Implementing the right thing in future aviation systems

Dr. Mallory S. Graydon

m.s.graydon@nasa.gov she | her | hers

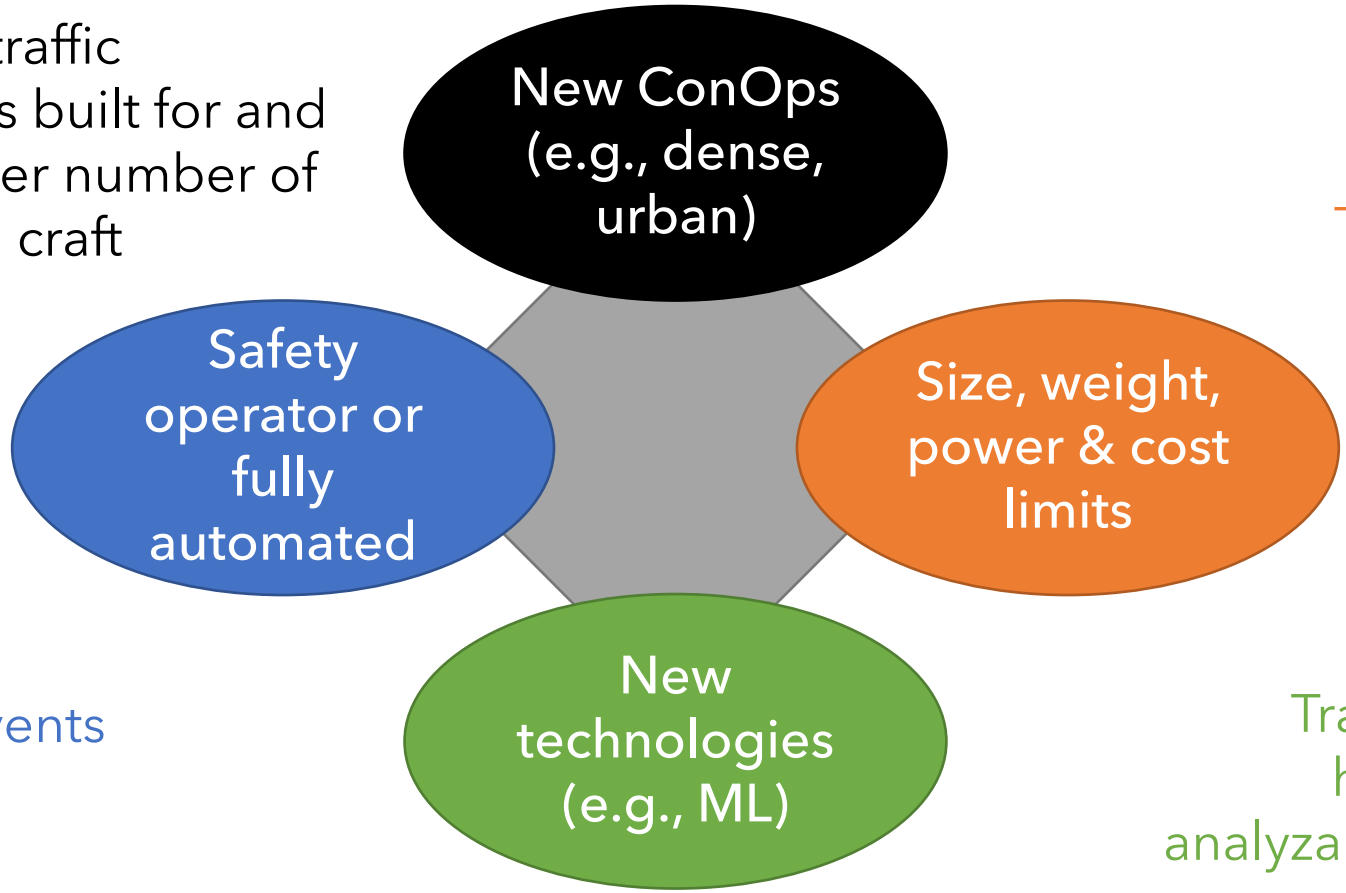
Safety Critical Avionics Systems Branch

NASA Langley Research Center, Hampton, Virginia, USA

Dependability, novelty, and frugality

Traditional air traffic management is built for and around a smaller number of human-piloted craft

Traditionally piloted aircraft rely on pilots to handle failures and unexpected events



Traditional transport category aircraft rely on robustly engineered, highly redundant computer systems

Traditional aircraft use highly deterministic, analyzable control software

Humans adapt

Human pilots adapt

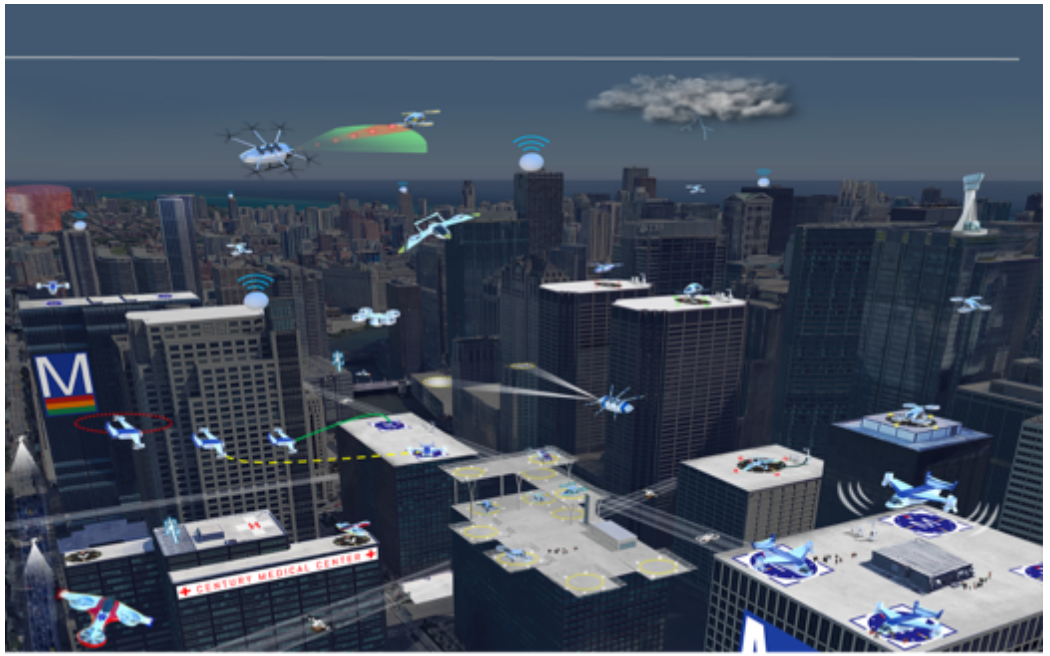
- Design philosophy on human–machine disagreements varies, but aircraft often turn to pilots when systems fail
- Suppose we have only a *safety operator*:
  - A human might be able to recognize dangers the machine doesn't
  - But a safety operator might lack *airmanship* skills
- Fully automated machines *must* handle *all* circumstances they find themselves in
  - Planned reactions to both failures and things happening in their environment need to be carefully thought through
  - Machines must be modified as cases are identified

How people get it right

- Learn from history
  - Read accident reports
  - Field feedback and monitoring, e.g.:
    - Data logging from engine controllers (FADECs) and other systems
    - NASA's Aviation Safety Reporting System
- Test assumptions, e.g. about how pilots react to things
  - The representativeness of the scenarios matters!
- Systematically explore and analyze scenarios
  - Early-lifecycle hazard analysis (e.g., FHA, STPA, etc.) is really useful

Preliminary hazard assessment

- We did partial, preliminary FHA & STPA on a *hypothetical* craft
  - Environment
    - Large city with tall buildings
    - Airspace shared with other craft
    - Unknown ATM/UTM in place
    - Broad range of weather conditions
  - eVTOL aircraft
    - Distributed electric propulsion
    - Wing-borne horizontal flight
    - Four passengers plus pilot
    - Limited autonomy



Loss of propulsion

- Loss of propulsion happens: engines fail, fuel freezes, etc.
  - Fixed-wing aircraft *glide*
  - Rotorcraft *autorotate*
- Small eVTOLs might lose propulsion:
  - Batteries explode
  - Motors and motor controllers fail
  - Computers and communications fail
- What happens when an eVTOL loses propulsion?
  - During cruise flight?
  - During vertical / forward flight transition?

Vertical flight control & failures

- Suppose an aircraft uses differential thrust for attitude control in vertical flight and a motor or motor controller fails
- What happens?
  - Can't autorotate with small rotors
  - Worst case design: lose attitude control *and* lift
    - And what if the vertiport is atop a tall building?
- Potential solutions:
  - Adaptive control algorithms
  - Variable pitch plus cross-shafting
  - Architectural redundancy

Possible weak point: transition

- Details depend on the transition mechanism!
- But transition might be near limits of both flight regimes:
  - E.g., airspeed high for vertical flight but low for horizontal
- And it'll be done at low altitudes
- What if transition is incomplete or asymmetric?
- What if propulsion or control fails during transition?

Situational awareness

- Suppose path planning/exec. fails during landing or deviation
- Will the pilot/operator have situational awareness?
  - Hard to maintain SA unless one is actively doing a task
  - Increased density might complicate, e.g., finding a vertiport pad
- How accurate & fast is correction from air control system?
- How well controlled will people & kit be at vertiport pads?

Unified control

- When craft switch between vertical & horizontal flight modes, some actuators might have different effects
  - E.g., in a tilt-rotor, thrust changes direction
- 'Unified control' is simpler for pilots: the controls always mean one thing and the computer uses actuators per the mode
- What happens when the computer fails?
  - One strategy for automation failure is to provide a robust direct control function and turn things over to the pilot
  - But what about pilot skill?
  - What about *mode confusion*?

Control handovers

- A fault affecting one control mode might not affect others
  - Suppose a failure in flight affects only vertical flight mode
  - It might go undetected until transition before landing
- Does the pilot/operator know what control mode is active?
- Is the pilot adequately skilled in horizontal & vertical modes?

Air traffic density

- Air traffic procedures must account for wind conditions, navigation performance, reaction & communication time, etc.
- Spacing sufficient for current craft would limit air traffic
- If computers fly more precisely, can we pack air more tightly?
- What happens when computers fail?
  - Will pilots have to hand-fly (without regular hand-flying to build skill)?
- What happens when communications fail?
  - Imagine a jammer is deployed in the area …

Crashworthiness as mitigation?

- Some proposed mitigations focus on *crashworthiness*
  - Ballistic parachutes
  - Energy absorbing materials
- These work to some degree in some cases
  - Parachutes slow impacts … if they are used at high enough altitude
  - Landing gear, fuselages, seats, etc. can absorb *some* impact energy
- But these mitigations mostly work on the occupants … risk to persons on the ground doesn't change much

Verifying new technologies

- In transport category aircraft, avionics often built to DO-178C
  - FAA recognizes DO-178C as a means of satisfying the regulations
  - DO-178C updates DO-178B, which was published in 1992
  - It relies on testing, analysis, traceability, change control, etc.
  - It seems to work: in accidents, software usually worked as designed
- Some proposed functionality depends on novel technologies
  - Adaptive control laws
  - Machine learning components (e.g., in detect-and-avoid)
- DO-178C might not be suited to these new technologies

Size, weight, power, & cost limits

- Transport-category aircraft avionics are designed for reliability
  - Weird stuff has been known to happen
  - Byzantine-fault tolerance is considered necessary in some systems
  - (In space, we even do radiation hardening!)
  - Avionics modules are often designed with redundant elements
  - But redundancy adds size, weight, and power demand
- Some UAM vehicles are small and have limited energy stores
  - This, plus cost pressures, create a desire to avoid using the highly fault-tolerant avionics boxes used in transport-category aircraft
- The question remains: what is good enough?

How will we evaluate risks?

- Once we've identified hazards and mitigations, how do we gauge remaining risk? How do we weigh trade-offs?
  - Are tilt rotors that can glide to a landing safer than multi-rotors that can handle a few failed motor or motor control units with ease?
- Quantitative risk studies
- Simulation might be heavily used:
  - Simulated flights to assess pilot/operator capabilities & responses
  - Simulations assess robustness of planned air traffic management
- But risk assumptions might & simulations might be unrealistic
  - Test flights & field feedback are essential

Conclusion

- Urban air mobility brings significant challenges
- There are multiple competing vehicle & air traffic concepts
- It is critical to:
  - Identify hazards and risks early in development
  - Monitor practice and performance in operation
  - Learn from the mistakes that will be made

Context (NOT PART OF SLIDES)

- Thu. 19 Nov.: 15-20 minutes presentation, 10–15 minutes Q&A
- Guidance from Phil: “Given your interests and work emphasis I'd say for this class a rant on the challenges of UAM op concepts sounds perfect. That's something they've probably heard the hype about but haven't learned to ask critical thinking questions about practical application. The other topics you mention [ML safety, efficacy of safety argumentation] I personally find important and interesting, but probably too advanced for them.”