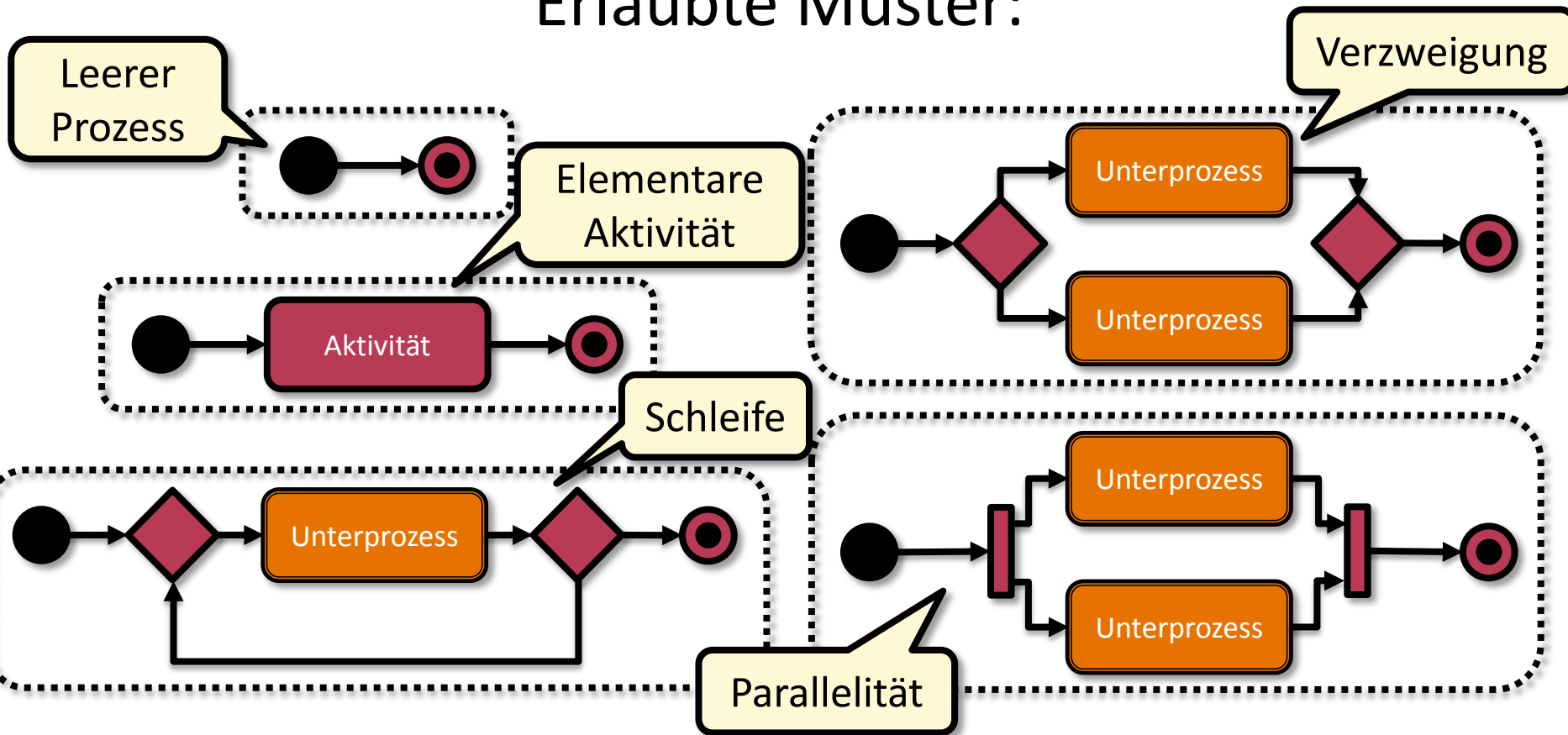


- Der terminierende Knoten stoppt den **ganzen** Prozess  
→ **DIE ANDERE AKTIVITÄT WIRD NIE ABLAUFEN**

# Wohlstrukturierte Prozessmodelle

- **Die Lehre:** Mit wohlstrukturierten Modellen können diese Fehler vermieden werden

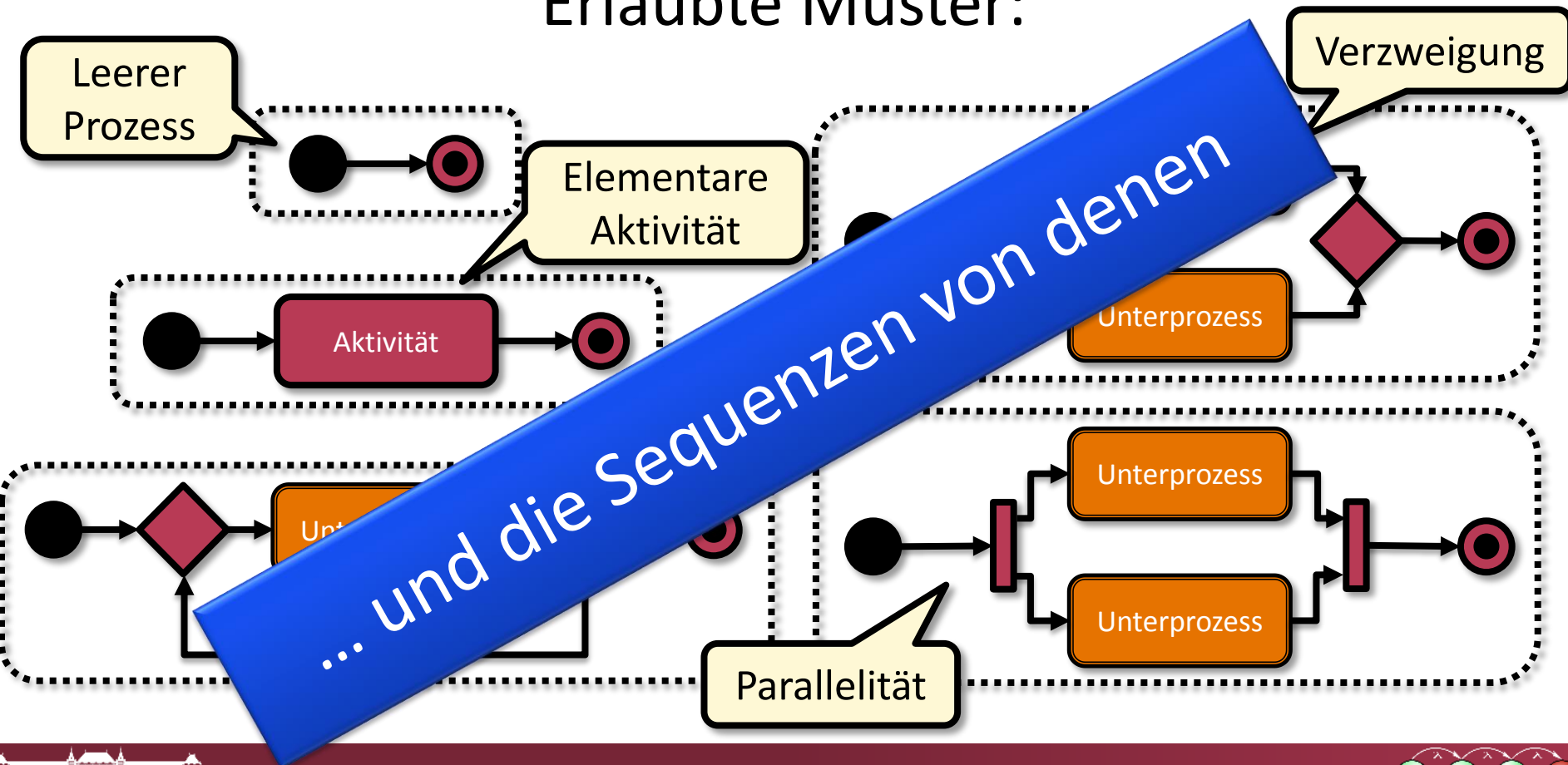
Erlaubte Muster:



# Wohlstrukturierte Prozessmodelle

- **Die Lehre:** Mit wohlstrukturierten Modellen können diese Fehler vermieden werden

Erlaubte Muster:



- Eine Funktion multipliziert zwei ganze Zahlen
  - abgeleitete Anforderung:
    - „Ist mind. die eine Zahl gerade, so ist auch das Produkt“
  - Sie kann durch den ganzen Code begleitet werden
    - „Ausführung im Kopf“
- **Symbolische Ausführung**
  - Anstatt den konkreten Werten wird das Programm mit Wertemengen ausgeführt
  - Die interessante Eingabewerte werden bestimmt
    - z.B. wo es interne Verzweigungen gibt
      - Welche Eingaben steuern die einzelnen Zweige an?

# Statische Überprüfung: Syntaktische Überprüfung

- Syntaktische Überprüfung: die Modellierungsumgebungen verbinden die logisch zusammengehörenden Elemente

**Schnittstellendeklaration:**

```
var clock: integer = 60
```

**Verwendung im Modell:**

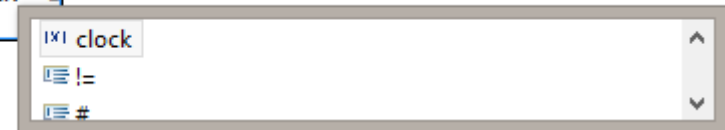
```
after 1 s [clock>0]/ clock-=1
```

- Syntaxgesteuerte Editoren

- Fehler während Bearbeitung → **Couldn't resolve reference**
- Moderne Umgebungen: Vorschlagen der Kandidaten

- Kode+Diagramm gemeinsam

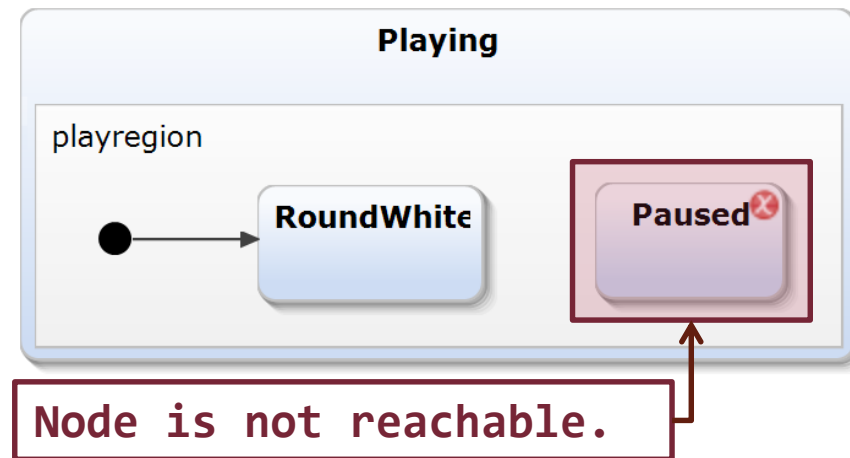
```
after 1 s [clock>0]/ clock-=1
```



- Programmieren: **fehlerhaft** während der Bearbeitung
- Modellieren: **korrekt** während der Bearbeitung

# Statische Überprüfung: Strukturelle Überprüfung

- Strukturelle Überprüfung: Untersuchung des Modellgraphen
- Suchen nach Fehlermuster während der Bearbeitung
- z.B. unerreichbarer Zustand:



- Weitere Überprüfungen: fehlender Anfangszustand, Verklemmung, fehlerhafte Wertzuordnungen, etc.

- Unterstützung von Entwurfsrichtlinien:  
Weitere Regeln können auch eingeführt werden
  - *Always* und *Oncycle*: für jedes Taktsignal feuervernde Ereignisse
  - Beliebige Frequenz → Typischerweise fehlerhaftes Verhalten

In der Hausaufgabe ist die Benutzung von *Always*- und *Oncycle*-Ereignissen strengstens **untersagt**.

Grundbegriffe

Stat. Überprüfung

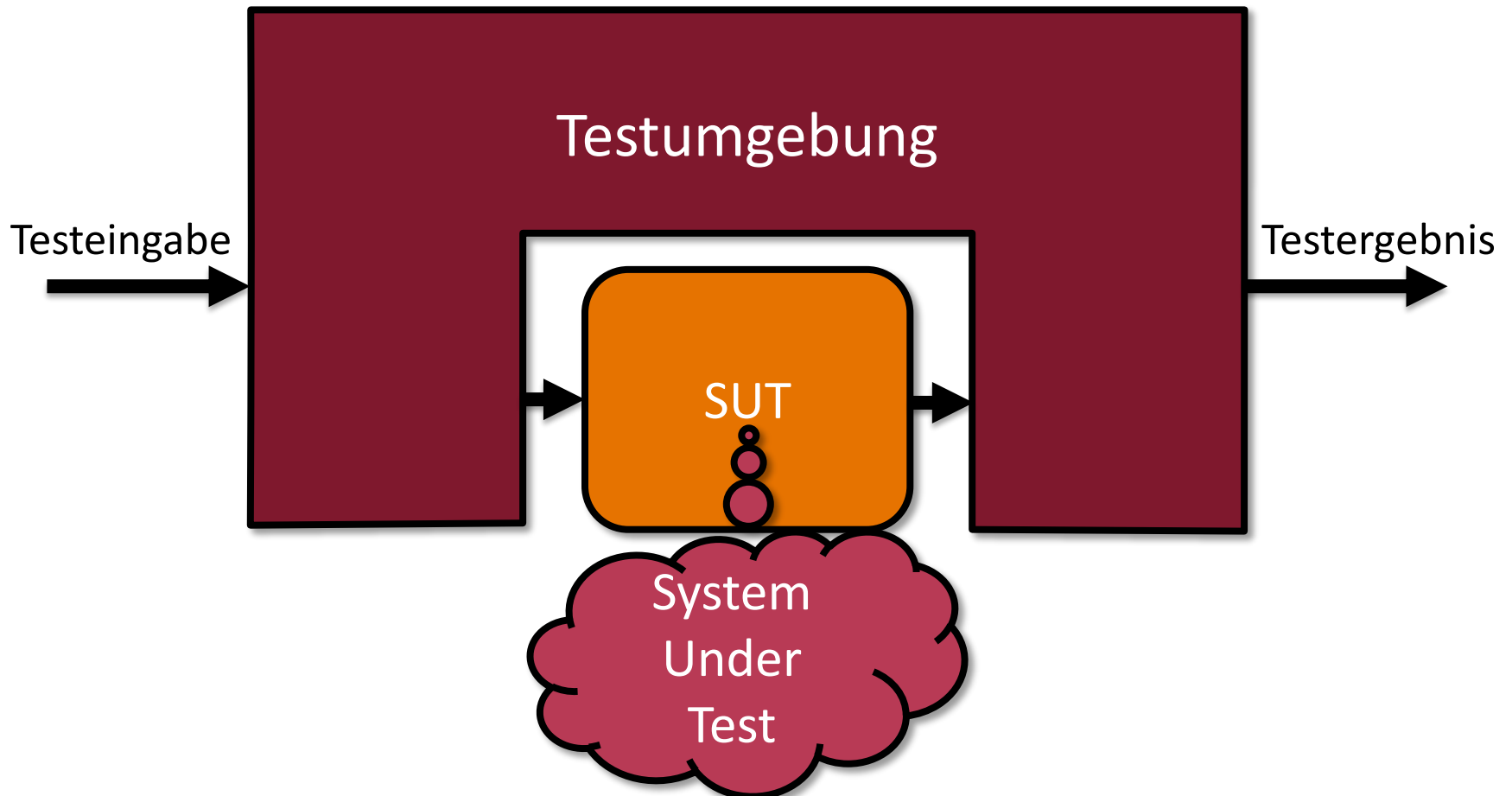
Testen

Formale Verifikation

# TESTEN



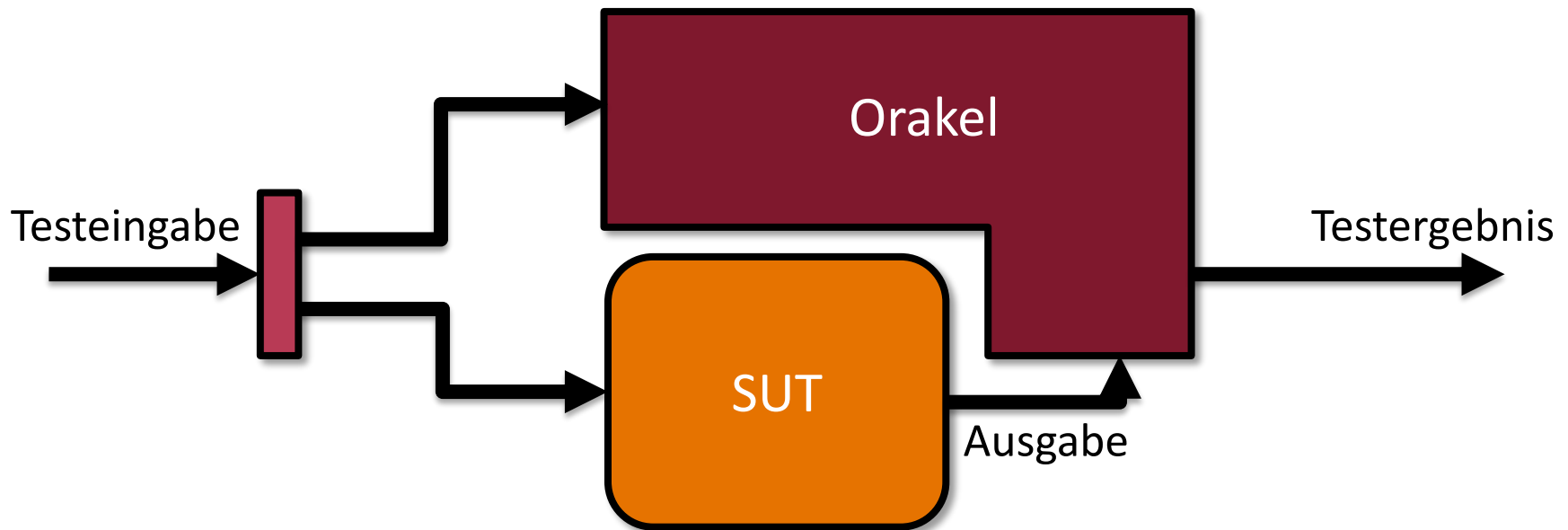
# Testen von Modellen



# Testen von Modellen

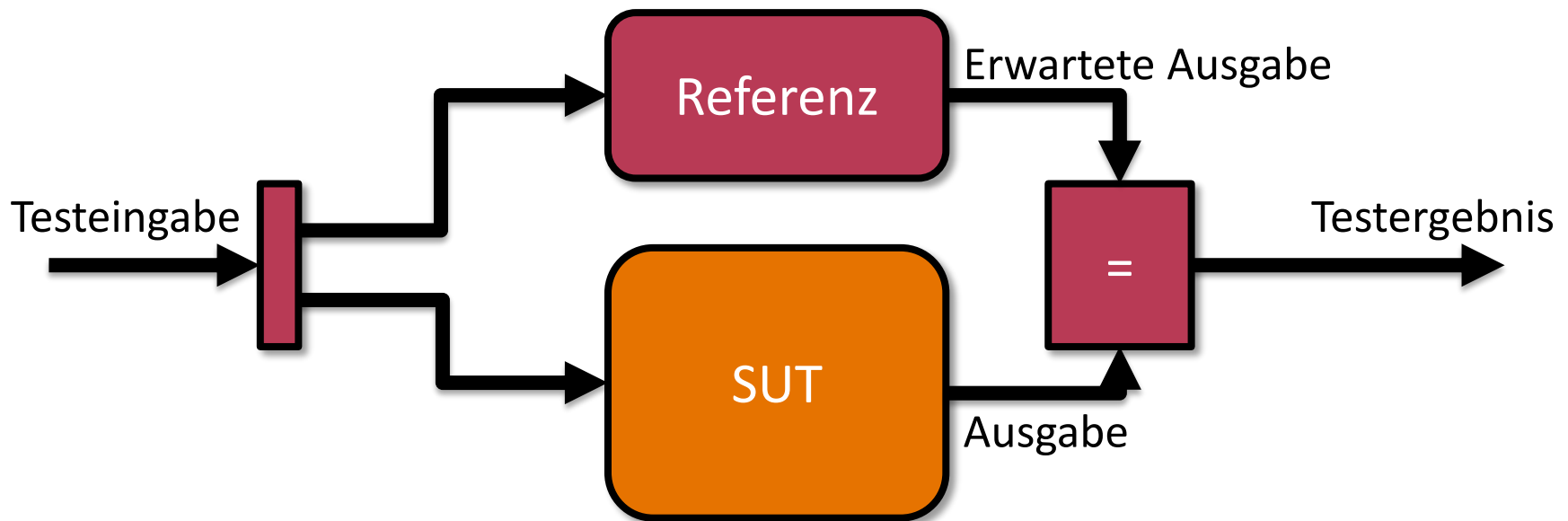
- **Das Orakel:**

Erzeugung und Vergleichung der erwarteten Ausgaben

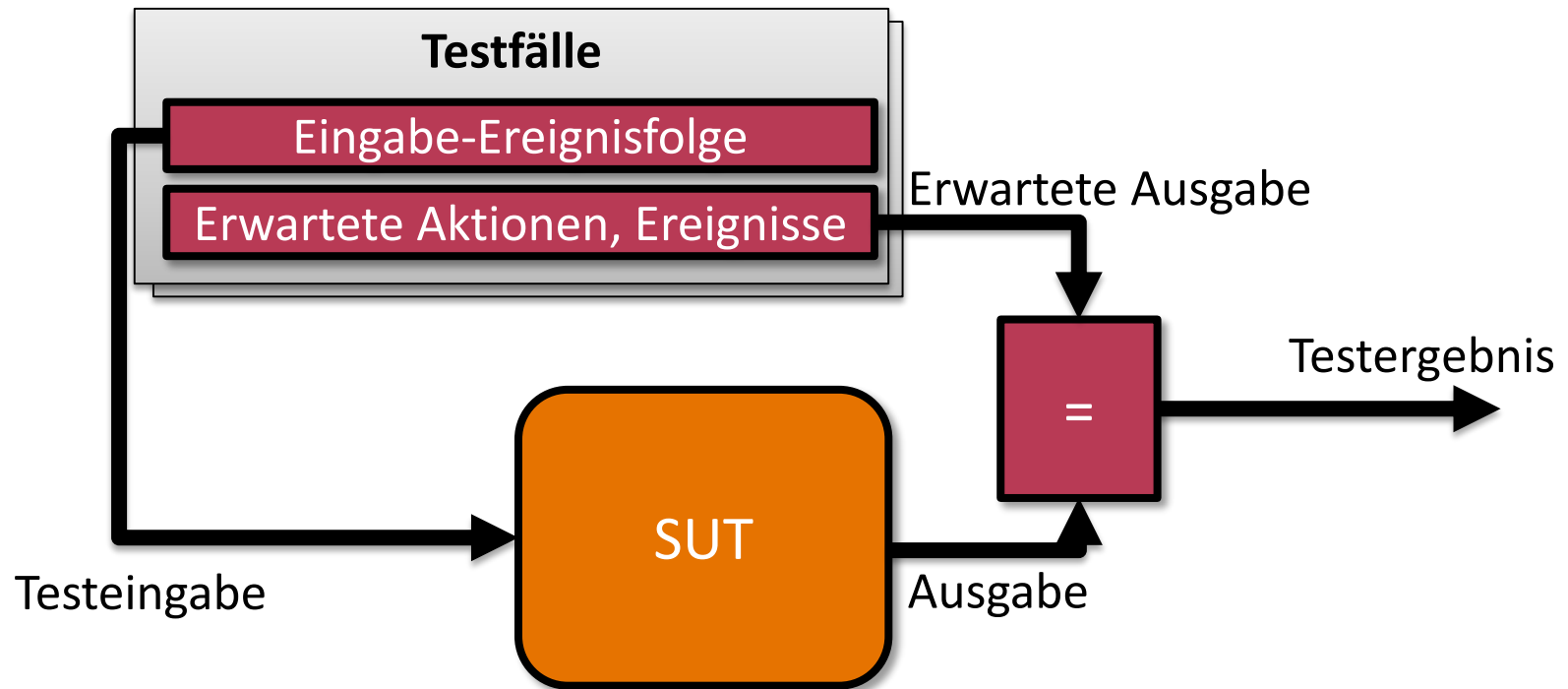


# Testen von Modellen

- **Referenz:** Sie produziert die erwartete Ausgaben anhand der Testeingaben.



# Testen von Modellen: Yakindu Zustandsmaschine



**Testfall Beispiel:** Im Einstellungsmenü kann die Anfangsbedenkzeit zwischen 1 und 3 Minuten in 5 Sekunden-schritten eingestellt werden.

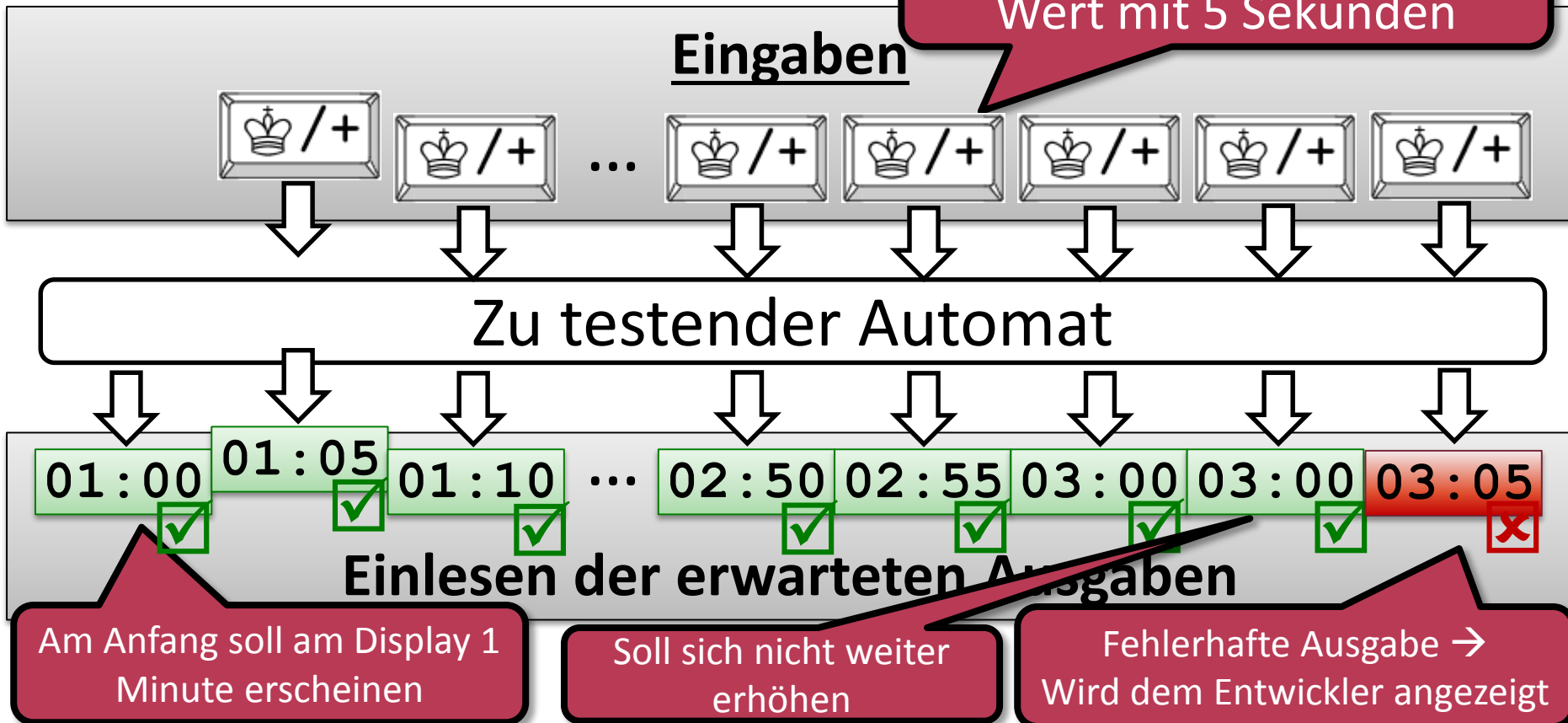
Eingaben

Zu testender Automat

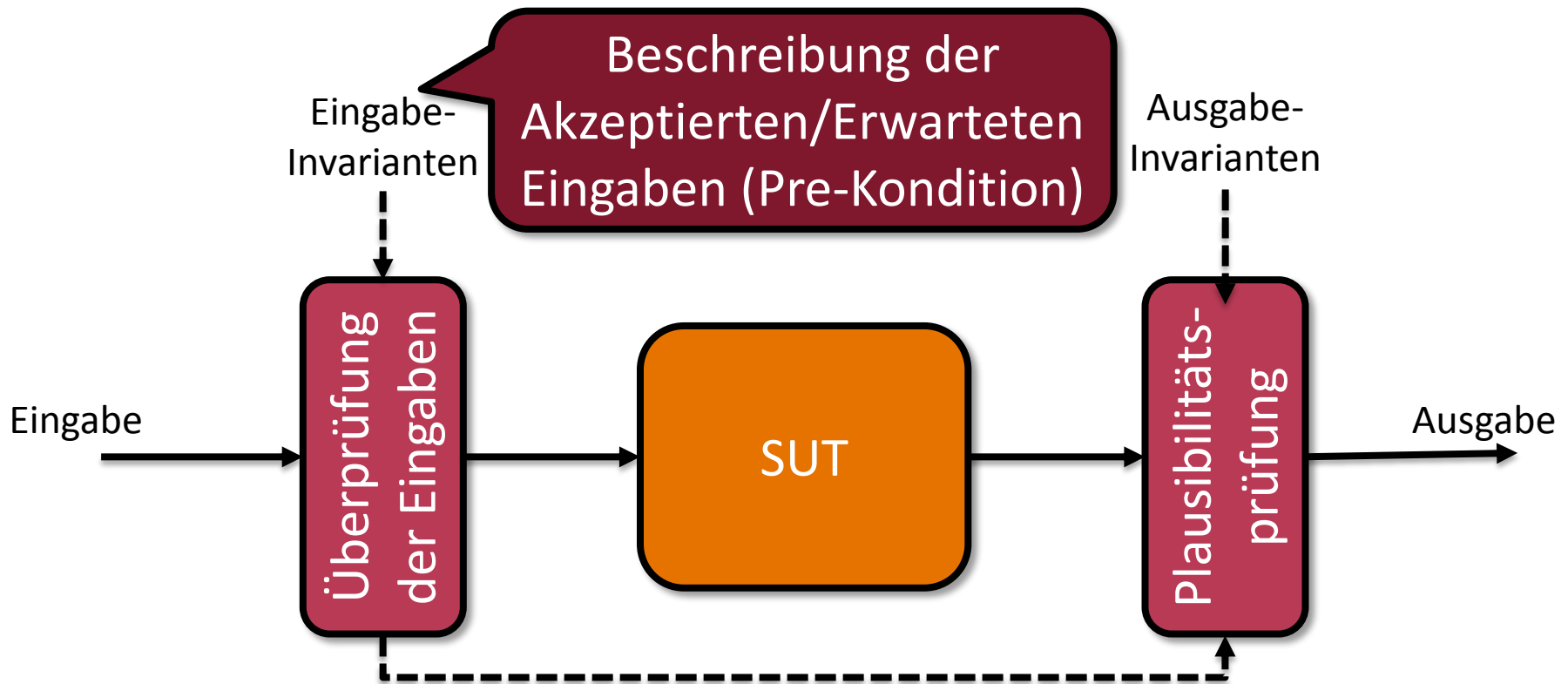
Einlesen der erwarteten Ausgaben

# Testen von Modellen: Yakindu Zustandsmaschine

**Testfall Beispiel:** Im Einstellungsmenü kann die Anfangsbedenkzeit zwischen 1 und 3 Minuten in 5 Sekunden-schritten eingestellt werden.

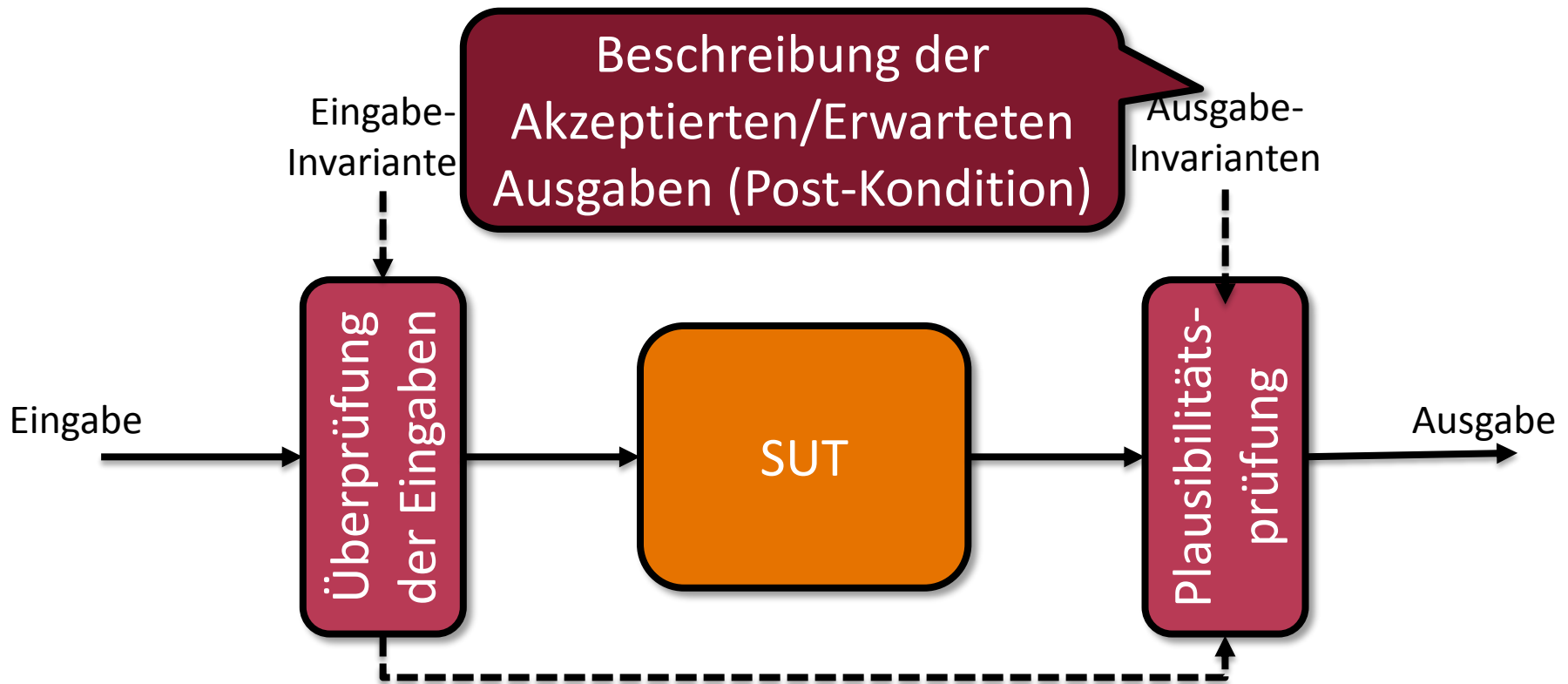


# Selbsttest (monitor)



- **Invariante Eigenschaft:**  
sie soll fortlaufend wahr sein

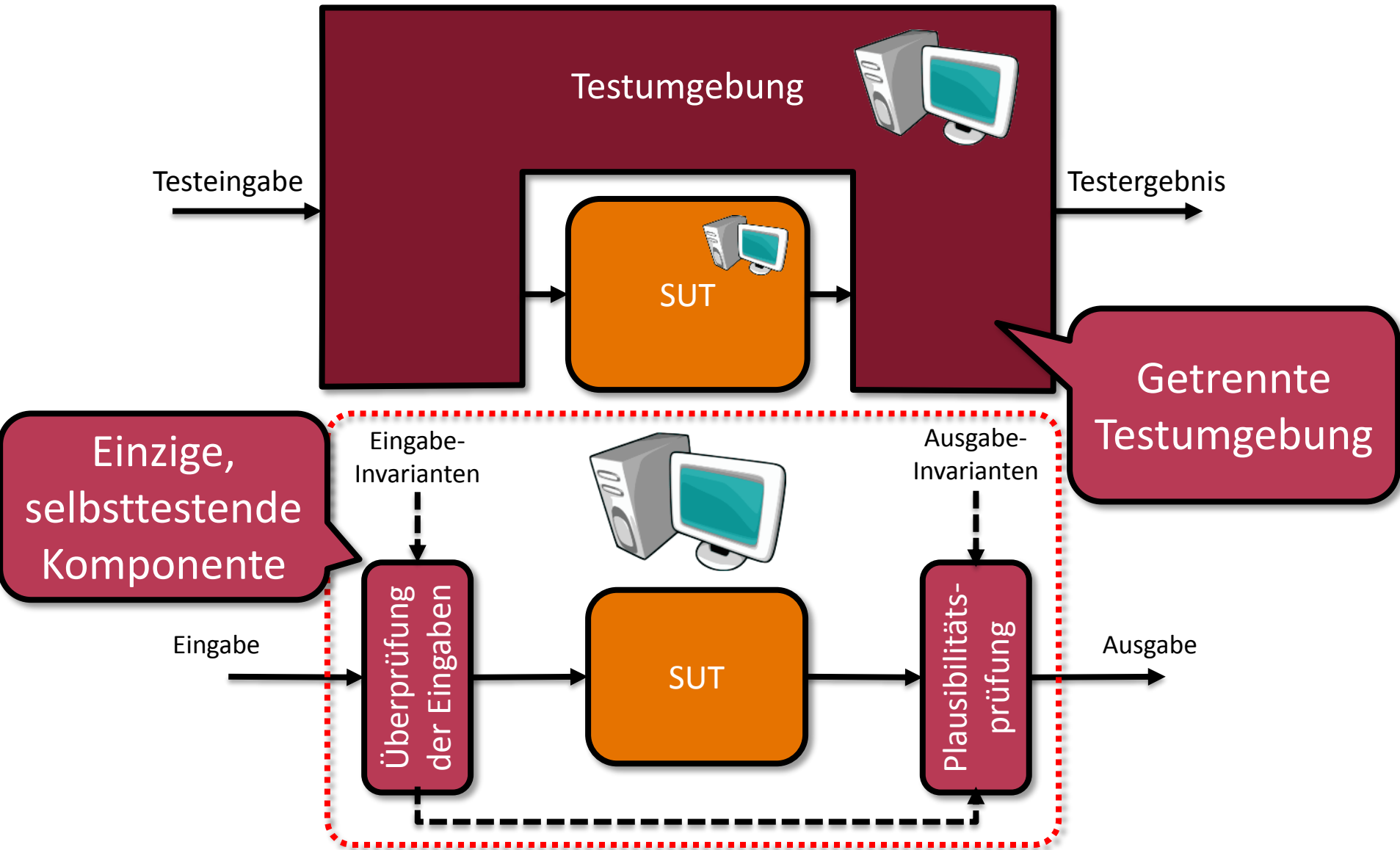
# Selbsttest (monitor)



- **Invariante Eigenschaft:**  
sie soll fortlaufend wahr sein



# Selbsttest vs. Externes Test



# Selbsttestendes Programm

Pre-Kondition: die Diskriminante soll nicht-negativ sein

```
void Roots(float a, b, c,  
          float &x1, &x2)  
{  
    float d = sqrt(b*b-4*a*c);  
  
    x1 = (-b + d)/(2*a);  
    x2 = (-b - d)/(2*a);  
}
```

Post-Kondition: beide Lösungen sollen Nullstellen sein

```
void RootsMonitor(float a, b, c,  
                 float &x1, &x2)  
{  
    // Pre-Kondition  
    float D = b2-4*a*c;  
    if (D < 0)  
        throw "Invalid input!";  
  
    // Ausführung  
    Roots(a, b, c, x1, x2);  
  
    // Post-Kondition  
    assert(a*x12+b*x1+c == 0 &&  
          a*x22+b*x2+c == 0);  
}
```

# Selbsttestendes Programm

## Exception (Ausnahme):

Von dem normalen abweichender, unerwarteter Fall, der **irgendwo anders behandelt wird**.

**Ursache:** falsche Bedienung.

```
float d = sqrt(b*b-4*a*c);
```

## Assert (Behauptung):

Fehlerzustand, auf dessen Behandlung der Code **nicht vorbereitet wurde**.

**Ursache:** fehlerhafte Implementation oder Laufzeitfehler.

```
void RootsMonitor(float a, b, c,  
                  float &x1, &x2)
```

```
{  
    // Pre-Kondition  
    float D = b2-4*a*c;  
    if (D < 0)  
        throw "Invalid input!";
```

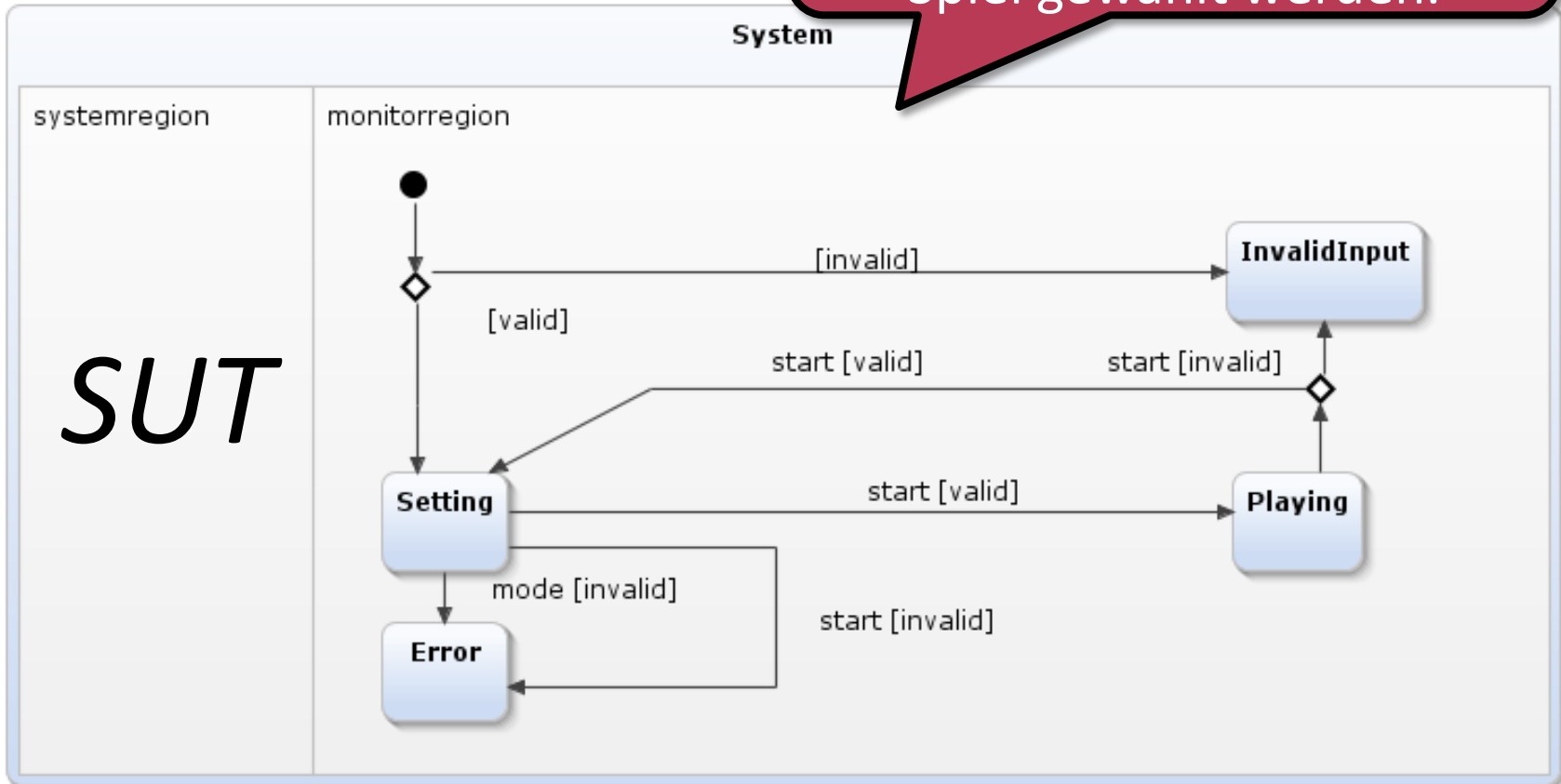
```
    // Ausführung  
    Roots(a, b, c, x1, x2);
```

```
    // Post-Kondition  
    assert(a*x12+b*x1+c == 0 &&  
           a*x22+b*x2+c == 0);  
}
```

# Selbsttest in Yakindu

- Die *SUT* und *monitor* Regionen laufen in parallel
  - Korrekter Fall:
    - Richtige Eingabe (valid)
    - Korrekte Funktion

In der Hausaufgabe kann zwischen Einstellung und Spiel gewählt werden.



# Selbsttest in Yakindu

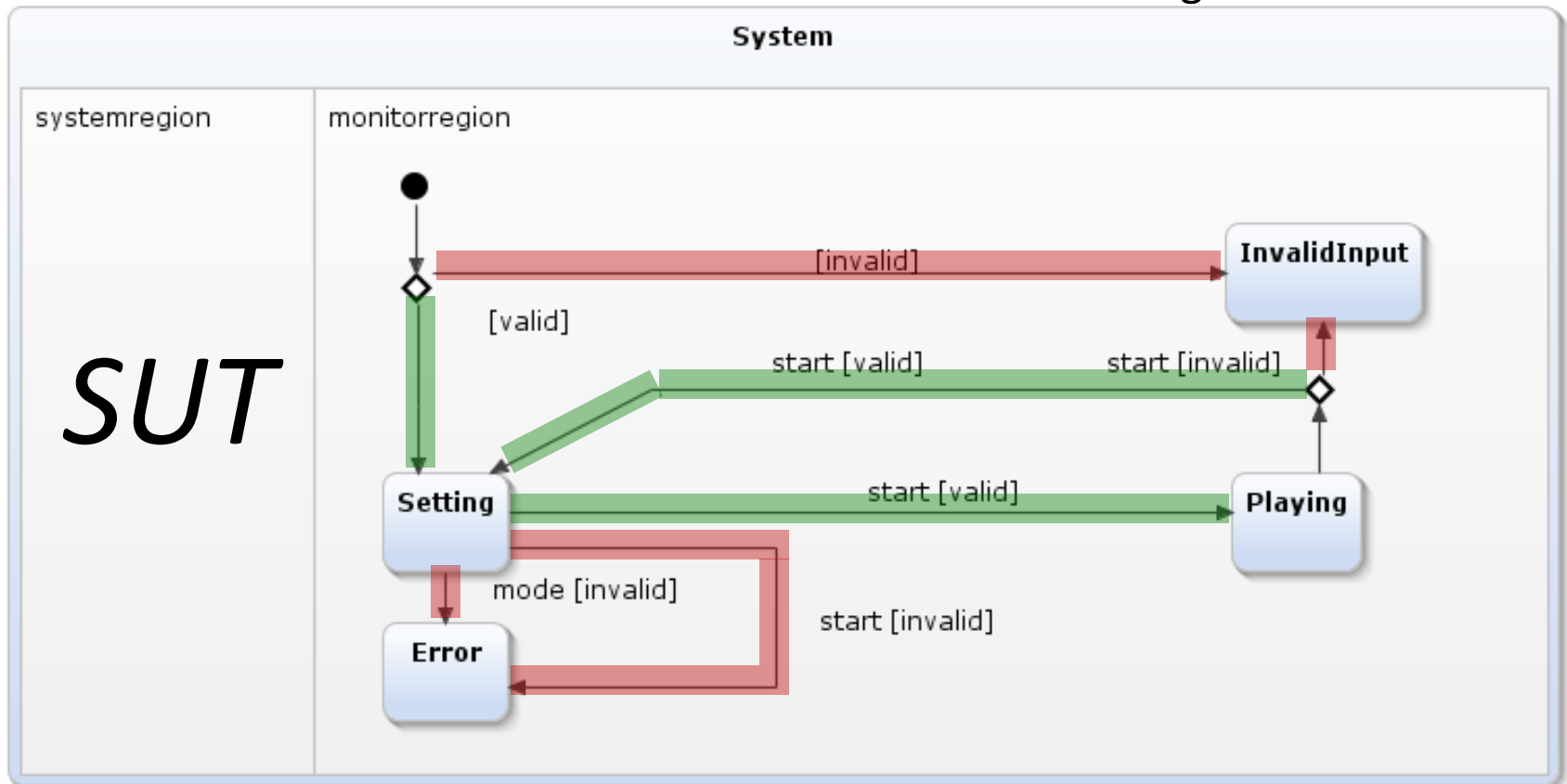
- Die *SUT* und *monitor* Regionen laufen in parallel

- Korrekter Fall:

- Richtige Eingabe (valid)
- Korrekte Funktion

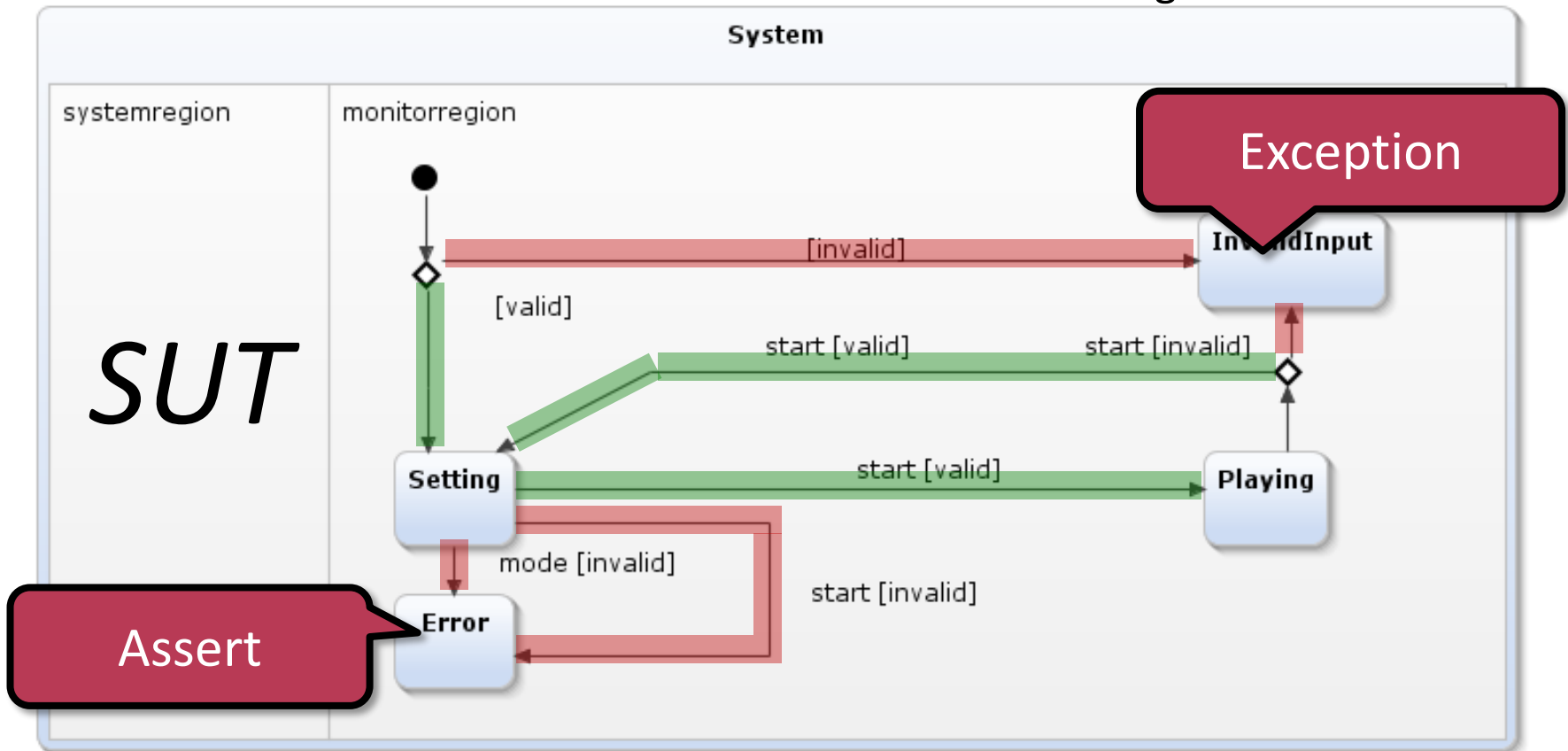
- Fehlerhafter Fall:

- Fehlerhafte Eingabe → InvalidInput
- Fehlerhafte Ausgabe → Error



# Selbsttest in Yakindu

- Die *SUT* und *monitor* Regionen laufen in parallel
  - Korrekter Fall:
    - Richtige Eingabe (valid)
    - Korrekte Funktion
  - Fehlerhafter Fall:
    - Fehlerhafte Eingabe → InvalidInput
    - Fehlerhafte Ausgabe → Error



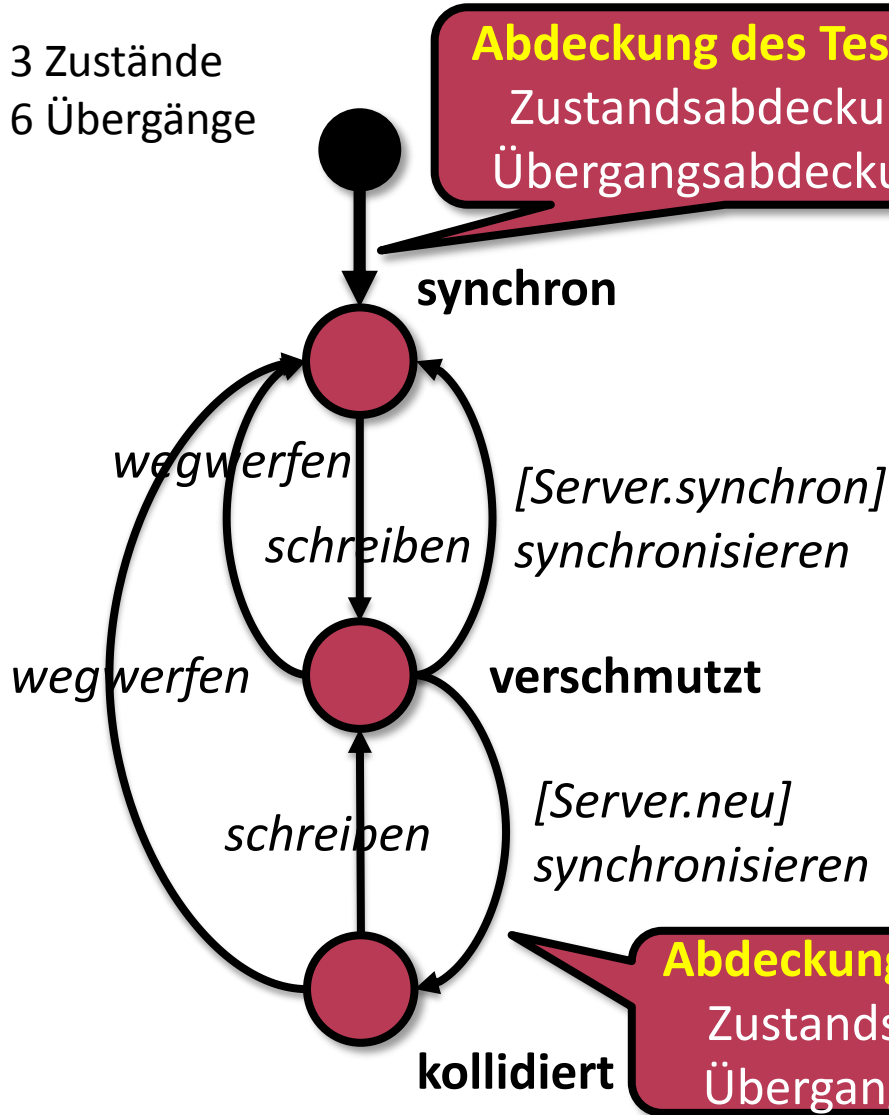
# Testen von Modellen

- Ausführen des Modells: Simulation
  - Auf gegebene Eingaben überprüfetes Verhalten
- Testfälle:
  1. Testeingaben
    - z.B. die Mitte und die zwei Enden eines Wertebereiches
  2. Erwartete Ausgaben

**Mit welchen Eingaben soll getestet werden?**

# Beispiel: Wolkenbasierte Datenspeicherung

3 Zustände  
6 Übergänge



## Abdeckung des Testsatzes 1:

Zustandsabdeckung: 66%  
Übergangsabdeckung: 33%

## 1. Testfall:

- schreiben
- wegwerfen

## 2. Testfall:

- schreiben
- synchronisieren  
[Server = neu]
- wegwerfen

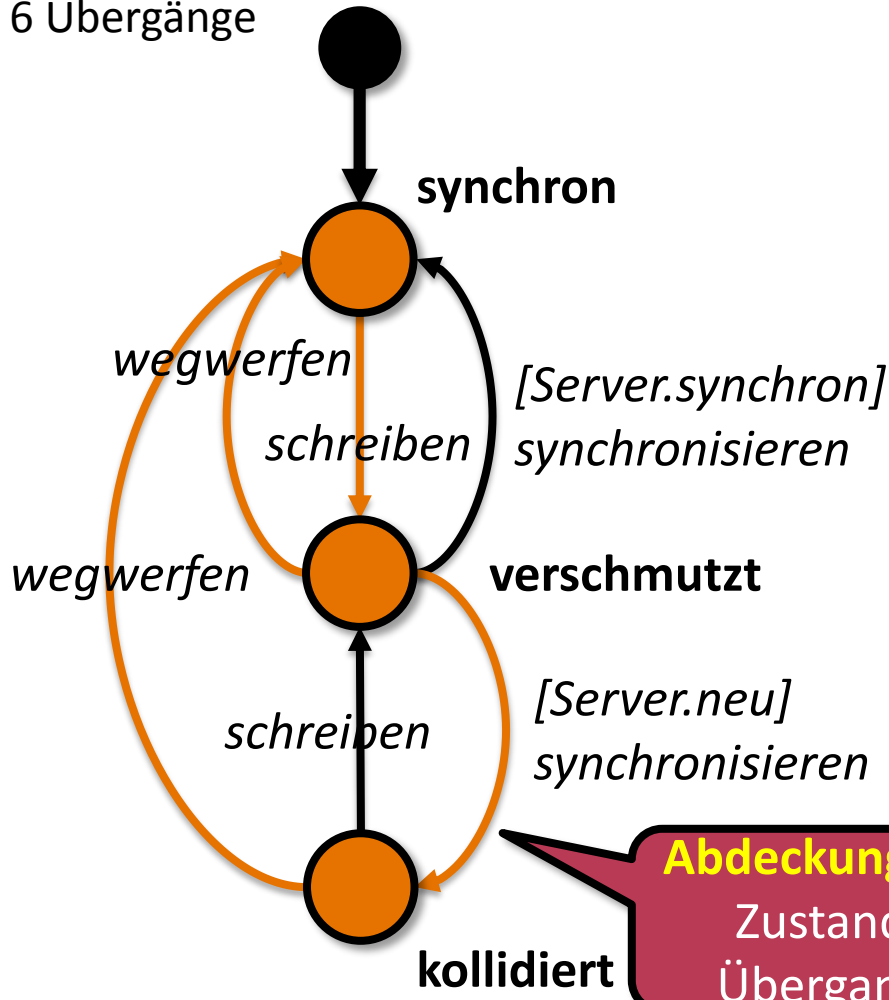
## Abdeckung des Testsatzes 1+2:

Zustandsabdeckung : 100%  
Übergangsabdeckung : 66%



# Beispiel: Wolkenbasierte Datenspeicherung

3 Zustände  
6 Übergänge



## 3. Testfall:

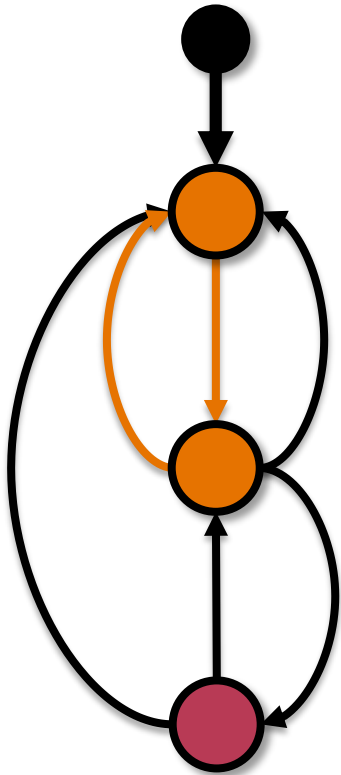
- schreiben
- synchronisieren  
[Server = neu]
- schreiben
- synchronisieren  
[Server = sync.]

# Abdeckung

Nach dem 1. Testfall:

Zustandsabdeckung:  $2/3=66\%$

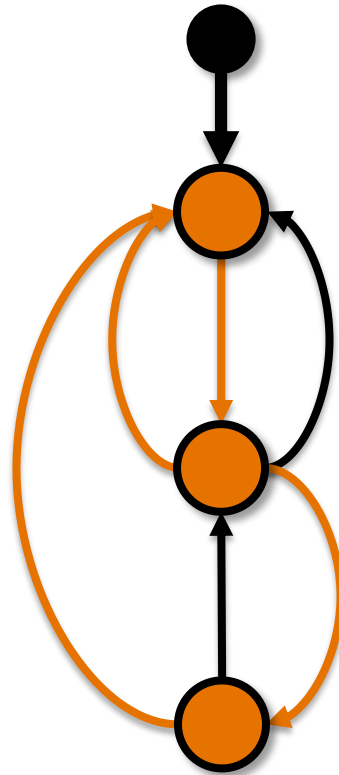
Übergangsabdeckung:  $2/6=33\%$



Nach dem 2. Testfall:

Zustandsabdeckung:  $3/3=100\%$

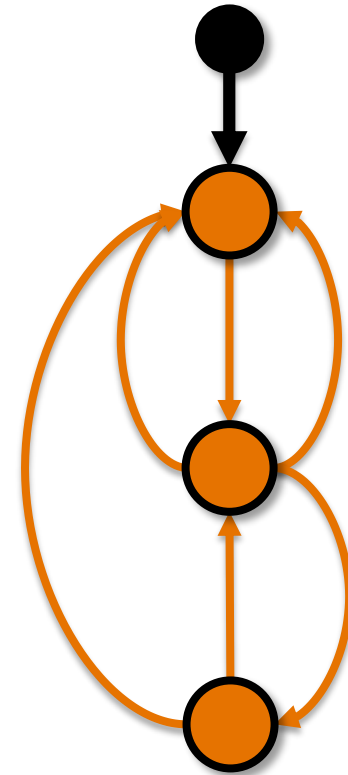
Übergangsabdeckung:  $4/6=66\%$



Nach dem 3. Testfall:

Zustandsabdeckung:  $3/3=100\%$

Übergangsabdeckung:  $6/6=100\%$



# Benutzen der getesteten Modelle

- **Softwaretesten:**
  - Wiederverwendung von Testsätzen (mit 100% Abdeckung)
  - Abdeckende Testeingaben (als Eingabe)
  - Vom Modell produzierte Ausgaben (als erwartete Ausgaben)
- **Monitoring:** Simulieren des Modells während Laufen der Software
  - Gleiche Eingaben für das Modell und das Programm
  - Vergleichung der Ausgaben → **Fehlererkennung**
- **Untersuchung der Aufzeichnungen/des Log:**
  - Monitoring mit den aufgezeichneten Ein- und Ausgaben

# Benutzen der getesteten Modelle

## ■ Softwaretesten:

- Wiederverwendung von Testsätzen (als Eingabe)
- Abdeckende Testeingaben (als Eingabe)
- Vom Modell produzierte Ausgaben (als erwartete Ausgaben)

**Vor** der  
Ausführung

## ■ **Monitoring:** Simulieren des Modells während Laufen der Software

- Gleiche Eingaben für das Modell und das Programm
- Vergleichung der Ausgaben → **Fehlererkennung**

**Während** der  
Ausführung

## ■ **Untersuchung der Aufzeichnungen:**

- Monitoring mit den aufgezeichneten

**Nach** der  
Ausführung

# Testdokumentation

- Die Testfälle und –Ergebnisse sollen dokumentiert werden!

Testspezifikation

- Was wird getestet?
- Anhand welcher Anforderungen?
- Mit welchen Eingaben?
- Welche Ausgaben sind erwartet?

-Report

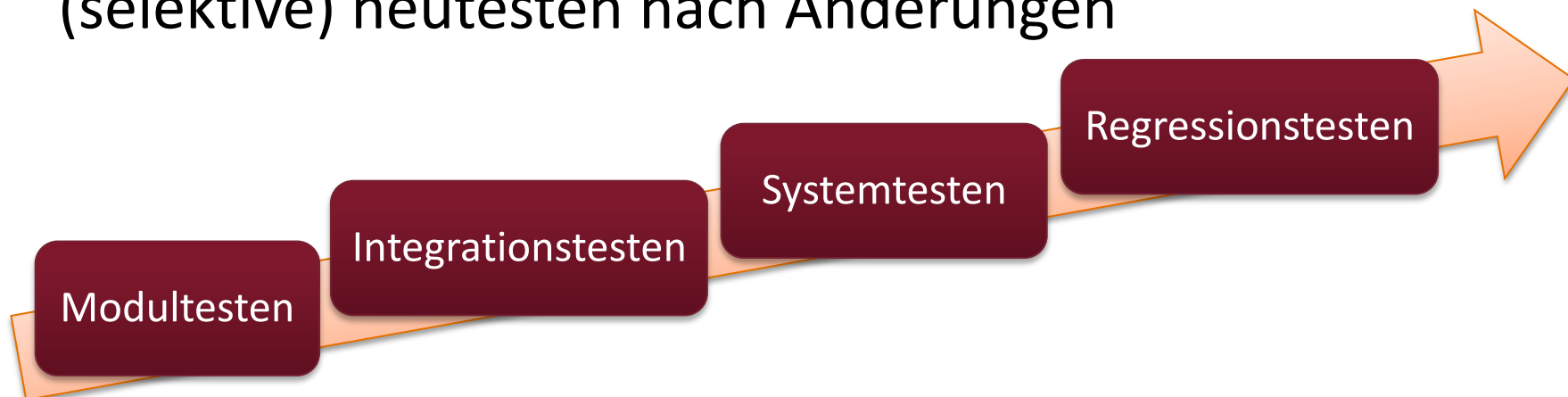
- Wurde es ausgeführt?
- Wenn ja, mit welchem Ergebnis?



- Nachweisbarkeit :
  - Aufdeckung von ungetesteten Kodeteilen und unüberprüften Anforderungen
  - Zurückverfolgbarkeit der Testergebnisse

# Testarten, Testphasen

- **Modultesten:**  
eine Komponente wird abgetrennt und so getestet
- **Integrationstesten:**  
mehrere Komponenten werden gemeinsam getestet
- **Systemtesten:**  
das ganze System zusammen wird getestet
- **Regressionstesten:**  
(selektive) neutesten nach Änderungen



Grundbegriffe

Stat. Überprüfung

Testen

Formale Verifikation

# FORMALE VERIFIKATION

# Formale Verifikation

- **Formale Verifikation:** Beweis der Korrektheit von Modellen/Programmen mit mathematischen Mitteln
  - Für mehr dazu siehe: Formale Methoden MSc-LVA
- **Möglichkeiten:**
  - **Modellprüfung** (model checking)
    - Erschöpfende Untersuchung aller möglichen Verhalten
  - **Automatischer Beweis der Korrektheit**
    - Automatisches Beweisverfahren anhand Axiomensysteme
  - **Konformanzuntersuchungen**
    - Überprüfung der Übereinstimmung von Modellen



# Modellprüfung

- **Modellprüfung:** Erschöpfende (vollständige) Untersuchung aller potentiellen Verhalten eines Modells anhand gegebener Anforderungen
    - Suchen nach Fehlverhalten
- **Gegenbeispiel**

Testen	Modellprüfung
Stichprobenartig	Erschöpfend/vollständig
Überprüft erwartete Ausgaben	Überprüft Zustandsfolgen
Kleiner Rechenaufwand	Grosser Rechenaufwand
Nicht beweisstark	Formaler Beweis