Transportation CPS Workshop
CPS for Aviation: Looking Forward
Controller Design for Safety Critical Systems

Claire Tomlin (UC Berkeley)

with Ian Mitchell (UBC), Alex Bayen (UCB), Jerry Ding (UCB), Rodney Teo (DSO), and Jung Soon Jang (Boeing)
Controller Design for Safety Critical Systems

Controller synthesis: to guarantee that a system satisfies a safety property
Controller Design for Safety Critical Systems

Controller synthesis: to guarantee that a system satisfies a safety property
**Safety Property** can be encoded as a condition on the system's **reachable set of states**

- In red, system may become unsafe.
- On boundary, apply control to stay out of red.
- In blue, system will stay safe.
Example 1: Collision avoidance control
Collision Avoidance Control

Simple demonstration

- **Pursuer**: turn to head toward evader
- **Evader**: turn to head right

Movies…
Collision Avoidance Control

http://www.cs.ubc.ca/~mitchell/ToolboxLS/
Extending to multiple aircraft
Example 2: Protocol design

Unsafe set without maneuver

Unsafe set with maneuver

Unsafe set with choice to maneuver or not?
Protocol Design

- Ability to choose maneuver start time further reduces unsafe set.
Implementation: a finite automaton

- It can be easier to analyze discrete systems than continuous: use reachable set information to abstract away continuous details.
Tested at Moffett Federal Airfield

Coast and turn EEM

EEM alert

Above threshold

Separation distance (m)

North (m)

East (m)

time (s)

Line up for take off

Normal
OwnShipSpd=31.6 m/s, OthShipSpd=31.0 m/s
OwnShipHdg=-4.4 deg, OthShipHdg=-19.6 deg
time=364.9 s
Tested at Edwards Air Force Base

T-33 Cockpit

[DARPA/Boeing SEC Final Demonstration: F-15 (blunderer), T-33 (evader)]
Blunder Zone is shown by the yellow contour.

Red Zone in the green tunnel is the intersection of the BZ with approach path.

The Red Zone corresponds to an assumed 2 second pilot delay. The Yellow Zone corresponds to an 8 second pilot delay.
Map View showing a blunder

The BZ calculations are performed in real time (40Hz) so that the contour is updated with each video frame.
Example 3: Automated Aerial Refueling

$\delta$ = Long. Tolerance for Catching Boom
$\Delta W$ = Lat. Tolerance for Catching Boom

Boeing, AFRL CERTA FCS Program
Directions

• AFOSR MURI: from controller design to code
• NASA: integrating short term collision avoidance methods with long term separation assurance schemes
• NASA: Super-dense regions (Hansman and Balakrishnan)
• AFRL: G-CAS, A-CAS, AAR