



# Aufgabenstellung zur Diplomarbeit

für

**Herrn Jan Schulz**

## **Fallstudie: Selektiver Schutz von eingebetteter Flugregler Software gegen Hardwarefehler**

### Aufgabenstellung:

Schrumpfende Strukturgrößen integrierter Schaltungen und zunehmende Komplexität ihrer Architektur, führen zu immer unzuverlässigerer Hardware (HW). Durch Hardwarefehler kann es zur Veränderung von sicherheitskritischen Daten kommen. Dies kann eine Sicherheitsverletzung nach sich ziehen, wenn falsche Ergebnisse unentdeckt bleiben. Die Erkennung dieser Fehler kann durch Hardware- oder Softwaremaßnahmen umgesetzt werden. Normalerweise können benutzerdefinierte, Hardware-basierte Lösungen eine bessere Leistung erzielen, allerdings erhöhen sie die Komplexität des Gesamtsystems. Software-basierte Lösungen erlauben den Einsatz von COTS-Hardware und sind flexibel anpassbar. Sie können automatisch angewandt werden, was die Entwicklungszeiten und -kosten reduziert. Dennoch haben aktuelle Software-basierte Lösungen einen Nachteil - ihren hohen Overhead. Das vorgeschlagene Forschungsprojekt konzentriert sich auf dieses Problem: *Wie kann der Overhead, von in Software implementierten HW-Fehler Erkennungsmechanismen (HWFE), unter Einhaltung der geforderten Systemzuverlässigkeit, minimiert werden?* Wir planen HWFE selektiv und nur auf die kritischsten Teile des Systems anzuwenden. Hierfür bewerten wir den Einfluss verschiedener HWFE auf die Zuverlässigkeit und Performanz der SW- und HW-Systeme. Das Hauptziel dieser Diplomarbeit ist die Entwicklung einer Fallstudie für den Schutz von eingebetteter Flugregler Software (EFCS). Diese Arbeit besteht aus drei Teilen: Entwicklung, Analyse und Dokumentation.

- Strukturierte Anforderungsdefinition

### *Entwicklung:*

- Analyse der bestehende Handel-C Version von EFCS
- Entwurf eines Modell, das Systemaufteilung, Kontroll- und Datenflussstrukturen des EFCS beschreibt
- Entwicklung einer C-Version von EFCS nach dem Software-Modell
- Testen der C-Version von EFC Software mit vorhandenen Testfällen

### *Analyse:*

- Kontrollfluss Analyse mit den bestehenden Testfällen
- Einbindung des C-Version von EFC Software mit einem physikalischen Modell des Flugzeugs
- Allgemeine Auswirkungsanalyse (FMEA oder HAZOP)
- Allgemeine Performance-Analyse

### *Dokumentation:*

- Doxygen Quellcode-Kommentierung
- Notwendige Software-Dokumentation
- Diplomarbeit

Prof. Dr.-techn. K. Janschek  
Verantwortlicher Hochschullehrer

Betreuer: Dr.-Ing. Andrey Morozov  
Bearbeitungszeitraum: 11.02.2013 - 11.08.2013