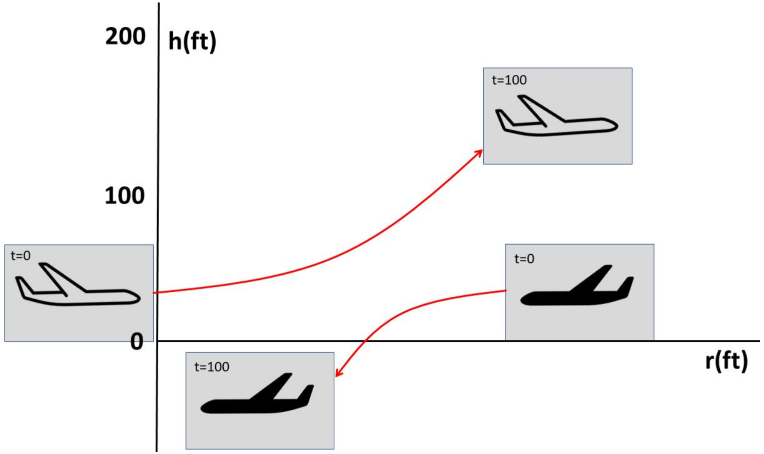
Formal Verification of Next-Generation Airborne Collision Avoidance System with Adversarial Intruder Behavior

Rachel Cleaveland
Advisor: André Platzer
Mentor: Stefan Mitsch

Background

- **Mid-air aircraft collisions** are increasing in likelihood as air space gets more congested
  - Collision avoidance maneuvers are performed as a last resort when two aircraft are on a collision course
  - It is imperative to **formally verify the safety of these maneuvers**



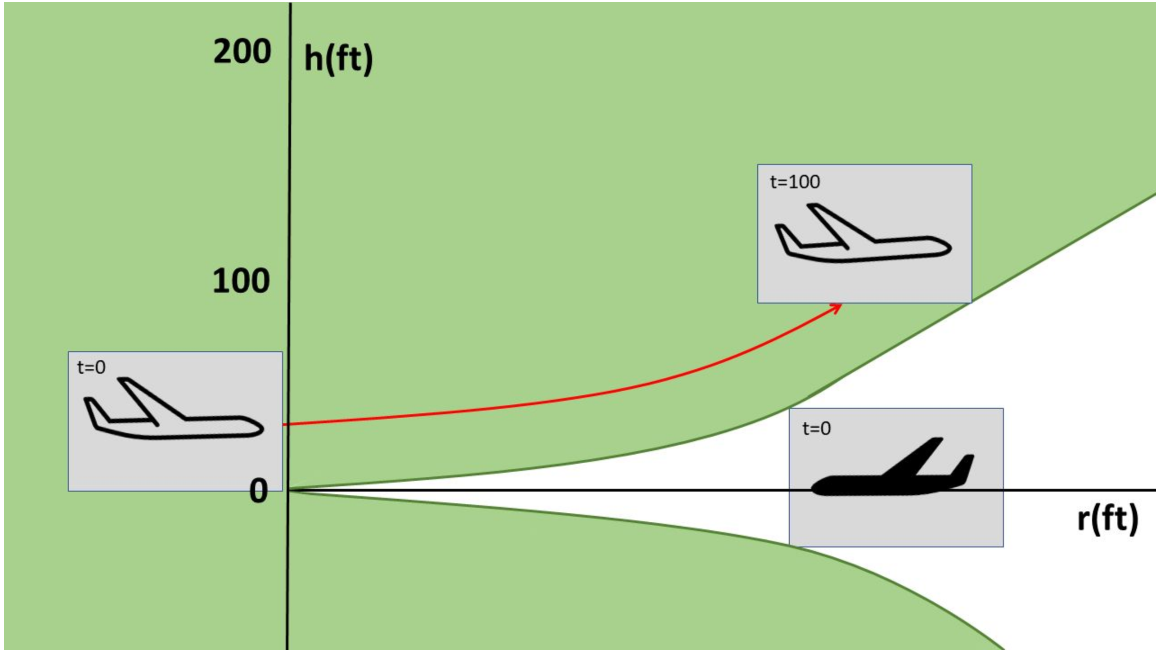
Background

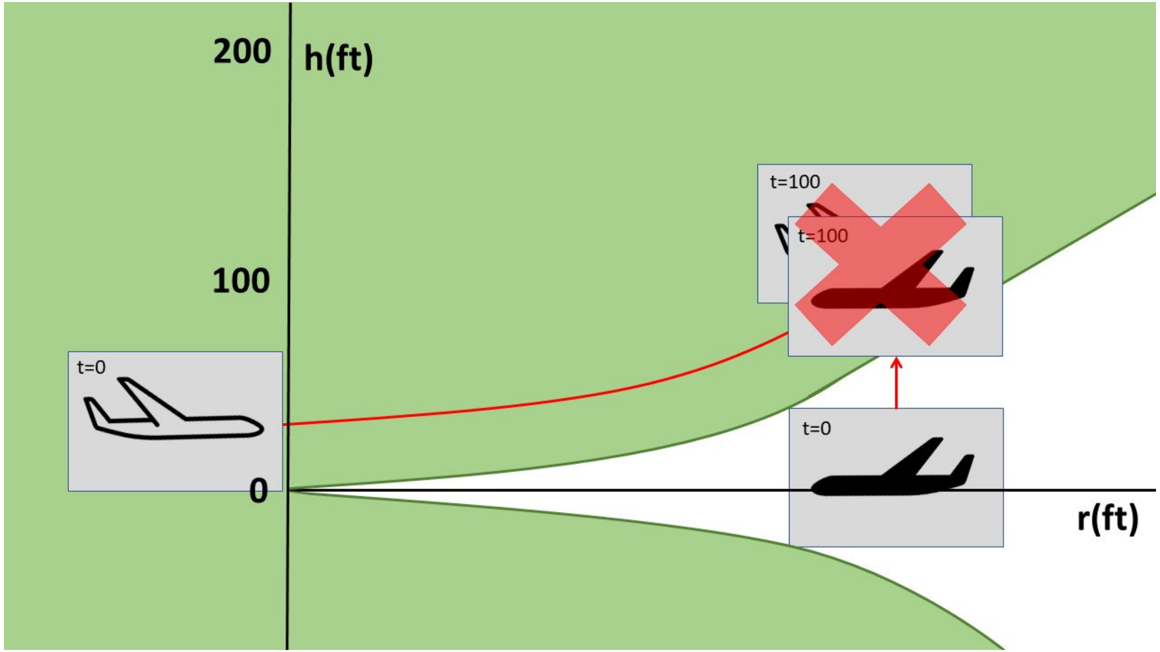
- **ACAS X** is a collision-avoidance system developed by the Federal Aviation Administration (FAA)
    - An advisory asks the pilot to maintain their vertical speed, or accelerate towards a new vertical speed
    - Uses the position and velocity of an ownship and intruders in its collision avoidance advisories

Previous Work

- Previous work has assumed **severe restrictions on the intruder's maneuverability** in their verification of ACAS X
  - Limits safety guarantees in real-world collision scenarios.

- Our previous work assumed that the intruder aircraft is approaching at a constant velocity, both horizontally and vertically.


200
h(ft)
100
t=100
t=0
t=0
0
r(ft)


200
h(ft)
100
0
r(ft)
t=0
t=100
t=100
t=0

Contribution

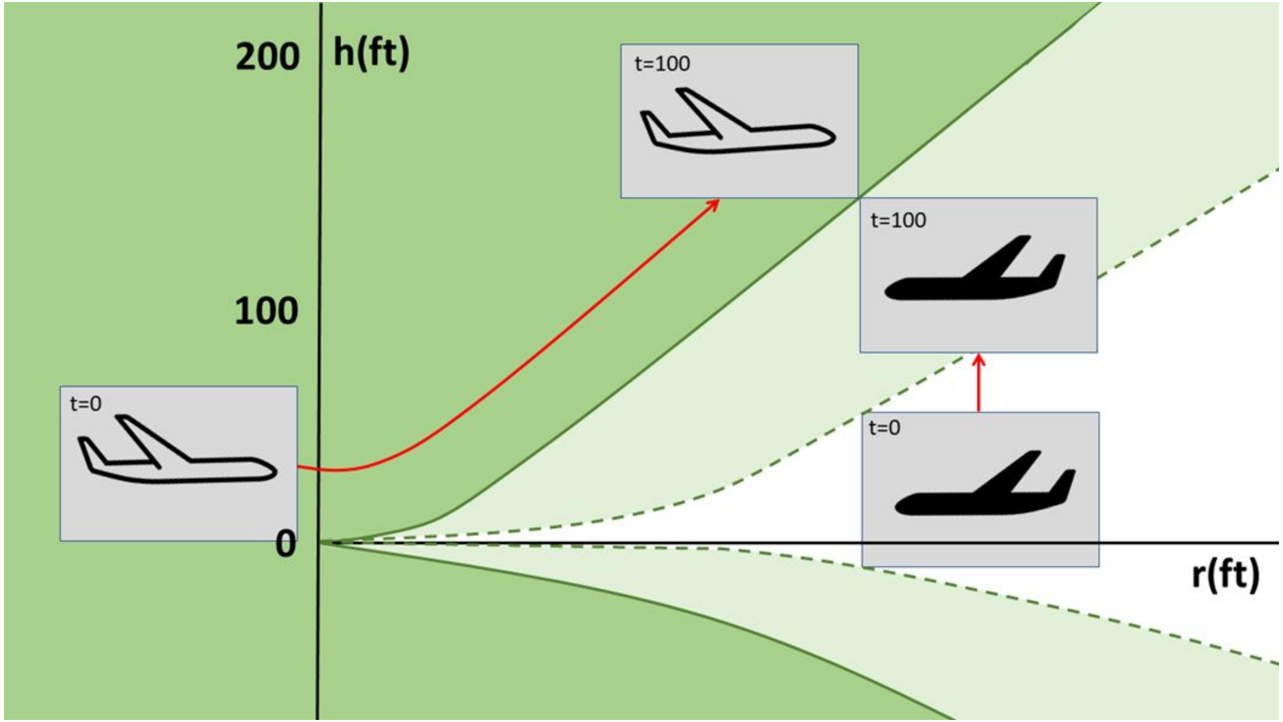
- My work represents aircraft encounters using Differential Game Logic (dGL)
  - dGL allows for the **modeling of an intruder aircraft that can change its flight path and velocity,** as opposed to the fixed flight paths of our previous work.
  - The ownship must have a **strategy to overcome any sequence of intruder maneuvers**.

This is the first work that we know of to apply hybrid games to the problem of aircraft collision-avoidance.

Contribution

- We reuse the idea of *safe regions* introduced in our previous work
  - A region is **safe** if for all possible ownship positions and velocities within the region, a near mid-air collision (NMAC) will never occur

Contribution



Contribution

If ACAS X issues an advisory, and following this advisory always keeps the ownship within a safe region, then this advisory is guaranteed to be safe.

Model Overview

1 $\text{init}() \wedge R(r, h, v, \text{advisory} = (w, v_{lo})) \rightarrow$

2 $[(\quad (\text{advisory} := (w, v_{lo}); ?R(r, h, v, \text{advisory} = (w, v_{lo}));)$

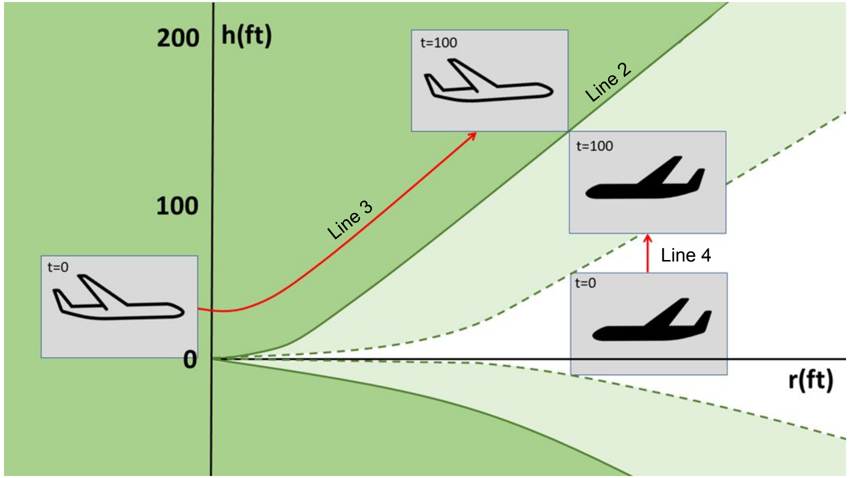
3 $\quad (a_o := \text{ownship}(\text{advisory});)^d$

4 $\quad (\boldsymbol{a_i} \mathbf{:= intruder} \;;$

5 $\quad\quad \{\text{motion}(a_o, a_i) \quad \& \quad \text{EDC}(v, v_{lo}, a, a_{lo})\}$

6 $\quad)^*$

7 $)^*](\neg\text{NMAC})$



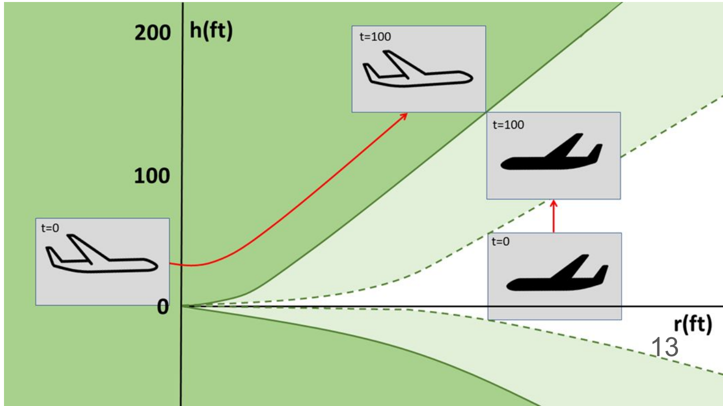
Results

Developed and proved seven hybrid game models verifying under appropriate assumptions that the ownship can always maneuver to safety.

Results

- Category 1: **Infinite-horizon**
  - Requires advisories to be safe indefinitely
  - Ownship must avoid collision *whether or not* a new advisory is issued
  - This is a rigid definition of safety

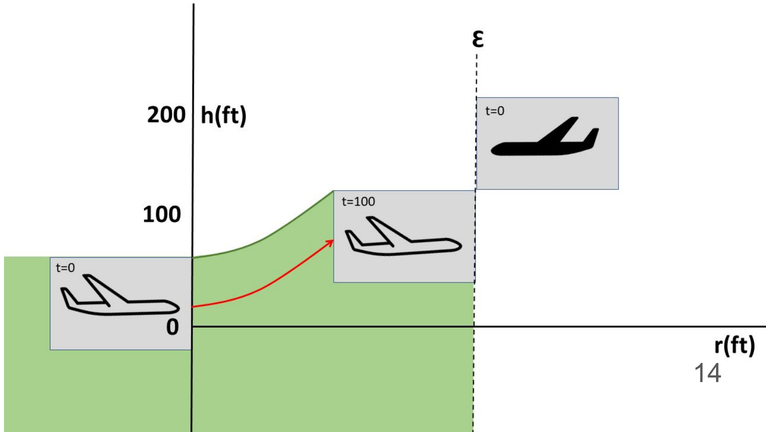
Model 1: non-maneuvering intruder
Model 2: vertically-maneuvering intruder
Model 3: horizontally-maneuvering intruder



Results

- Category 2: **Finite-horizon**
  - Proves safety of advisories only up to Ɛ-time
  - No liveness: does not give formal safety guarantees after Ɛ-time
  - Stepping-stone to the safeable models

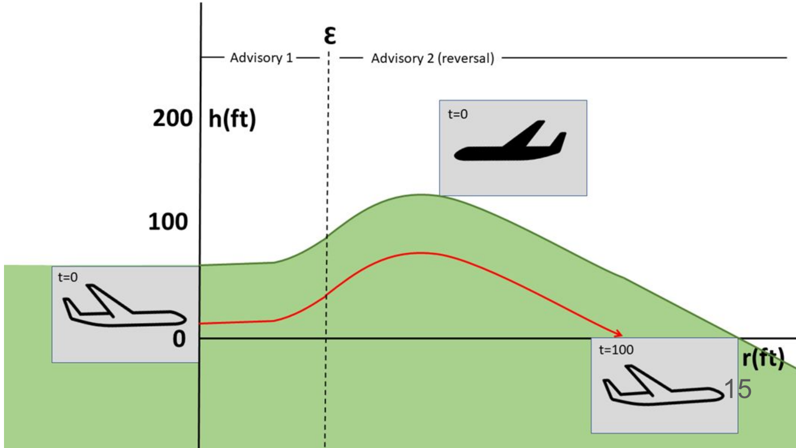
Model 4: non-maneuvering intruder
Model 5: vertically-maneuvering intruder



Results

- Category 3: **Safeable**
  - An advisory is *safeable* if and only if it is safe, or can be made safe in the future via subsequent advisories
  - Proves Ɛ-time safety with liveness: advisories are safe after Ɛ-time if there exists a follow-up advisory which is safe indefinitely

Model 6: non-maneuvering intruder
Model 7: vertically-maneuvering intruder



Conclusion

- Applied hybrid games to the verification of ACAS X
  - Proved that against an intruder with limited maneuverability, an ownship given a safe ACAS X advisory can always find a verifiably safe path.

Future Work

- Develop and prove bounded-time and safeable models in which the intruder has horizontal maneuverability

- Develop models for an intruder which can simultaneously maneuver horizontally and vertically

- Ownship collision-avoidance maneuvers are currently limited to the vertical direction
  - Expand ownship maneuverability to the horizontal direction