Implementing the right thing in future aviation systems

Dr. Mallory S. Graydon

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

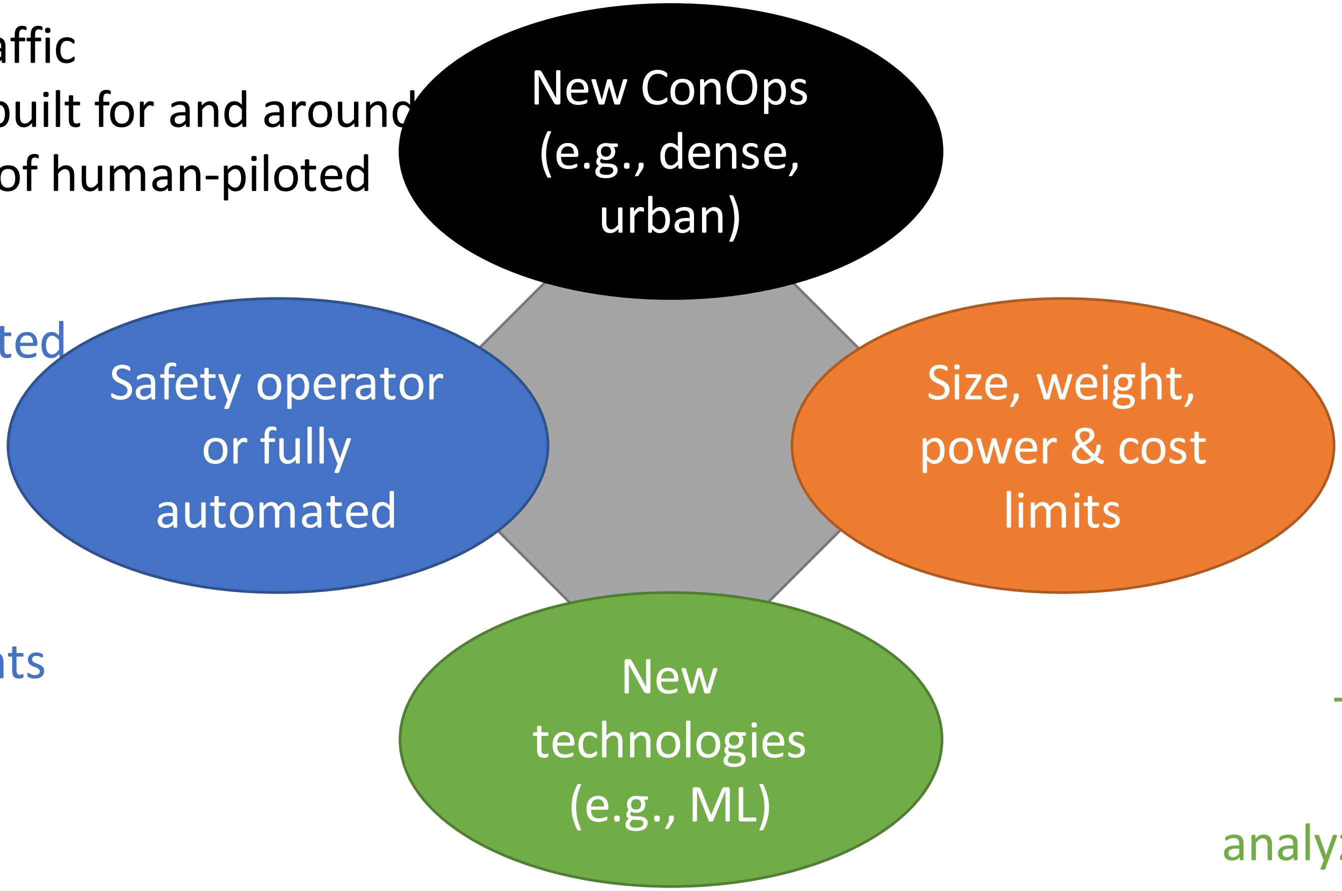
Safety Critical Avionics Systems Branch

NASA Langley Research Center, Hampton, Virginia, USA

Dependability, novelty, and frugality

Traditional air traffic management is built for and around 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
- Humans have pulled off some spectacular saves
  - TACA 110 (1988): Hail from a heavy thunderstorm disables both engines, crew lands on canal bank near NASA site (link)
  - UA 232 (1989): Crew landed plane with no operable flight control surfaces, saving half of those aboard (link)
- … even if they don't save the day every time

Human ~~pilots~~ ⇧ safety operators adapt?

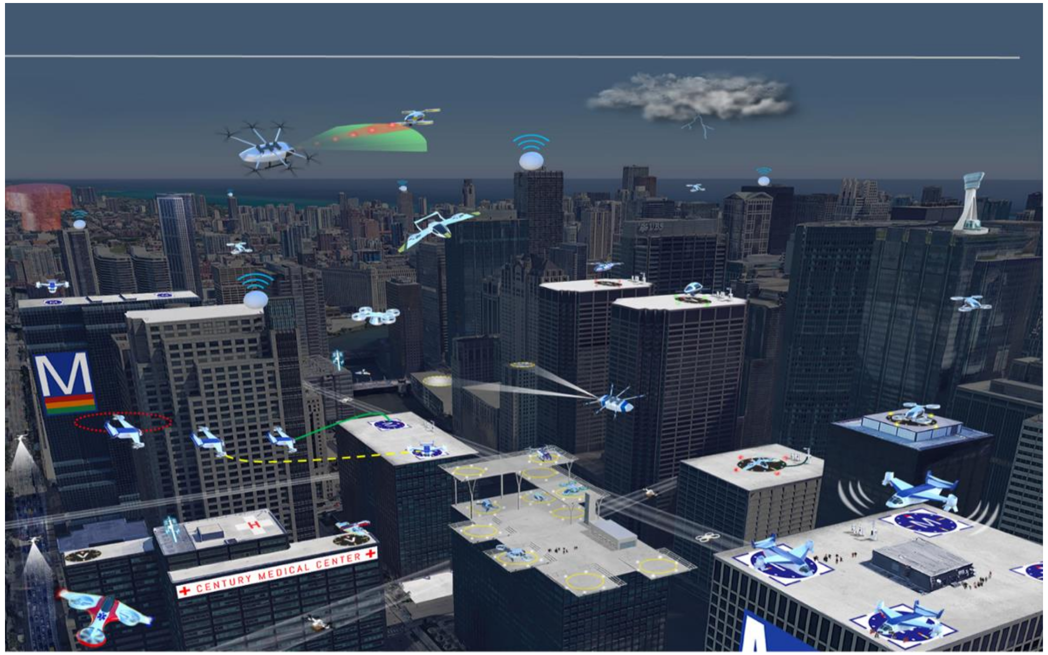
- Design philosophy on human–machine disagreements varies, but aircraft often turn to pilots when systems fail
- Suppose we have only a *safety operator*:
  - A human might be able to recognize dangers the machine doesn't
  - But a safety operator might lack *airmanship* skills
- *Fully* automated machines *must* handle *all* circumstances
  - Planned reactions to both failures and things happening in their environment need to be carefully thought through
  - Responding to multiple failures is very hard (e.g., QA 32 link)
  - Machines will need to be modified as cases are identified

How people get it right

- Learn from history
  - *Read accident reports* (link)
  - Field feedback and monitoring, e.g.:
    - Data logging from engine controllers (FADECs) and other systems
    - NASA's *Aviation Safety Reporting System* (link)
- 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

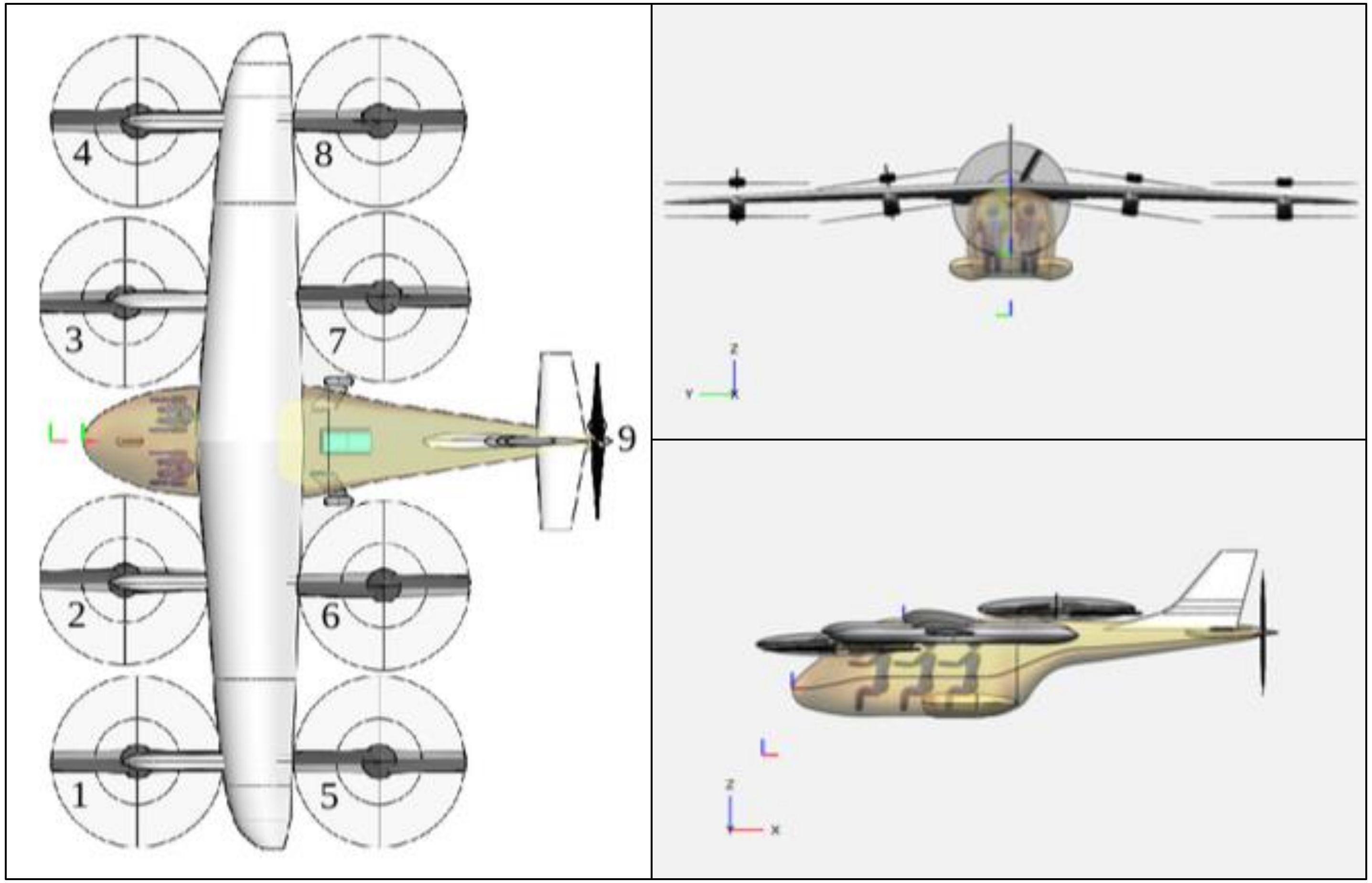
Preliminary hazard assessment

- We did partial, preliminary FHA & STPA on a *hypothetical* craft
  - Environment
    - Large city with tall buildings, small UAS, transport aircraft, birds, etc.
    - 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



Aircraft designs are progressing

- NASA researchers are exploring many designs, including *lift + cruise* (link)
  - 8 RPM-controlled lifting rotors + pusher propeller
  - Ailerons, elevator, and rudder
  - Airbrakes are being considered



Loss of propulsion

- *Loss of propulsion happens*: engines fail, fuel freezes, etc.
  - Fixed-wing aircraft *glide* to a *dead-stick landing*
  - Rotorcraft *autorotate*
- Sooner or later, an eVTOL will lose propulsion:
  - Batteries overheat and/or catch fire
  - Motors and motor controllers fail
  - Computers and communication links 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?
  - Worst case design: lose attitude control *and* lift
    - And what if the vertiport is atop a tall building?
- Potential solutions:
  - ~~Can't autorotate with small rotors~~
  - Multiple rotors + adaptive control algorithms
  - Variable pitch plus cross-shafting
  - Architectural redundancy

Possible weak point: transition

- Details depend on the transition mechanism!
- Some transition plans skirt the limits of both flight regimes:
  - Rotors provide less effective control at higher speeds
  - Elevators/ailerons less effective at lower speeds
  - Stall speeds impose limits
  - If the gap between limits is small, there is not much room for error …
- What if transition is incomplete or asymmetric?
- What if propulsion or control fails during transition?

Unified control

- Different control effectors used in vertical vs. horizontal flight
- *Unified control* helps enable *simplified vehicle operation*: controls mean one thing and the computer actuates by mode
- What happens when effectors fail?
  - Might occur suddenly, e.g., unannunciated failure of unused effector
  - Computer compensation hides feedback about limits of control
- What happens when the computer fails?
  - *Could* provide robust direct control functions to pilots
    - Can any humans hand-fly the aircraft? Can the intended humans do so?
    - What about *mode confusion*?

Verifying new technologies

- In transport category aircraft, avionics are built to *DO-178C* (link)
  - FAA recognizes DO-178C as a means of satisfying the regulations (link)
  - DO-178C (2011) updates DO-178B (1992)
  - Relies on testing, analysis, & traceability w.r.t. specified requirements
  - 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)
- *Requirements-centric standards such as DO-178C might be ill-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* (link)
  - *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?

- After ID-ing hazards, how do we gauge risk & make trade-offs?
  - E.g., which is safer: a tilt rotor that can dead-stick or a multirotor?
- Quantitative risk studies
- Simulation might be heavily used:
  - … to assess pilot/operator capabilities & responses
  - … to explore controllability & stability
  - … to assess planned air traffic management schemes
- But risk assumptions & simulations might be unrealistic
  - Test flights & field feedback are essential

Conclusion

- Advanced air mobility (AAM) 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

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

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 reestablishing awareness and choosing the correct response
- How accurate & fast is correction from air control system?
- How well controlled will people & kit be at vertiport pads?

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
- Could more precise computer control pack airspace tighter?
- What happens when computers fail?
  - Many eVTOL designs require computer control for stability
  - Can pilots fly precisely enough with simplified basic controls?
- What happens when communications fail?
  - Imagine a jammer is deployed in the area …