# Formale und semiformale Methoden für eingebettete Software

## Inhalt

Der Begriff “formale Methoden” fasst eine Vielzahl von **Techniken zur mathematischen Modellierung und Verifikation** von Computersystemen zusammen: formale Spezifikationssprachen (z.B. ‘Z’), Automaten, Temporallogik, Prozesskalküle, Model-Checking usw. Sie werden in der Softwaretechnik und in der industriellen Praxis in sicherheitskritischen Bereichen angewendet um Fehlerfreiheit zu beweisen oder plausibel zu machen, um Betriebssicherheit zu gewährleisten und um technische Systeme auf die Erfüllung von Anforderungen zu überprüfen.

Sowohl formale als auch semiformale Methoden haben eine strikt definierte **Syntax und Semantik** für Sprachelemente. Semiformale Modelle eignen sich typischerweise zur unzweideutigen Kommunikation von Systemanforderungen und -eigenschaften, darüber hinaus auch zu einfachen Modellanalysen, z.B. einer Duplikatserkennung.

Formalen Methoden liegt zusätzlich ein **Kalkül** zugrunde, darin unterscheiden sie sich von semiformalen Ansätzen und gängigen Programmiersprachen. Man kann mit formalen Modellen also “rechnen”: Man kann sie ineinander und in kanonische Darstellungen transformieren, sie so vergleichen und weitergehende Eigenschaften, auch Systemeigenschaften, analysieren. Die zugrunde liegende Annahme ist: besitzt das Modell eine Eigenschaft, dann besitzt das modellierte System sie auch.

Ist die Erstellung eines korrekten formalen Modells weniger aufwendig als die fehlerfreie Beschreibung des gewünschten Verhaltens in einer Programmiersprache, so ermöglicht die formale Spezifikation u.U. nicht nur eine **frühzeitige Analyse** des geplanten Systems, sondern ist auch kosteneffizient. Der Einsatz formaler Methoden in der industriellen Software-Entwicklung steht jedoch noch ganz am Anfang.

### Voraussetzungen

- **In diesem Seminar sind nur Masterstudenten zugelassen.**
- Ggf. ist Vorwissen für die Bearbeitung einzelner Themen von Vorteil.
- Bitte geben Sie relevantes Vorwissen bei Ihrer Anmeldung mit an, um Ihre Chance auf Zuteilung zu erhöhen.

### Themen

- Scalable Error Detection using Boolean Satisfiability

    - Betreuer: Dr. rer. nat. Dimitri Bohlender
    - Geeignet für: Master
- Slicing Abstractions
    - Betreuer: Hendrik Simon, M.Sc.
    - Geeignet für: Master
- Why does Astree scale up?
    - Betreuer: Hendrik Simon, M.Sc.
    - Geeignet für: Master
- C2E2: A Verification Tool for Stateflow Models
    - Betreuer: Dr. Ing. Ibtissem Ben Makhlouf
    - Geeignet für: Master
- Syntax Error Repair for a Java-based Parser Generator
    - Betreuer: Dr.-Ing. Mathias Obster
    - Geeignet für: Master
- Supervisory Control of Discrete-Event Systems via IC3
    - Betreuer: Dr.-Ing. Florian Ottersbach (Göbe)
    - Geeignet für: Master
    - Der betreuende Mitarbeiter ist zurzeit im Ausland. Daher ist nur eine Fernbetreuung via E-Mail und Skype möglich.
- Convex optimization proves software correctness
    - Betreuer: Christian Dernehl, M.Sc.
    - Geeignet für: Master
- Efficient model checking of PSL safety properties
    - Betreuer: Marc Förster, M.Sc.
    - Geeignet für: Master
- Contracts-refinement proof system for component-based embedded systems
    - Betreuer: Marc Förster, M.Sc.
    - Geeignet für: Master

## Organisation

Es wird eine Einführungsveranstaltung geben in der die Themen und der zeitliche Ablauf des Seminars vorgestellt werden. Abgeschlossen wird das Seminar durch eine schriftliche Ausarbeitung auf Deutsch oder Englisch, sowie einer mündlichen Präsentation.

Dieses Seminar wird organisatorisch zusammen mit zwei weiteren Themen unter dem Titel „Ausgesuchte Themen zur Eingebetteten Software“ geführt. Es gibt einen gemeinsamen Lernraum im L2P, eine gemeinsame Campus-Veranstaltung und eine gemeinsame Einführungsveranstaltung. Die Notenmeldung erfolgt jedoch unter dem entsprechend gewählten Titel.

### Terminplanung

Mittwoch, 7.10.2015 – Kickoff
Donnerstag, 8.10.2015 – Themenwahl
Donnerstag, 29.10.2015 – Abgabe Structure & Bibliography
Freitag, 30.10.2015 – Abmelde-Deadline
Sonntag 6.12.2015 – First Version
Sonntag 17.1.2016 – Final Version

Sonntag 7.2.2016 – Slides Draft

### Sprache

- Organisation: Deutsch/Englisch
- Thematische Bearbeitung (Ausarbeitung + Präsentation): Deutsch oder Englisch.

### Hinweise zur Anmeldung

Die Anmeldung erfolgt über die Zentrale Vergabe von Studien- und Seminarplätzen. Bitte geben Sie eventuelle Vorkenntnisse dort an. Eine Anmeldung über das Campus System ist nicht erforderlich.

### Kriterien für eine erfolgreiche Teilnahme

- Verfassen einer schriftlichen Ausarbeitung (Abgabe als PDF) und Einhaltung der Rahmenbedingungen (Siehe Einführungsveranstaltung)
- Folien und Abschlussvortrag (Abgabe der Folien als PDF oder ppt(x))
- Einhaltung aller Fristen
- Anwesenheit bei allen Pflichtterminen

### Art der Veranstaltung

Seminar (4 ECTS)

### Campus/L2P

L2P ist aktiv ab ca. 6-8 Wochen vor Vorlesungsbeginn
Campus Link

### Rückfragen

Für Rückfragen wenden Sie sich bitte an Dr.-Ing. Mathias Obster.