Formal Verification of Distributed Aircraft Controllers
Sarah M. Loos, David Renshaw, and André Platzer
Computer Science Department, Carnegie Mellon University

ABSTRACT
As airspace becomes ever more crowded, air traffic management must reduce both space and time between aircraft to increase throughput, making on-board collision avoidance systems ever more important. These safety-critical systems must be extremely reliable and work properly under every circumstance. In tough scenarios where a large number of aircraft must execute a collision avoidance maneuver, a human pilot under stress is not necessarily able to understand the complexity of the distributed system and may not take the right course, especially if actions must be taken quickly. We consider a class of distributed collision avoidance controllers designed to work even in environments with arbitrarily many aircraft. We prove the controllers never allow aircraft to get too close to one another, even when new planes approach an in-progress avoidance maneuver. Because these safety guarantees always hold, the aircraft are protected against unexpected emergent behavior which simulation and testing may miss.

METHODS
Distributed aircraft controllers are distributed hybrid systems, which we model and verify using quantified differential dynamic logic (QDfL) [1]. Below are a few selected rules from the QfL proof calculus, categorized loosely as discrete or continuous transitions.

CASE STUDY
Verified Big Disc Protocol
Figure 2. We illustrate one possible trajectory of a collision avoidance maneuver under the Big Disc protocol. The current direction of flight of aircraft $i$ is given by the indexed variable $d[i]$ as a 2D unit vector. The variable $s[i]$ is the position of the center of $i$‘s buffer disc. The aircraft need not always turn at its maximum angular velocity; we require only that the aircraft remain within the disc by cycling in its original direction.

Figure 3. The buffer zone in this protocol is a disc of radius $\min(r[i])$ centered at a point distance $\min(r[i])$ away from $s[i]$, in a direction perpendicular to $s[i]$ motion either to the left or the right. Thus the aircraft is always on the edge of its disc, and during collision avoidance, the aircraft follows the circumference of its disc. An aircraft may flap its circling direction during free flight, causing the disc to jump to the other side of the aircraft; however, before an aircraft can flip its circling direction, it must check that it may do so safely.

TOOLS
KeY's user is our automated theorem-prover for differential dynamic logic [2]. KeYmaera is a distributed theorem-prover for quantified differential dynamic logic, which handles distributed hybrid systems [3].

CONTRIBUTIONS
• We provide a formally verified distributed system of aircraft with curved flight dynamics.
• Our controller only does fixed aircraft trajectories with no corners or instantaneous changes of ground speed.
• We prove our controller is safe for an arbitrarily large number of aircraft. This guarantee is necessary for high-traffic applications such as crowded commercial airspace, UAV maneuvers, and robotic swarms.
• Other aircraft may enter an avoidance maneuver already in progress and safety for all aircraft is guaranteed still.
• We use arithmetic coding to reduce proof complexity and branching.
• We prove that even when the interactions of many aircraft cause unexpected emergent behavior, all resulting control choices are still safe.
• We present hierarchical and compositional techniques to reduce a very complex system into smaller, provable pieces.

REFERENCES
This poster is based on research presented in full in:

