
Kristin Yvonne Rozier
University of Cincinnati

Dagstuhl Seminar on Formal Foundations for Networking
February 10, 2015
Overview

Net-enabled aircraft are being designed now!

**Goal:** reduce the cost of aircraft by migrating towards software and net-enabled/cloud-based architecture and capabilities

**Method:**
- reduce aircraft **weight**
- increase **automation**
- move from hardware to **software**
- move from aircraft-based systems to **fleet-based systems**
- reduce **maintenance**
Design Paradigm

**Increase:**

- software networking
- digital communications
- automation for
  - cockpit systems development
  - aircraft avionics advances
  - ground-to-air interaction

**Decrease cost:**

- of operations
- of maintenance and inventory of mechanical parts
- of customizing and certifying new
  - aircraft cockpit designs
  - wiring
  - control systems
  - flight management algorithms

How will we automatically verify these designs?

Laboratory for Temporal Logic

Kristin Yvonne Rozier

Challenge: Net-Enabled Aircraft
Challenge 1: Cockpit Design Costs and Complexity

Cockpit: highly complex hybrid system

- many heavy mechanical parts
- software
- hardware
- instrumentation
- control systems
- flight management system
- interfaces
- trip-switches
- other sub-systems
- customized for every aircraft type

Boeing 787 Cockpit:
wheel column alone weighs over 400 lbs
Challenge 1: Cockpit Design Costs and Complexity

Cockpit: highly complex hybrid system

- many heavy mechanical parts
- software
- hardware
- instrumentation
- control systems
- flight management system
- interfaces
- trip-switches
- other sub-systems
- customized for every aircraft type

Boeing 787 Cockpit: wheel column alone weighs over 400 lbs

We have not solved the formal verification problem for current cockpits.
Challenge 1: Cockpit Design Costs and Complexity

Cockpit: highly complex hybrid system

- many heavy mechanical parts
- software
- hardware
- instrumentation
- control systems
- flight management system
- interfaces
- trip-switches
- other sub-systems
- customized for every aircraft type

Boeing 787 Cockpit: wheel column alone weighs over 400 lbs

We have not solved the formal verification problem for current cockpits. How do we scale to net-enabled cockpits?
Challenge 2: Electrical Wiring Weight and Complexity

Replace wires with wireless

- fly-by-wire better than mechanical control
- wiring is both complex and heavy
- wiring is customized for every aircraft type
- wiring must be manually fitted for every aircraft

How will we verify these hybrid wired/wireless networks?
A350: electrical systems installation

A380-800 has about 100,000 wires, 470 km long, 5700kg of weight + additional 30% weight for wiring harnesses

Typical wiring installation in A380 crown area (above ceiling panels)
Cost of Aircraft Weight

1 ton = $7.2B revenue
Challenge 3: Software Systems for Each Aircraft and Increasing Management Cost

Now:
- flight controls, trajectory, and information management systems on every plane
- fleet management limited to resources on each aircraft
- software development, certification, and installation billed per aircraft

Future:
- move hardware to software
  - easier to upgrade/maintain
- move local software to cloud or network of same-type aircraft
  - decrease fleet inefficiency/down-time per aircraft for upgrades
- software for a fleet, not for a plane
  - easier fleet management
Challenge 3: Software Systems for Each Aircraft and Increasing Management Cost

Now:
- flight controls, trajectory, and information management systems on every plane
- fleet management limited to resources on each aircraft
- software development, certification, and installation billed per aircraft

Future:
- move hardware to software
  - easier to upgrade/maintain
- move local software to cloud or network of same-type aircraft
  - decrease fleet inefficiency/down-time per aircraft for upgrades
- software for a fleet, not for a plane
  - easier fleet management

**Harder to formally verify . . .**
What can we take off before we take off?

A350/A380 cockpits’ on-board information management systems: how much can be moved?
Challenge 4: Aircraft-Centric Operations

Networked aircraft → optimal planning

- more direct flights
- less fuel, crew fatigue, time
Previous Work: V&V of Automated Air Traffic Control System Designs


Challenge 5: Must be safer! Real-time and Redundant

- improved intra-aircraft networks
- improved inter-aircraft/ground network technology

Need real-time information about critical parts!
Need redundant/back-up systems!
Previous Work: Real-time System Health Management for Intelligent, Autonomous UAS


ARMD Seedling Phase I

- designing for increased software operations
- networked/cloud-based systems for individual aircraft + fleet operations
- wired → wireless
- modularity
- real-time connectivity: faster upgrades, lower maintenance
Need to Develop: New Cockpit Design

- wireless
- software-enabled controls
- digital, continuous, reconfigurable displays
- interaction with runtime monitors?
- cloud-controlled operations?

NASA and partners are looking to design initial prototypes this year!

Ex. Goal: reduce at least 1 ton of weight/aircraft
New Cockpit: Can We Move These to Software?

- Wheel column, yoke, & back drive (Boeing); joystick (Airbus)
- Thrust levers for propulsion control
- Brake pedals/levers
- Rudder pedals
- Display and flight management system interactions
- Trip switches, knobs, controls
- Flap setting, spoiler levers
- Landing gear controls
Need to Develop: New Fleet Operations Design

- aircraft as networks
- network of aircraft
- cloud architecture supporting fleet operations
New Fleet Architecture:

Can We Move These to the Cloud?

- trajectory planning/re-planning
  - fuel optimality
  - weather
  - traffic
- scheduling connections: passengers, crew, aircraft
- emergency assistance

What are the constraints?

What flight management systems cannot be moved to the cloud?
Need to Formally Reason About:

- Runtime monitoring/real-time system health management
- Integrity, reliability, latency of communications
- Security, encryption, trustworthiness of data
- Network mobility, software-defined networking
- Fault-tolerant networking
- Cloud resource availability, security, aircraft synchronization
- Redundancy & back-up systems
ECON Design Team, by group

- 4 NASA Aeronautics Centers & JPL
- 14 Industry Partners
- 6 Academic Institutions
- **1 Formal Methods expert so far . . .**
Overview

Net-Enabled Aircraft Design

Current Project Status

Join the Team!

ECON Design Team, by group

- NASA Aeronautics Centers (ARC, AFRC, GRC, LaRC), & JPL
  - PI: Parimal Kopardekar, NASA Ames Research Center

- 14 Industry Partners
  - Aurora, Boeing, CAFÉ Foundation, FedEx, GE, Gulfstream, Harris Corp, M2C Aerospace, NextGen AeroSciences, Nissan, Rockwell Collins, Sensurion/United, Terrafugia, Verizon, outside SMEs
    - Additional interest: CISCO, Northrup Grumman

- 6 Academic Institutions
  - U. Cincinnati, MIT, Georgia Tech, Penn State, U. Massachusetts, U. Colorado

- 1 Formal Methods expert so far . . .
Conclusion

Lighter Cheaper Safer

- ECON is happening now
- Formal methods involved from initial design time
- How do we meet this challenge?
  - What restrictions do we need to make to enable FM?
  - How do we rise to the design-analysis challenge?
  - Runtime verification and integration into the cockpit too
- Future UAS applications

Join the team!
rozierky@uc.edu; parimal.h.kopardekar@nasa.gov