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 prove 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 repository1 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.

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

1https://github.com/pheidlauf/AeroBenchVV
References

