Aufgabenstellung

Masterarbeit

Digitale Zertifikate für die automatische Konfiguration einer adaptiven Avionikplattform.

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

Kontext

Software für konventionelle Avioniksysteme im zivilen Luftverkehr wird bei der Integration in ein Luftfahrzeug statisch konfiguriert. Dies beinhaltet unter anderem die Zuordnung von Applikationen auf Rechenmodule oder die Festlegung von Kommunikationspfaden. Dadurch ist die Integration von Avioniksystemen mit einem hohen zeitlichen und finanziellen Aufwand verbunden und Ressourcen werden während des Betriebes nicht optimal ausgenutzt. Am ILS wird an zukunftsweisenden Avionik-Plattformen geforscht, die selbstständig Entscheidungen über ihre Konfiguration treffen und adaptiv auf Änderungen im System, in der Umgebung oder bezüglich des Betriebszustandes reagieren können. Damit soll der Entwicklungs- und Integrationsaufwand von Avioniksystemen trotz steigender Komplexität verringert, und Ressourcen sollen besser ausgenutzt werden. Hierbei muss allerdings sichergestellt werden, dass automatisch generierte Konfigurationen korrekt sind, da eine falsche Konfiguration zu einem kritischen Fehler führen kann.

Aufgabe

In dieser Arbeit soll ein neuartiger Ansatz erarbeitet werden, um automatisch generierte Konfigurationen mit einem digitalen, kryptographischen Zertifikat abzusichern. Das Zertifikat soll dabei garantieren, dass die Konfiguration geforderte Eigenschaften erfüllt und konsistent ist. Als Basis dient das Konzept der am ILS entwickelten Plug-and-Fly Plattform. Das digitale Zertifikat soll mit einem Succinct Non-Interactive Argument of Knowledge (SNARK), einem modernen kryptographischen Verfahren, umgesetzt werden. In einem ersten Schritt soll ein Konzept für die Umsetzung eines solchen digitalen Zertifikates mithilfe von SNARKs erstellt werden. Als nächstes sollen verschiedene Software-Frameworks für SNARKs verglichen und hinsichtlich ihrer Tauglichkeit für die Aufgabe evaluiert werden. Schließlich sollen geeignete nachzuweisende Eigenschaften einer Konfiguration ausgewählt werden und ein Proof-of-Concept in Software umgesetzt werden. Eine angemessene Dokumentation und Präsentation der Arbeitsergebnisse ist obligatorisch.

Die Arbeitsschritte im Einzelnen:

1. Literaturrecherche
   a) Verifiable Computing und SNARKs
   b) Plug-and-Fly Konzept des ILS
2. Konzeptionierung
   a) Auswahl von durch ein Zertifikat nachzuweisenden Eigenschaften
   b) Evaluierung und Auswahl eines geeigneten SNARK Softwareframeworks
3. Implementierung
   a) Formulierung der Zertifikateigenschaften als SNARK-Circuit entsprechend des gewählten Frameworks
   b) Entwicklung, Umsetzung und Validierung eines Proof-of-Concept
4. Dokumentation der Ergebnisse und Verfassen einer Abschlussarbeit

Ideale Voraussetzungen

Der/die Kandidat/in verfügt über sehr gute Programmierkenntnisse und bringt die Fähigkeit mit, sich in neue Themengebiete schnell einzuarbeiten.

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.