Testing a Run-Time Assurance Framework Coupled with Integrated Risk Mitigation Capabilities for Autonomous Urban UAS Flights

Ersin Ancel, Andrew Moore, Steven Young,
Evan Dill, Cuong (Patrick) Quach, and Kyle Smalling
NASA's Langley Research Center

Safety Session - DASC 2024
October 1, 2024

System-Wide Safety

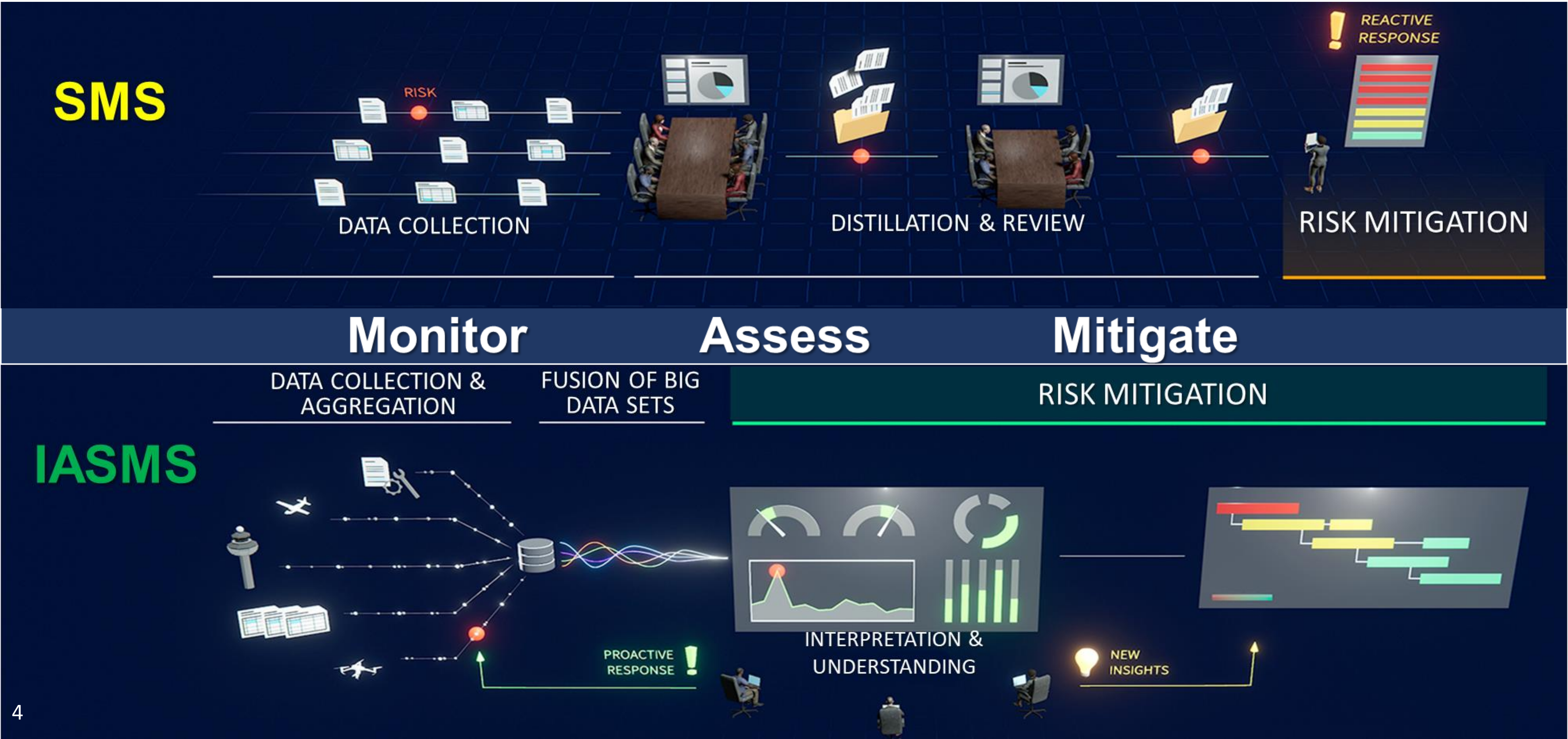
Outline

- Background and In-time Aviation Safety Management System (IASMS)
- Flight System Software Architecture
- Flight Tests
  - Aircraft and Range
  - Phase I and Phase II Testing
  - Flight 097 Results
  - Flight 115 Results
- Next Steps & Concluding Remarks

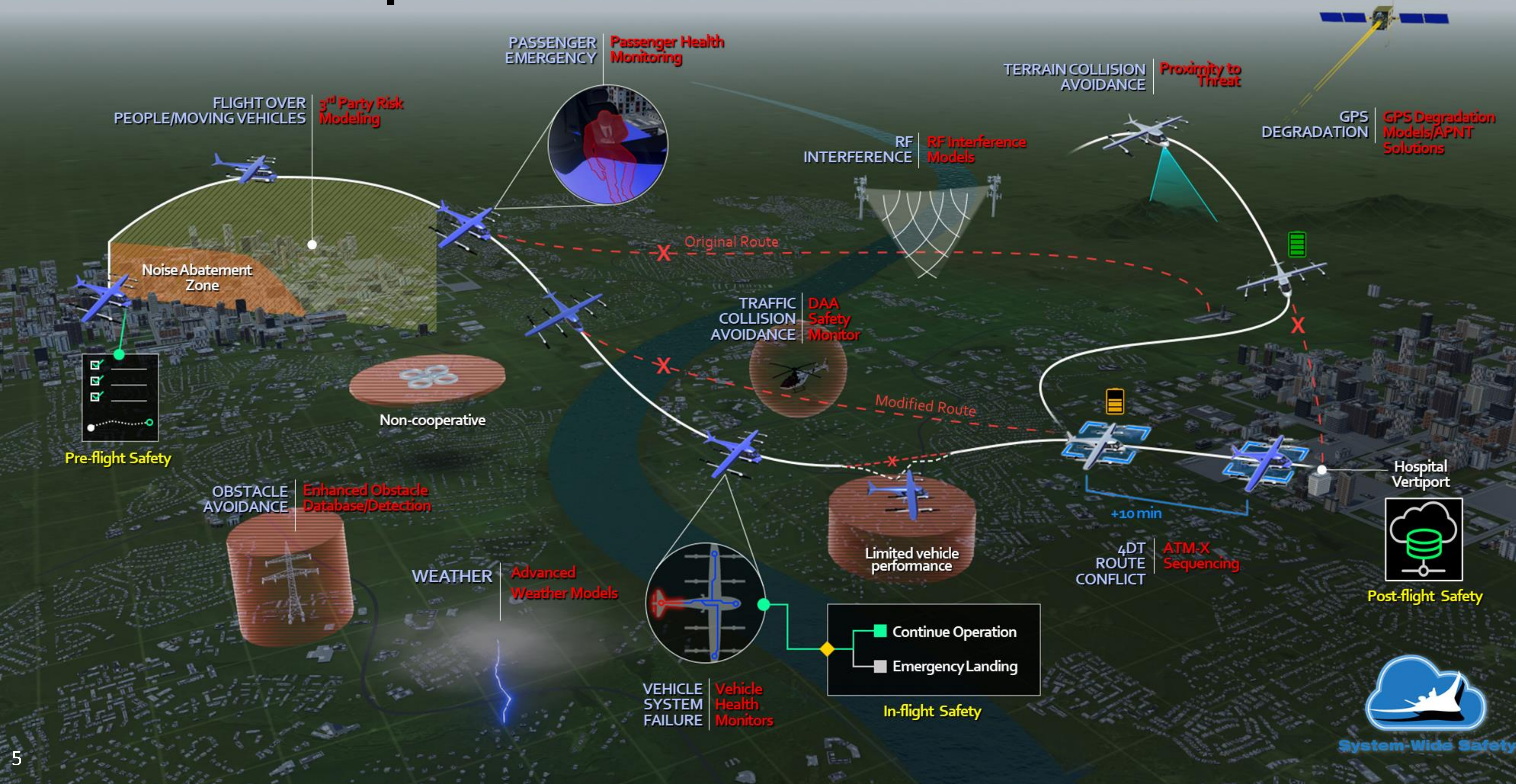
Background and IASMS

- Funded by the System-Wide Safety (SWS) Project
- Informed by the National Academies and NASA Strategic Implementation Plan (SIP)
- Comprised of high-level capabilities (Monitor, Assess, and Mitigate) spanning operational phases (pre-flight, in-flight, and post-flight)
- Decomposed into lower-level Services, Functions, Capabilities (SFCs), residing on board, on the ground, and/or cloud
- Improved real-time detection and automated mitigation of domain-specific hazards by developing predictive capabilities

IASMS Concept of Operations



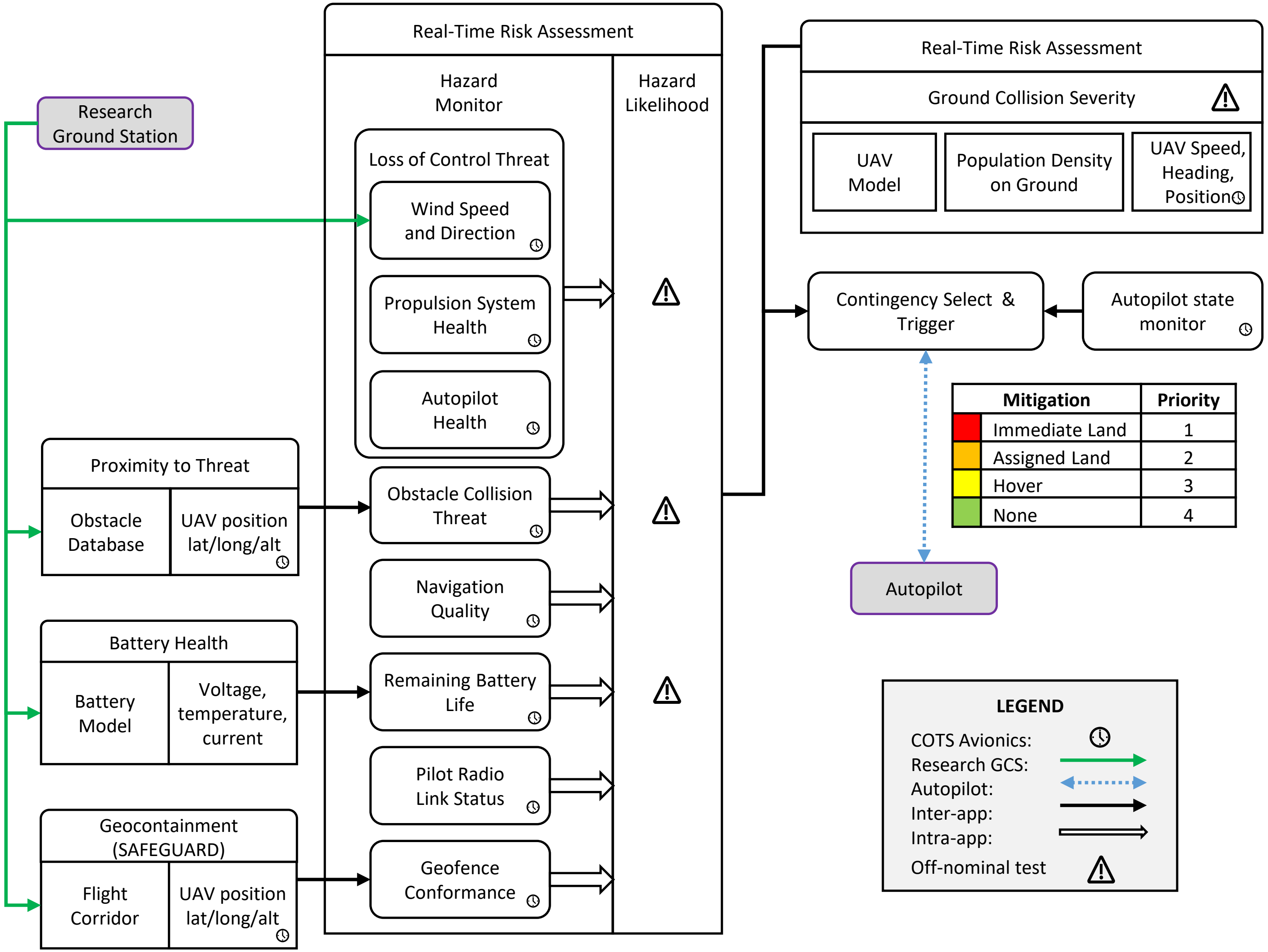
IASMS Implementation



Flight System Software Architecture

- SFCs with Run-time Assurance (RTA) approaches
  - NASA Class C and Class D
  - Execution independent of the unassured autopilot
- In-time risk management with autopilot monitoring, proximity monitoring, and conformance monitoring functions
- Hazards
  - Navigation loss
  - Command & control link loss
  - Unsafe proximity to obstacles
  - Geocontainment
  - Aircraft loss of control
    - Propulsion system
    - Power system
    - Autopilot malfunction
    - Wind presence
- Ground Collision Severity

Onboard Software Architecture



Mitigation	Priority
Immediate Land	1
Assigned Land	2
Hover	3
None	4

LEGEND

COTS Avionics:
Research GCS:
Autopilot:
Inter-app:
Intra-app:
Off-nominal test

Mitigated Actions for Tracked Hazards

- Mitigation actions include Land, Assigned Land (Return-to-Launch), Hover, None
- Based on hazard thresholds, and their priority, research hardware changes the autopilot mode
  - Autopilot is already in Auto mode
  - CST is engaged/enabled

Hazard Detected	Mitigation		Priority
Navigation Loss		Immediate Land	1
Battery Loss		Immediate Land	1
Command/Control Link Loss		Assigned Land	2
Proximity to Obstacle		Hover	3
Loss of Control		See Below	

	Loss of Control Severity			
Loss of Control Likelihood	Minimal	Minor	Major	Catastrophic
Frequent				
Probable				
Remote				
Improbable				

Key					
	Immediate Land		Assigned Land		None

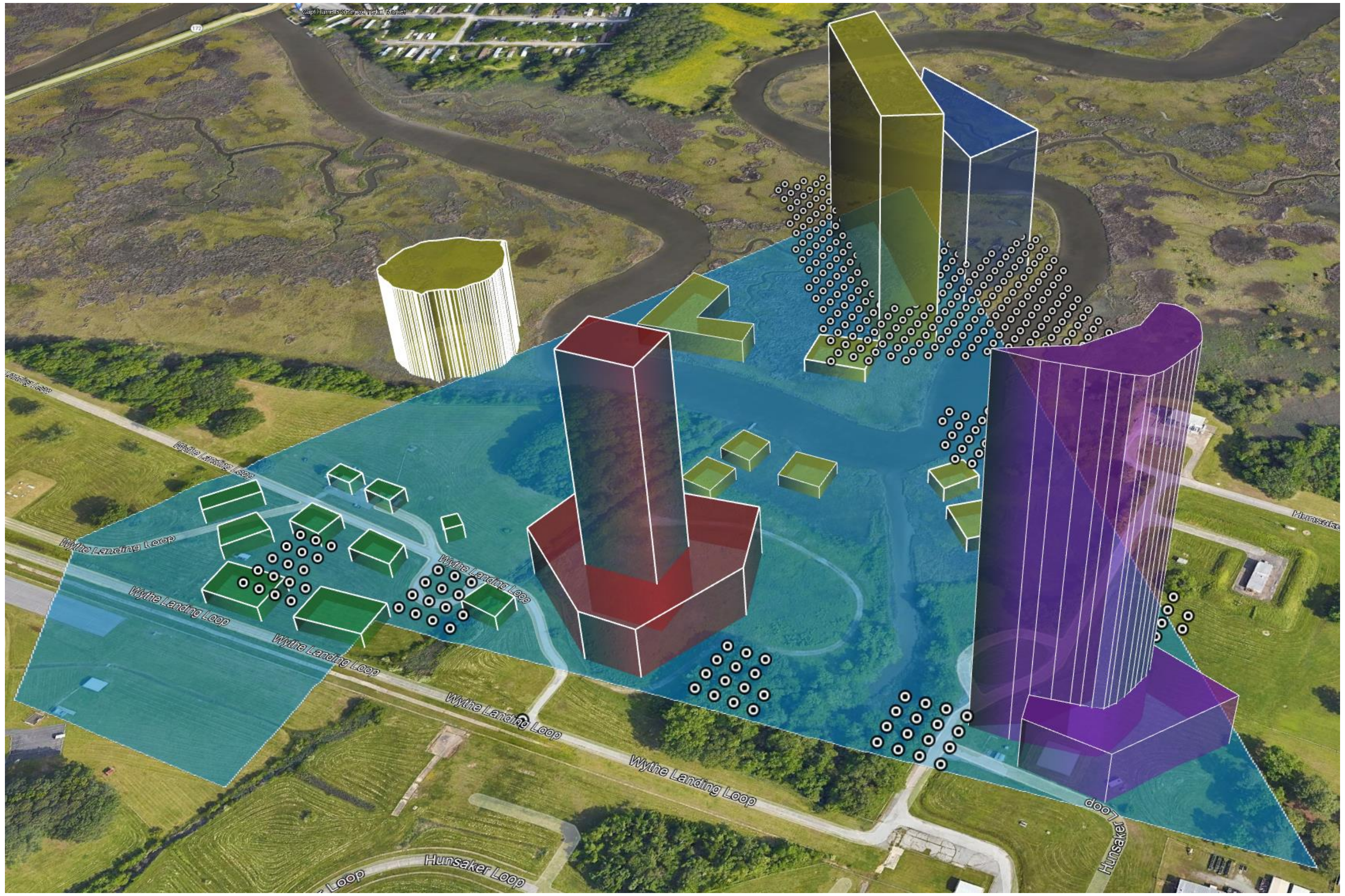
System-Wide Safety

Aircraft

- Modified Tarot T18 Octocopter
  - 2x Intel Next Unit Computing (NUC) nodes
  - Various research sensors, switches, upgraded speed controllers, radios, and associated electronics supporting the research payload
  - SAFEGUARD module
  - Radio-controlled cut-off relays to isolate the autopilot per NASA Class C Software requirements

Flight Range and Path

- NASA's City Environment Range Testing for Autonomous Integrated Navigation (CERTAIN) range
- Virtual buildings, simulated population activity in varying densities, and geofence
- Departure and arrival legs of a longer air taxi operation with ~600m legs , up to 104m altitude



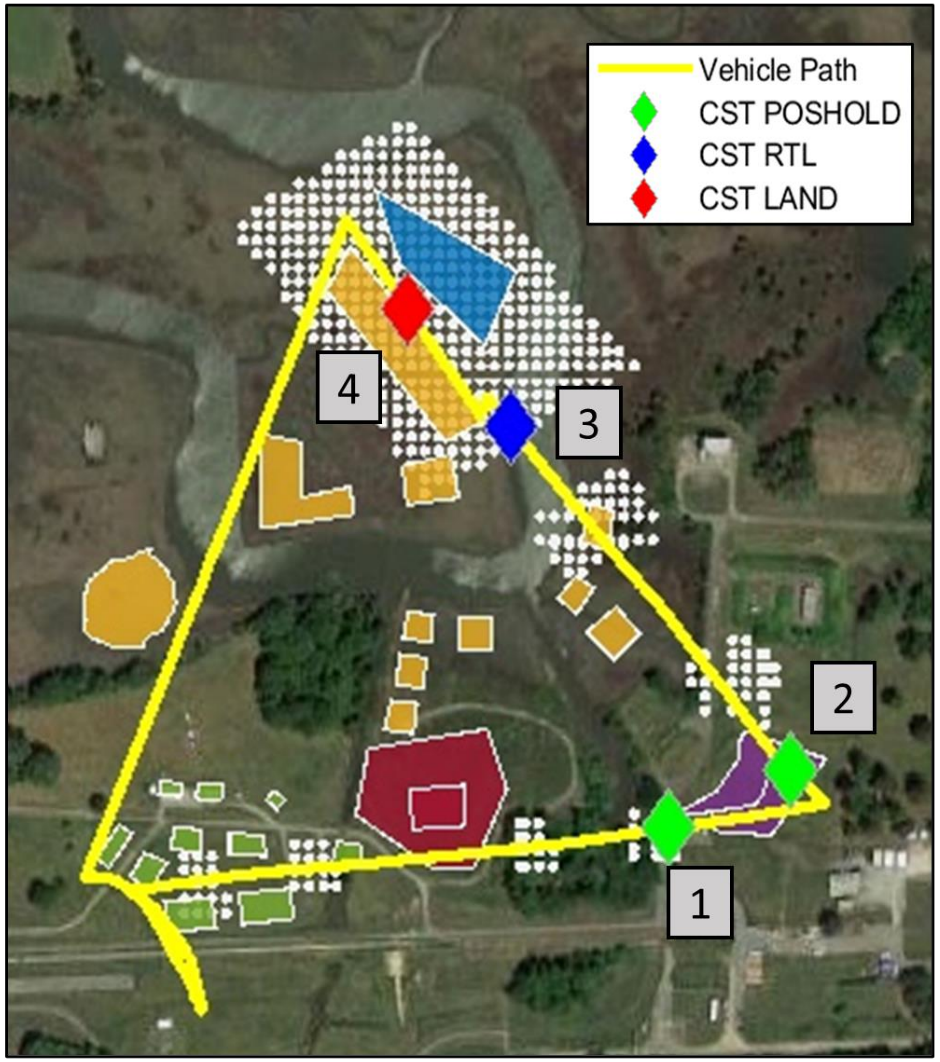
System-Wide Safety

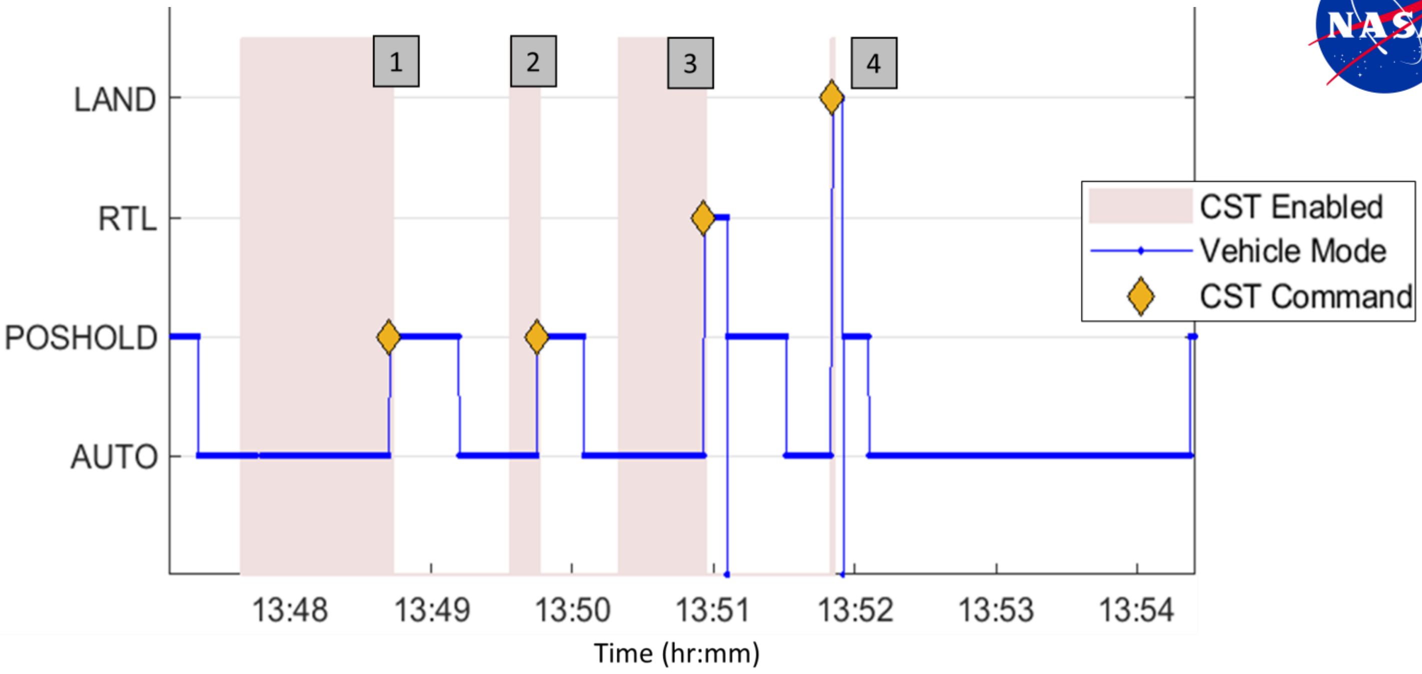
Sample Flight Test Results

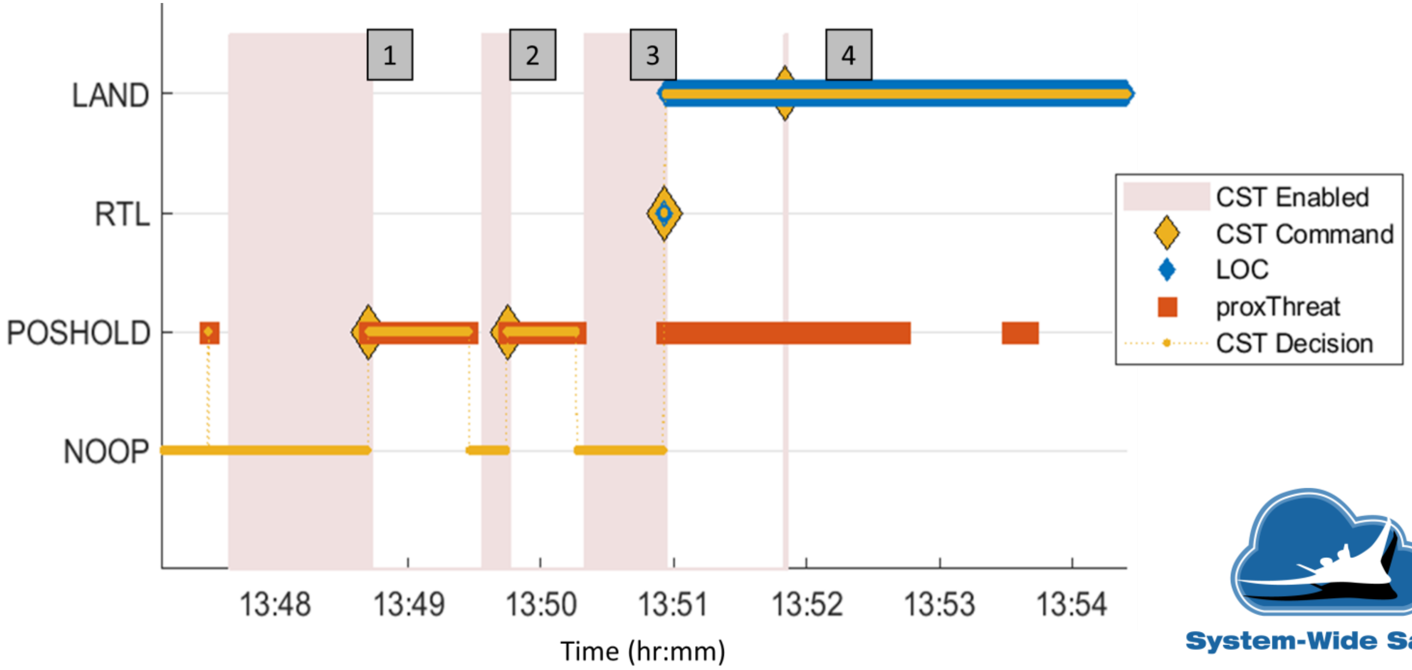
- Phase I Testing
  - Experiments conducted in the secondary computing system with no control over the autopilot mitigation actions
  - 61 Flights between August 2021 and July 2022*
- Phase II Testing
  - Experiments conducted in the primary NUC computer capable of controlling the vehicle autopilot
  - 54 flights between July 2022 and October 2023
- Flight 097
- Flight 115

*Flight Testing In-Time Safety Assurance Technologies for UAS Operations - AIAA 2022-3458
Design and Testing of an Approach to Automated In-Flight Safety Risk Management for sUAS Operations - AIAA 2022-3459

F097 Overview

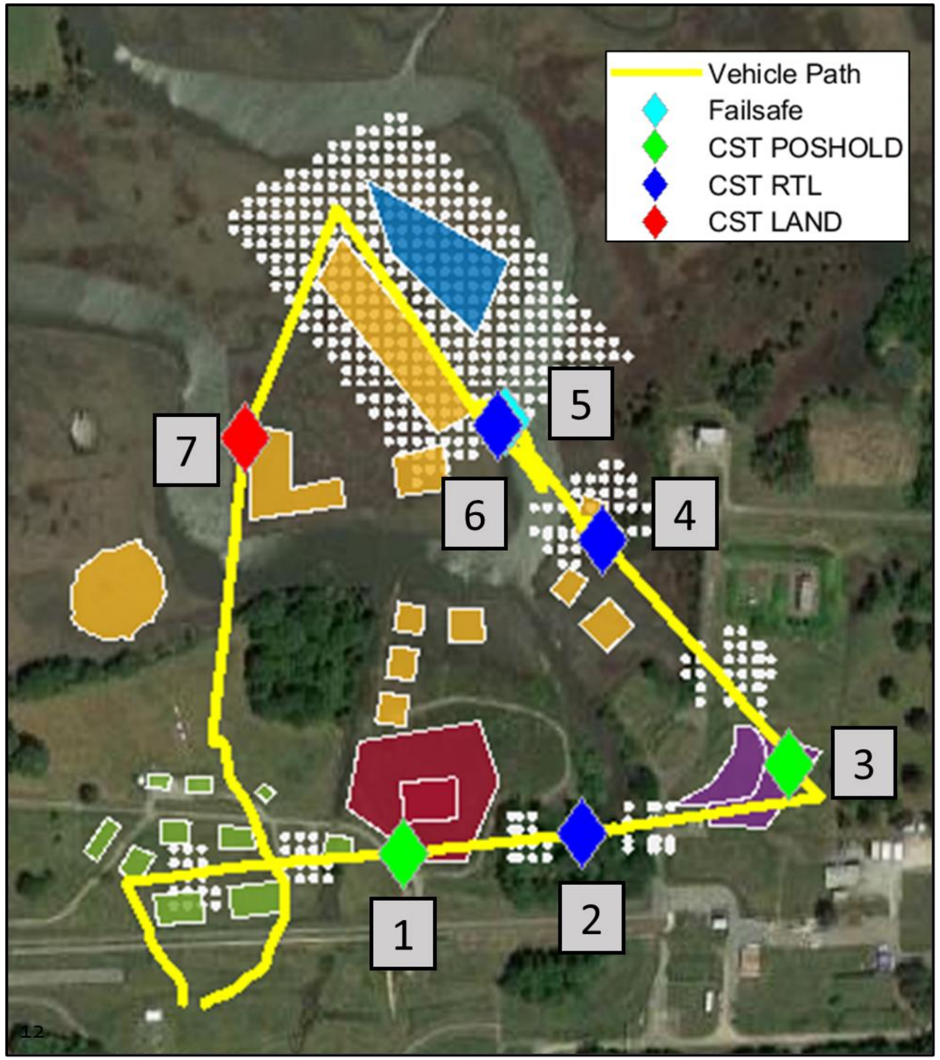


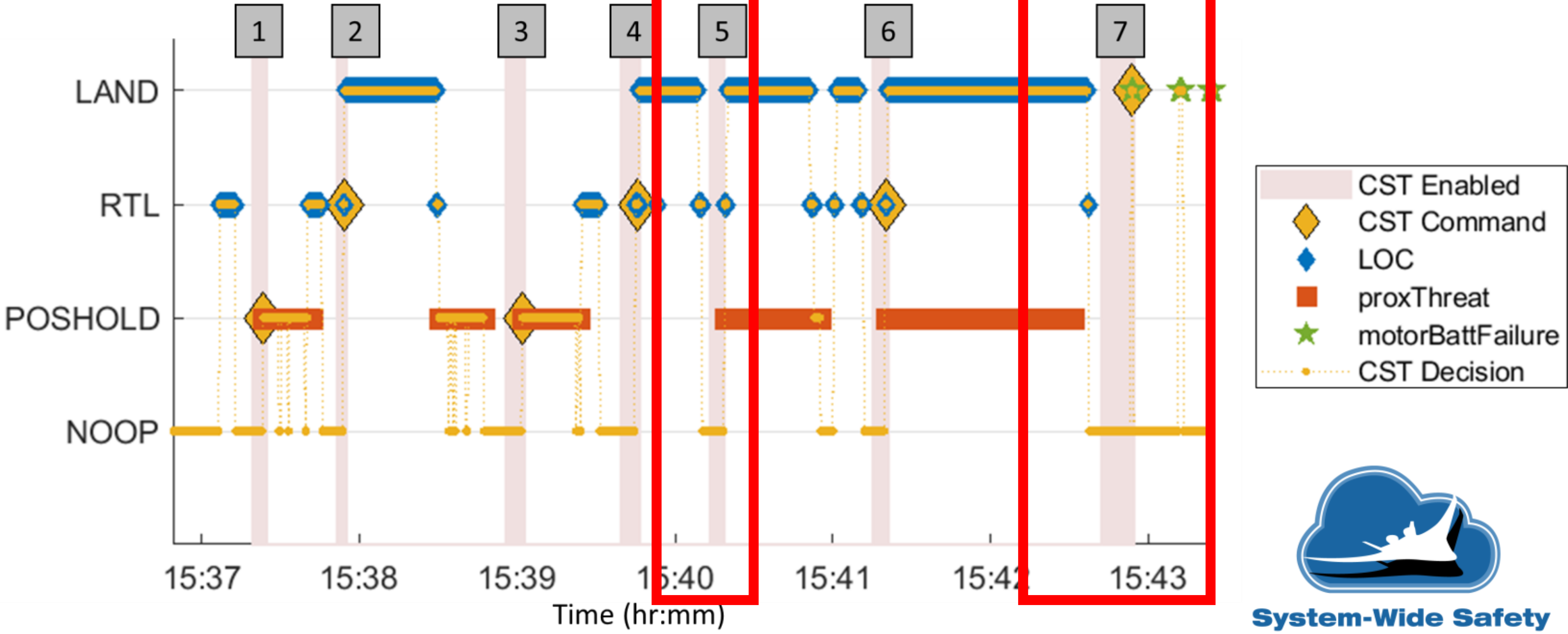




System-Wide Safety

F115 Overview





System-Wide Safety

Next Steps & Concluding Remarks

- Extensive development and flight testing of more than 20 airborne, ground, and cloud-based SFCs were used to evaluate the IASMS concept and inform the capabilities of future highly-autonomous aircraft
- Second phase of an automated decision-making capability was demonstrated in flight using a virtual city and softcoded threshold values to simulate failures and observe automated decision making
- Flight testing including automated decision making with self-separating aircraft (Detect and Avoid – DAA) is currently underway
- Parallel subproject within SWS will demonstrate these capabilities in increasingly complex flight scenarios/use cases

Acknowledgments

The work presented here was supported by the System-Wide Safety project in NASA's Aeronautics Research Mission Directorate's Airspace Operations and Safety Program (AOSP).

Thank you!

Questions?

System-Wide Safety