Formal Verification of the F-16 Aircraft Ground Collision Avoidance System

Background

Formal verification is often applied to guarantee correct functionality of safety critical systems whose failure would endanger human lives, and also for applications for which tests on the real system are very expensive. One application that meets both of these criteria is the ground collision avoidance system of the F-16 aircraft model. The goal of this thesis is to verify correct functionality of the ground collision avoidance system with formal verification techniques.

Description

The ground collision avoidance system of the aircraft is modeled as a hybrid automaton with nonlinear dynamics. For the verification of the system, reachability analysis is used to proof that the set of reachable states does not intersect the ground. For this thesis, the CORA toolbox [1] is used to compute the reachable set.

The thesis includes the following steps: First, the model of the system described in [3], for which MATLAB and Python code is provided on a public repository[1] should be converted to the SpaceEx format [2], which is a standard modeling language for hybrid systems. Next, the reachability toolbox CORA should be used to verify the model. Since CORA implements several different algorithms and approaches for the reachable set computation, it should be evaluated which technique is best suited to verify the ground collision avoidance system.

Graphic taken from [2]

Tasks

- Creation of a system model in SpaceEx format
- Verification of the system using the reachability toolbox CORA
- Evaluation of the performance of the different verification approaches implemented in CORA on the ground collision avoidance system
- *Optional:* Verification of other automated aircraft maneuvers
- *Optional:* Development of improvements for CORAs verification approaches

[1] https://github.com/pheidlauf/AeroBenchVV
[2] https://fas.org/man/dod-101/sys/ac/f-16.htm

Technische Universität München

Fakultät für Informatik

Lehrstuhl für Echtzeitsysteme und Robotik

Supervisor:
Prof. Dr.-Ing. Matthias Althoff

Advisor:
Niklas Kochdumper, M.Sc.

Research project:
ARCH competition

Type:
BA/MA

Research area:
Reachability Analysis, Hybrid Systems

Programming language:
MATLAB

Required skills:
Very good mathematical background, programming in MATLAB

Language:
English, German

Date of submission:
16. Juli 2019

For more information please contact us:

Phone: +49.89.289.18144

E-Mail:
niklas.kochdumper@tum.de

Internet: www6.in.tum.de

References

[1] Matthias Althoff. An introduction to cora 2015. In *ARCH@ CPSWeek*, pages 120–151, 2015.

[2] Scott Cotton, Goran Frehse, and Olivier Lebeltel. The spaceex modeling language, 2010.

[3] Peter Heidlauf, Alexander Collins, Michael Bolender, and Stanley Bak. Verification challenges in f-16 ground collision avoidance and other automated maneuvers. volume 54 of *EPiC Series in Computing*, pages 208–217. EasyChair, 2018.

Technische Universität München

Fakultät für Informatik

Lehrstuhl für Echtzeitsysteme und Robotik