

MODEL CHECKING

1 - EINFÜHRUNG

Sommersemester
2009

Dr. Carsten Sinz, Universität Karlsruhe

Software-Qualität

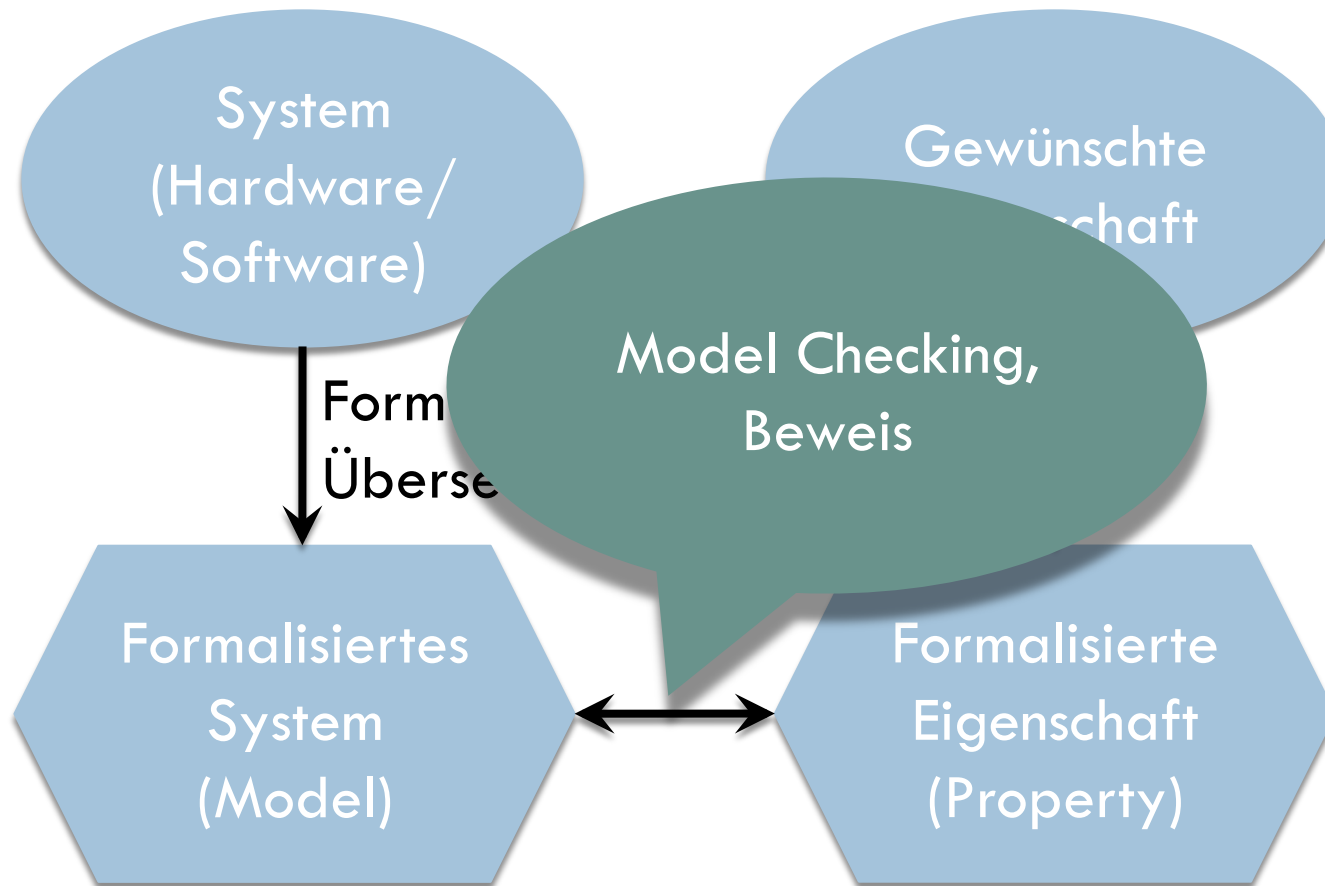
2

- ***Buggy smartphone software is “new reality”***
RIM-CEO Jim Balsillie über die fehlerhafte Software des Blackberry Storm (Jan. 2009)
- ***„(...) Software verification (...) has been the Holy Grail of computer science for many decades, but now in some very key areas, for example driver verification, we’re building tools that can do actual proofs about the software and how it works in order to guarantee the reliability.”***
Bill Gates, WinHEC 2002



Model Checking

3



Beispiel 1: Zune Z2K9

4

“Am 31. Dezember 2008 fielen weltweit alle Zune-Geräte der ersten Generation aus. Ursache war ein interner Fehler bei der Handhabung von Schaltjahren“

Heise Online, 03.01.2009



Z2K9: Source Code

5

```
BOOL ConvertDays(UINT32 days,
                 SYSTEMTIME* lpTime)
{
    int dayofweek, month, year;
    UINT8 *month_tab;

    //Calculate current day of the week
    dayofweek = GetDayOfWeek(days);

    year = ORIGINYEAR;
```

days =
366 ?

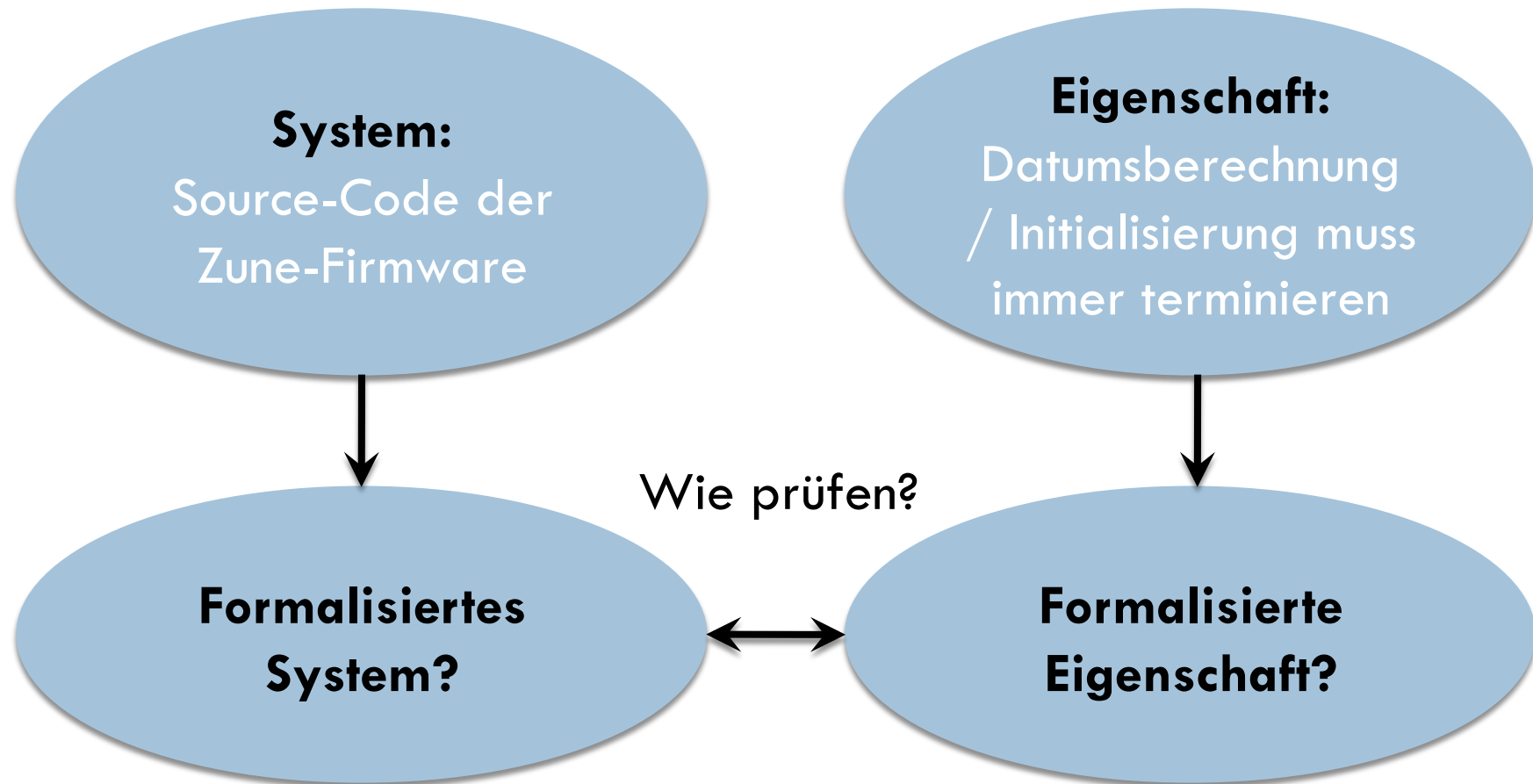


```
while (days > 365)
{
    if (IsLeapYear(year))
    { if (days > 366)
      {
          days -= 366;
          year += 1;
      }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

...

Z2K9: Formalisierung

6



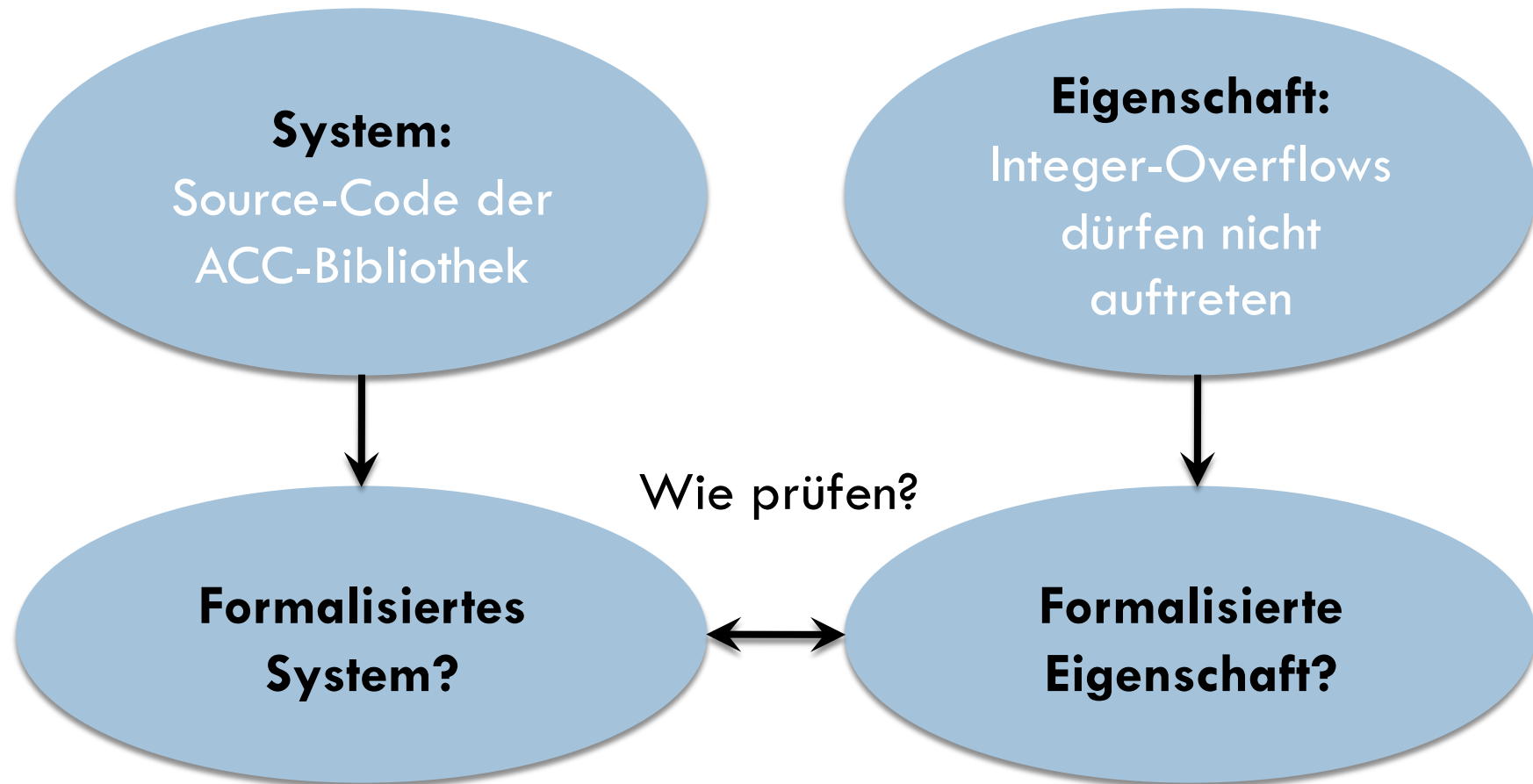
Beispiel 2: Bosch ACC

7

- Nicht öffentlich verfügbar.

Bosch ACC: Formalisierung

8



Beispiel 3: Automobil-Konfiguration

9

C270CDI - Elegance - Microsoft Internet Explorer

Mercedes-Benz

Fahrzeugklasse: C-Klasse

Karosserie und Motorwahl: C270CDI EUR 33.408,00

Design/Ausstattungslineie: Elegance EUR 1.798,00

Lacke: Magmarot EUR 0,00

Polster: anthrazit "Cambri" EUR 0,00

Sonderausstattung:

<input checked="" type="checkbox"/> Antenne für Telefon	0,00
<input checked="" type="checkbox"/> Außenspiegel elek	243,80
<input checked="" type="checkbox"/> Komfort-Klimatisie	591,80
<input checked="" type="checkbox"/> Lautsprecher(7 Stü:	0,00
<input checked="" type="checkbox"/> MB-Telefon Stand	893,20
<input checked="" type="checkbox"/> Bedien- und Anze	2.847,80

Limousinen

Benzin	Diesel
C180K	C200CDI
C200CGI	C220CDI
C200K	C270CDI
C240	C30 AMG
C2404M	C320
C32 AMG	C3204M

Classic Elegance Avantgarde

Unilackierung

Stoff

Design Klimatisierung Komfort Lenkung/Schaltung Radio/ Kommunikation Räder und Fahrwerk Sicherheit Sitze Technik

Produktinformation

- Preisblatt
- Preisfinder
- 360° Außenansicht
- 360° Innenansicht

Modellinformation

Die C-Klasse Limousinen C 270 CDI LIMOUSINE

Sitze/Türen: 5/4
Motortyp: 5-Zyl. Diesel
Leistung: 125 kW (170 PS)
Hubraum: 2665 ccm

Grundpreis: 33.408,00 EUR

Hier geht es weiter

- Angebot anfordern
- Konfiguration drucken
- Leasing und Finanzierung

Ergebnis der Auswahl: Gesamtpreis EUR 39.782,20

Ergebnis anzeigen Online Suche

Neue Konfiguration

Front Seite Heck

Fertig. Internet

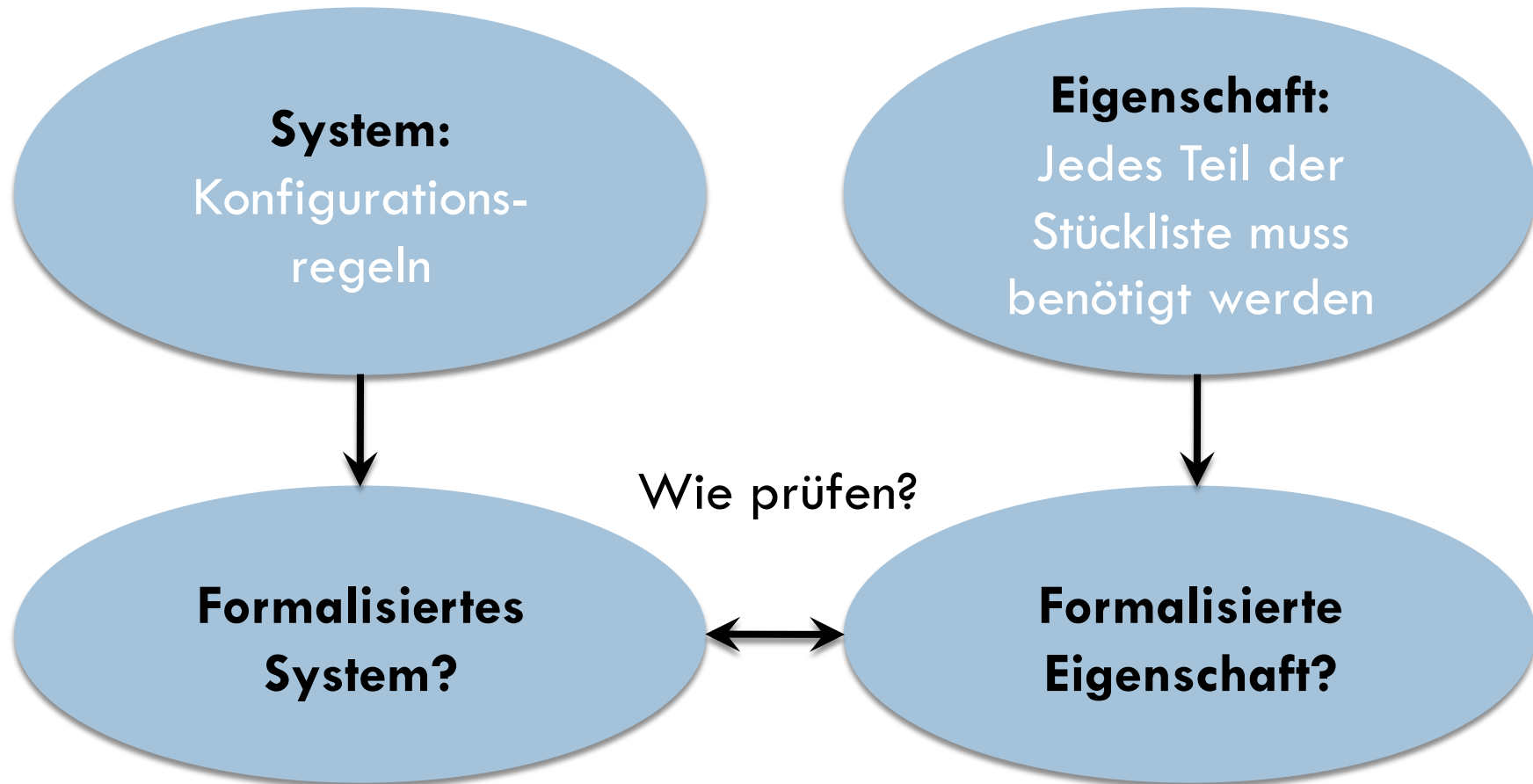
Regeln zur Automobil-Konfiguration

10

- Nicht öffentlich verfügbar.

PKW-Konfiguration: Formalisierung

11



Vorlesungsinhalte

12

- Automatentheorie, temporale Logiken (LTL, CTL)
- SAT-Solving und binäre Entscheidungsdiagramme
- Explicit State Model Checking
- Symbolic Model Checking
- Bounded Model Checking
- Software Bounded Model Checking
- Werkzeuge: SPIN, SMV, BLAST, CBMC
- Anwendungen

Organisatorisches

13

- **Übungen:**
 - ▣ 14-tägig, Do 15:30-17:15, Seminarraum -107
 - ▣ Beginn am 06.05.2009
 - ▣ Teilnahme an Übungen nicht zwingend, aber empfohlen
- **Prüfung:**
 - ▣ Mündlich, Vertiefungsgebiet: Theoretische Grundlagen
- **Literatur:**
 - ▣ E. Clarke, O. Grumberg, D. Peled: Model Checking (MIT Press, 1999)
 - ▣ K. McMillan: Symbolic Model Checking (Kluwer, 1993)