Nutzen der Automatentheorie zur Verbesserung der Sicherheit durch Verifikation in IT-Systemen von KRITIS-Betreibern

Gustav Grabolle

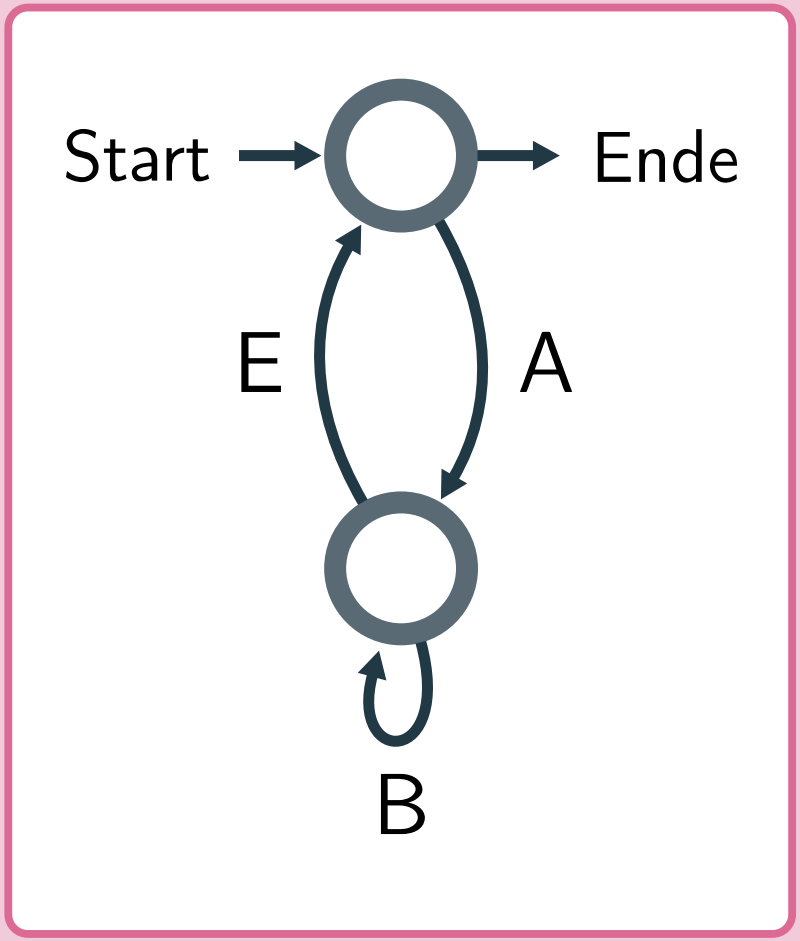
Halle
August 4, 2025

Theoretische Grundlagen

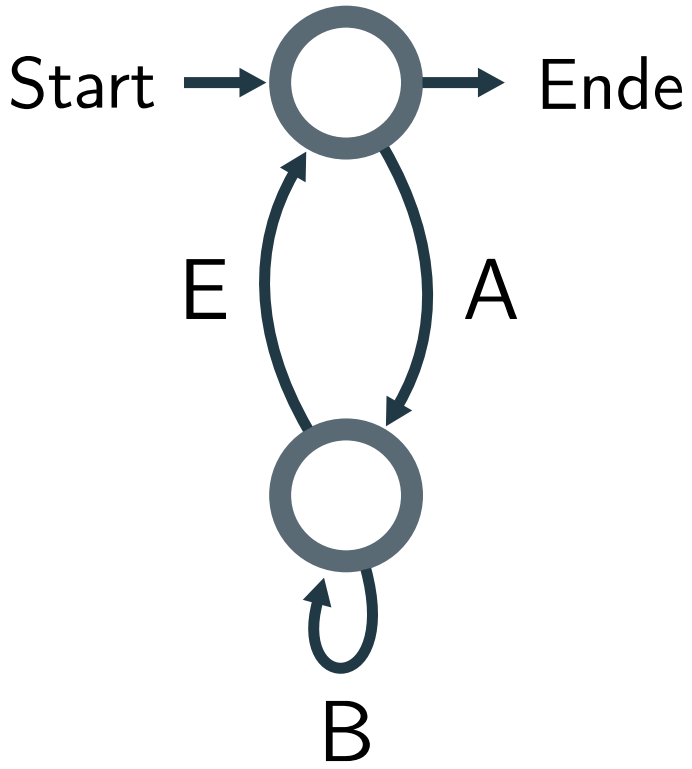
Praktische Einsicht

KRITIS Einsatz

Was sind diese Automaten?

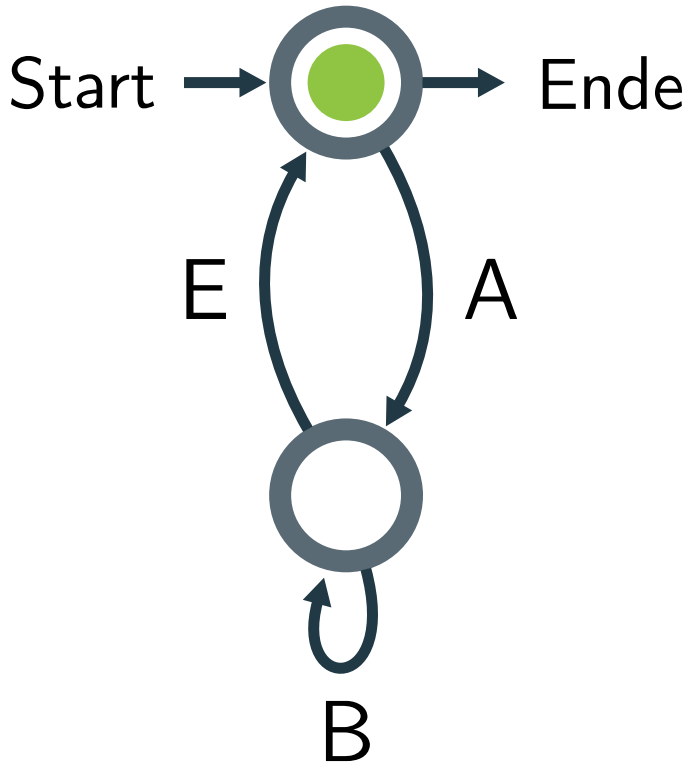


Was sind diese Automaten?



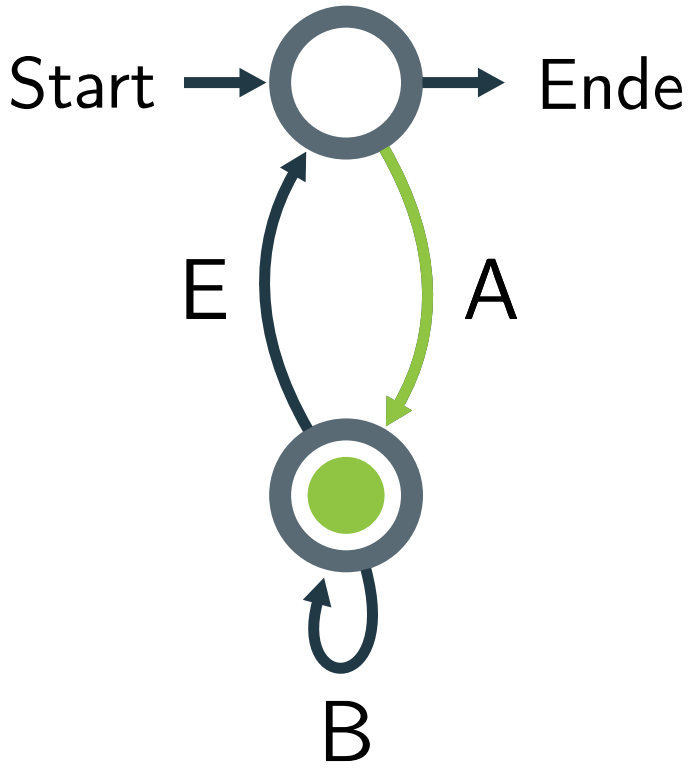
ABE

Was sind diese Automaten?



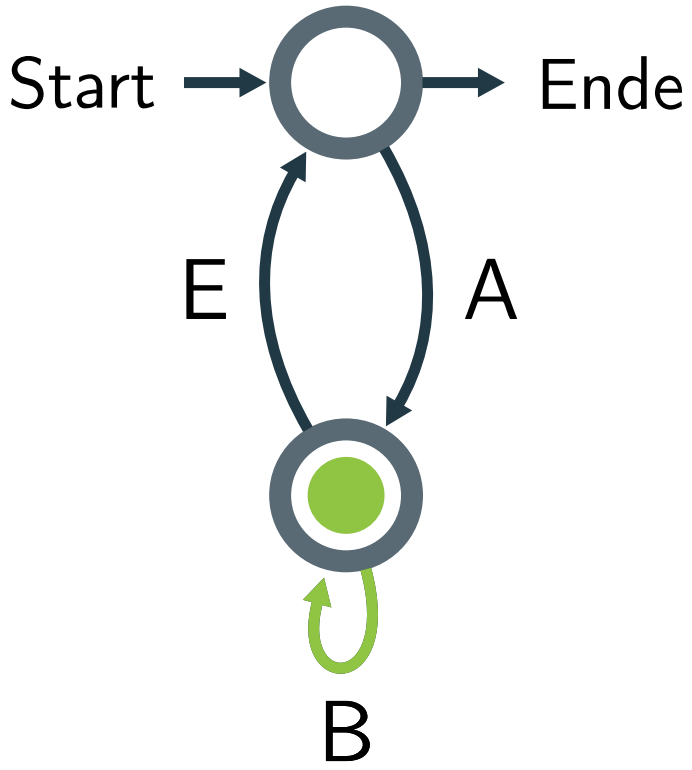
ABE

Was sind diese Automaten?



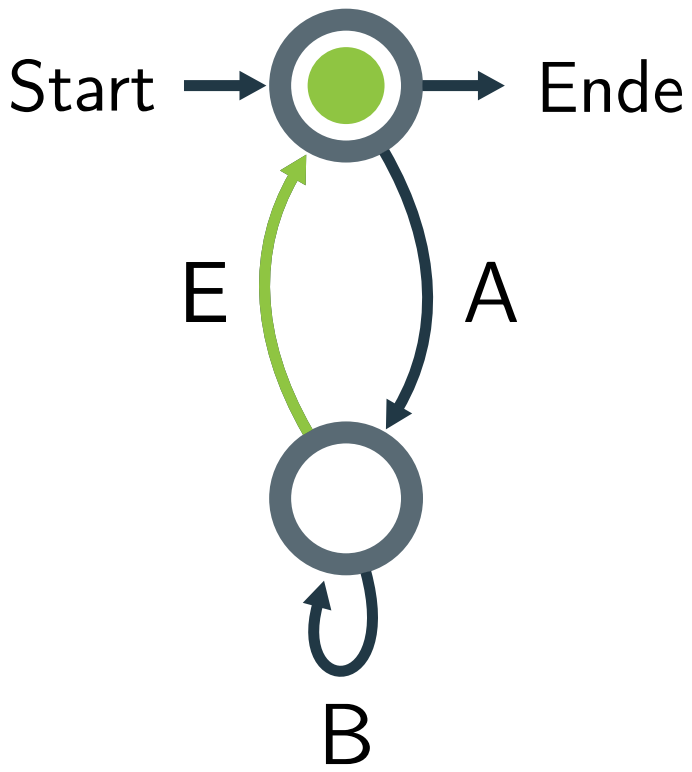
ABE

Was sind diese Automaten?



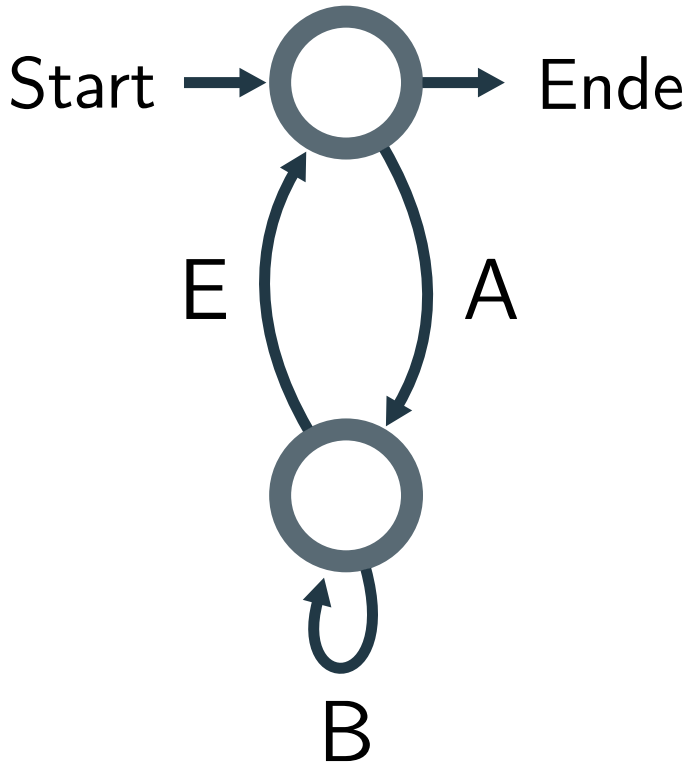
ABE

Was sind diese Automaten?



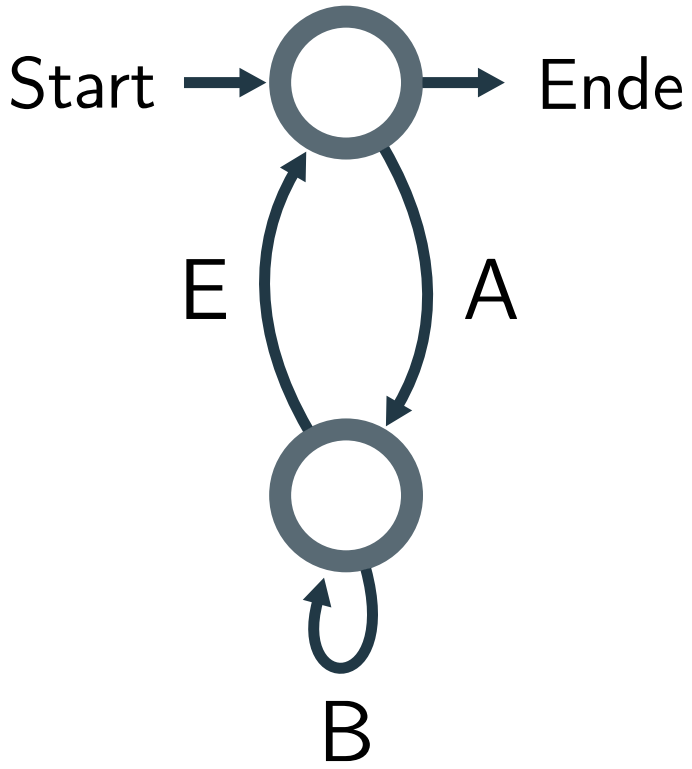
ABE

Was sind diese Automaten?



ABE

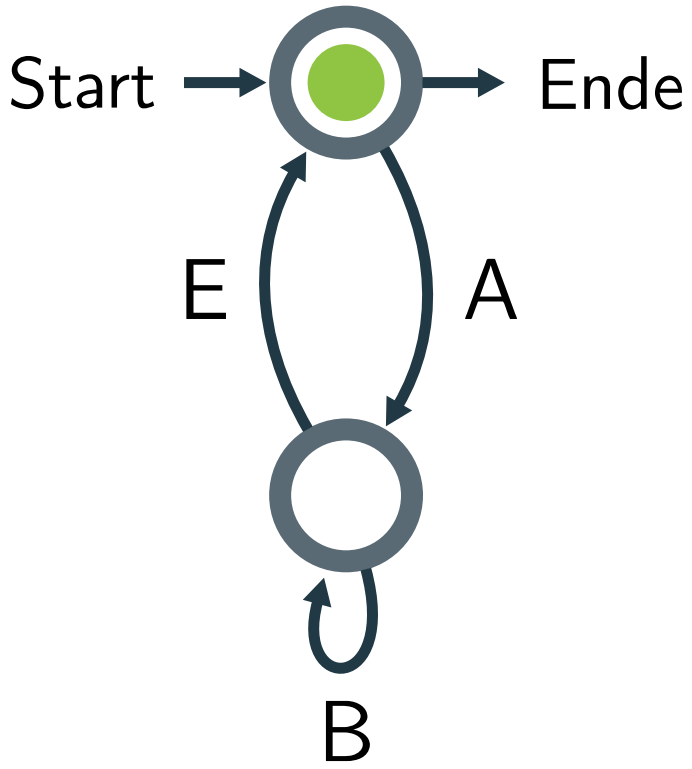
Was sind diese Automaten?



ABE

AAE

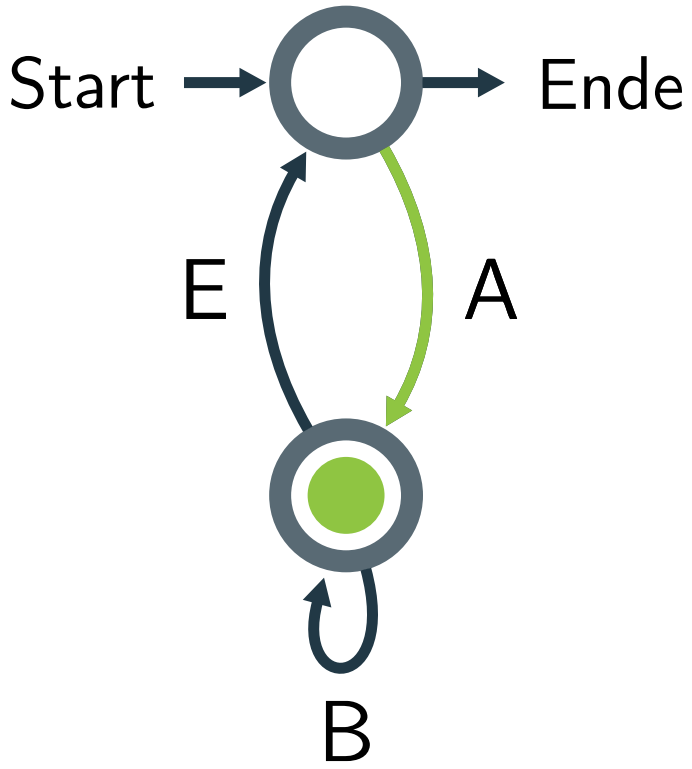
Was sind diese Automaten?



ABE

AAE

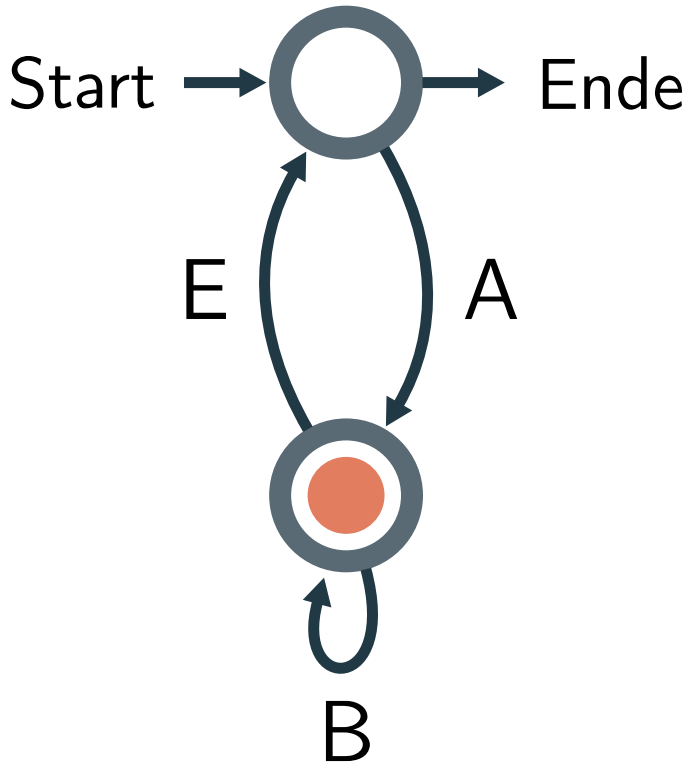
Was sind diese Automaten?



ABE

AAE

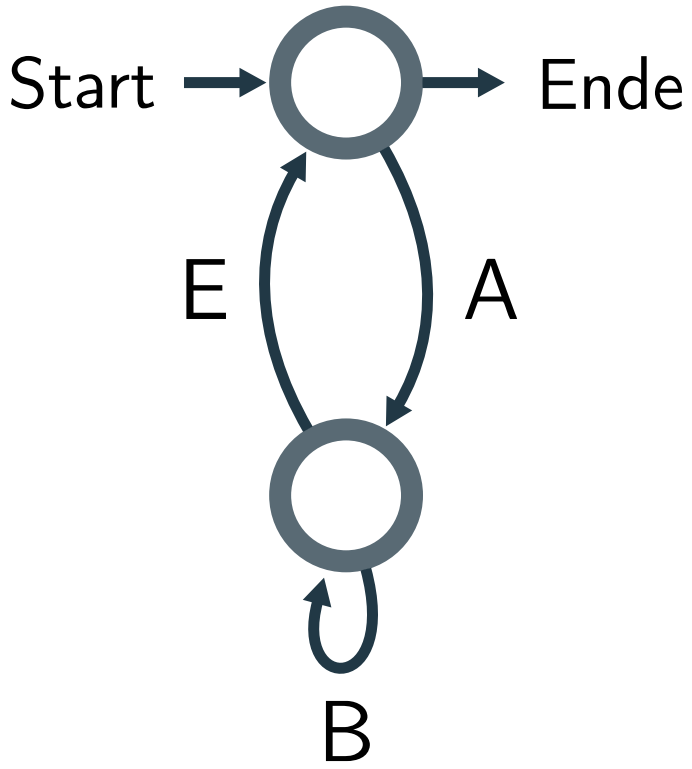
Was sind diese Automaten?



ABE

AAE

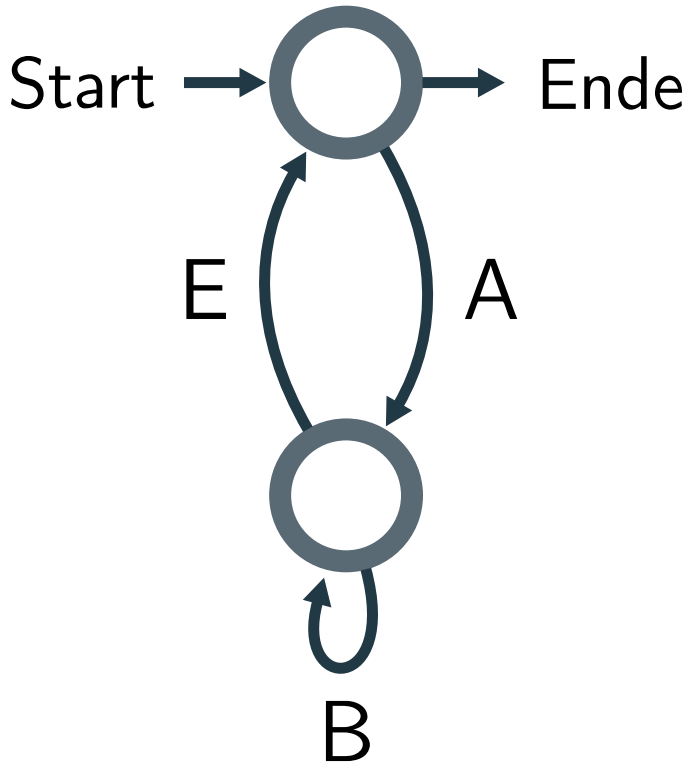
Was sind diese Automaten?



ABE ⭘

AAE ✖

Was sind diese Automaten?

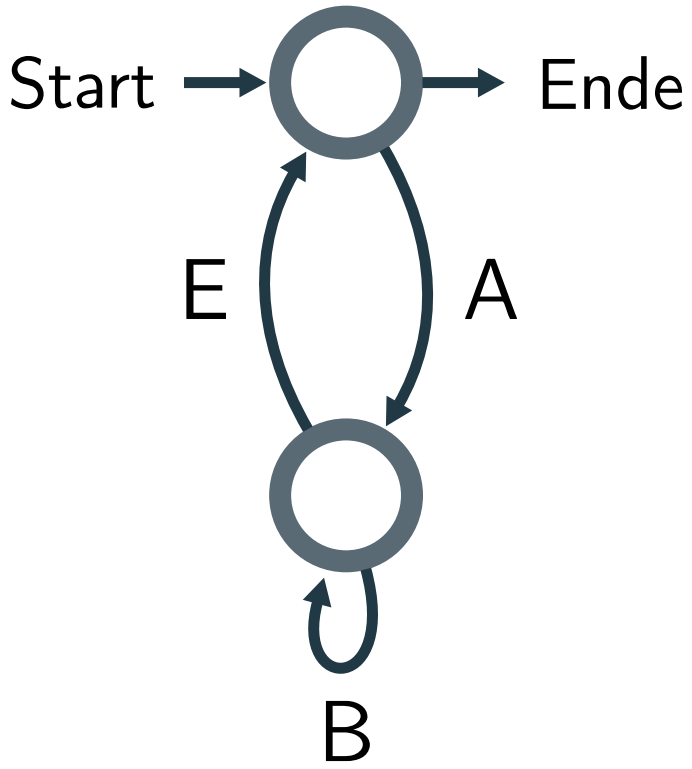


ABE ⭘

AAE ✖

ABEAE

Was sind diese Automaten?



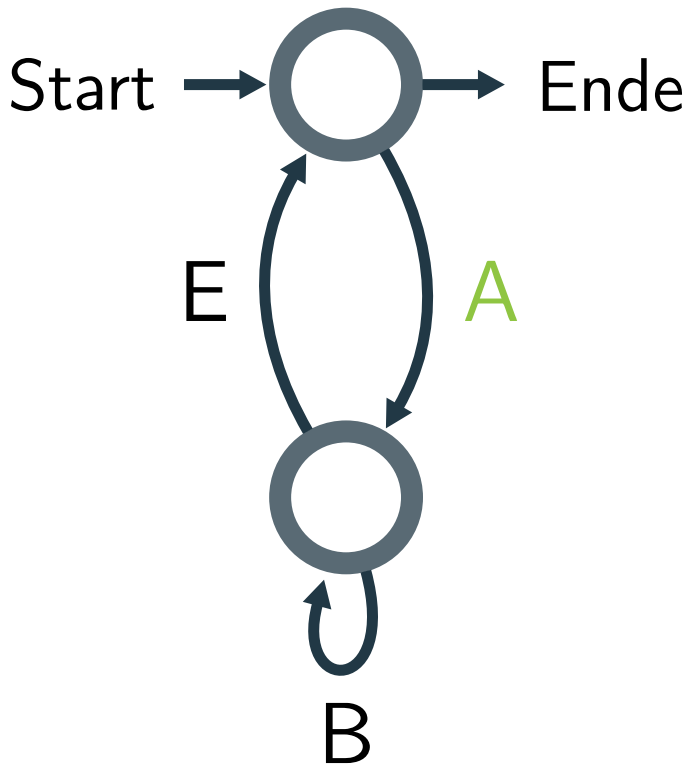
ABE ⭘

AAE ✖

ABEAE ⭘

Was sind diese Automaten?

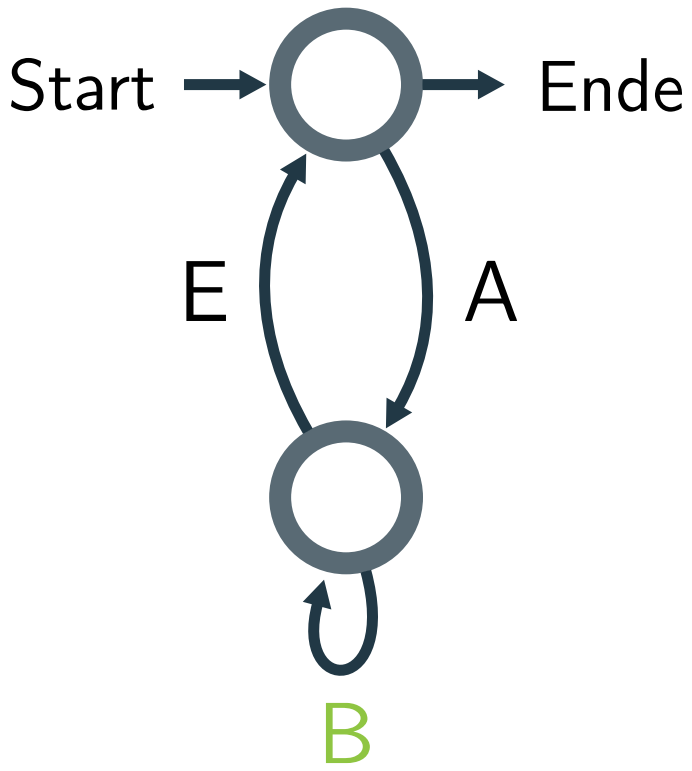
A $\hat{=}$ Aufnahme



ABE ⭘
AAE ✖
ABEAE ⭘

Was sind diese Automaten?

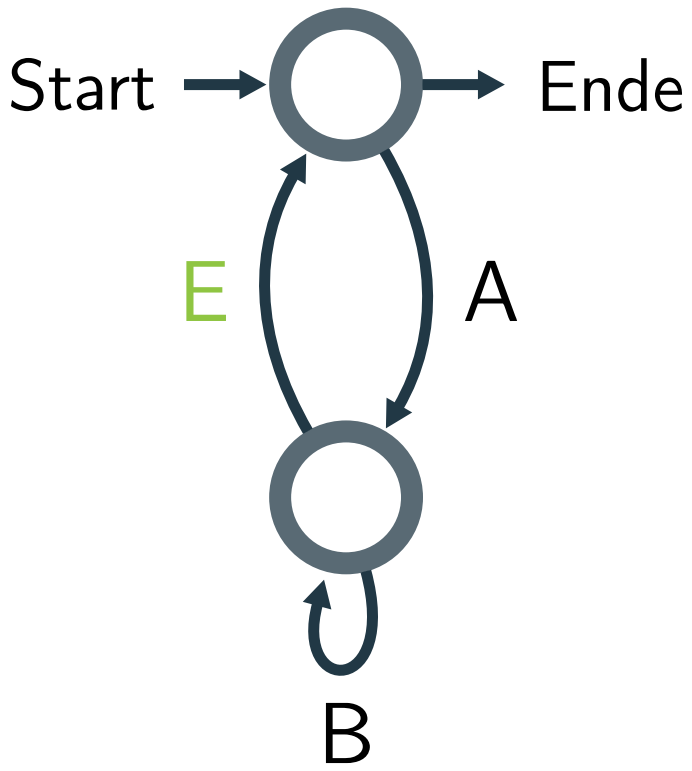
A $\hat{=}$ Aufnahme B $\hat{=}$ Bearbeitung



ABE	⊙
AAE	✖
ABEAE	⊙

Was sind diese Automaten?

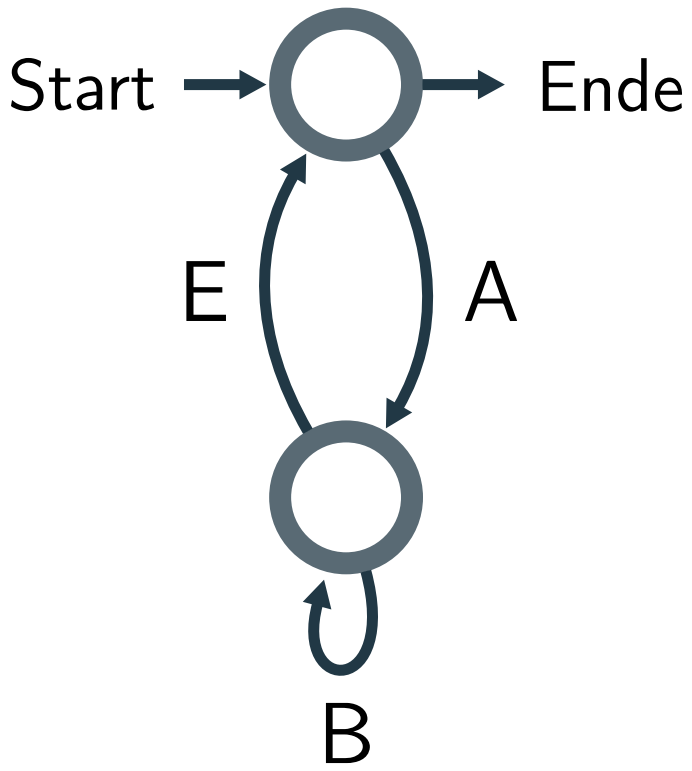
A ≙ Aufnahme B ≙ Bearbeitung E ≙ Einreichung



ABE ⊙
AAE ✖
ABEAE ⊙

Was sind diese Automaten?

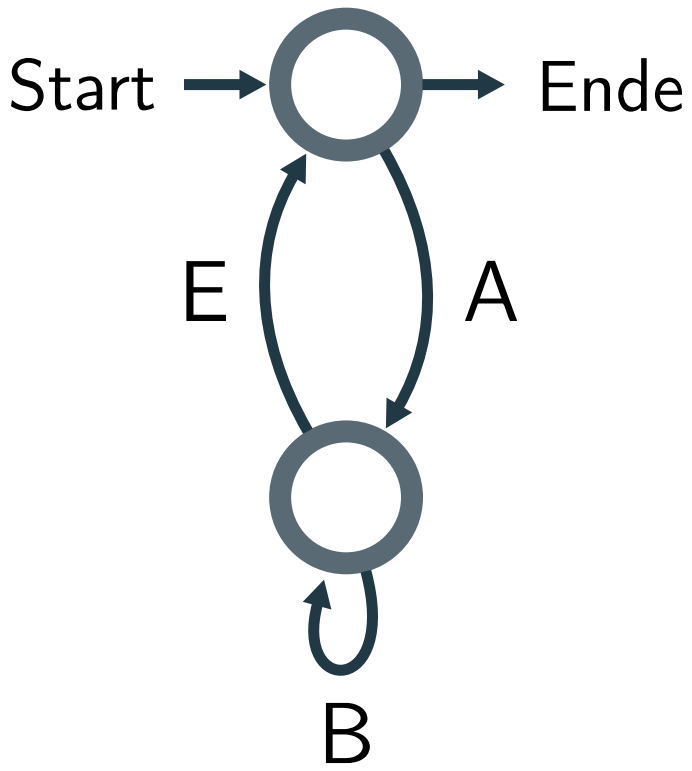
A ≙ Aufnahme B ≙ Bearbeitung E ≙ Einreichung



ABE ⊙
AAE ✖
ABEAE ⊙

Was sind diese Automaten?

A ≙ Aufnahme B ≙ Bearbeitung E ≙ Einreichung

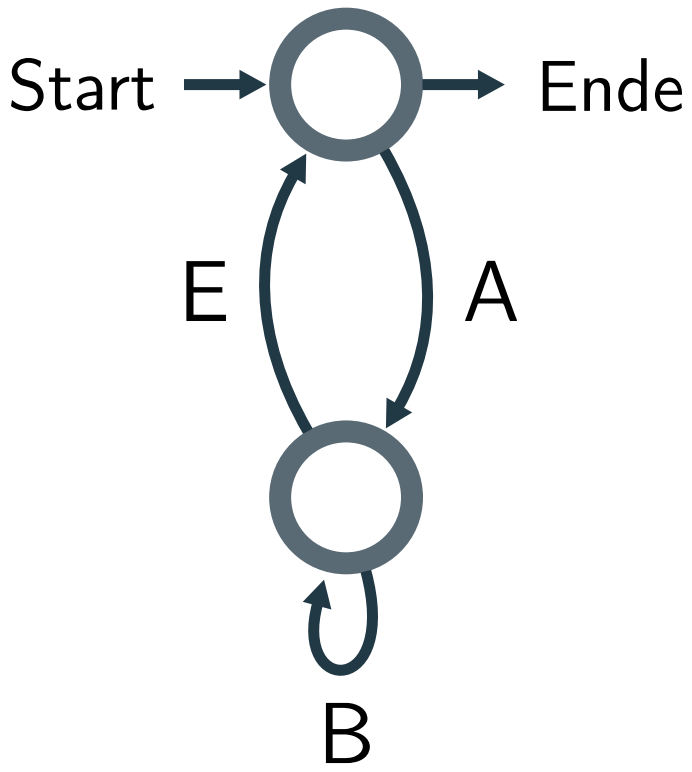


ABE ⭘
AAE ✖
ABEAE ⭘

Jede Aufnahme benötigt eine Einreichung, bevor eine neue Aufnahme erfolgt.

Was sind diese Automaten?

A $\hat{=}$ Aufnahme B $\hat{=}$ Bearbeitung E $\hat{=}$ Einreichung



ABE ⊙
AAE ✖
ABEAE ⊙

Jede Aufnahme benötigt eine Einreichung, bevor eine neue Aufnahme erfolgt.

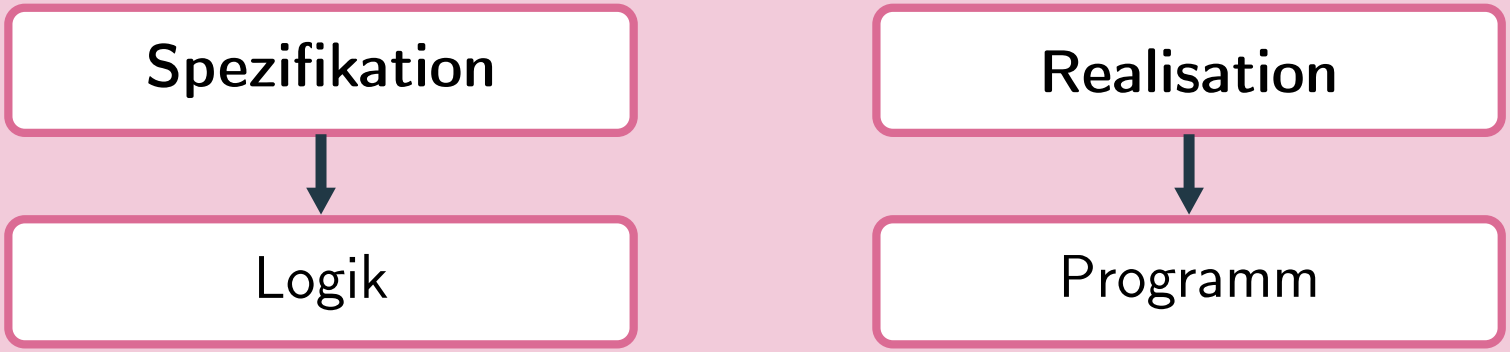
$|u|_A = |u|_E$ oder $|u|_A = |u|_E + 1$

Verifikation mit Modelchecking

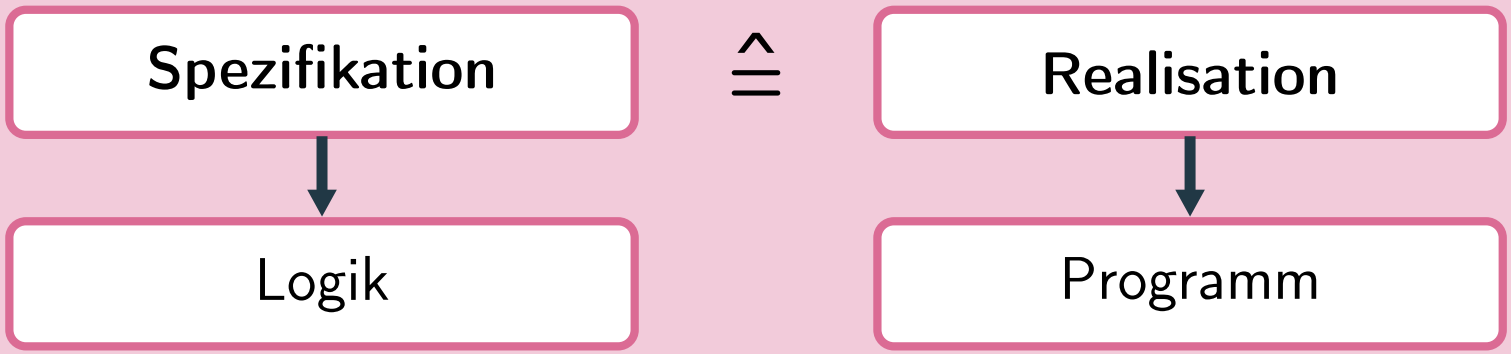
Spezifikation

Realisation

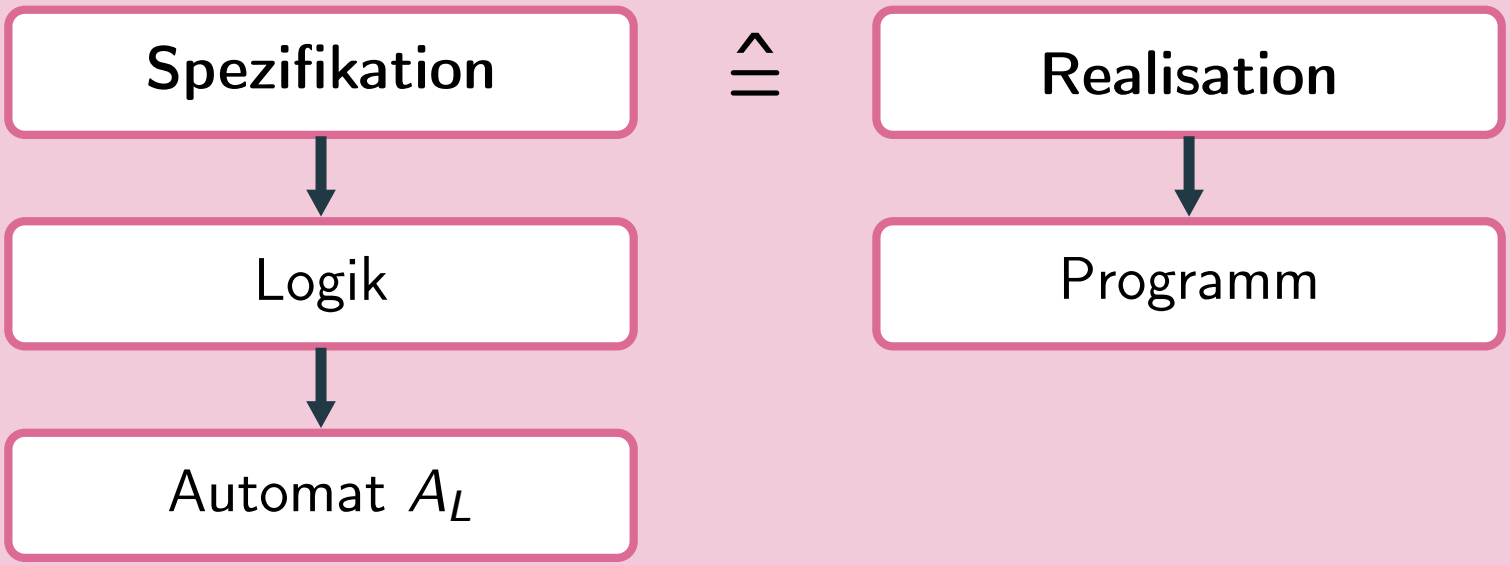
Verifikation mit Modelchecking



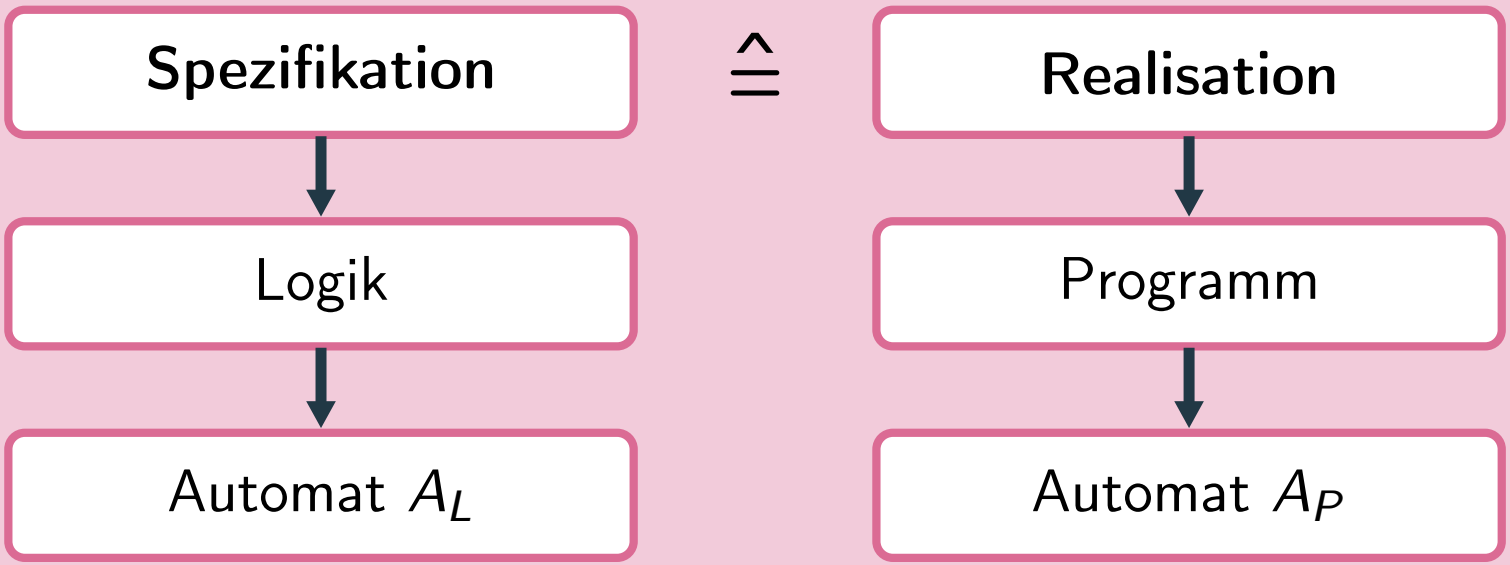
Verifikation mit Modelchecking



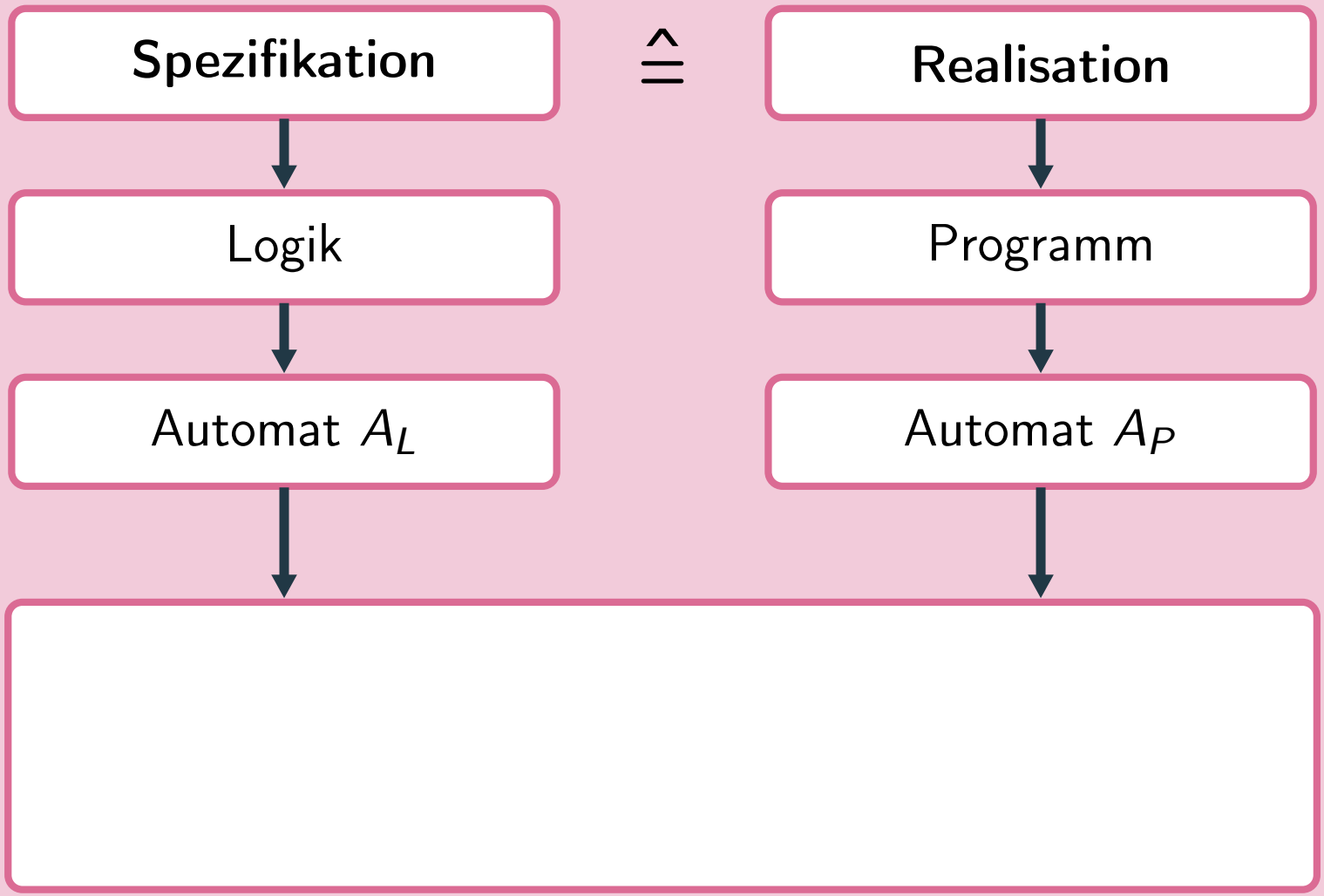
Verifikation mit Modelchecking



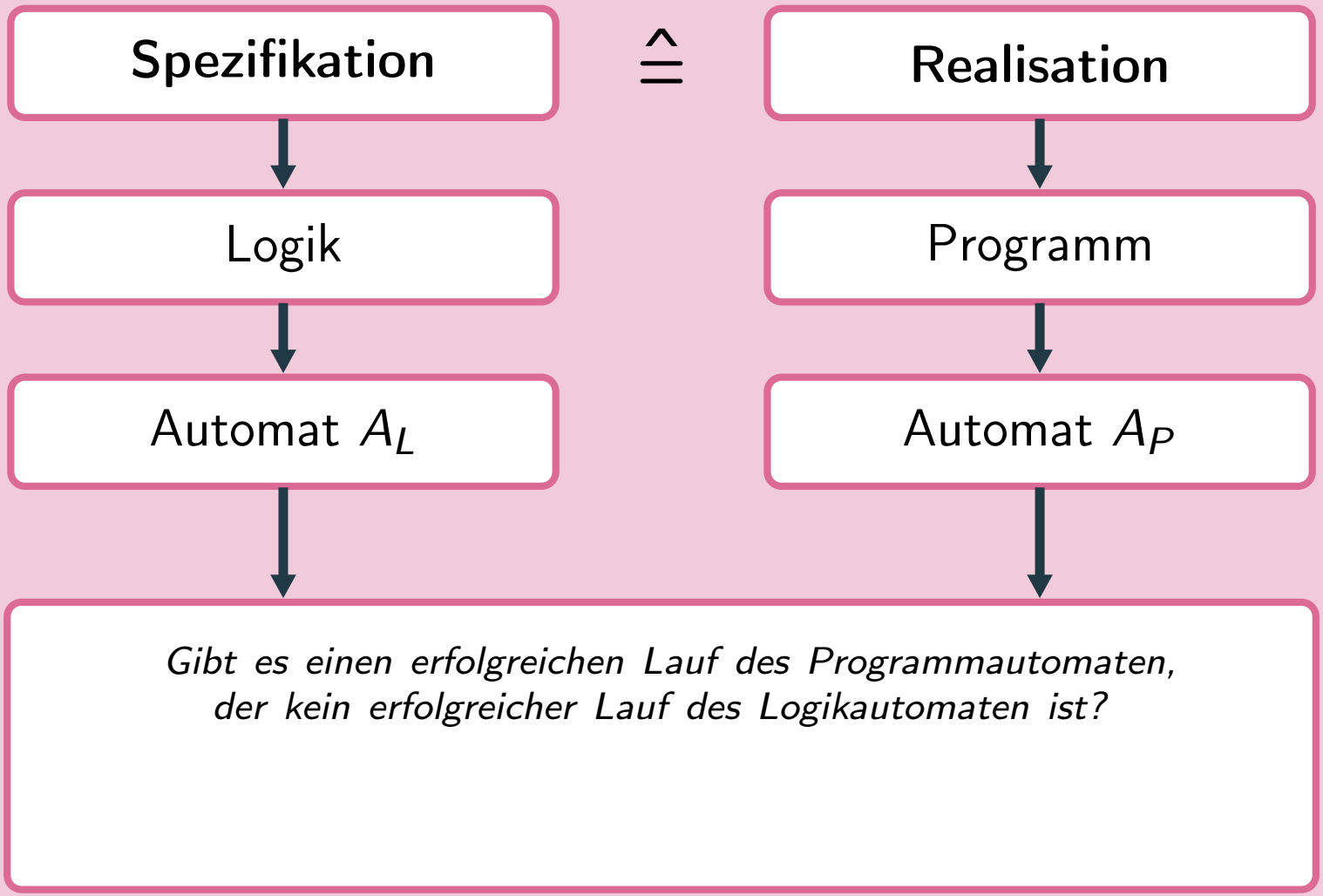
Verifikation mit Modelchecking



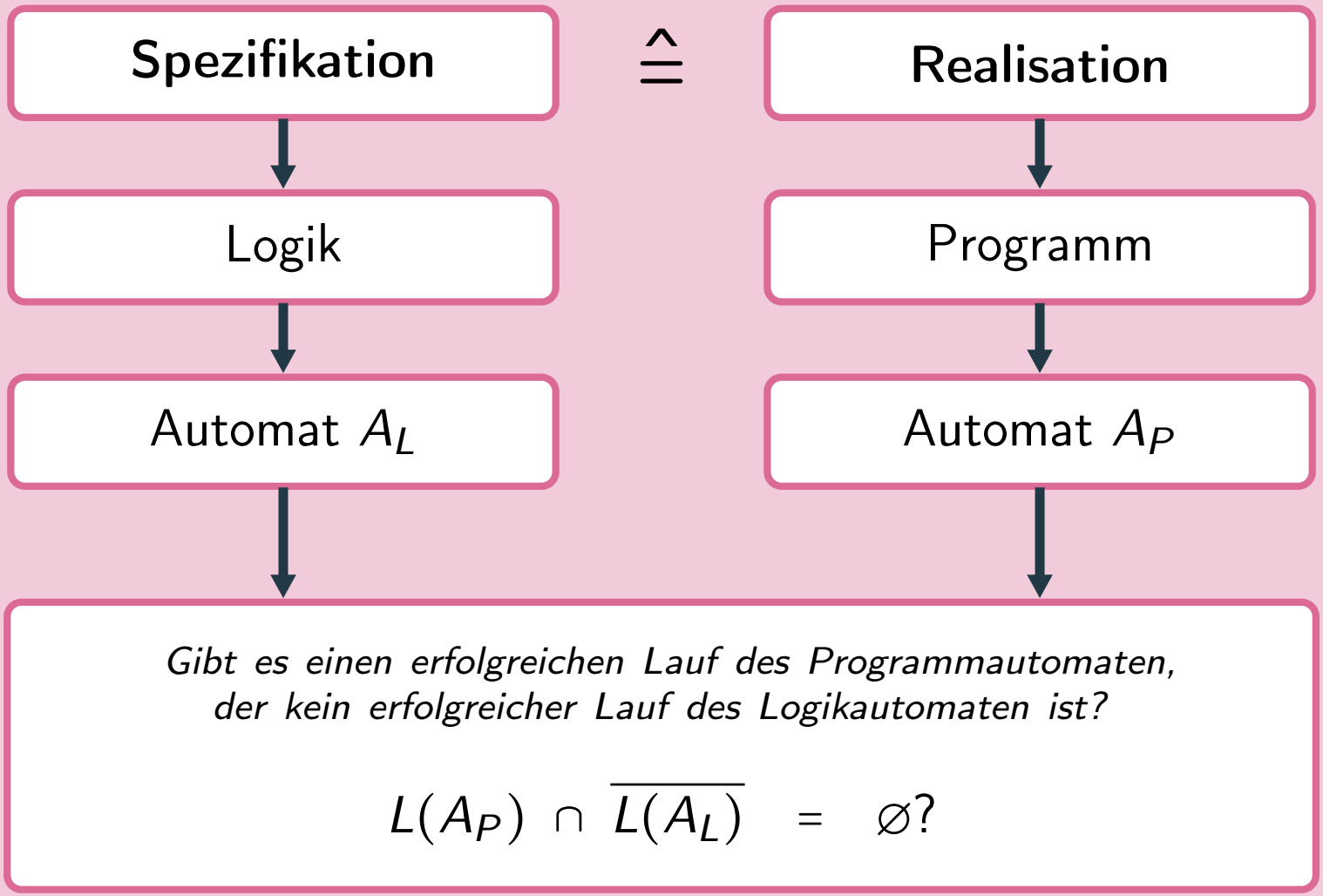
Verifikation mit Modelchecking



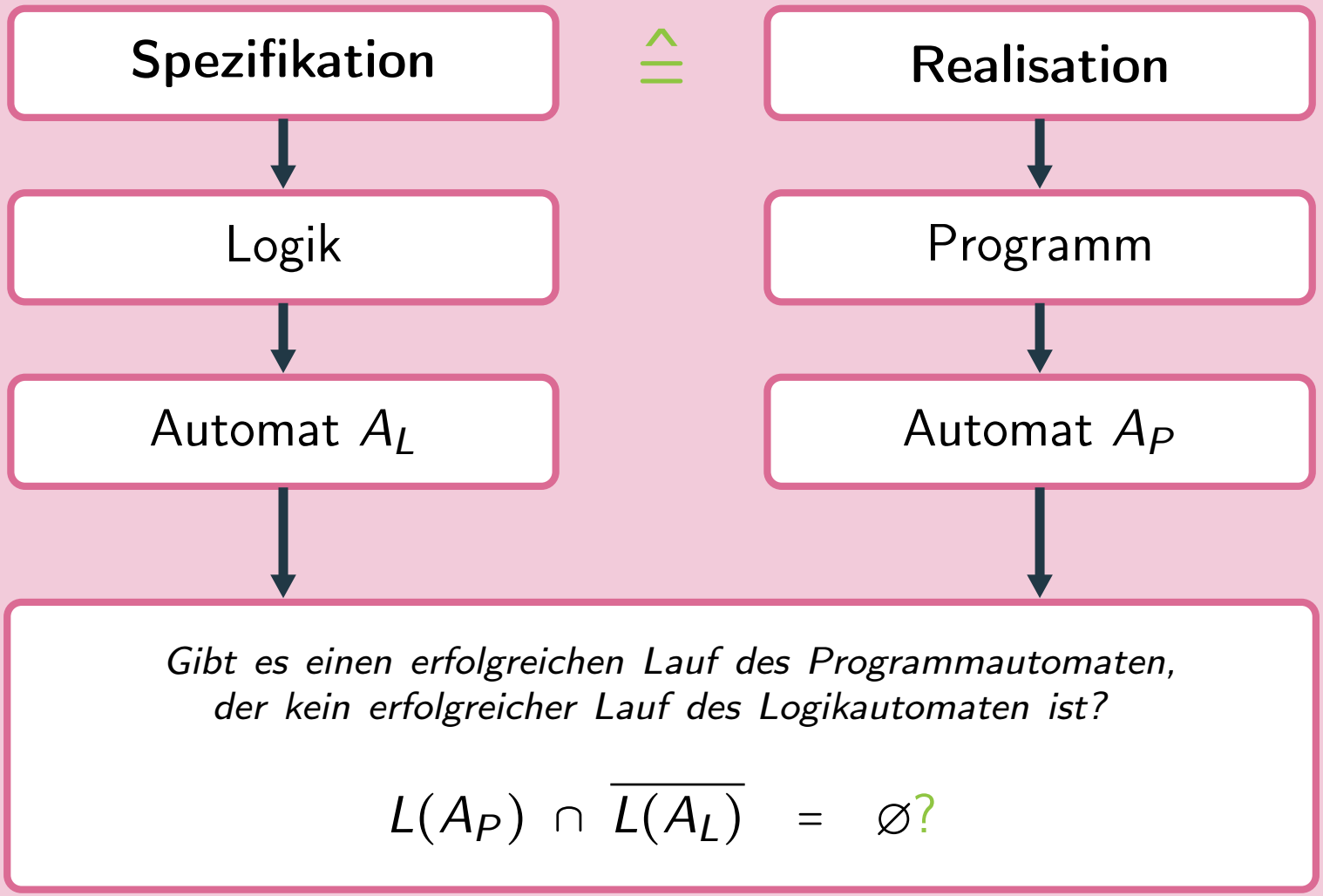
Verifikation mit Modelchecking



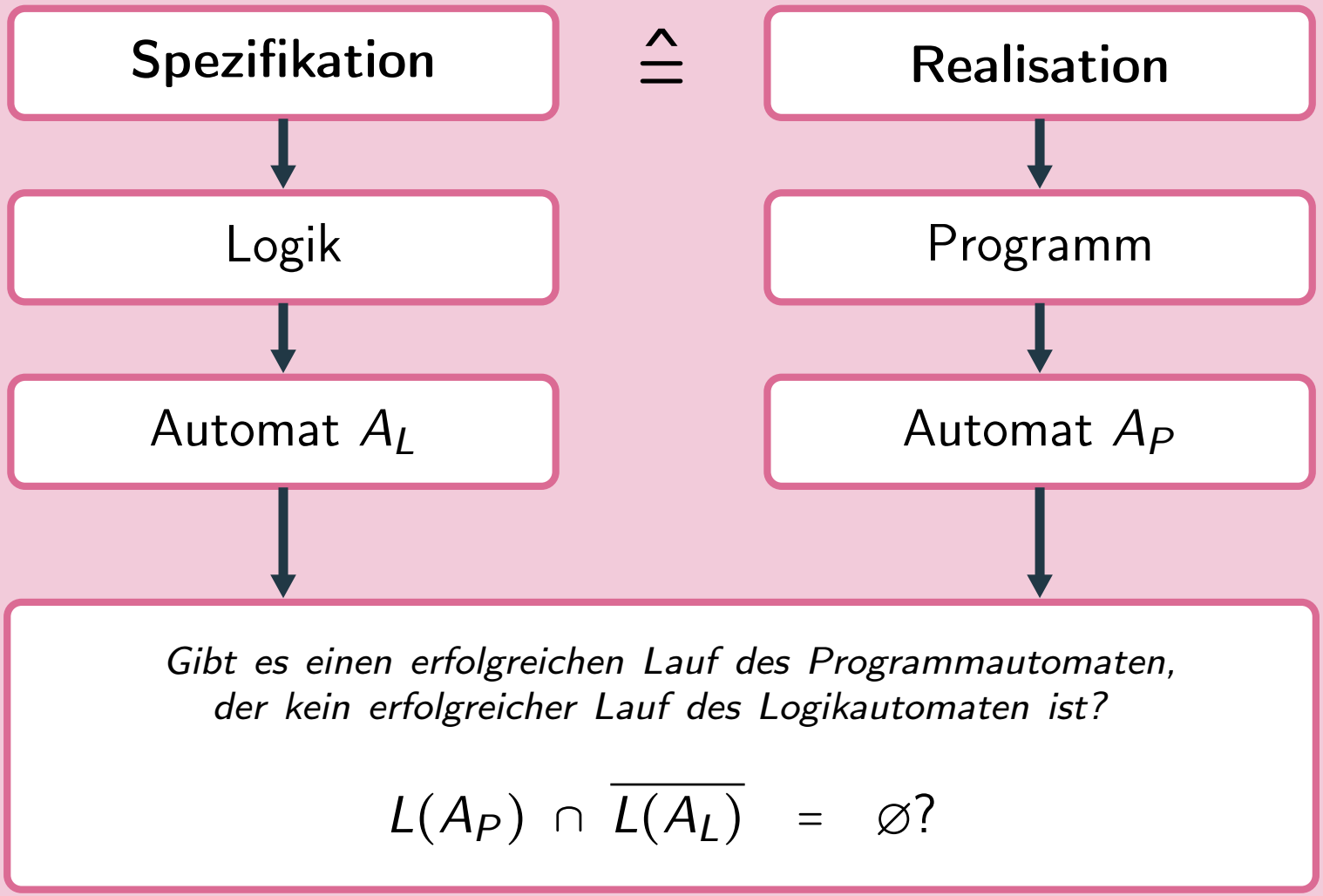
Verifikation mit Modelchecking



Verifikation mit Modelchecking



Verifikation mit Modelchecking



Modelchecking in Aktion: Promela+LTL+Spin

Modelchecking im Finanzwesen

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

Ergebnisse:

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

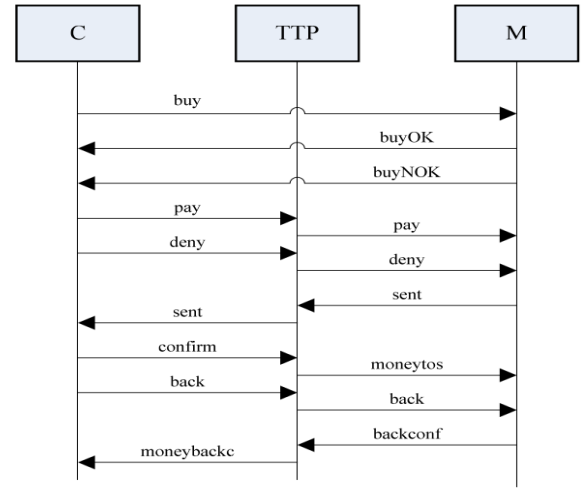


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

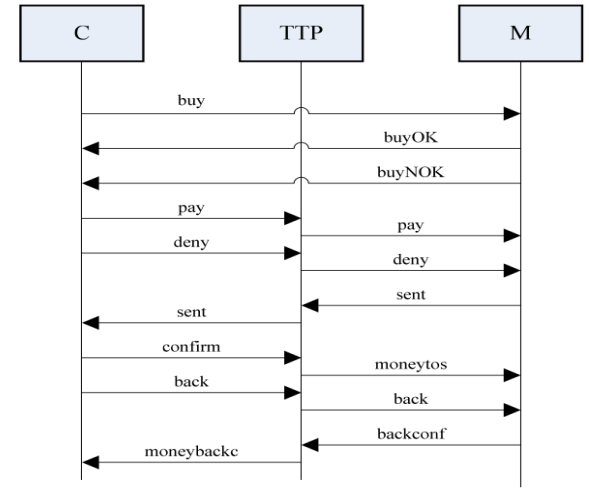


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

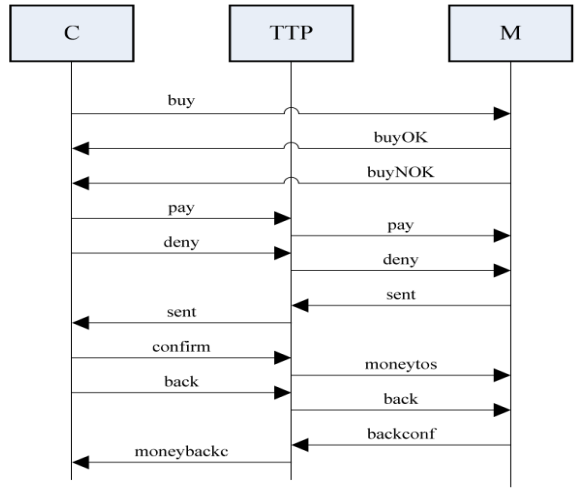


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

- Modell in Promela

```
.....
chan customer_netpay=[0] of {mtype};
chan customer_seller=[0] of {int};
chan seller_netpay=[0] of {mtype};
chan netpay_customer=[0] of {mtype};
chan seller_customer=[0] of {mtype};
chan netpay_seller=[0] of {mtype};
.....
```

Figure 5. Fragment of the channels' definition in PROMELA

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

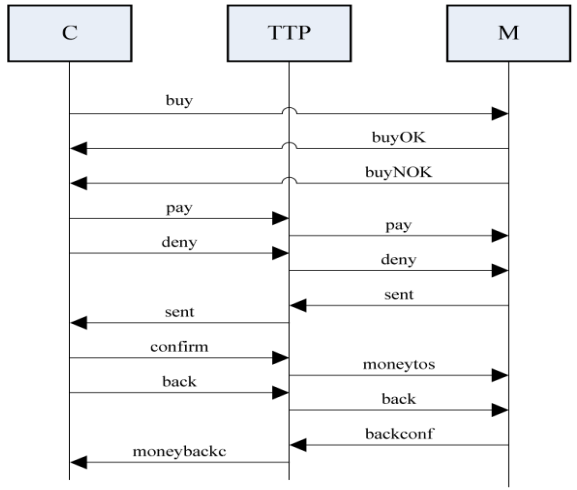


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

- Modell in Promela
- Spezifikation in LTL

```
……
chan customer_netpay=[0] of {mtype};
chan customer_seller=[0] of {int};
chan seller_netpay=[0] of {mtype};
chan netpay_customer=[0] of {mtype};
chan seller_customer=[0] of {mtype};
chan netpay_seller=[0] of {mtype};
……
```

Figure 5. Fragment of the channels' definition in PROMELA

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

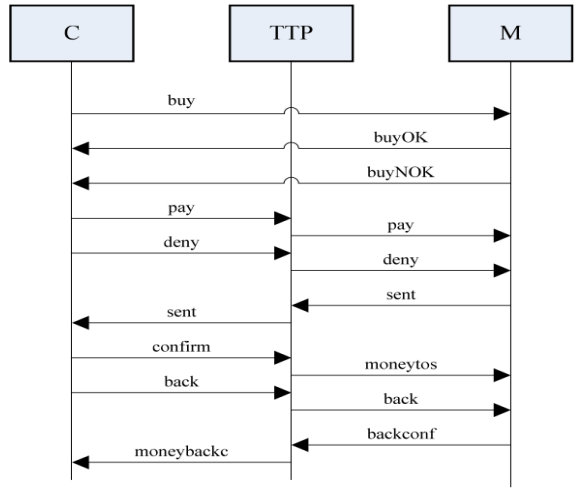


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

- Modell in Promela
- Spezifikation in LTL
- Erfolgreiche Verifikation des Modells

```
.....
chan customer_netpay=[0] of {mtype};
chan customer_seller=[0] of {int};
chan seller_netpay=[0] of {mtype};
chan netpay_customer=[0] of {mtype};
chan seller_customer=[0] of {mtype};
chan netpay_seller=[0] of {mtype};
.....
```

Figure 5. Fragment of the channels' definition in PROMELA

Modelchecking im Finanzwesen

Model Checking and Verification of the Internet Payment System with SPIN

Wei Zhang et al., Journal of Software, Vol. 7, No. 9, September 2012.

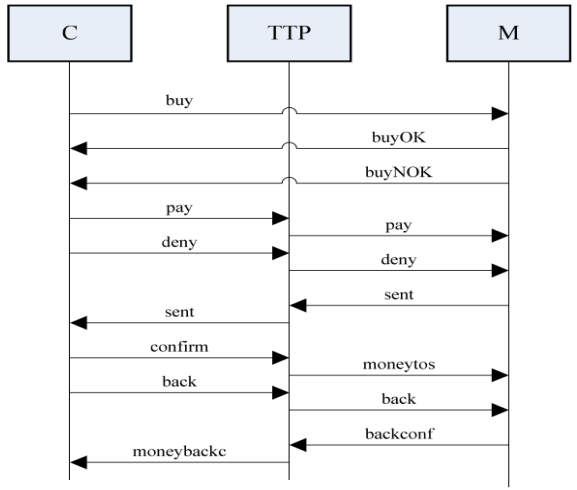


Figure 1. Massage flow in the Internet Payment Systems

Ergebnisse:

- Modell in Promela
- Spezifikation in LTL
- Erfolgreiche Verifikation des Modells

```
……
chan customer_netpay=[0] of {mtype};
chan customer_seller=[0] of {int};
chan seller_netpay=[0] of {mtype};
chan netpay_customer=[0] of {mtype};
chan seller_customer=[0] of {mtype};
chan netpay_seller=[0] of {mtype};
……
```

Figure 5. Fragment of the channels' definition in PROMELA

Der Preis der Sicherheit

Der Preis der Sicherheit

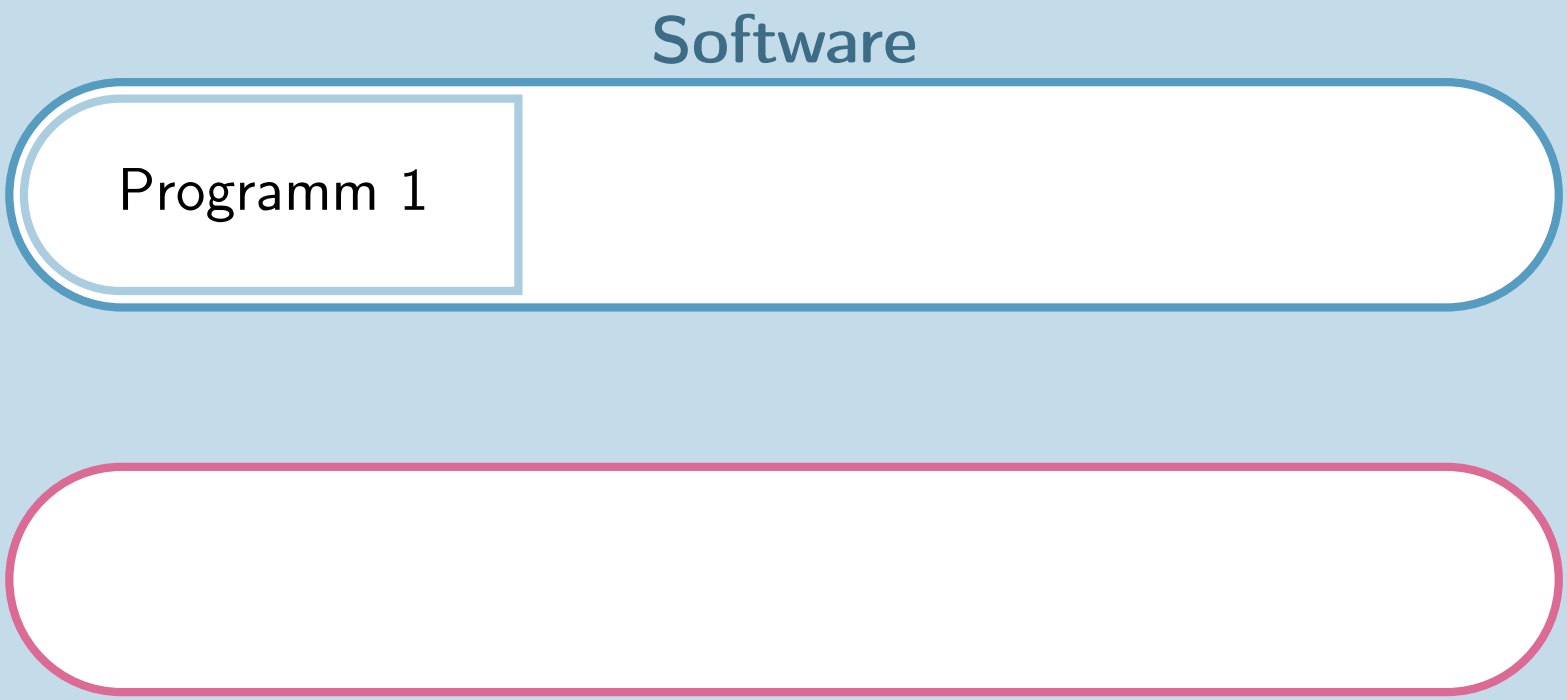
Software

Der Preis der Sicherheit

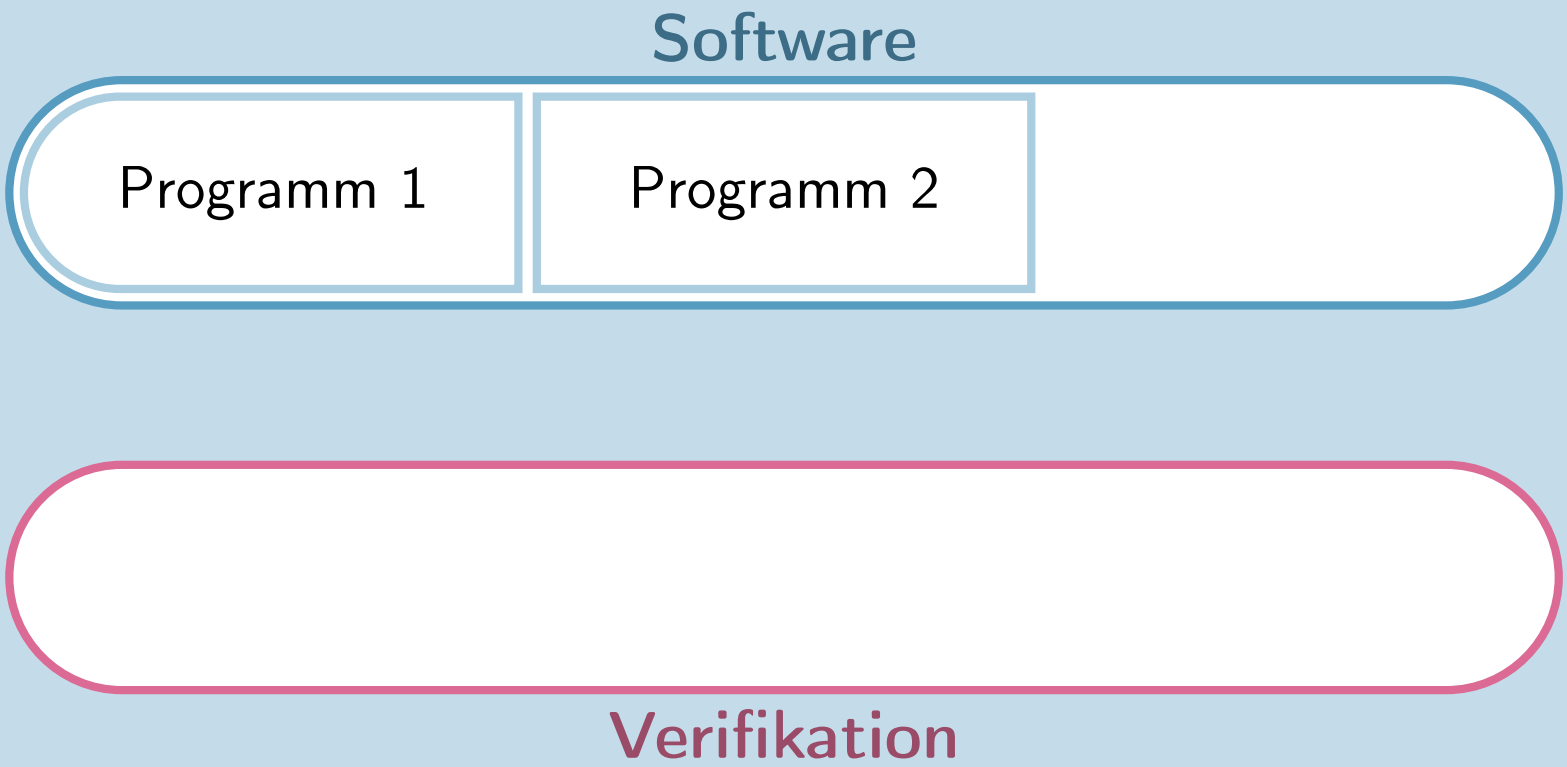
Software

Verifikation

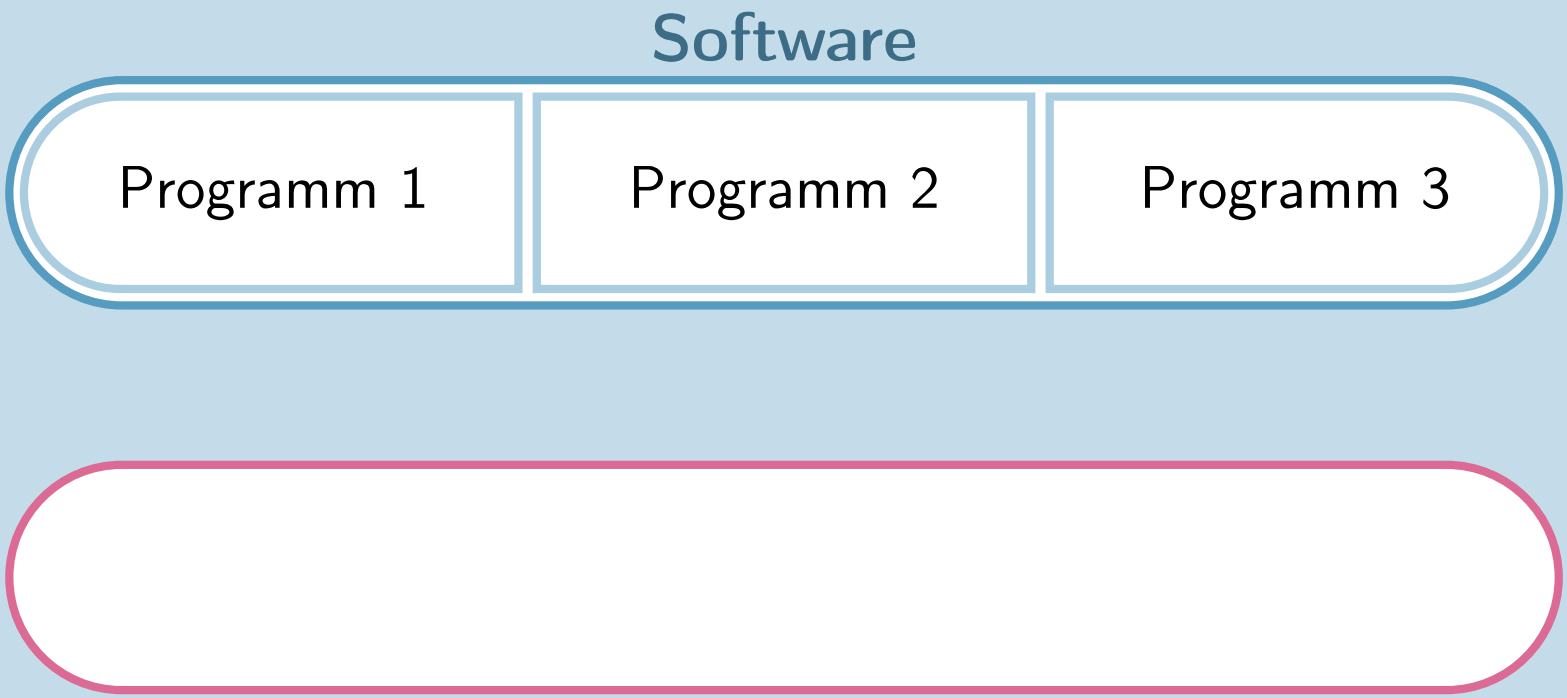
Der Preis der Sicherheit



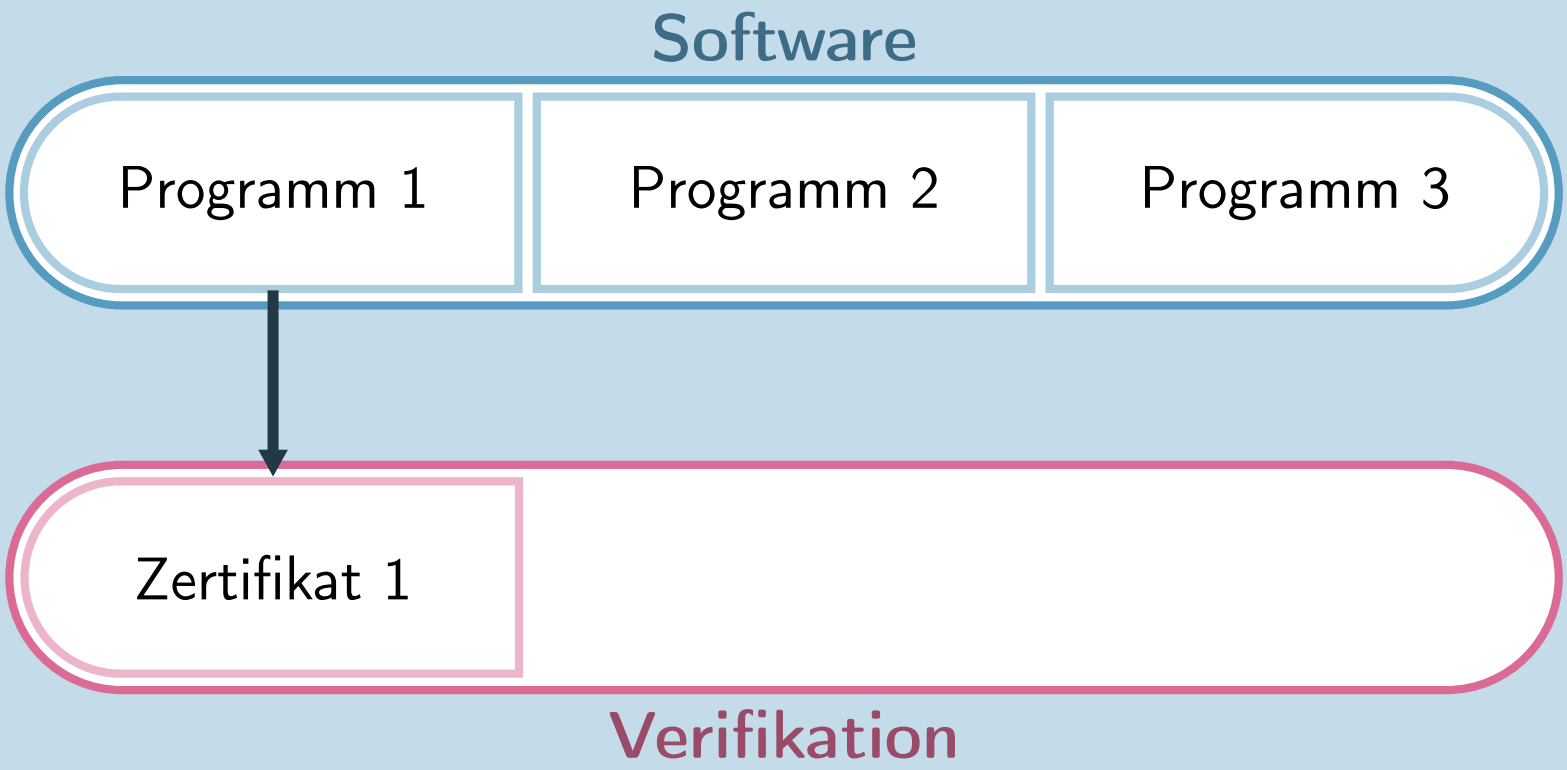
Der Preis der Sicherheit



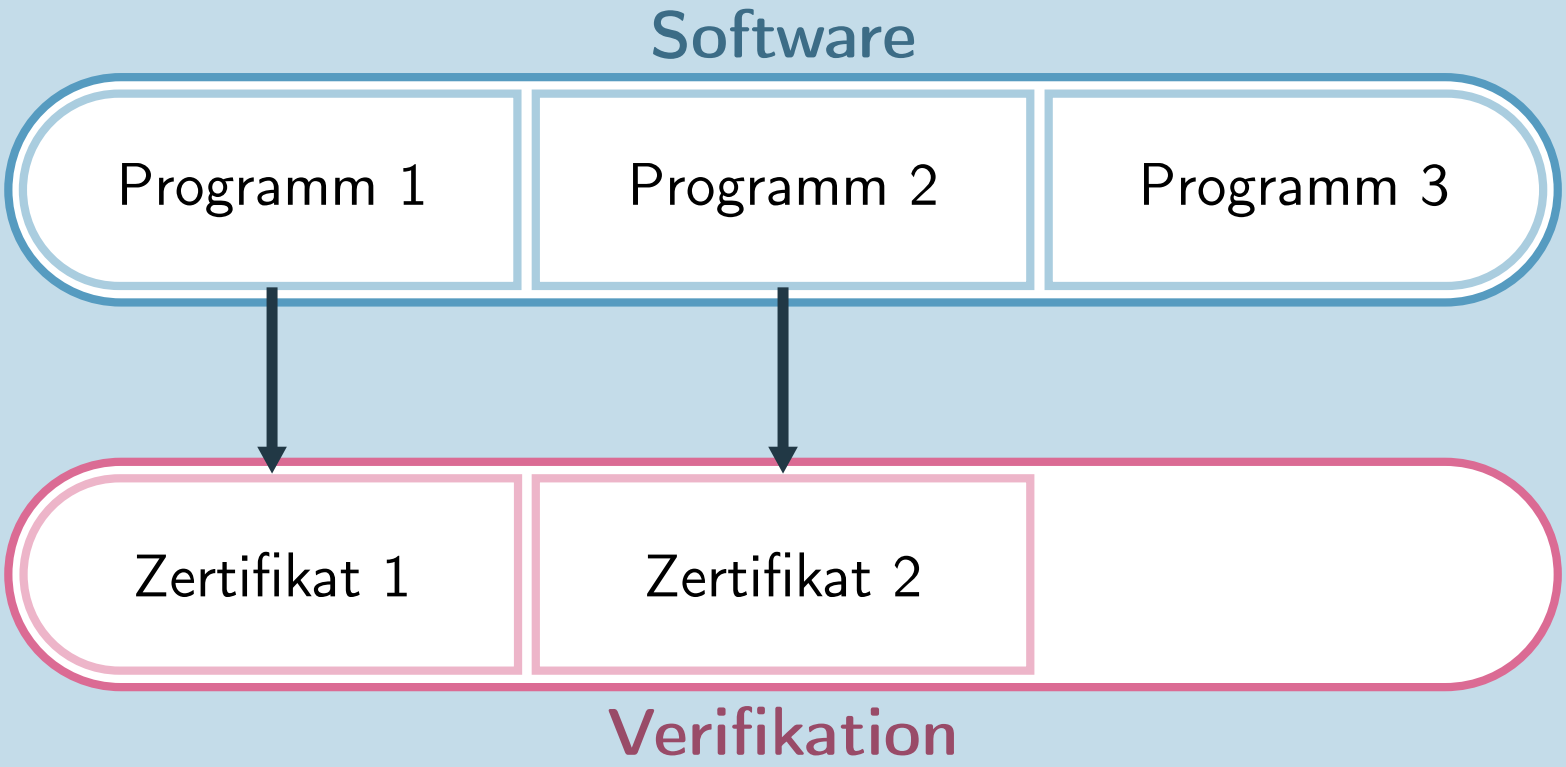
Der Preis der Sicherheit



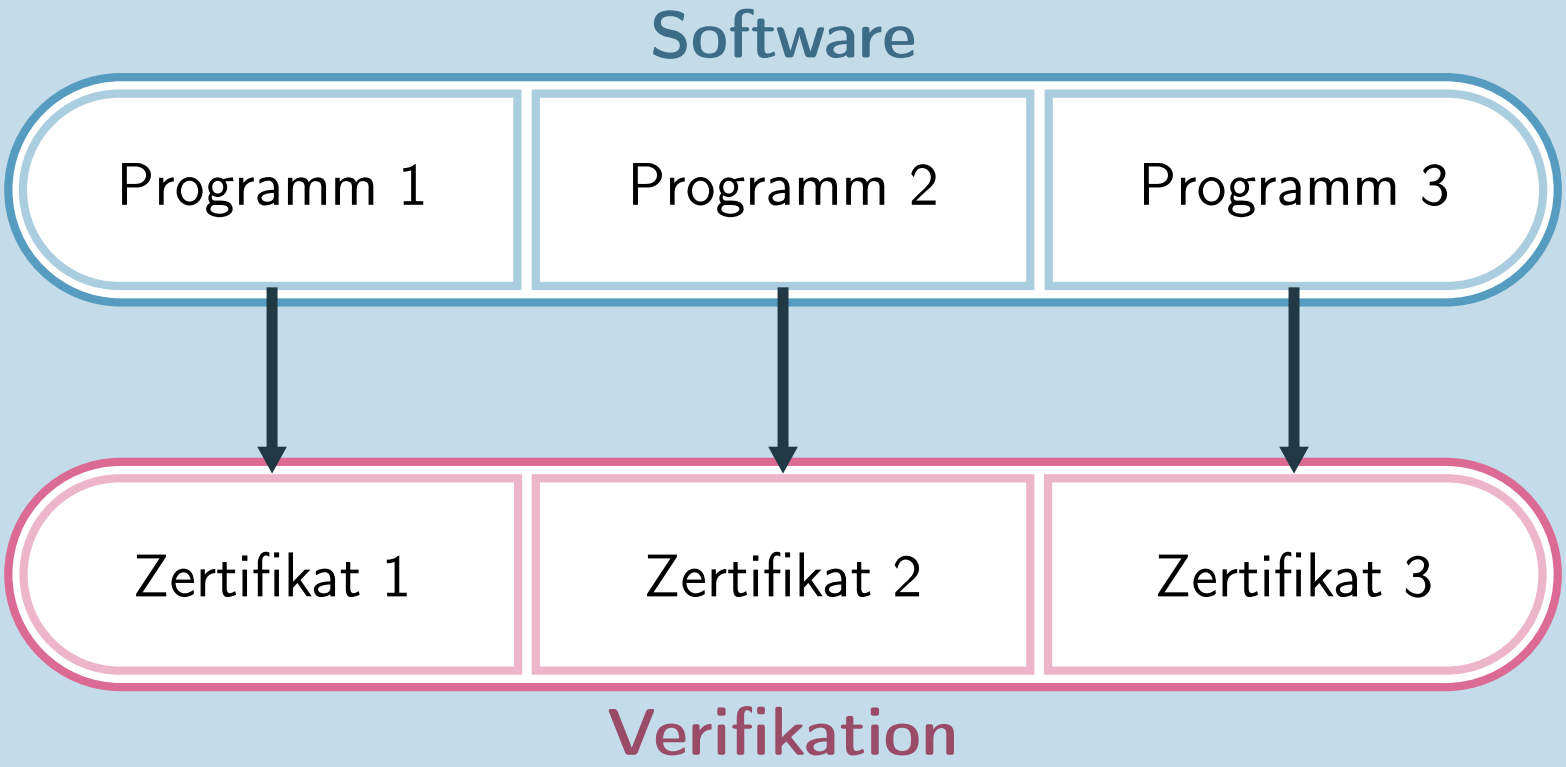
Der Preis der Sicherheit



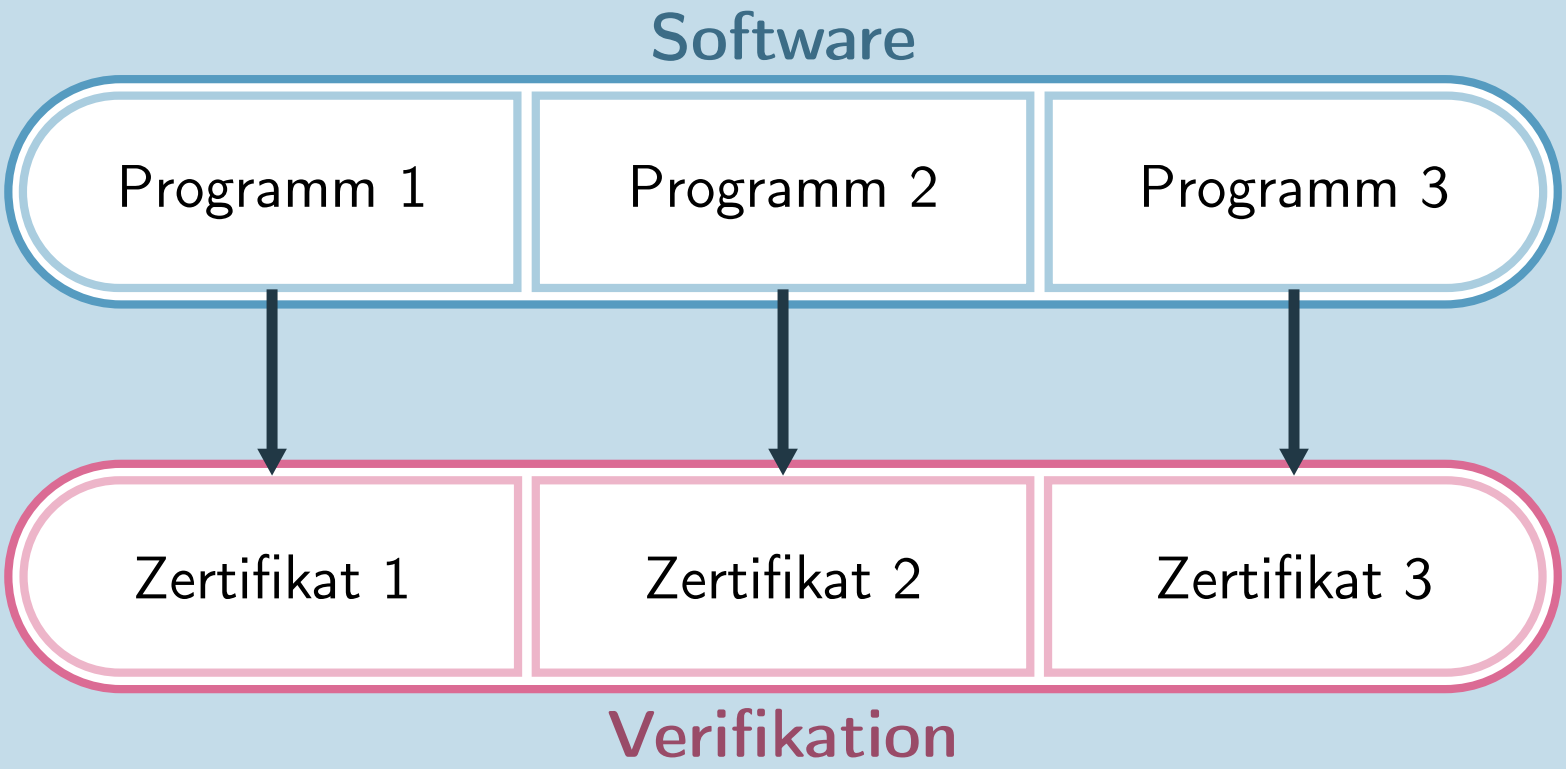
Der Preis der Sicherheit



Der Preis der Sicherheit



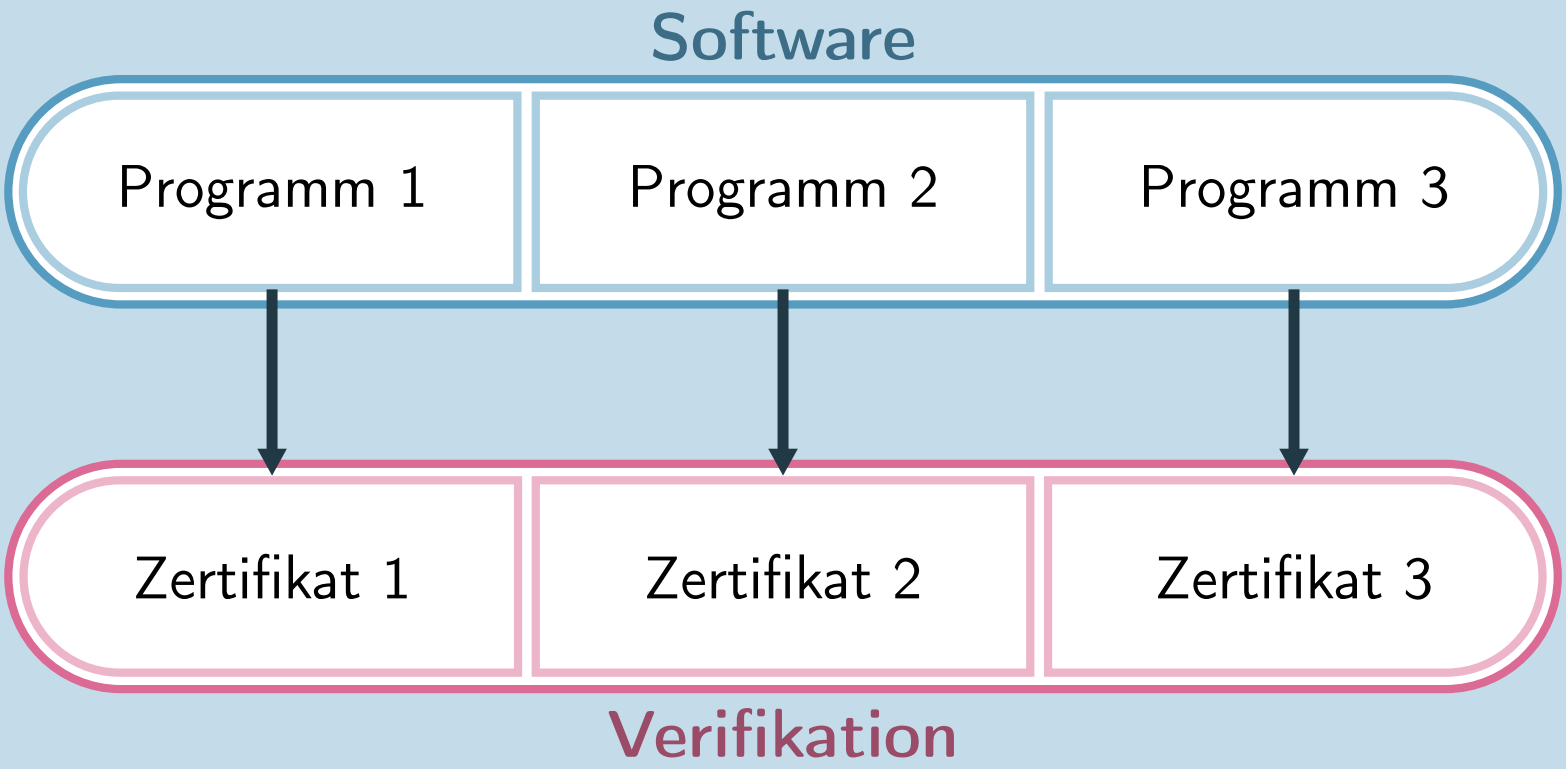
Der Preis der Sicherheit



Kosten Verifikation

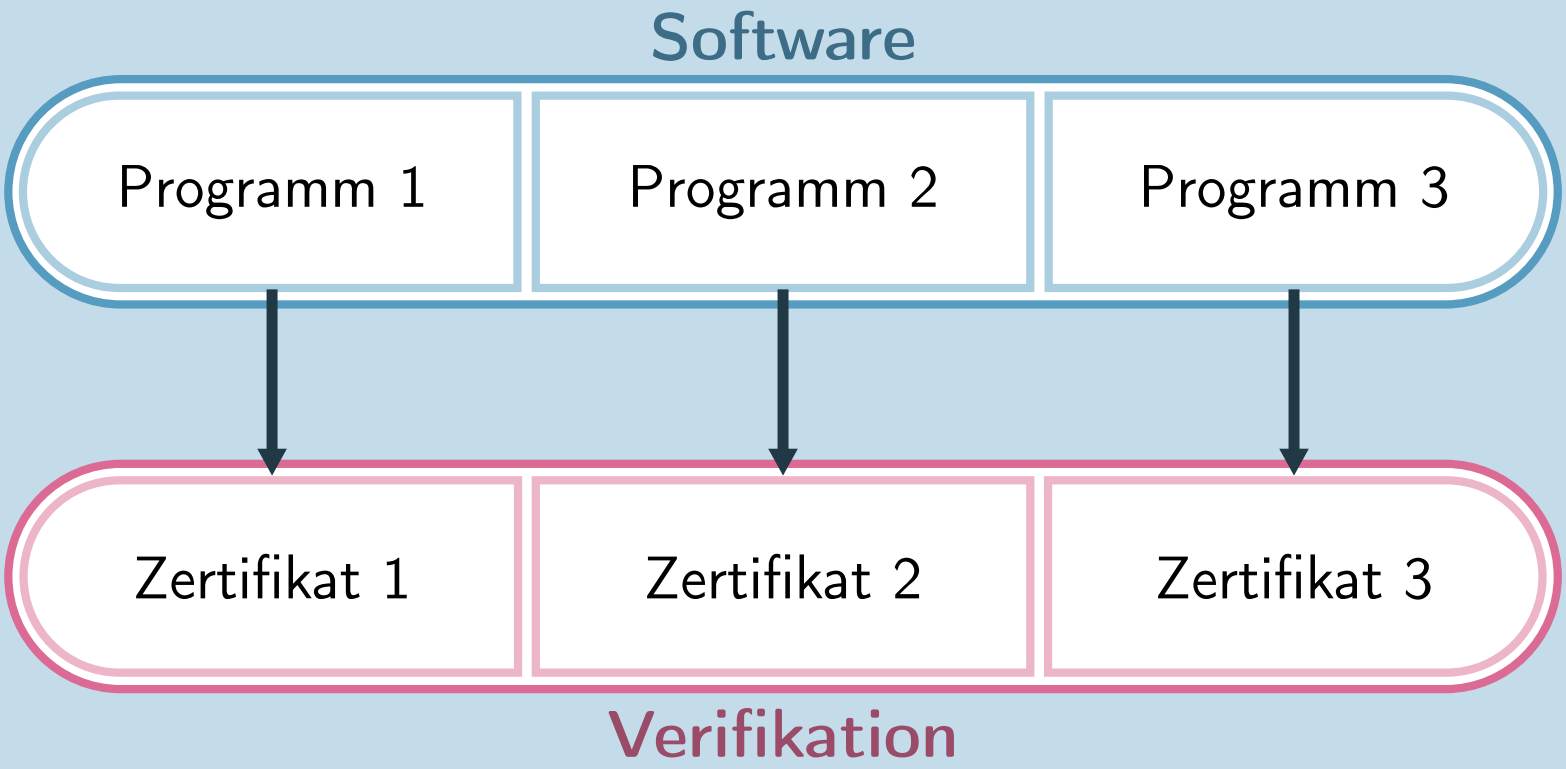
Kosten Systemausfall

Der Preis der Sicherheit



Kosten Verifikation $>$ Kosten Systemausfall

Der Preis der Sicherheit



Kosten Verifikation $<$ / $>$ Kosten Systemausfall

Modelchecking in Bahnsteuerungssystemen

Proving Completeness of Properties in Formal Verification of Counting Heads for Railways

---

Kinder, Sebastian, and Rolf Drechsler, 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007). IEEE, 2007.

Modelchecking in Bahnsteuerungssystemen

Proving Completeness of Properties in Formal Verification of Counting Heads for Railways

---

Kinder, Sebastian, and Rolf Drechsler, 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007). IEEE, 2007.

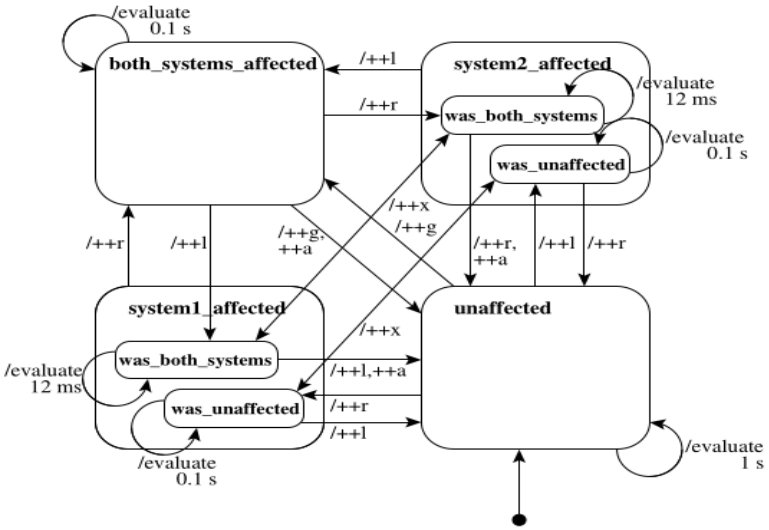


Figure 4. FSM of the Counting Head [8]

Modelchecking in Bahnsteuerungssystemen

Proving Completeness of Properties in Formal Verification of Counting Heads for Railways

---

Kinder, Sebastian, and Rolf Drechsler, 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007). IEEE, 2007.

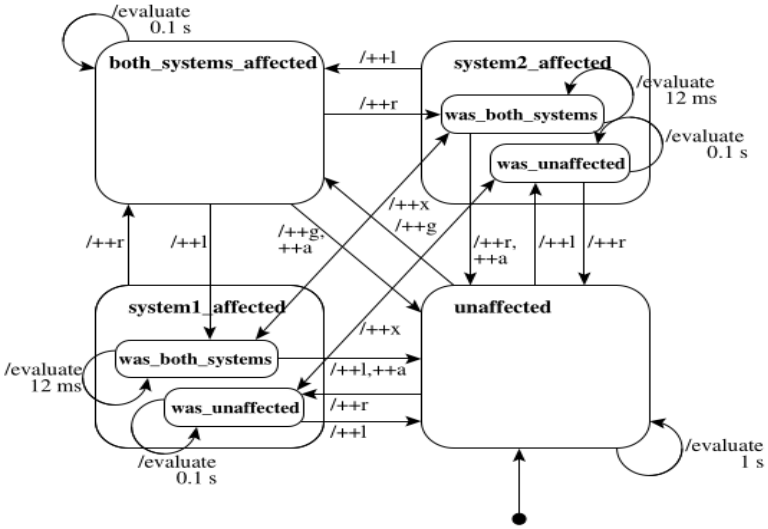
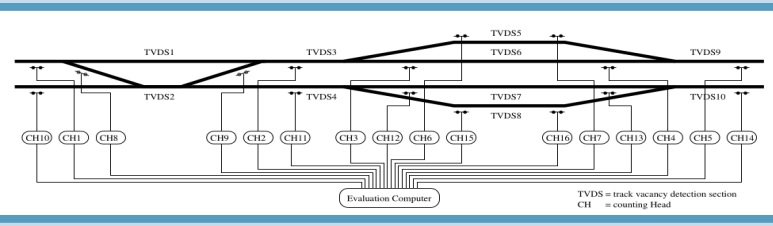


Figure 4. FSM of the Counting Head [8]



Modelchecking in Bahnsteuerungssystemen

Proving Completeness of Properties in Formal Verification of Counting Heads for Railways

---

Kinder, Sebastian, and Rolf Drechsler, 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007). IEEE, 2007.

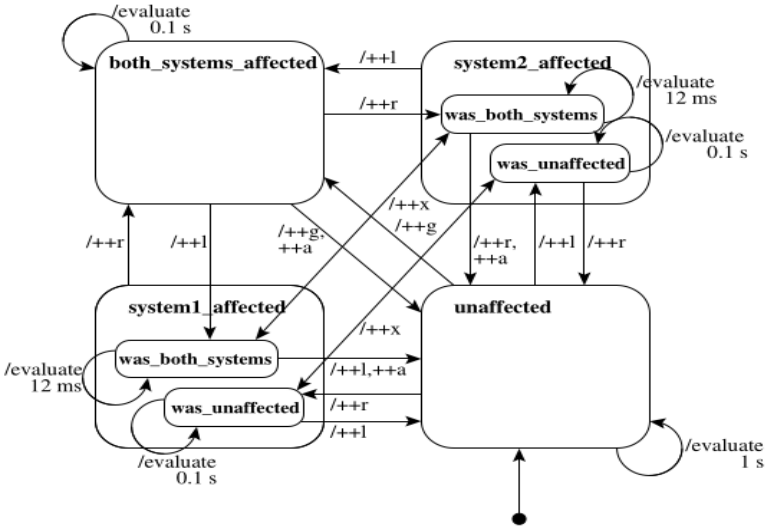
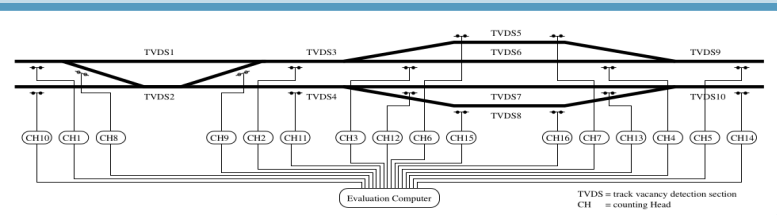


Figure 4. FSM of the Counting Head [8]

Verifikation in Minuten!



Who will check the checkmen?

Who will check the checkmen?

$$
\begin{aligned}
&\Box\,(\text{notfall} \rightarrow \Diamond\,(\text{alarm} \wedge \Box\,(\text{alarm} \rightarrow \bigcirc(\text{alarm}\ \mathcal{U}\ \text{quittierung}))) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \mathcal{P}(\text{alarm})) \\
&\wedge\ \Box\,(\text{alarm} \rightarrow \bigcirc(\neg\text{alarm}\ \mathcal{U}\ \text{quittierung})) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \bigcirc(\neg\text{alarm}\ \mathcal{U}\ \text{notfall})) \\
&\wedge\ \Diamond_{\leq 5}\,(\text{teamgerufen}) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \Diamond\,(\text{behebung} \wedge \text{grundzustand})))
\end{aligned}
$$

Who will check the checkmen?

$$
\begin{aligned}
&\Box\,(\text{notfall} \rightarrow \Diamond\,(\text{alarm} \wedge \Box\,(\text{alarm} \rightarrow \bigcirc(\text{alarm}\ \mathcal{U}\ \text{quittierung}))) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \mathcal{P}(\text{alarm})) \\
&\wedge\ \Box\,(\text{alarm} \rightarrow \bigcirc(\neg\text{alarm}\ \mathcal{U}\ \text{quittierung})) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \bigcirc(\neg\text{alarm}\ \mathcal{U}\ \text{notfall})) \\
&\wedge\ \Diamond_{\leq 5}\,(\text{teamgerufen}) \\
&\wedge\ \Box\,(\text{quittierung} \rightarrow \Diamond\,(\text{behebung} \wedge \text{grundzustand})))
\end{aligned}
$$

Wo ist der Fehler?