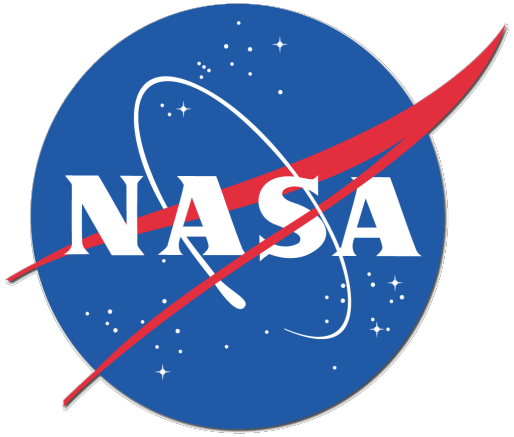
Implementing the right thing in future aviation systems



Dr. Mallory S. Graydon

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

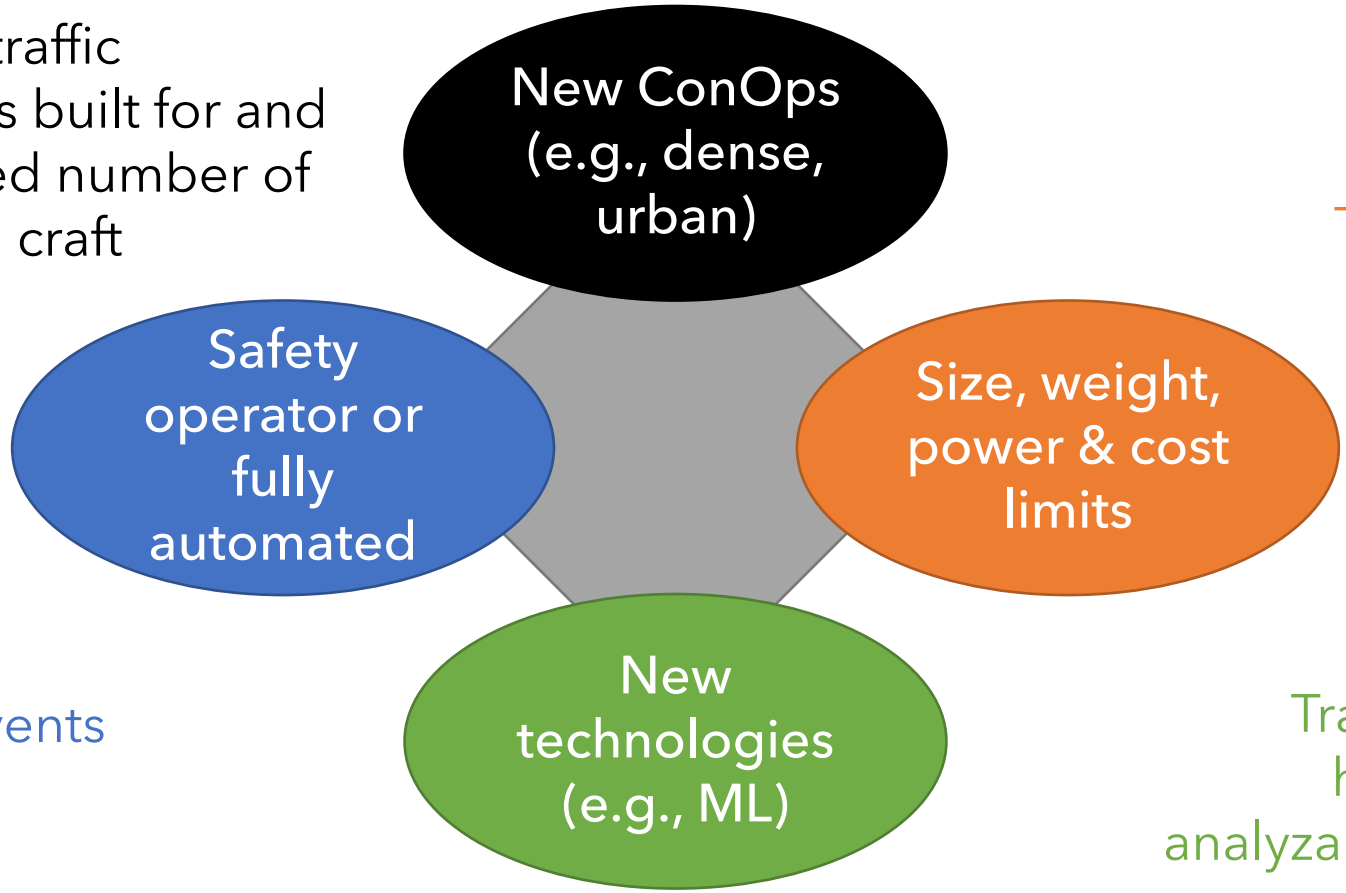
Safety Critical Avionics Systems Branch

NASA Langley Research Center, Hampton, Virginia, USA

Dependability, novelty, and frugality

Traditional air traffic management is built for and around a limited 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)
  - BA 9 (1994): Volcanic ash disables all four engines, crew manages a descent, restart, and landing (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~~⇧Machines adapt?

- Design philosophy on human–machine disagreements varies, but aircraft often turn to pilots when systems fail
- Suppose we have *no pilot at all*:
  - Human staff takes up seats and gets paid rather than pays
- *Fully* automated machines *must* handle *all* circumstances
  - It is difficult enough to diagnose foreseen single failures
    - E.g., it took the QA 32 crew an hour to work through the EICAS failure checklists resulting from one engine failure (link)
  - Multiple failures are exponentially harder
  - Machines will need to be modified as cases are identified

Human ~~pilots~~⇧safety operators adapt?

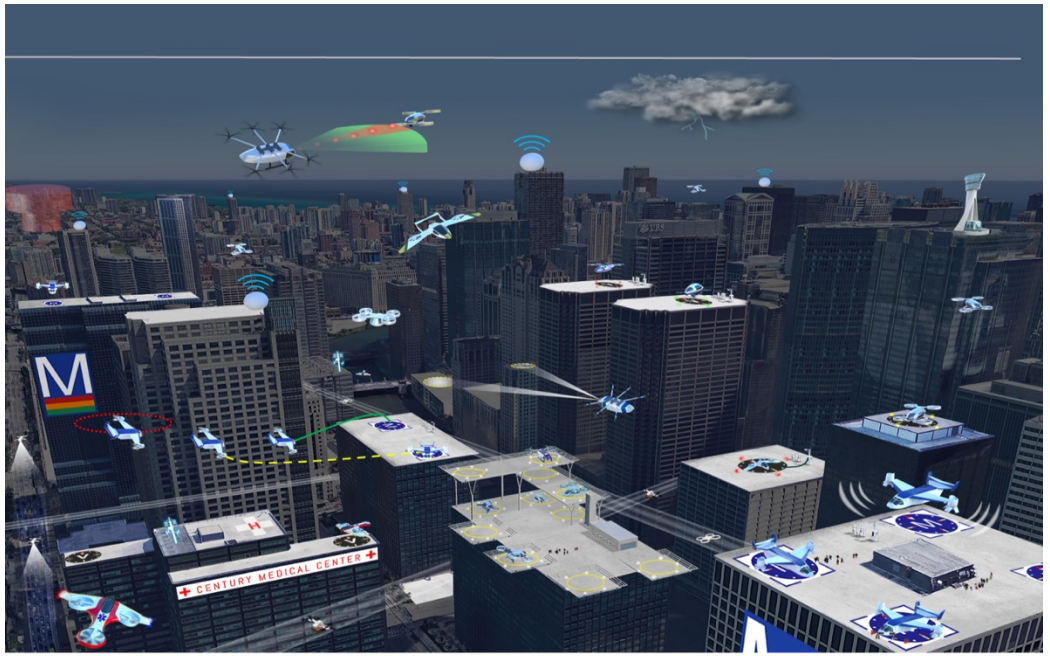
- Design philosophy on human–machine disagreements varies, but aircraft often turn to pilots when systems fail
- Suppose we have a *safety operator* rather than a pilot
  - (*Simplified vehicle operations* might obviate traditional piloting skill.)
  - A human might be able to recognize dangers the machine doesn't
  - If they have no traditional piloting skills, how will they intervene?
    - A big red 'land now' button still requires working computers, etc.
    - How common are safe landing spaces in urban areas?
    - How good will automation be at finding them? (link)
  - Can the craft be hand-flown at all?
  - How good will operators' *airmanship* be?

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

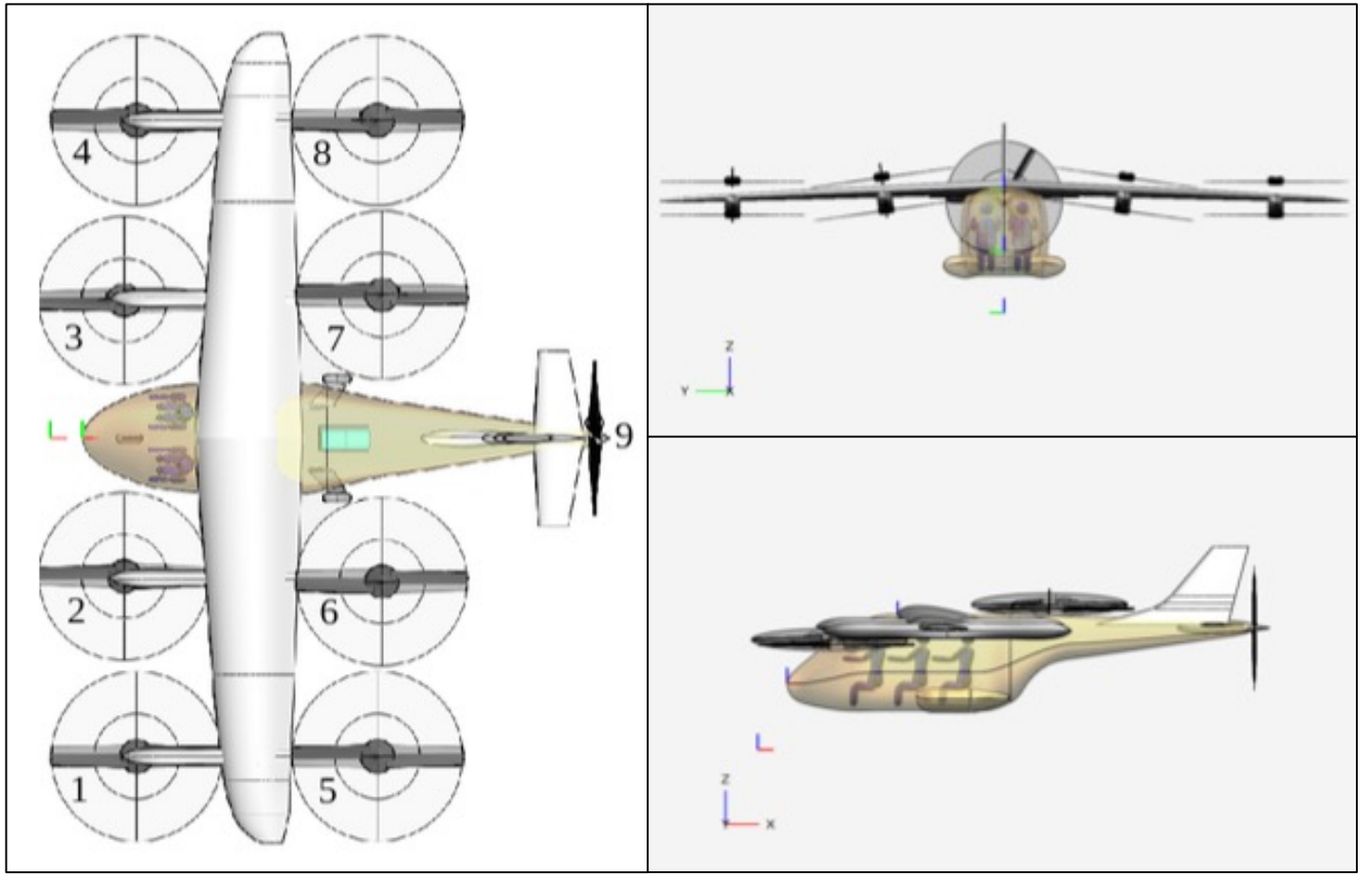
Preliminary hazard assessment

- 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



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?

Crew mitigations for loss of power

- What can the crew do if power is lost in wingborne cruise?
  - The traditional answer: dead-stick a landing
    - *Reversionary control schemes* if computers fail
    - Backup power
  - Can we find *suitable emergency landing sites* in urban areas?
    - If a computer is to identify them, can it?
    - Do they even exist in sufficient numbers?
  - Will the craft maintain flight control when power is lost?
    - Will there be redundant power to flight control surfaces?
    - Are the flight control surfaces sufficient when the rotors are inoperative?
    - Are any necessary computers sufficiently reliable?
  - Does the pilot/operator have sufficient skill?

Crew mitigations for loss of power

- 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 mitigations:
  - ~~Can't autorotate with small rotors~~
  - Variable pitch plus cross-shafting
  - Multiple rotors + adaptive control algorithms
  - Architectural redundancy

What if a sensor or computer fails?

- Fixed-wing civil aircraft are *aerodynamically stable* by design
- Multi-rotor aircraft are stabilized by sensors and computers
  - Hand-flying is probably not an option
- *Computers and sensors fail*
- Redundancy helps, but it's expensive and imperfect
  - *Managing failed components* in software is tricky (e.g., Qantas 72 link)
  - Even redundant sensors simultaneously fail (e.g., MA 134 link)
- Is the remaining risk acceptable?
  - We accept some risk in light airplanes and rotorcraft …

Building robust avionics

- Software for transport category aircraft is built to *DO-178C* (link)
  - FAA recognizes DO-178C as a means of satisfying the regulations (link)
  - Relies on testing, analysis, traceability, change control, etc.
  - Seems to work: in accidents, software usually worked as designed
  - ML approaches might be ill-suited to DO-178C-style assurance
- Computers on transport category aircraft are highly redundant
  - *Weird stuff happens* (link)
  - *Byzantine-fault tolerance* is considered necessary in some systems
  - In space, we even do *radiation hardening*!
- This robustness adds expense, size, weight, power, and cost

How will we evaluate risks?

- After IDing 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

Above all, be humble

- Aviation regulations are said to be written in blood
- One lesson of the past: risk lurks in novelty
- Aviation has a strong, transparent safety culture
  - Industry understands the need for a safety reputation
  - Accept the leak of engineering "secrets" in incident/accident reports
  - Don't let blame get in the way of understanding what happened
- Some general advice
  - Don't build things we don't know how to validate
  - Don't claim credit for engineering techniques of unknown efficacy
  - Don't take on too much novelty at once

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
  - Build an open, robust, humble safety culture

Backup slides

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 …

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, change control, etc.
  - 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 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?