

MASTERARBEIT

Fehlertoleranz durch Verifiable Computing für eine Drohnenflugsteuerung



INSTITUT FÜR LUFTFAHRTSYSTEME

Ansprechpartner:

M.Sc. Johannes Reinhart
Universität Stuttgart
Institut für Luftfahrtssysteme
Pfaffenwaldring 27
70569 Stuttgart
+49 (0)711 685 67093
johannes.reinhart@ils.uni-
stuttgart.de

Kontext

Sicherheitskritische digitale Flugsteuerungen haben höchste Anforderungen an Zuverlässigkeit und Verfügbarkeit. Die vergleichsweise hohen Fehlerraten von digitalen Steuergeräten erfordern den Einbau von robusten Fehlertoleranzmechanismen. Diese müssen Fehler zuverlässig erkennen und deren Ausbreitung verhindern. Konventionelle Systeme erreichen dies durch Replikation von Steuerrechnern und durch den Vergleich deren Ausgaben (Voting und Monitoring). Moderne kryptographische Verfahren aus dem Bereich des Verifiable Computing ermöglichen einen neuartigen Ansatz, um Fehler zu erkennen: Mit Succinct Non-Interactive Arguments of Knowledge (SNARKs) lassen sich kryptographische Signaturen für Berechnungen erstellen, die eine Korrektheit des Ergebnisses garantieren. So können Fehler erkannt werden, ohne zusätzliche Replikation von Computern. Die Anwendung und Eignung von SNARKs für sicherheitskritische Avioniksysteme wird am ILS erforscht. Es werden Methoden entwickelt, die speziell auf die Anforderungen von sicherheitskritischen Echtzeitsystemen angepasst sind.

Aufgabe

Aufgabe ist es, eine durch SNARKs verifizierbare Lageregelung zu entwickeln und diese auf einen Multikopter Labordemonstrator zu integrieren. Dazu muss ein vorhandenes Software-Framework für Verifiable Computing für den Einsatz auf ressourcenbeschränkte Mikrocontroller portiert werden. Im Anschluss soll ein SNARK-basiertes Fehlertoleranzkonzept für die Flugsteuerung der Drohne entwickelt und auf dem Demonstrator integriert werden. Zum Schluss soll die Funktionsweise des Konzeptes demonstriert und evaluiert werden. Eine angemessene Dokumentation und Präsentation der Arbeitsergebnisse ist obligatorisch.

Die Arbeitsschritte im Einzelnen:

1. Literaturrecherche
 - a) Verifiable Computing und SNARKs
 - b) Fehlertoleranzmechanismen für hochsicherheitskritische Systeme in der Luftfahrt
2. Konzeptionierung
 - a) Entwicklung eines SNARK-basierten Fehlertoleranzkonzeptes für vorhandenen Drohnen-Demonstrator
3. Implementierung
 - a) Einarbeitung in Softwareframework für SNARKs
 - b) Portierung des Frameworks auf Mikrocontroller
 - c) Umsetzung des Fehlertoleranzkonzeptes
 - d) Validierung und Evaluierung
4. Dokumentation der Ergebnisse und Verfassen einer Abschlussarbeit

Ideale Voraussetzungen

Der/die Kandidat/in verfügt über sehr gute Kenntnisse in C, C++ und Mikrocontrollerprogrammierung. Gute Kenntnisse in der Regelungstechnik sowie aus der Vorlesung Luftfahrtsysteme sind hilfreich.

Beginn:

Abgabe:

Betreuer: M.Sc. Johannes Reinhart

Prüfer: Prof. Björn Annighöfer

Datum, Unterschrift Betreuer: _____

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.