Universität Stuttgart

Institut für Luftfahrtsysteme

Prof. Björn Annighöfer
Prof. Zamira Daw

Kontakt
Prof. Björn Annighöfer
Pfaffenwaldring 27
70569 Stuttgart
+49 711 685-62703
bjoern.annighoefer@ils.uni-stuttgart.de

https://www.ils.uni-stuttgart.de/

31.03.2025

Aufgabenstellung

Bachelorarbeit

Machbarkeit und Bewertung praktischer formaler Verifikation von C-Funktionsblöcken für Plug&Fly Avionik

Aktuelle Avioniksysteme bestehen aus standardisierten Rechnern, die statisch und individuell konfiguriert werden. Die Konfigurationsdaten die Kommunikationswege und die Zuordnung von Softwareanwendungen zu den Rechnern. Bei größeren Systemen gibt es Millionen von Konfigurationsparametern, deren Erstellung und Prüfung sich sehr zeitaufwändig und fehleranfällig ist. Selbstorganisierende Avioniksysteme sollen sich selbst automatisch auf Grundlage der verfügbaren Hardware, ihrer Eigenschaften und der auszuführenden Funktionen konfigurieren. Eine kontinuierlicher Selbstkonfiguration kann die Fehlertoleranz erhöhen und den Ressourcenverbrauch senken. Derzeit entwickeln wir eine selbstkonfigurierende Avionikplattform namens *Plug&Fly Avionik* (PAFA). Wir konnten am Prüfstand zeigen, dass mit PAFA selbständig die Flugsteuerung eines Oktokopters erkannt, konfiguriert und betrieben werde kann. Eine Grundlage für die Zulassung von PAFA-Systemen ist die Annahme, dass nur korrekte Basisbausteine, sogenannte Tasks (s. Abbildung 1), benutzt werden um Systemfunktionen zu bilden.

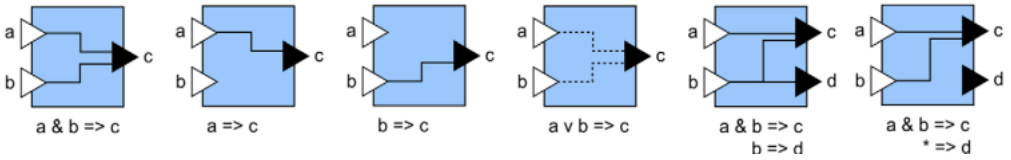

Abbildung 1: Beispiele für PAFA-Tasks

Aufgabe
Ziel dieser Arbeit ist es eine praktische Methode für die formelle Verifikation von PAFA-Task aufzubauen und zu bewerten. Formale Verifikation heißt, dass die Korrektheit von Funktionen auf Basis von mathematischen Ausdrücken automatisiert überprüft wird. Dazu sind Tools wie SMTSolver oder NuSVM verfügbar. Die Methode soll für bestehender PAFA-Tasks entwickelt werden. Diese bilden einfache Funktionen, wie Konstanten, Summation, Skalierung, Signalweichen oder P-Regler ab und sind in C implementiert. Es soll eine Toolkette[1] eingerichtet werden die bestehenden C-Code automatisch verifiziert werden kann. Es sollen PAFA-Tasks um Vor- und Nachbedingungen erweitert werden, die automatisiert verifiziert werden. Die Methode soll an einem ausgewählten Satz von PAFA-Tasks demonstriert und bewertet werden. Als Bewertungskriterien können z.B. Resultate, Laufzeit, Nachvollziehbarkeit des Ergebnisses oder Bedingungen gewählt werden, aber auch eigene. Optional soll geprüft werden, ob Vor-, Nachbedingungen oder Verifikationsergebnisse mit den Tasks abgelegt werden können, um sie zur Laufzeit zu nutzen. Eine angemessene Dokumentation der Arbeit und eine Vorstellung in einem Abschlussvortrag ist obligatorisch.

[1] Z.B. M. Botincan, M. Parkinson, and W. Schulte, “Separation Logic Verification of C Programs with an SMT Solver,” Electr. Notes Theor. Comput. Sci., vol. 254, pp. 5–23, Oct. 2009. oder *MATLAB Poly-Space Code Prover*

Arbeitsschritte:

- Einarbeitung
  - Formale Verifikation (insbesondere für C-Code)
  - PAFA-Task (genereller Aufbau und bestehende Tasks)
  - Auswahl von Verifikationssoftware
- Aufbau der Formalen Verifikation
  - Einrichtung der Verifikationssoftware
  - Erarbeitung der Schritte zur Verifikation von PAFA-Tasks
  - Erweiterung eines Tasks um Vor- und Nachbedingungen
  - Machbarkeitsnachweis an einem PAFA-Task
  - Überprüfung der Verifikationsergebnisse
- Demonstration und Bewertung
  - Festlegung von Bewertungskriterien
  - Verifikation weitere PAFA-Tasks
  - Bewertung aller Ergebnisse
- Dokumentation der Ergebnisse
- Abschlusspräsentation

Beginn: _____

Ende: _____

Betreuer 1: Prof. Zamira Daw

Betreuer 2: Prof. Björn Annighöfer

Prüfer 1: Prof. Björn Annighöfer

Prüfer 2: Prof. Zamira Daw

Datum, Unterschrift Student: _____

Rechtliche Bestimmungen: Der/die Bearbeiter/in ist grundsätzlich nicht berechtigt, irgendwelche Arbeits- und Forschungsergebnisse, von denen er/sie bei der Bearbeitung Kenntnis erhält, ohne Genehmigung des/der Betreuers/in dritten Personen zugänglich zu machen. Bezüglich erreichter Forschungsleistungen gilt das Gesetz über Urheberrecht und verwendete Schutzrecht (Bundesgesetzblatt I/S. 1273, Urheberschutzgesetz vom 09.09.1965). Der/die Bearbeiter/in hat das Recht, seine/ihre Erkenntnisse zu veröffentlichen, soweit keine Erkenntnisse und Leistungen der betreuenden Institute und Unternehmen eingeflossen sind. Die von der Studienrichtung erlassenen Richtlinien zur Anfertigung der Bachelor-/Masterarbeit sowie die Prüfungsordnung sind zu beachten.