UNIVERSITÄT KOBLENZ · LANDAU
Fachbereich 4: Informatik

ADAPT

Formale Verifikation von SOA-basierten automotiven Software-Systemen

Christian Schwarz
Universität Koblenz-Landau

Marco Wagner
Hochschule Heilbronn

Gesellschaft für Informatik
Fachgruppe Betriebssysteme

8.11.12 Herbsttreffen in Koblenz

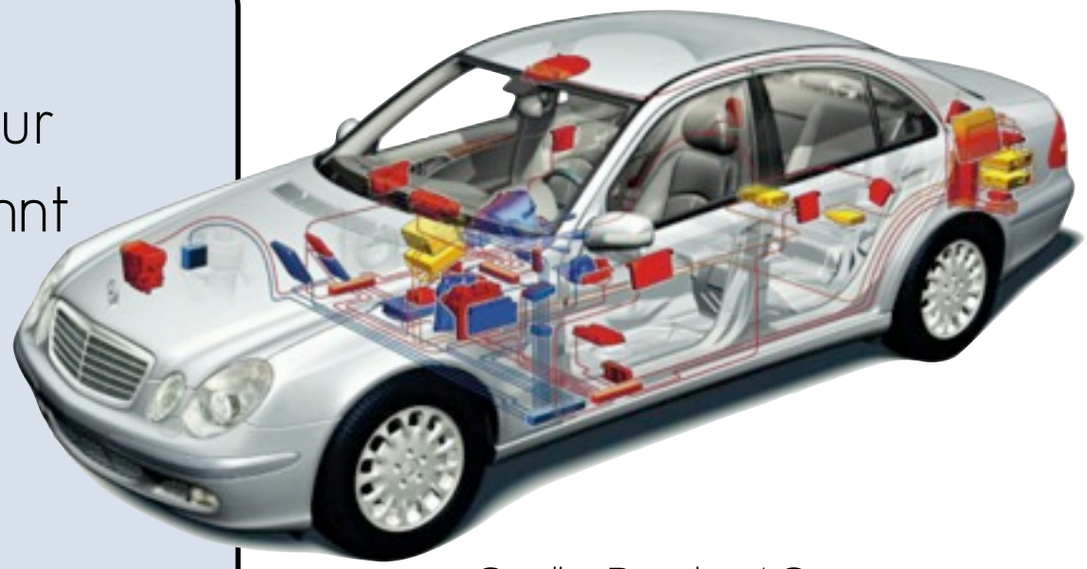
Verteilte Fahrer-Assistenz-Systeme

Heutige Fahrer-Assistenz-Systeme

- statische Software- und Systemarchitektur
- Architektur zum Design-Zeitpunkt bekannt

Beispiele:

- Spurerkennung
- Einpark-Assistent



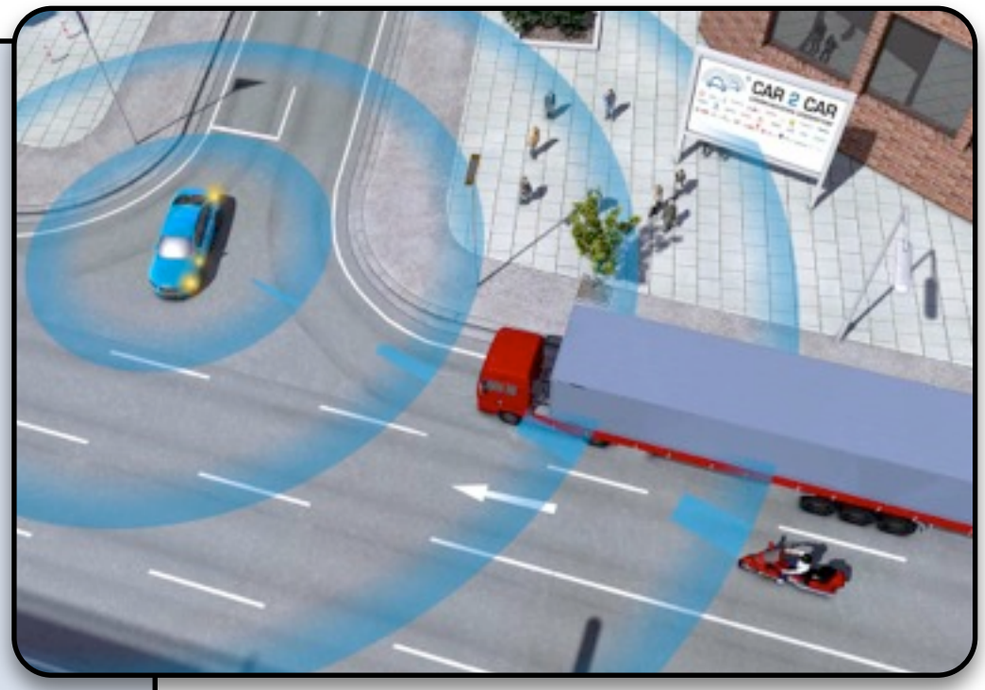
Quelle: Daimler AG

Zukünftige Fahrer-Assistenz-Systeme

- verteilt auf verschiedene Entitäten
- Systemarchitektur ändert sich zur Laufzeit

Beispiele:

- Car-to-Car Kommunikation
- Car-to-Infrastructure Kommunikation
- FAS für Fahrzeugespanne



Quelle: car-to-car.org

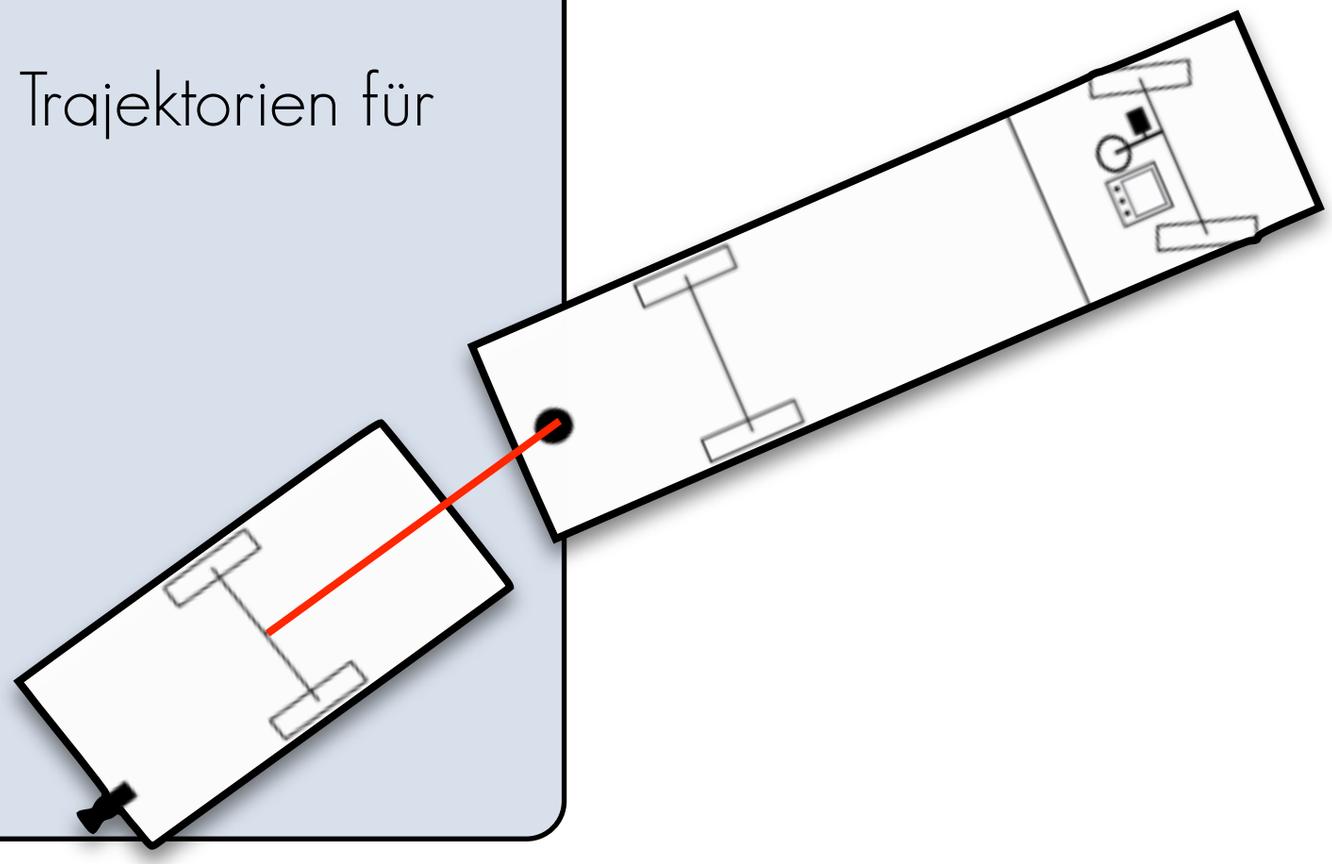
Fallbeispiel

FAS für das Rückwärtsfahren mit Anhänger

Fallbeispiel: Komponenten

FAS für das Rückwärtsfahren mit Anhänger

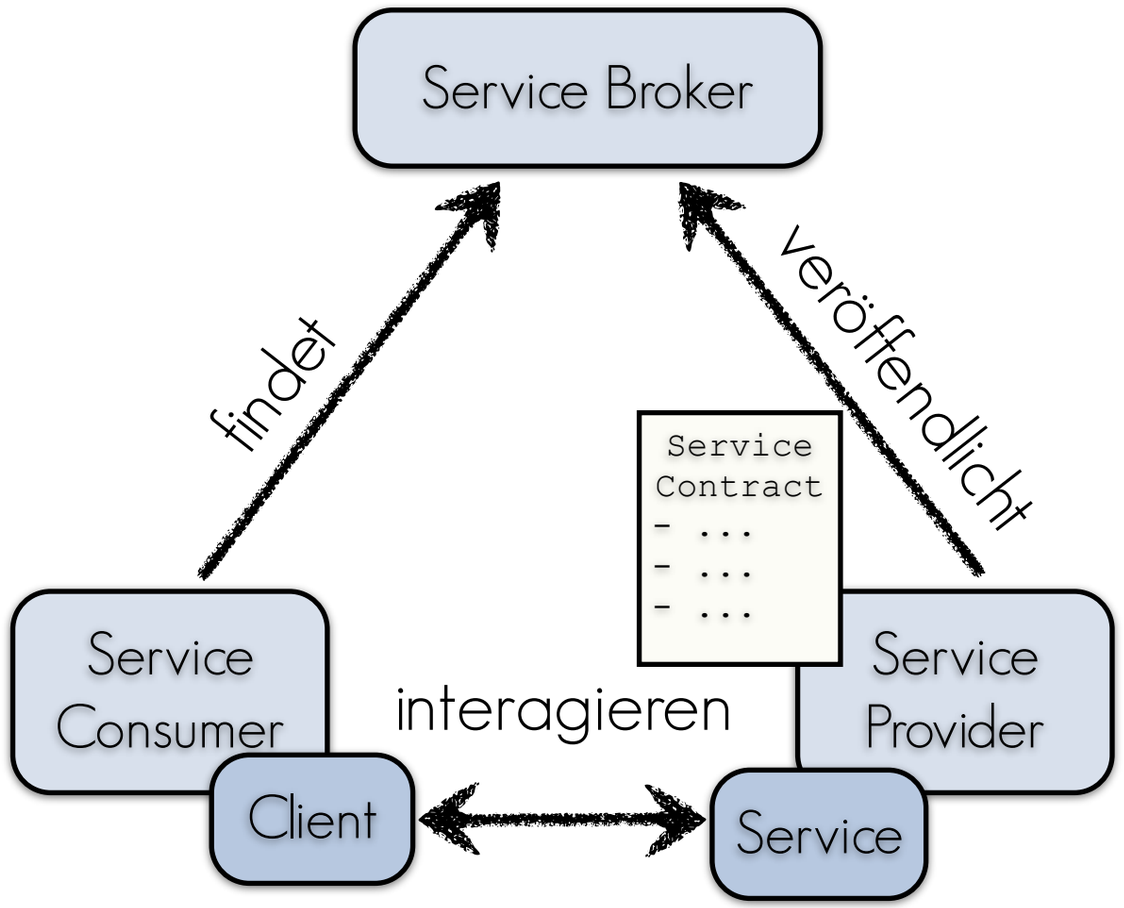
- Sensoren:
  - Lenkwinkelsensor
  - Einknickwinkelsensor
  - Rückfahrkamera
- Assistenzlogik: Berechnung der Trajektorien für
  - Anhänger
  - Fahrzeuggespann
- Ausgabe:
  - Overlay
  - Video-Ausgabe



Service Orientation

Service Orientation

- Erleichtert den Umgang mit Verteiltheit und Heterogenität und verbessert Wiederverwendbarkeit
- Implementiert Kapelung mit definierten Schnittstellen
- Erlaubt Dienste zu finden

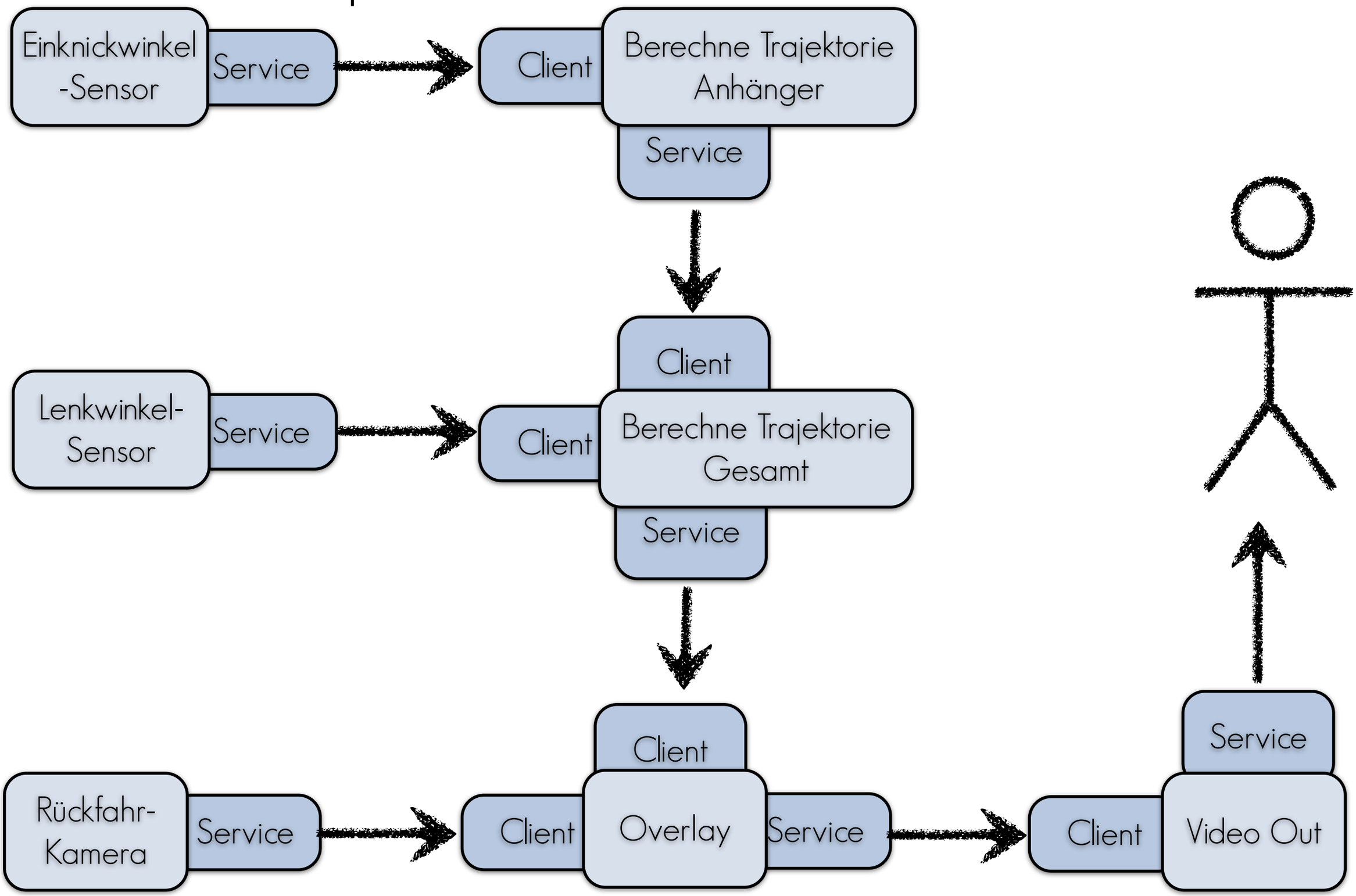


Quelle: w3c.org

Automatische Re-Orchestrierung

- Automatische Anpassung der Software im Falle einer Systemänderung

Fallbeispiel: Service-Orientiertes Modell



Formale Verifikation

Verifikation

- Sicherheitskritische Systeme müssen validiert werden
- Insbesondere sollten sicherheitskritische Systeme, die zur Laufzeit erzeugt werden zur Laufzeit validiert werden.

Model Checking

- Vollautomatisches Verfahren
- Überprüft, ob eine gegebene Spezifikation bestimmte, in Temporal-Logik gegebene, Eigenschaften hat (Sicherheit, Deadlock-Free..)
- Generiert im Fehlerfall ein Gegenbeispiel

Temporale Konsistenz als Sicherheitsbedingung

Temporale Konsistenz

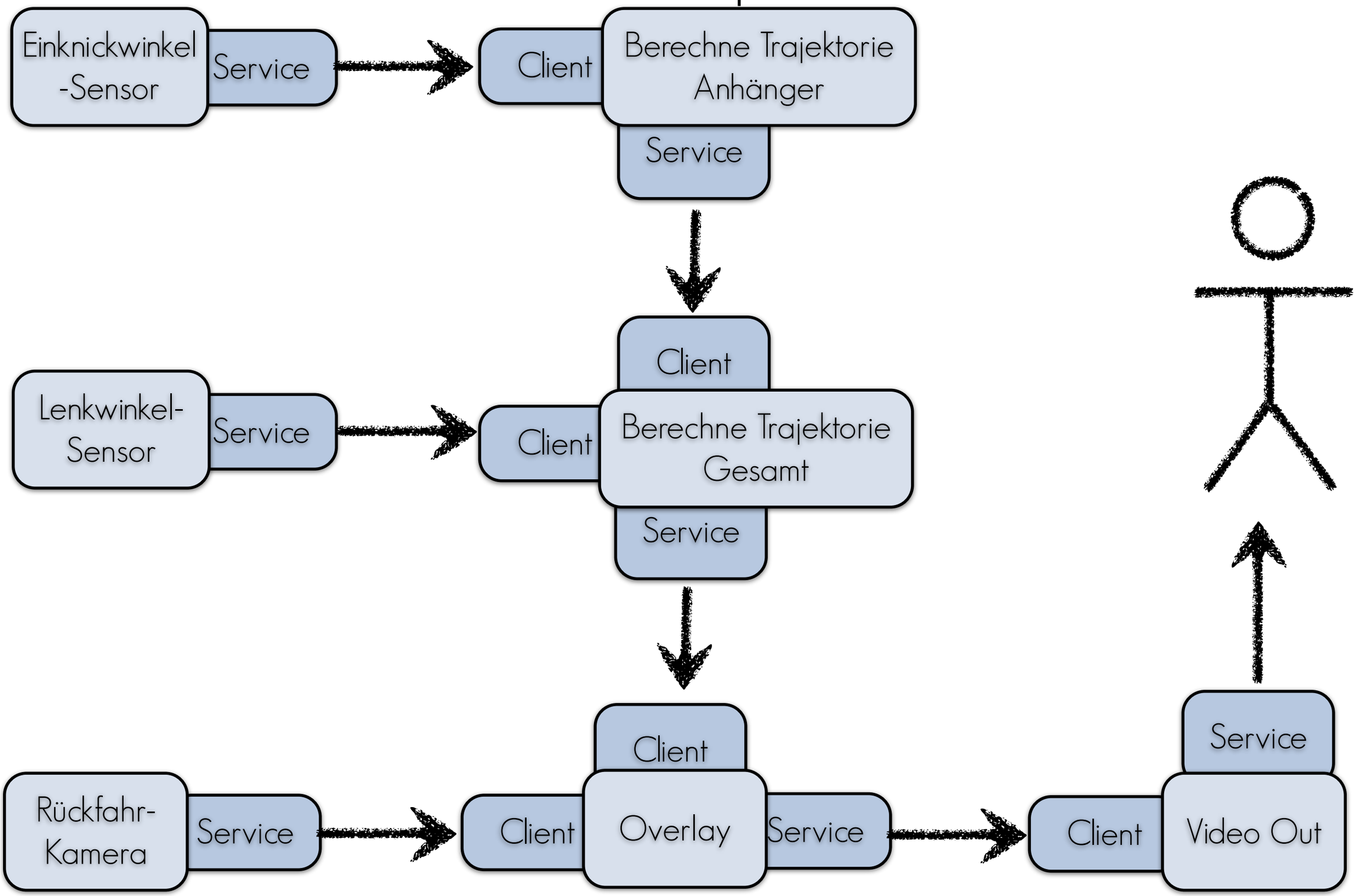
Ein System ist *temporal konsistent* bezüglich Δt

gdw. seine Ausgaben nicht auf Eingaben basieren, die älter sind als Δt.

Fallbeispiel: eine Sicherheitsbedingung

Die vorgestellte Rückfahrassistenz ist sicher, wenn sie temporal konsistenz bezüglich 100ms ist.

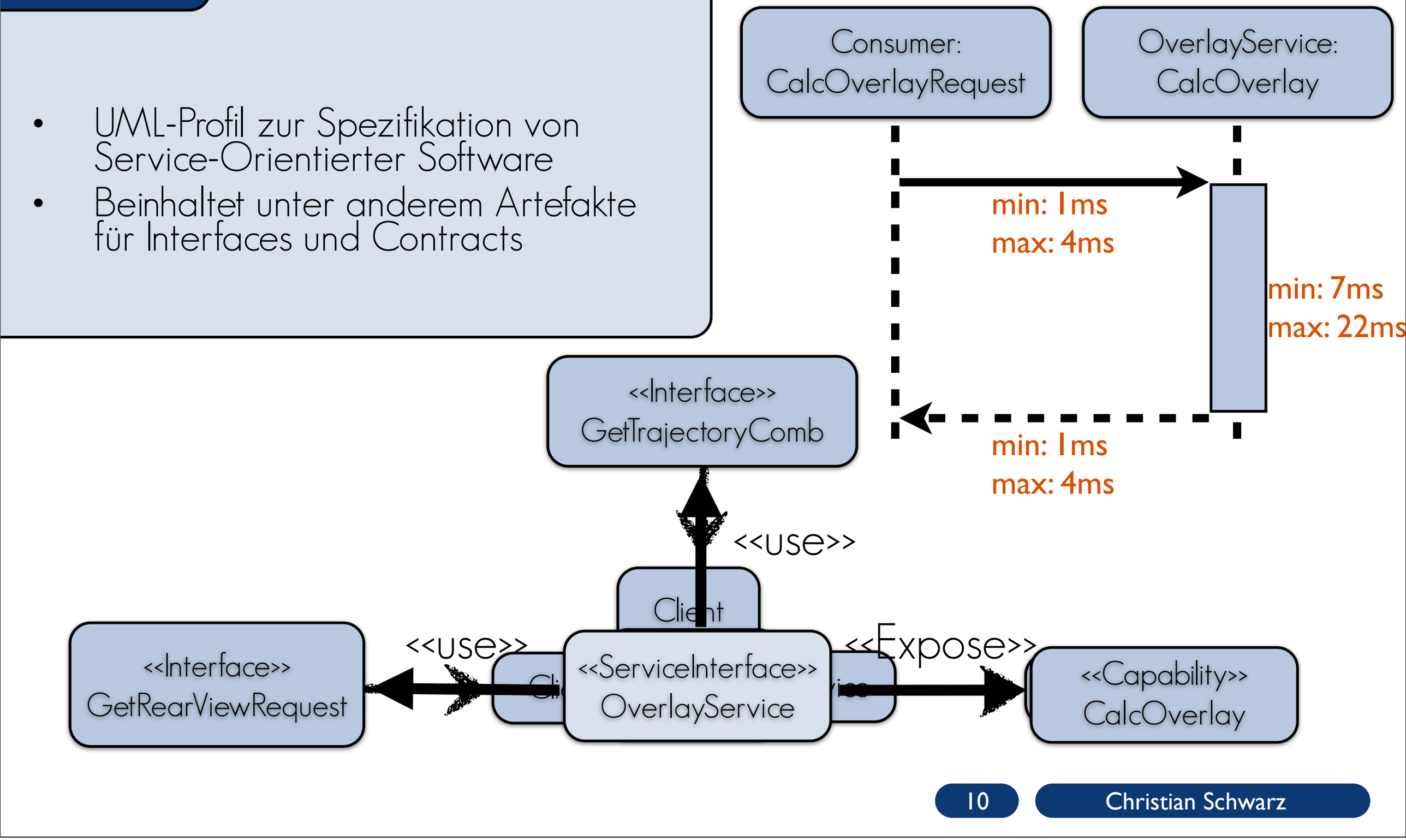
Fallbeispiel



Fallbeispiel: SoaML

SoaML

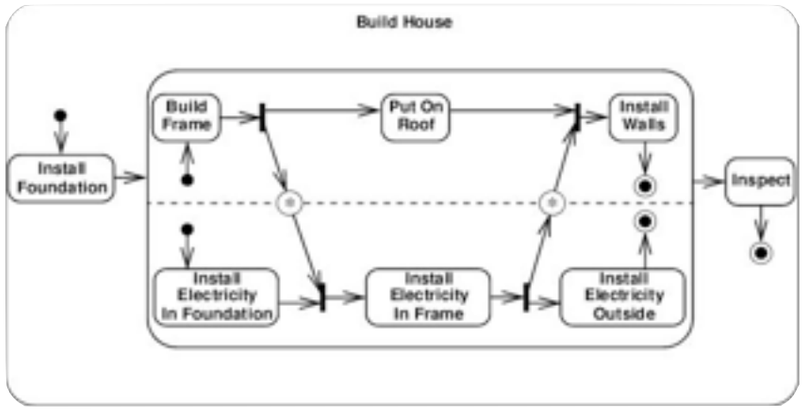
- UML-Profil zur Spezifikation von Service-Orientierter Software
- Beinhaltet unter anderem Artefakte für Interfaces und Contracts



Hybride Systeme

Diskrete Systeme

- Diskrete Zustandsübergänge
- Zustandsautomaten, Aktvitätsdiagramme, …



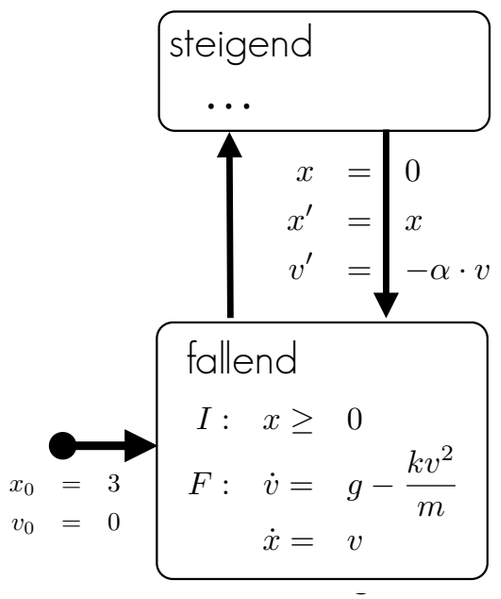
Physikalische Systeme

- kontinuierliche Zustandsübergänge
- Differentialgleichungen

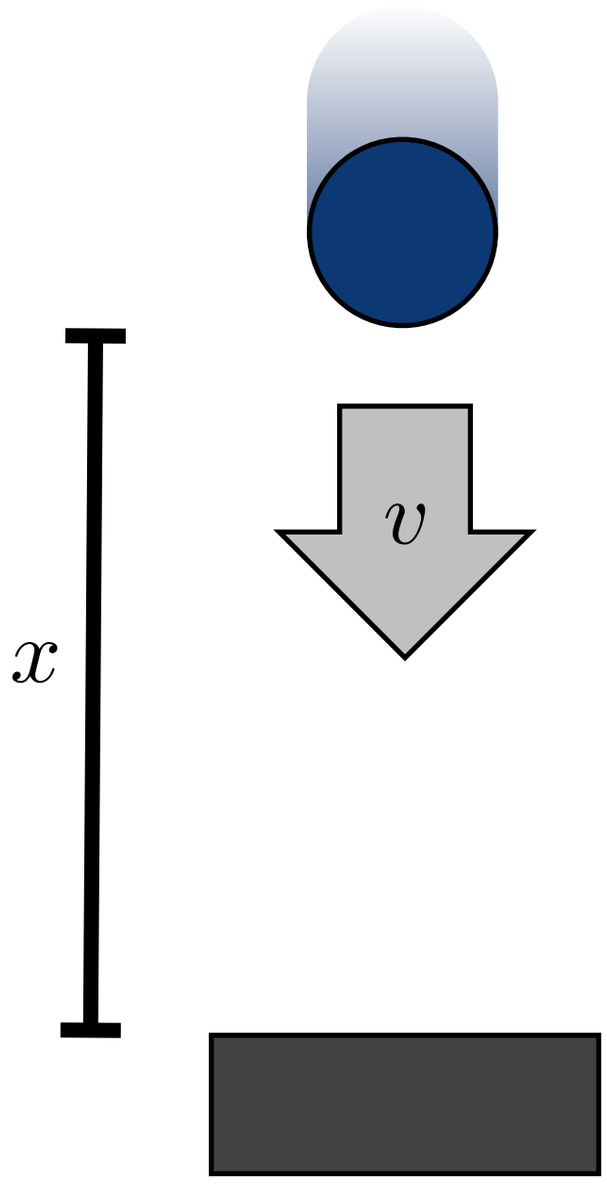
$$\dot{v} = g - \frac{kv^2}{m}$$

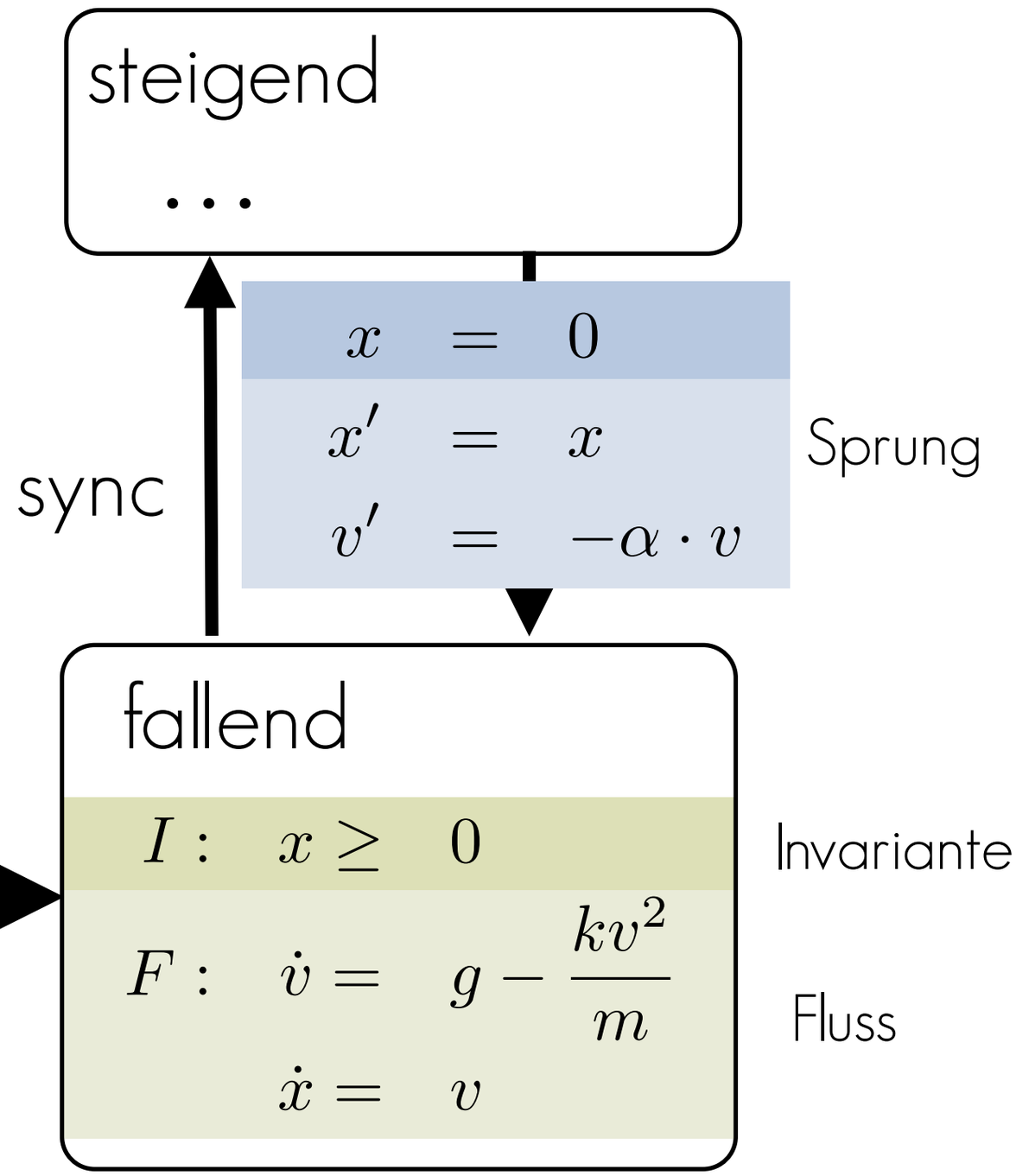
Hybride Systeme

- kontinuierliche und diskrete Zustandsübergänge
- Hybride Automaten

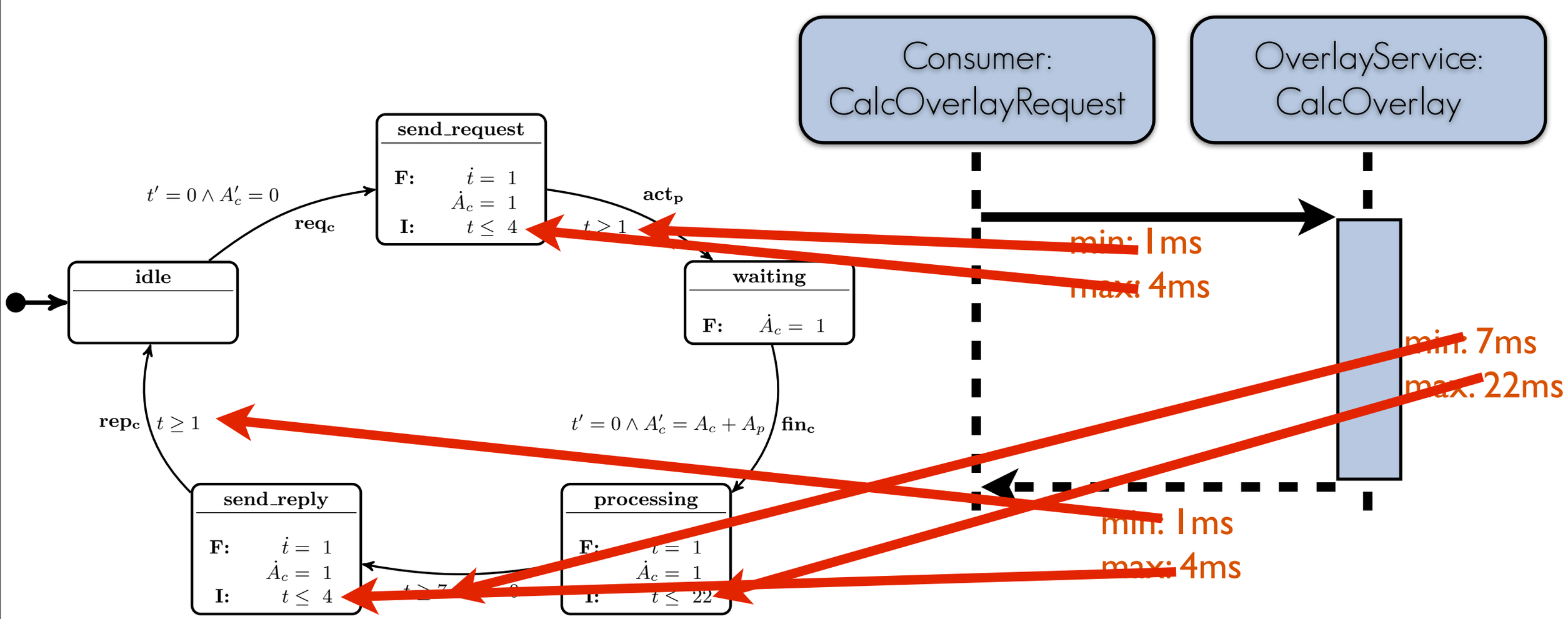


Hybride Automaten

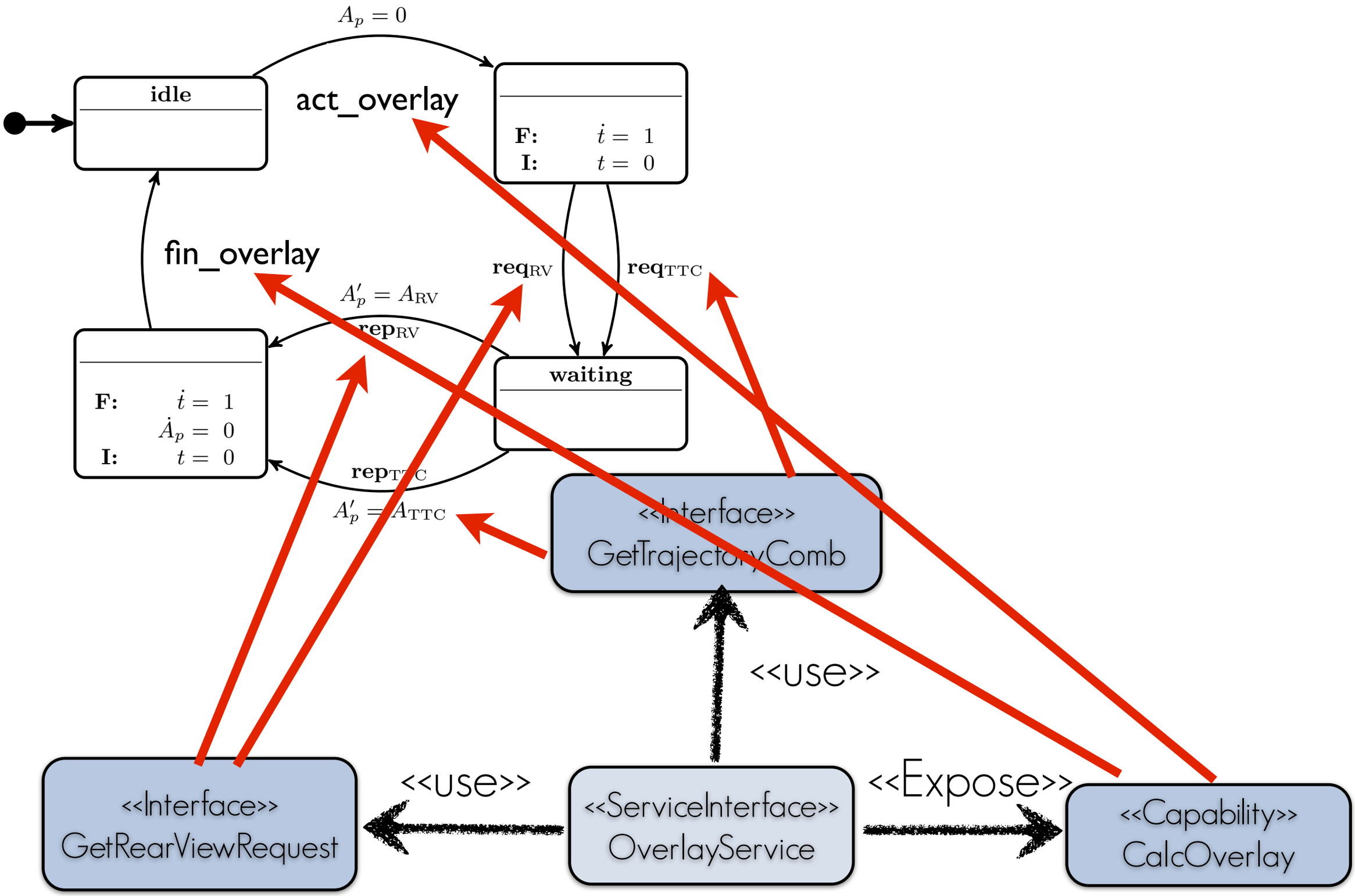




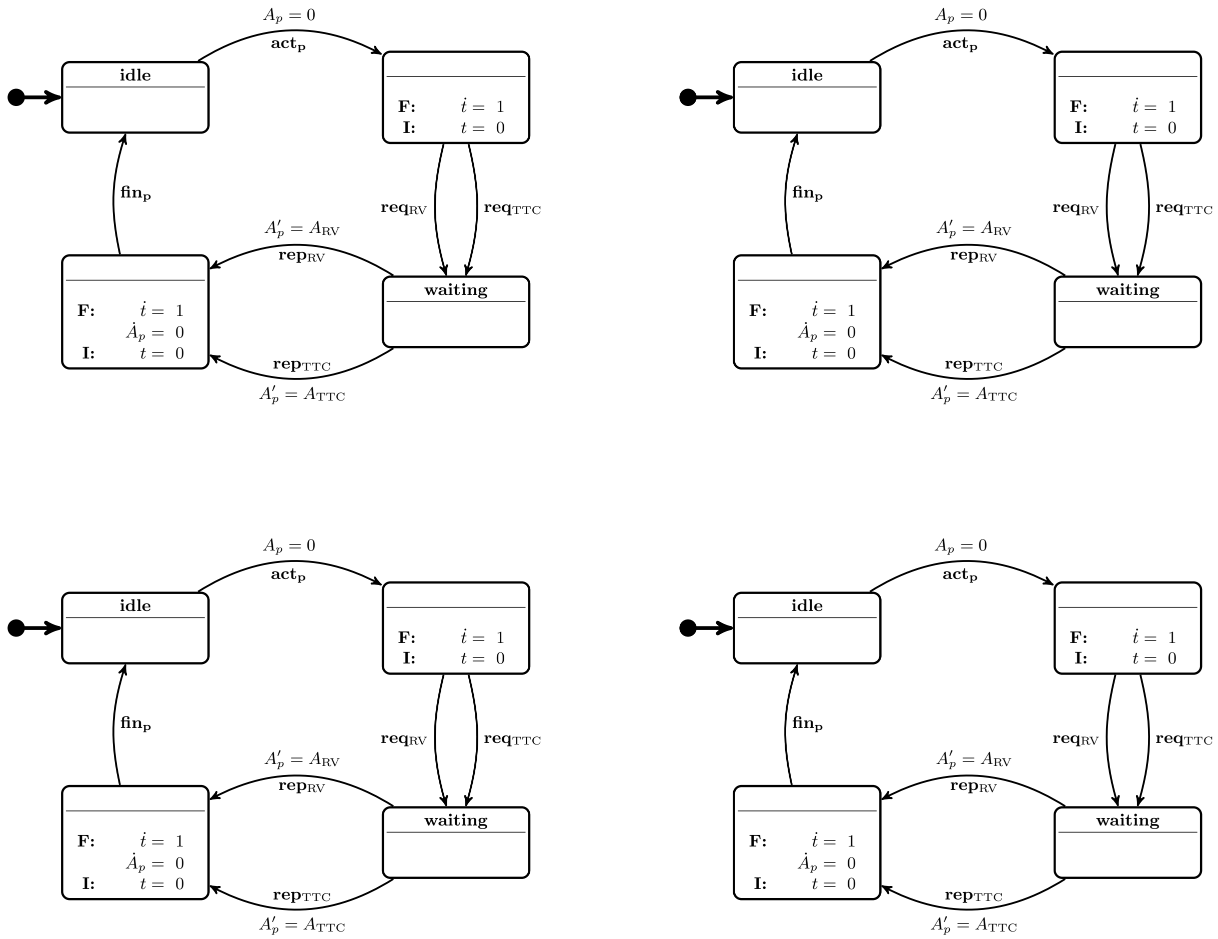
Transformation of Contracts

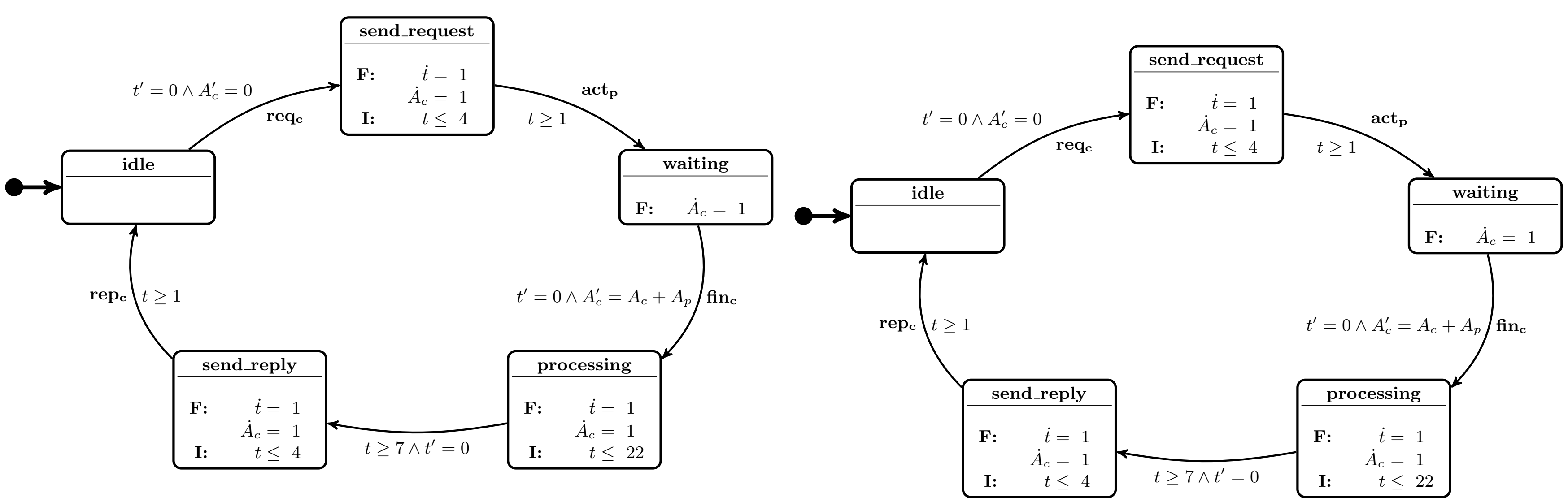


Transformation of Interfaces



Verifikation





Standard-

Modelchecking-Tools

Beweis

oder

Gegenbeispiel

Zukünftige Arbeiten

- Komplexere Sicherheitsbedingungen
- Ausnutzung von Gegenbeispielen für die Orchestrierung

Vielen Dank für Ihre Aufmerksamkeit