Challenges in Safe Remote Operations: Lessons from Aerospace

Alwyn E. Goodloe
a.goodloe@nasa.gov

Natasha Neogi
natasha.a.neogi@nasa.gov

Lara Humphrey
laura.r.humphrey@nasa.gov

NASA Langley Research Center

Introduction

- I will be discussing several issues that arise in remote operations
- Remote operation has a long history at NASA
  - Not always in a safety critical setting
- The presentation is intended to elicit discussion so feel free to interrupt

Flavors of Remote Operation

- There is a range of possible operational paradigms for remote operations. For example:
  1. Remote assistance, e.g., by a service provider to provide support and assistance
  2. Remote management, e.g., to allow a remote controller to assist when a systems requires authority to progress in its mission
  3. Remote control e.g., could extend from limited system guidance (of high-level functions) to full remote control of system (with associated delays)

NASA's History with Remote Operations

- Aeronautics directorate has been flying uninhabited aerial systems (UAS) for many years
  - Significant restrictions (e.g., pilot line of sight, restricted test ranges, etc.)
- Space exploration has decades of experience at real remote operation
  - Safety is a minimal concern

Characteristics

- A system is monitored and controlled by operators located at such a distance that they cannot physically intervene to correct issues that may arise
- Reliable communication between operator and system is critical
- The operator needs to maintain situational awareness
  - Systems sensors
  - External sensors (ground-based RADAR)
  - Line of sight

Hazards and Threats

- Hazard and threat analysis are the first steps on the road to safe and secure systems
  - Often ignored by those new to safety-critical domains
- Critical components will break and do so in malicious ways
  - Byzantine faults vs crash faults
- Communication will fail
  - How are you going to handle loss of communication and control
- There will be malicious actors who will attack your system
  - NASA doesn’t do research in security
  - The expertise resides in DoD, Homeland Security, etc.

Space Exploration I

- NASA remotely operates deep space probes, orbiters, and rovers across the solar system
- Not safety critical
- Missions last years or even decades
- Little or no redundancy
- Limited computational resources and no cryptography

Space Exploration II

- Communication is irregular, as NASA loses contact with space probes on a regular basis, so it is built into the operations
  - Automation compensates for temporary loss of comms
  - Permanent loss of communication -> loss of mission
- Pace of operations is typically very deliberate (slow)
  - Rovers may move a few meters a day
- There is a quiescent mode to which the system can default
- Uploading patches is a regular occurrence
- Working around HW failures
  - Using digital twins for decades
- Rebooting is a common solution
- These solutions may not translate to earthbound setting easily

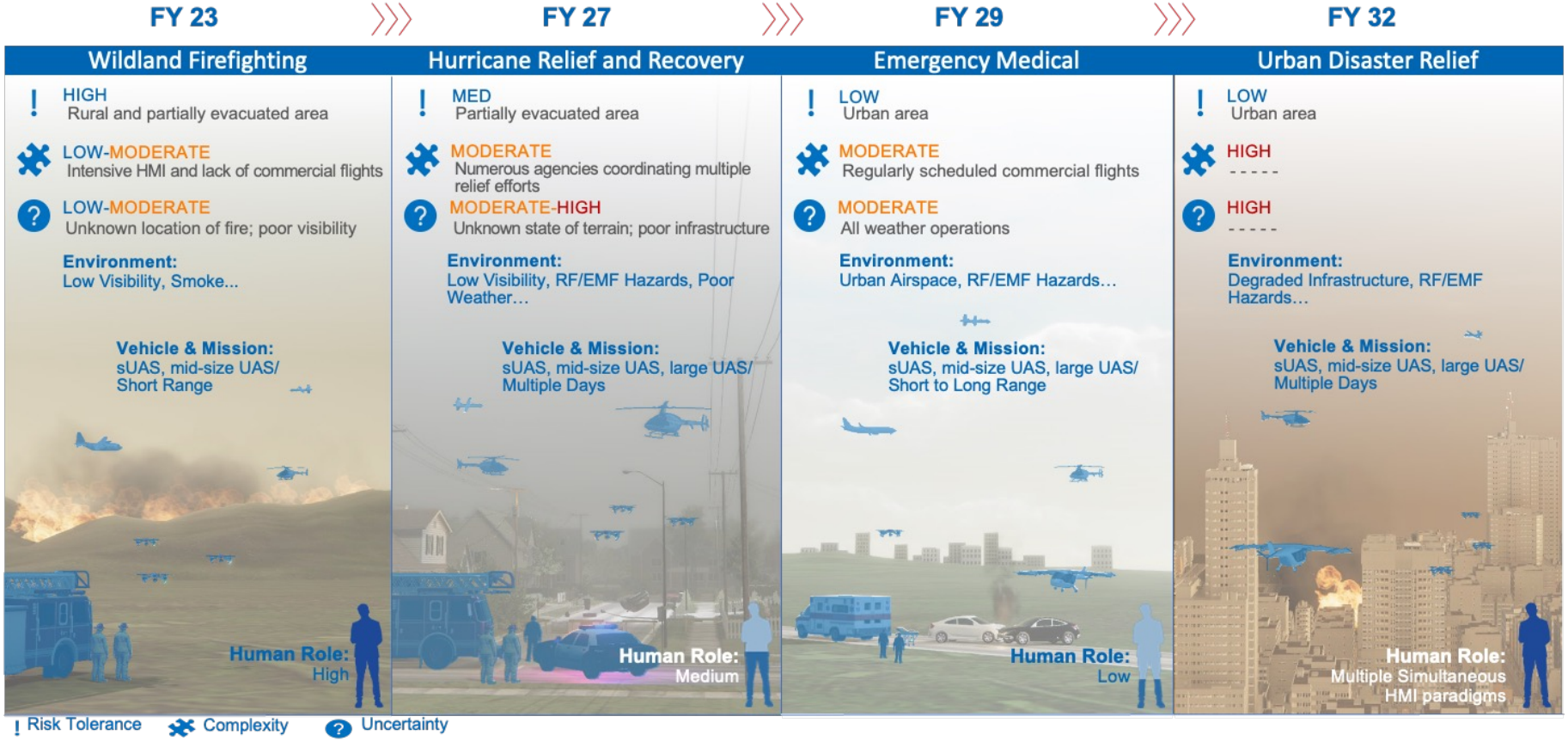
Humans in Space

- Space is a very unforgiving environment in which to operate
- Mixed crew and remote operations
  - Astronauts are often part of the “remote operations” by doing prescribed tasks
- Remote operations are planned and analyzed on ground
  - JSC has extensive simulation facilities
- Astronauts can compensate for lost communication
- NASA’s planned Lunar Gateway will have long periods when it is unoccupied, so it will be remotely operated during those times
  - A lot of automation is planned, and details are being worked out
- Robonaut program is an example of addressing challenges of robotic systems operating in close proximity to humans in space
  - The robotic limbs are engineered not to damage space suits

Remote UAS Operation

- Pose a danger to people and property on the ground and other vehicles in the air
- Flight-critical software needs to be certified
  - NASA, FAA, DOD
- Restrictions on operations
- Operational Design Domain (ODD) less complex than self-driving cars
- Even mid-size UAS typically lack hardened/redundant systems
- Communications with the ground and GPS are both unreliable
- Securing the system is often an afterthought for non-DoD operation
- New technical challenge focusing on developing new ConOps
  - Disaster relief

Example: Disaster-Oriented UAS Remote Operations



Criticality Creep

- Criticality creep occurs when high-criticality functions are misidentified and treated like low criticality functions
  - Sometimes a function starts as a low-criticality function but becomes high-criticality when the scope or operation of the system changes through the life cycle
  - Often there is a cost incentive
- What decisions/computation must be done on vehicle and what can be done on a ground station or in the cloud?
- We are increasingly seeing potential critical functions being proposed to be done in the cloud
- Systems and safety engineers need to be on guard against this

Robust Systems Needed

- Remote operations is often predicated on a mental model “operator sends command, command received, command executed”
- Operators expect to trust the data coming from the uninhabited aerial vehicle (UAV)
- Operators not in line of sight of UAV and lacking external means of observing the system such as RADAR much trust the messages
- Remotely operated systems are going to have to be constructed to be fault-tolerant
- Cost of design and assurance may outweigh the cost savings of remote operations

Secure Operations

- Intercepting and hijacking unsecured UAS are well within the means of even relatively unsophisticated attackers
- DARPA HACMS illustrated how to secure embedded devices (UAS, robotics, cars) against many common attacks
- That sort of security remains rare for a number of reasons
  - Workforce lacks skills and knowledge
  - Embedded system hardware constraints
  - The cost is viewed as prohibitive
    - Often the instinct is to invest in 'hot topics' (e.g., AI, Large Language Models, etc.) which may not be useful to the operation

Unreliable Comms for UAS

- Procedures -- call the FAA tell them you have a rogue UAS
- Make full autonomous operation the fallback
- Geofence – guarantee that vehicle will stay in a defined area
  - NASA's highly assured, rugged SAFEGUARD system
- Automated collision avoidance
  - Avoid touching paint
- Automated self-separation NASA DAIDALUS
- Task and path planning
- ICAROUS – NASA's framework for enabling autonomous operations
- Automation to land vehicle in predefined location(s) if comms are lost

Things to consider when opting for remote operations

- **The function allocation should focus on safety:** A structured methodology should be used to allocate functions between onboard and offboard (i.e., ground/cloud-based) to improve safety and increase resilience.
- **Provide highly reliable and secure communications:** Both safety and security must be considered in the communication link requirements.
- **Provide rich information:** The information sent must be rich and in real time, and available to all agents to encourage a practice for double-checking.
- **Establish fault tolerance and redundancy in technical systems and/or human resources, as well as warnings:** If redundancy is missing in safety critical elements, safety will be compromised. Establish a culture that encourages use of human redundancy when applicable for safety (e.g., 2 pilots in cockpit).
- **Consider the existence of a 'quiescent/safe state' and the pace of the operations when designing safety into the system:** The ability to control, mitigate, and eliminate hazards will depend on whether operations can be interrupted with no safety- or mission-critical effects.

Questions?

Contact Information:
Alwyn E. Goodloe
+1-757-864-5064
a.goodloe@nasa.gov