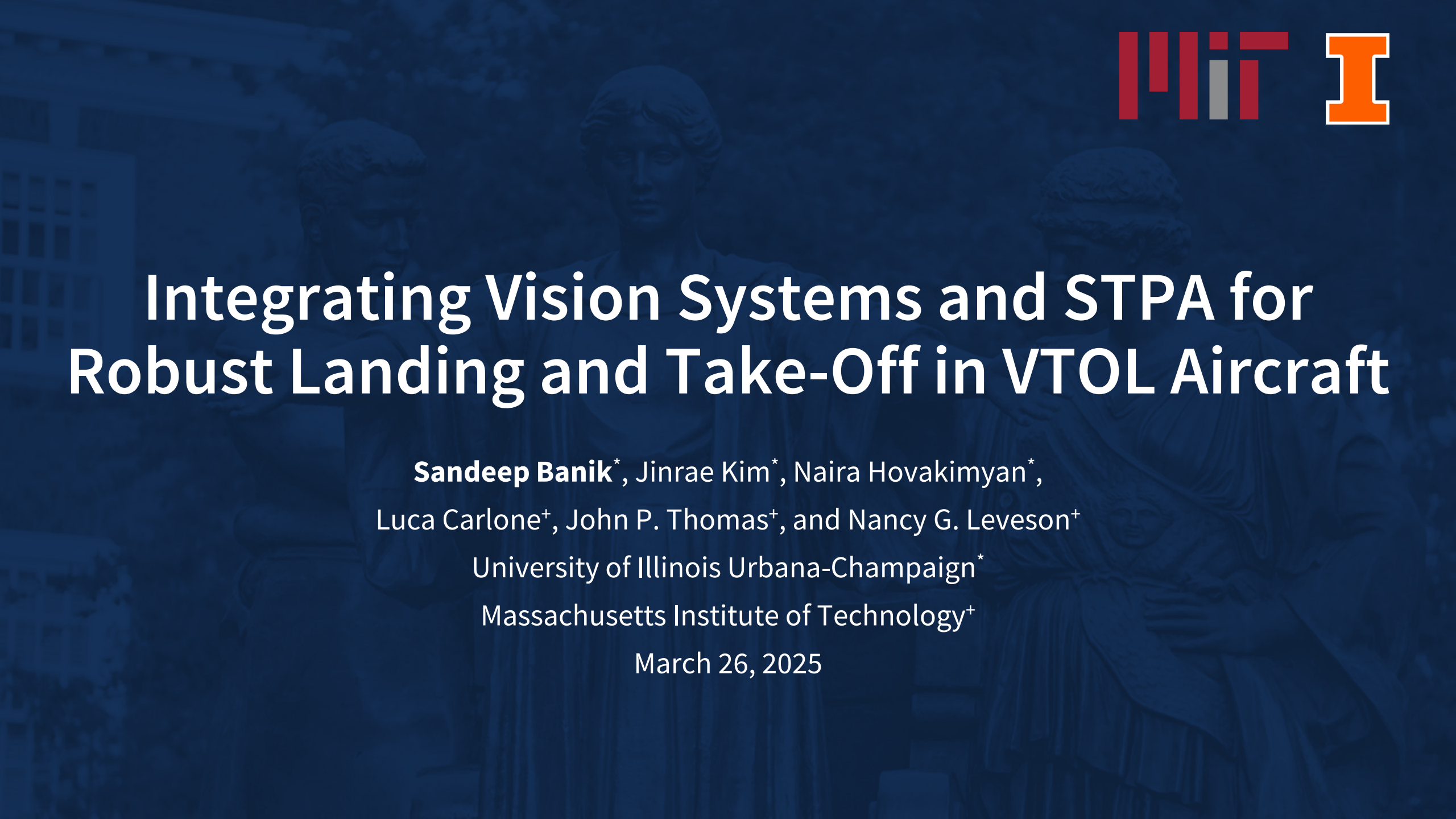
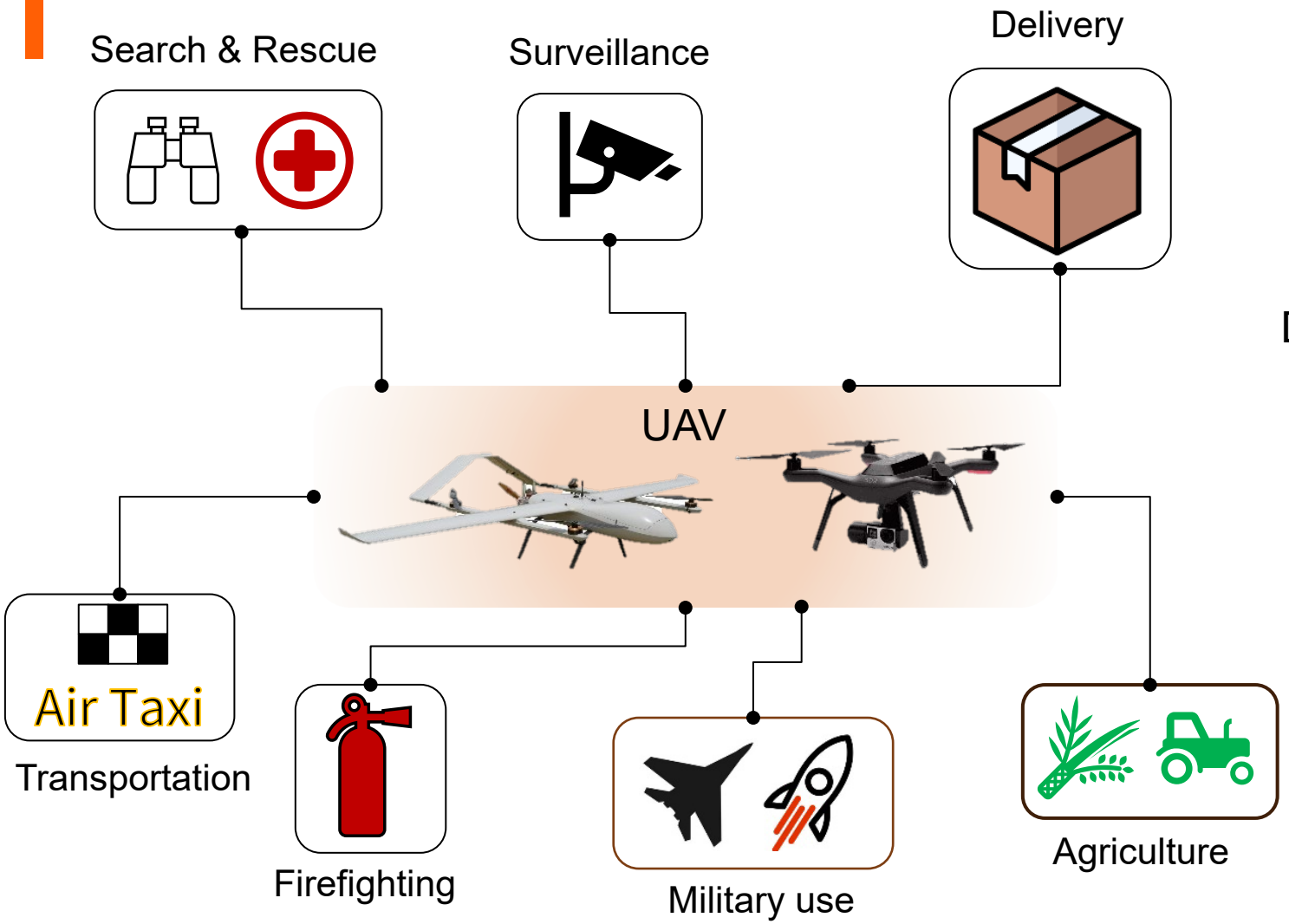


Integrating Vision Systems and STPA for Robust Landing and Take-Off in VTOL Aircraft

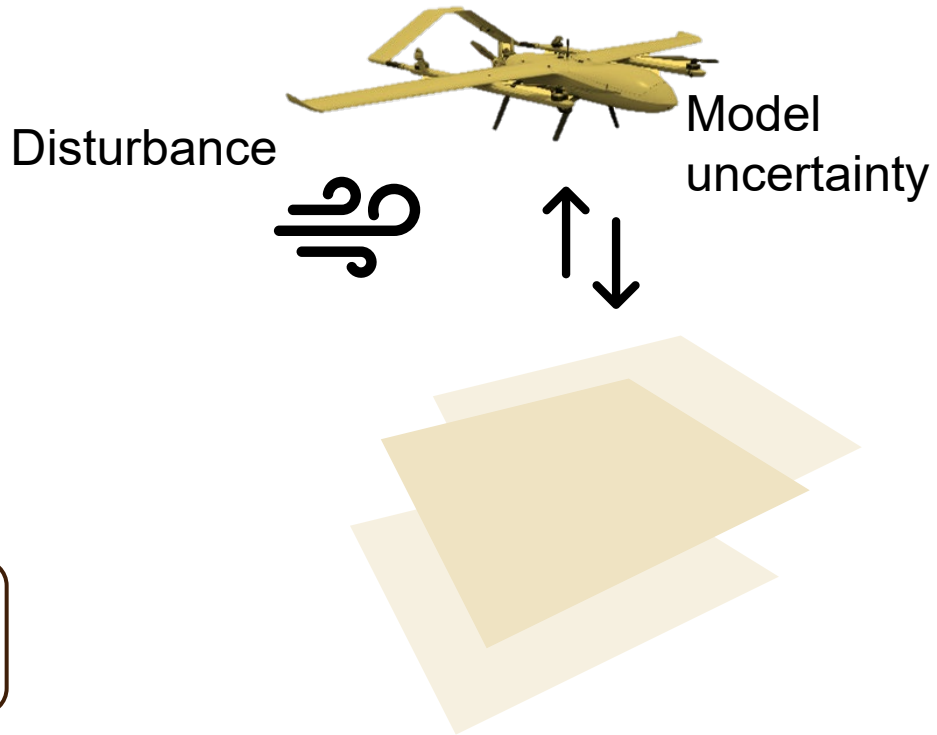
Sandeep Banik[*], Jinrae Kim[*], Naira Hovakimyan[*],
Luca Carlone[+], John P. Thomas[+], and Nancy G. Leveson[+]
University of Illinois Urbana-Champaign[*]
Massachusetts Institute of Technology[+]

March 26, 2025

Introduction



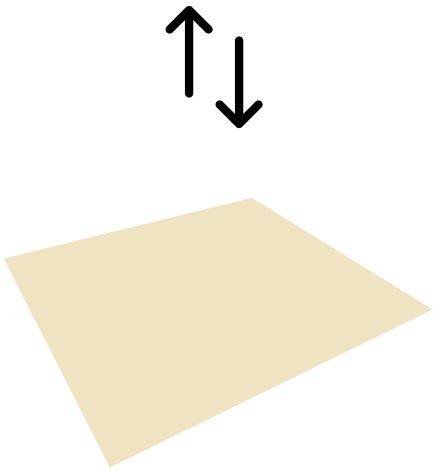
Critical phase – take-off and landing



Motivation

Critical phase – take-off and landing



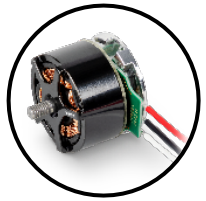




Camera

Autopilot



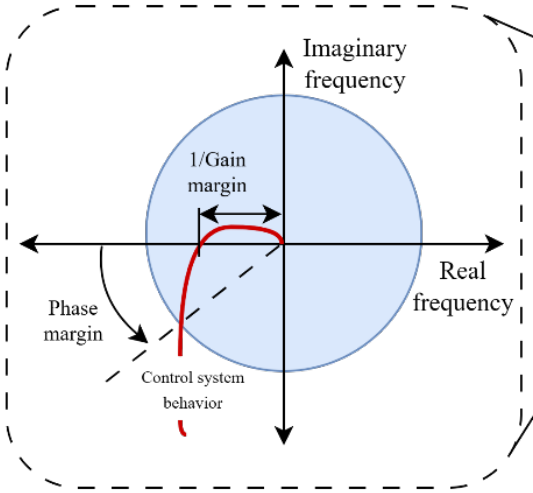


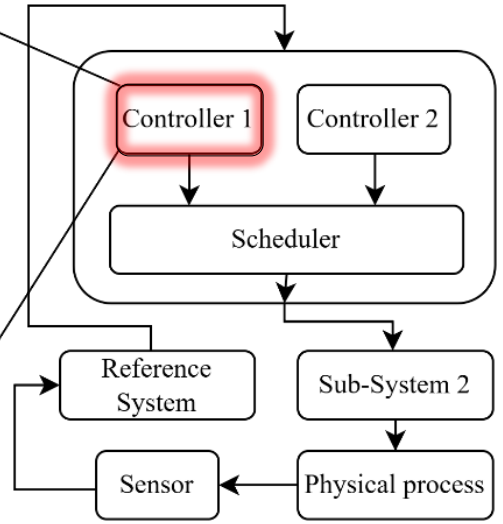
Motor

RC remote



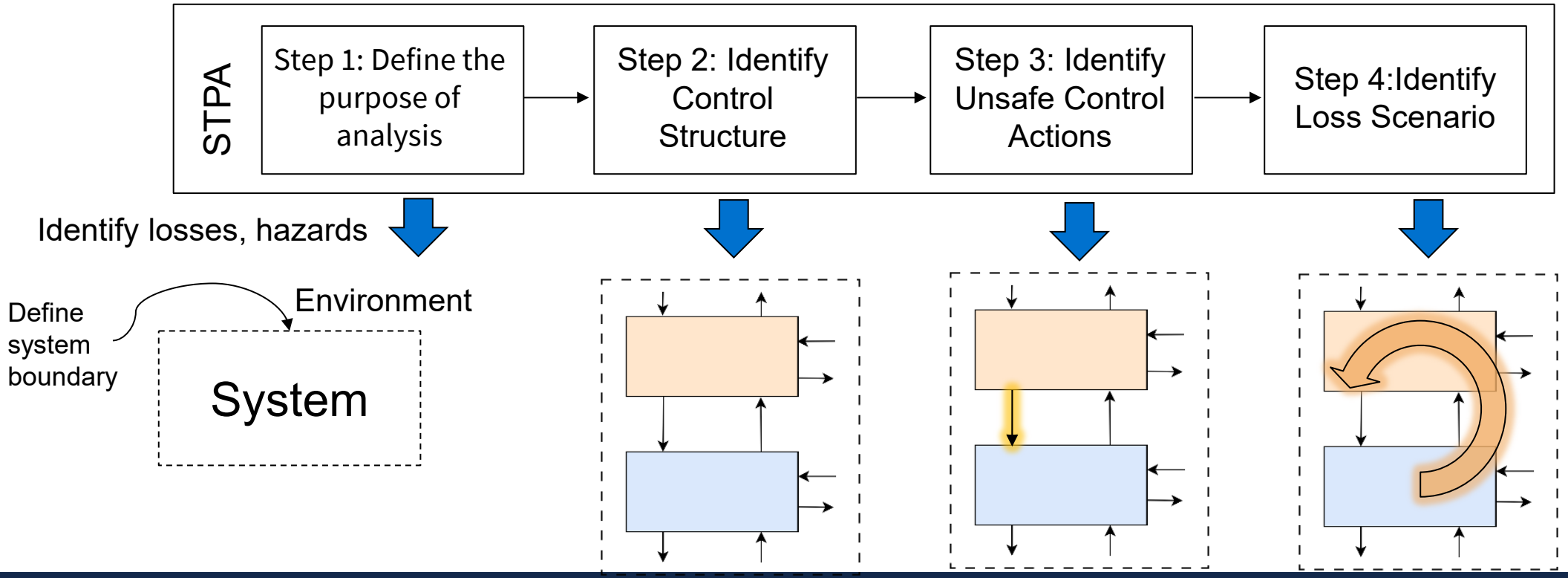
- ❑ Interconnected components
- ❑ Individual components designed independently
- ❑ Top-down systematic approach to identify hazards
- ❑ Scenario generation





STPA at a glance

- System-theoretic process analysis (STPA) – A comprehensive method to identify potential hazards, unsafe control actions, and design constraints in complex systems.

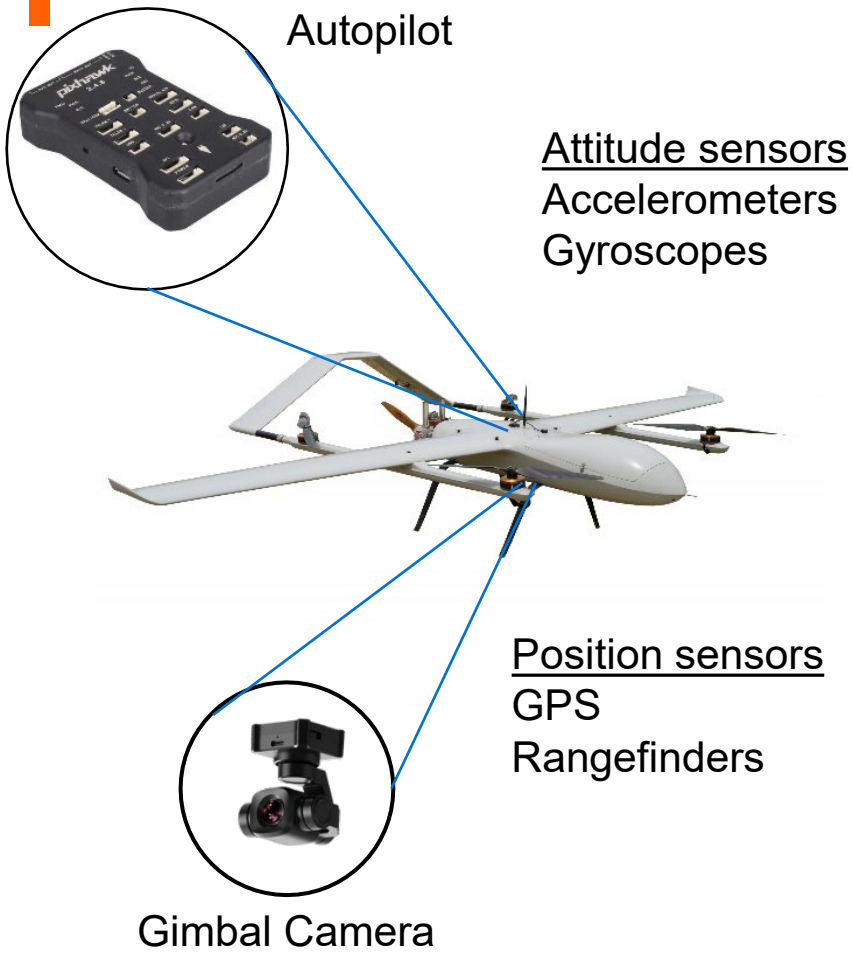


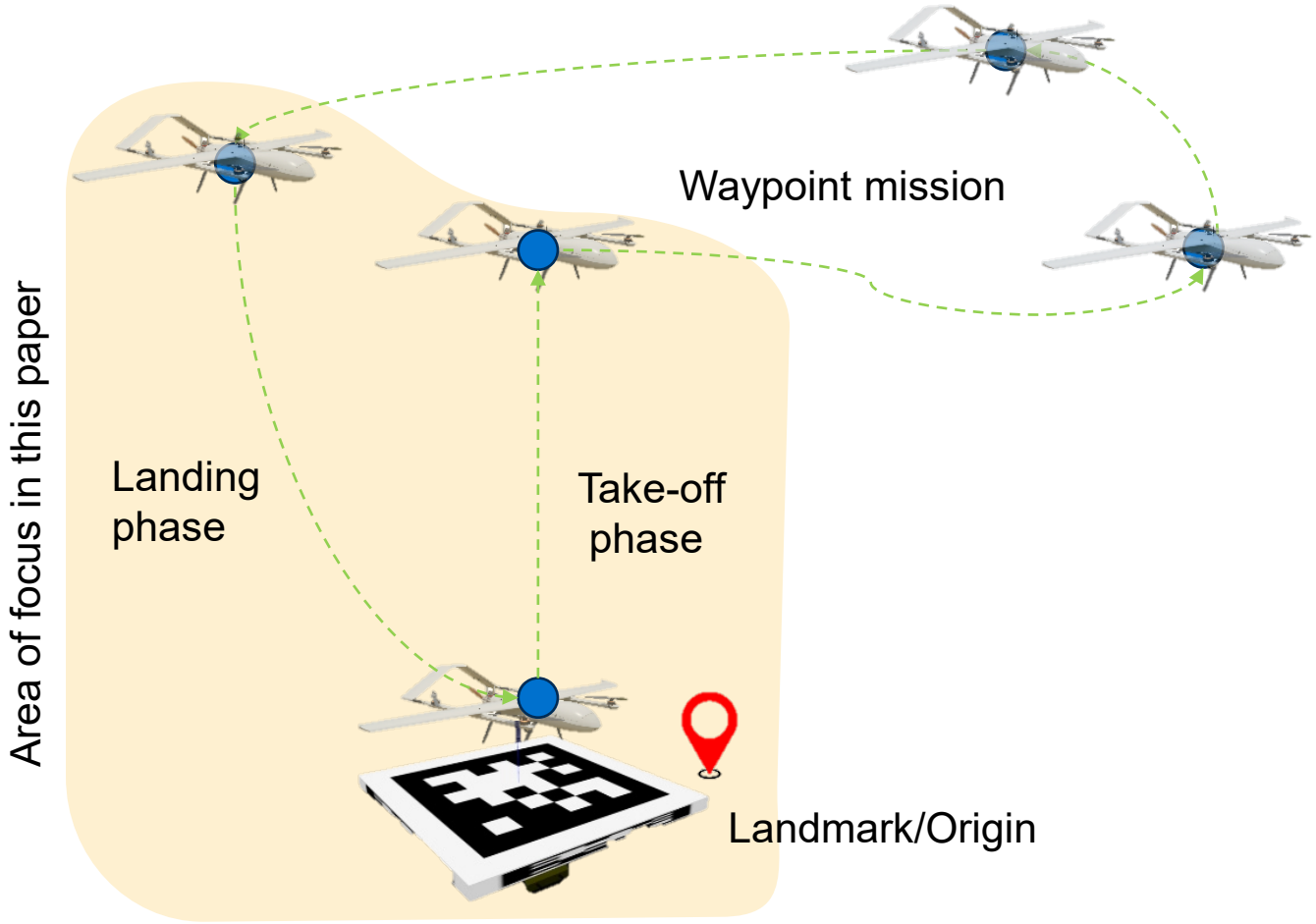
Existing Literature

- Nancy G. Leveson. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.
- Chen, Jieyu, Shuguang Zhang, Yi Lu, and Peng Tang. "STPA-based hazard analysis of a complex UAV system in take-off." In 2015 International Conference on Transportation Information and Safety (ICTIS), pp. 774-779. IEEE, 2015.
- Graydon, Mallory, Natasha A. Neogi, and Kimberly Wasson. "Guidance for designing safety into urban air mobility: Hazard analysis techniques." In AIAA Scitech 2020 Forum, p. 2099. 2020.
- Filho, Bemildo Alvaro Ferreira, and Moacyr Machado Cardoso Junior. "Preliminary Analysis to aid Regulatory Agencies in the eVTOL Certification Process using System Theoretic Process Analysis (STPA)." In Proceedings of the 2024 Air Transportation Symposium.

In this work, we expand the control structure to multiple levels, with a specific focus on vision-based systems and multirotor controller, to identify precise control actions that could become unsafe and propose mitigation strategies to address them.

Problem Description





System Description

Host VTOL UAV

1. Control mode I – Remotely piloted by a human pilot on the ground (human in the loop)
2. Control mode II – Piloted by an autonomous system (autonomy in the loop)





Autopilot

Components - guidance logic, flight controllers (for both multi-rotor and fixed-wing configurations), tilt schedulers, and estimators.

Ground Control Station

Provides real-time telemetry, including positional data, attitude information, battery status, and other critical system parameters.



Losses (Step 1)

- L-1: Loss or damage to host UAV or its environment.
- L-2: Loss of credibility or reputation.
- L-3: Loss of future test capability.
- L-4: Inability to collect data for analysis.

Hazards (Step 1)

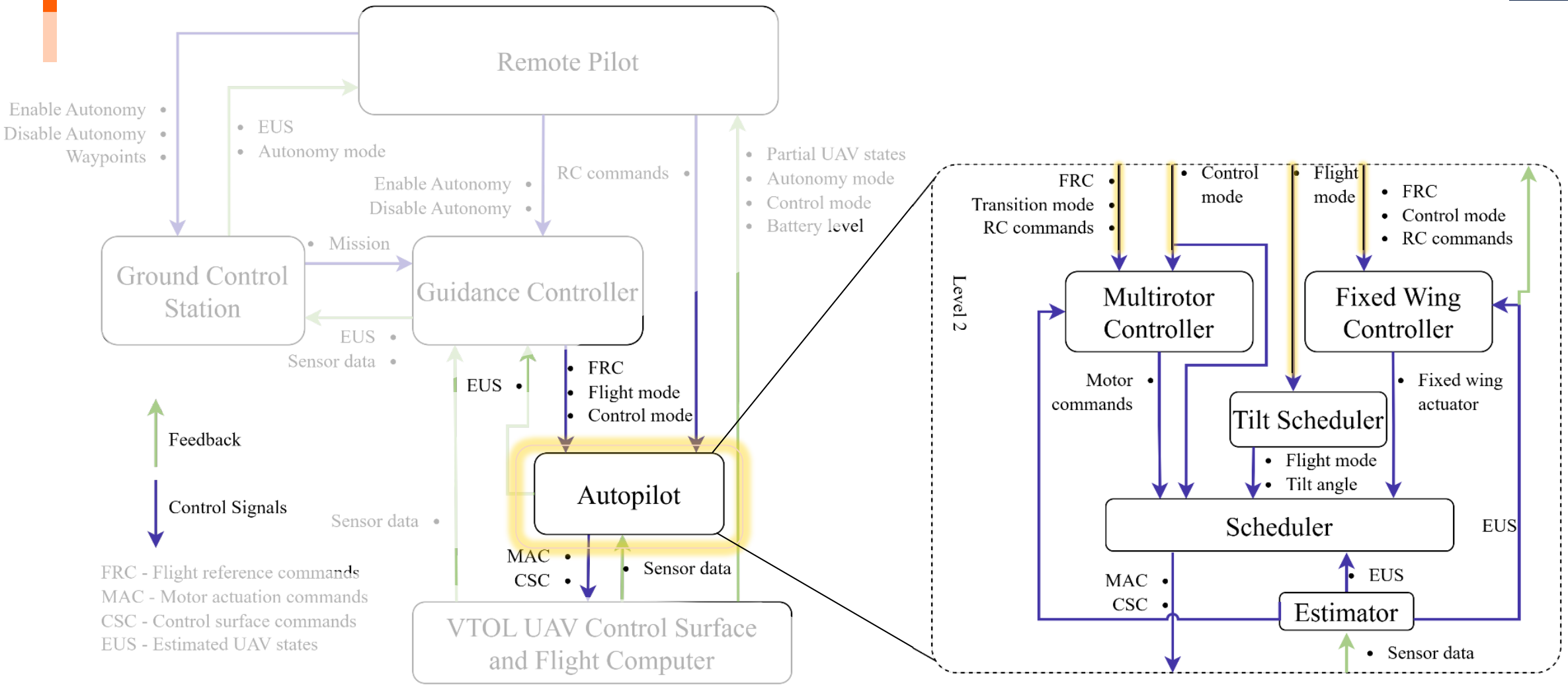
#	Hazard	Connection to losses
H-1	Host UAV too close to objects	[L-1, L-2, L-4]
H-2	Host UAV too close to other aircraft	[L-1]-[L-4]
H-3	Host UAV departs authorized test area	[L-1]-[L-4]
H-4	Host UAV lands outside the authorized landing area	[L-1]-[L-4]
H-5	Host UAV unable to provide useful test data	[L-3,L-4]
H-6	Host UAV becomes uncontrollable	[L-1]-[L-4]

Control Structure (Step 2) – Level 1

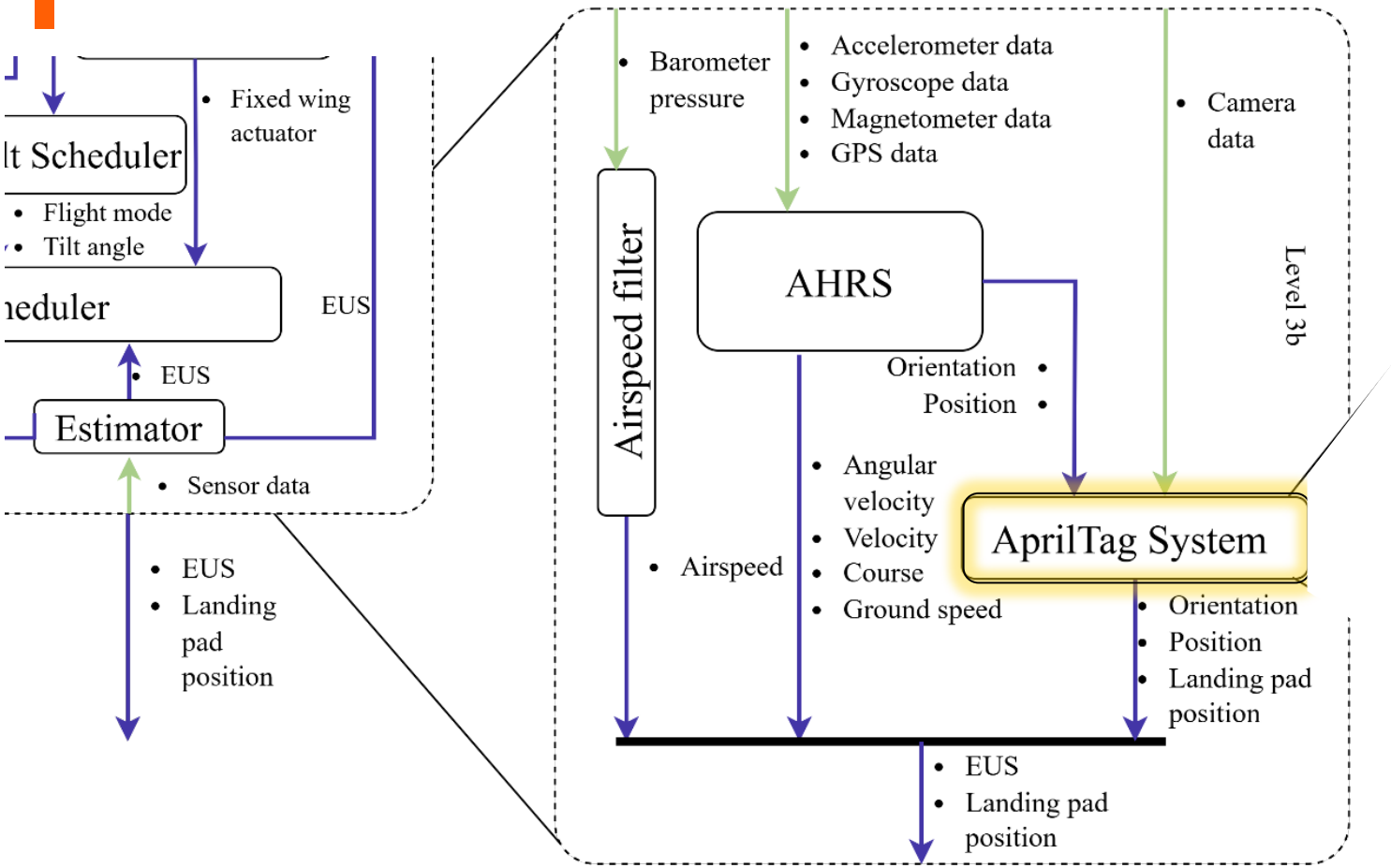


Remote Pilot

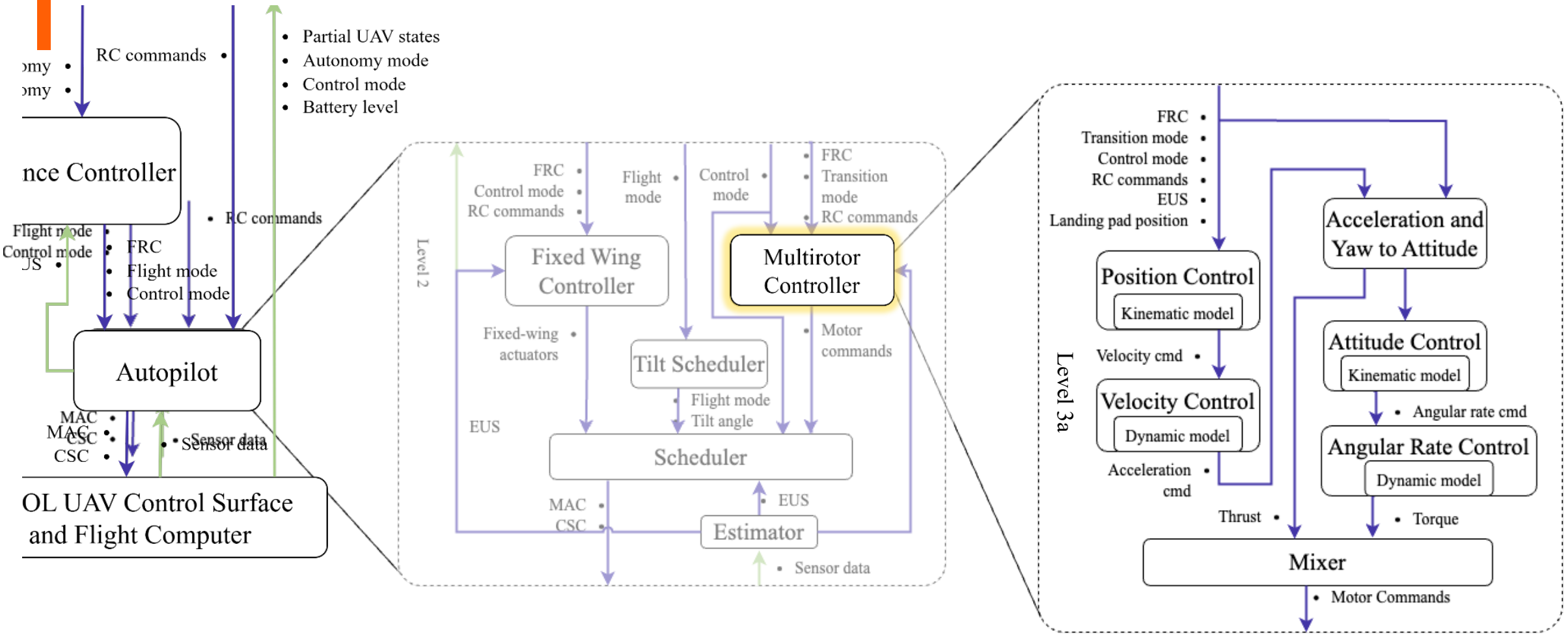
Control Structure – Level 2



Control Structure – Level 3b & 4

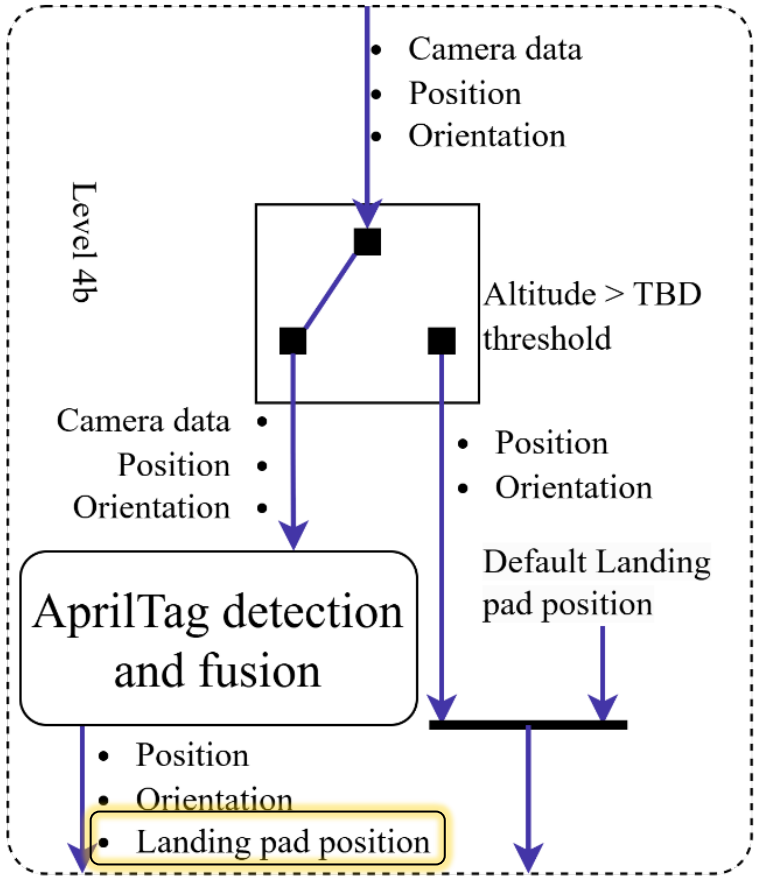


Control Structure – Level 3a

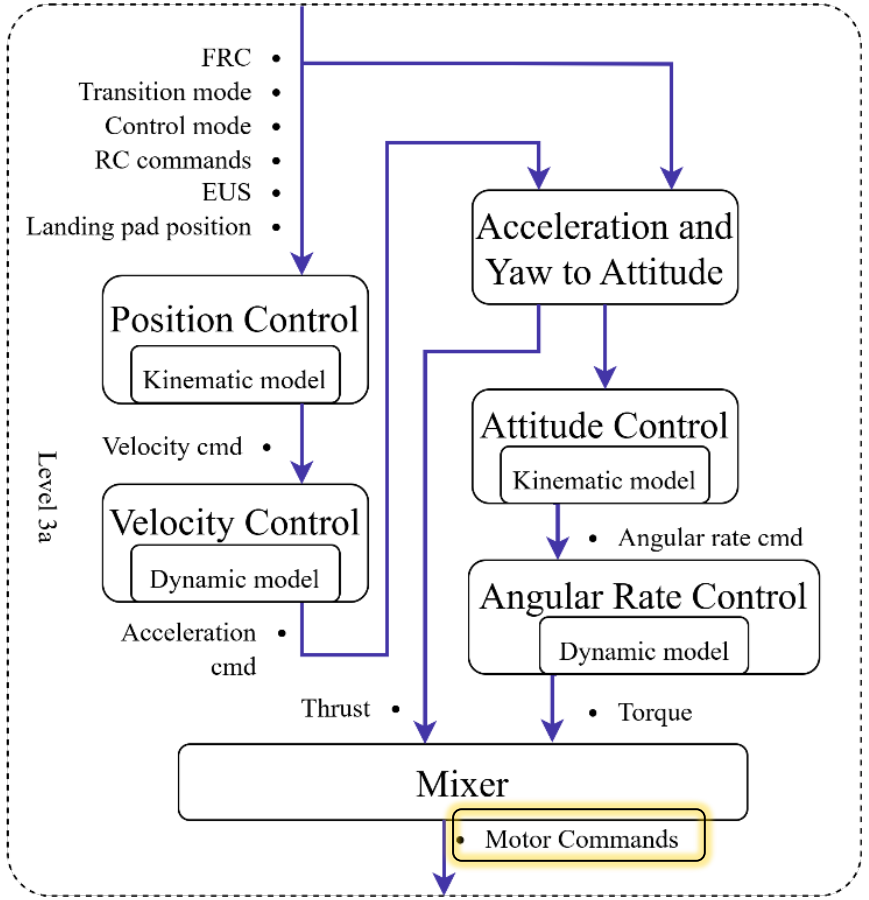


Identify Unsafe Control Actions

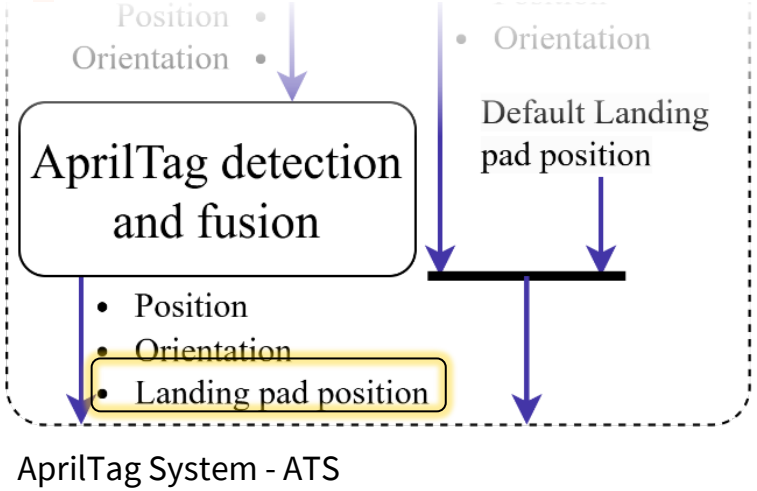
Landing pad position



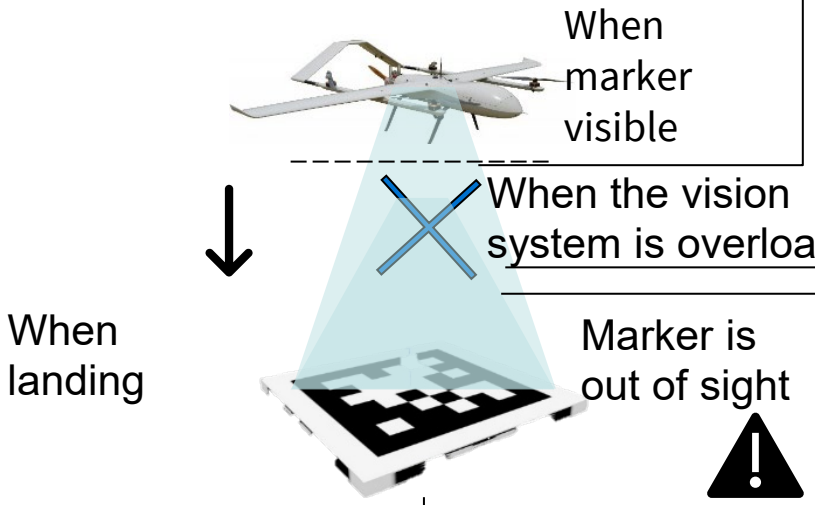
Motor commands



Identify Unsafe Control Actions (UCA) – Step 3 (a)



AprilTag System - ATS



Not providing causes hazards

UCA-1: ATS does not provide landing pad position - [H-3,H-4,H-6]

Providing causes hazards

UCA-2: ATS provides landing pad position - [H-3, H-4, H-6]

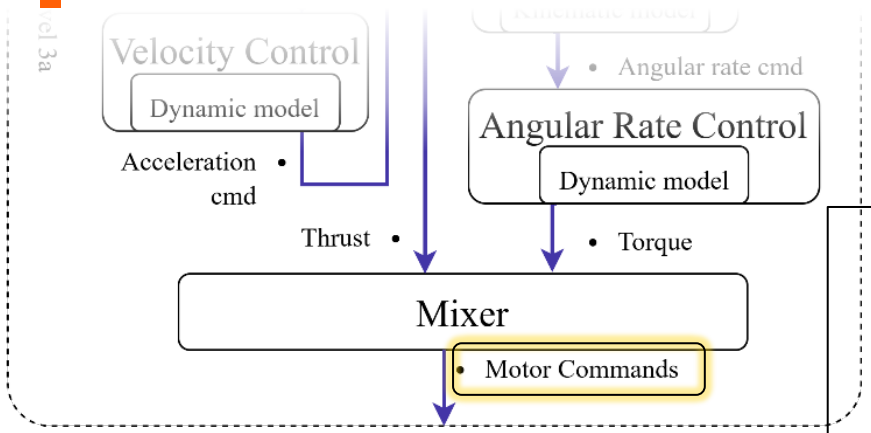
Too early, too late, out-of-order

UCA-3: ATS provides out-of-order landing pad position - [H-3, H-4, H-6]

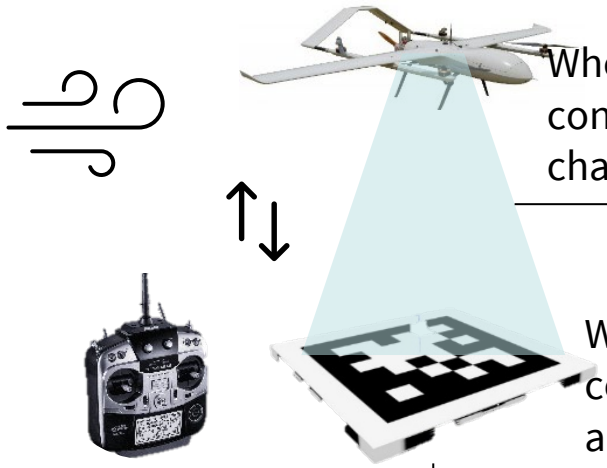
Stopped too soon, applied too long

UCA-4: ATS stopped providing landing pad position - [H-4]

Identify Unsafe Control Actions (UCA) – Step 3 (b)



Multirotor controller - MC



When wind conditions change

When RC commands are received

Not providing causes hazards

UCA-5: MC does not provide motor actuation [H-1, H-3 H-6]

Providing causes hazards

UCA-6: MC provides motor actuation [H-1]-[H-6]

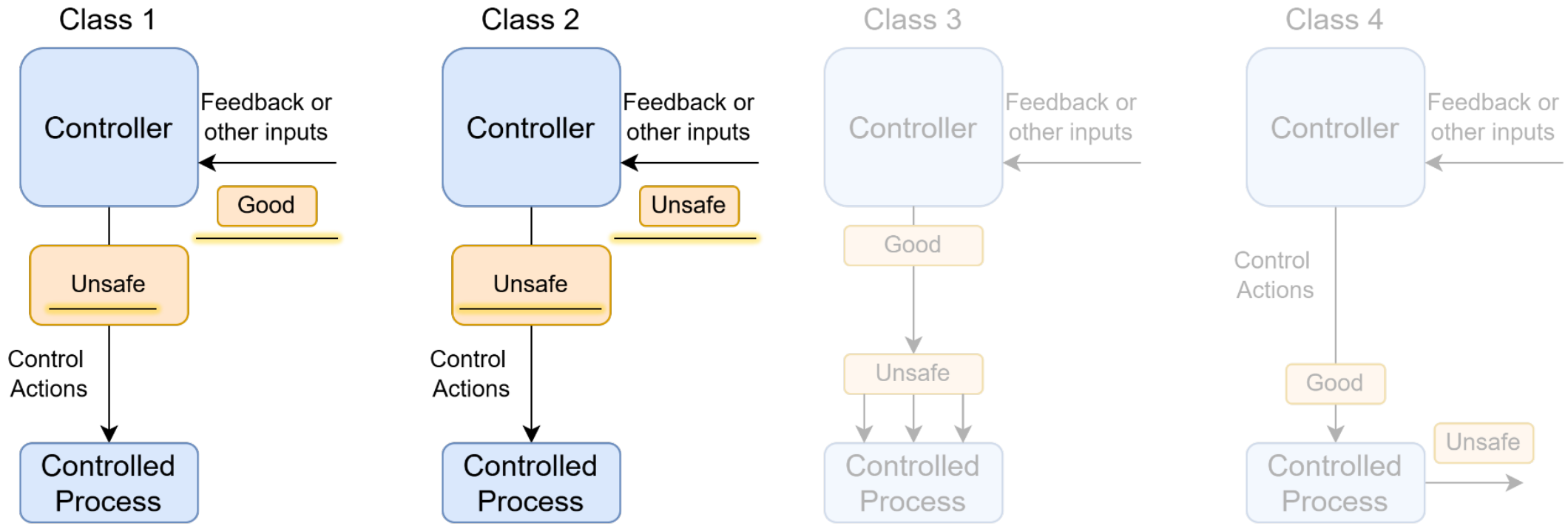
Too early, too late, out-of-order

[redacted]

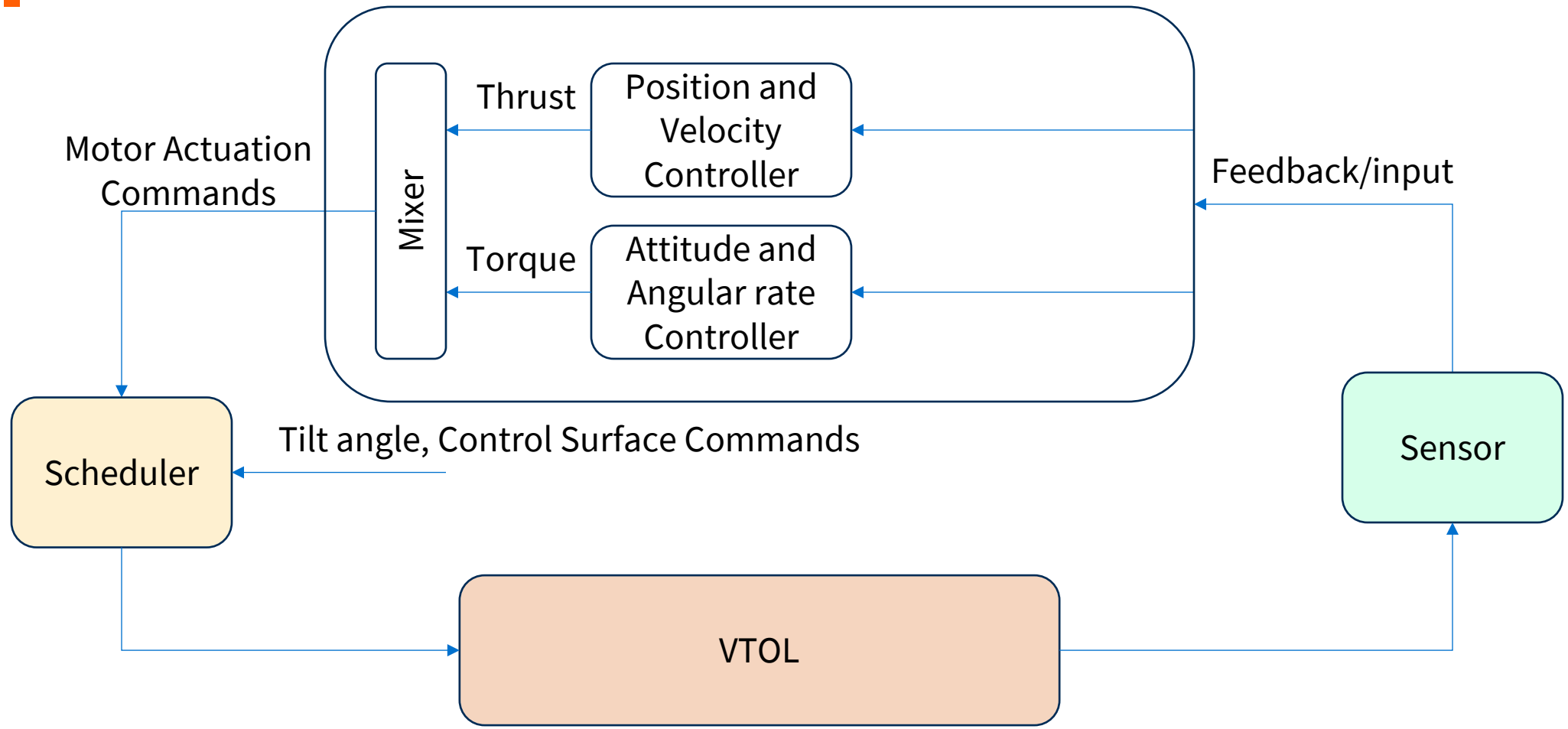
Stopped too soon, applied too long

[redacted]

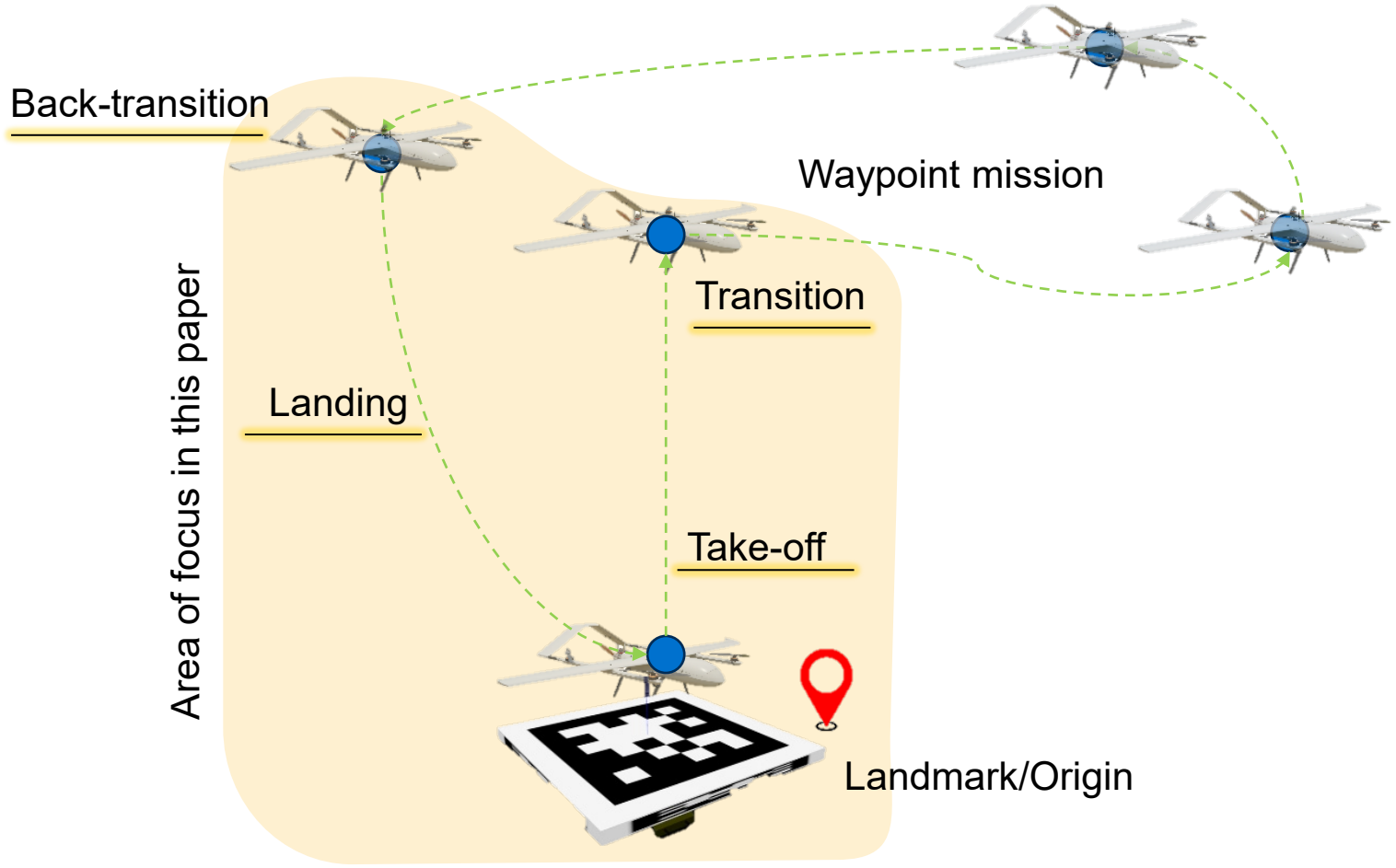
Loss Scenarios



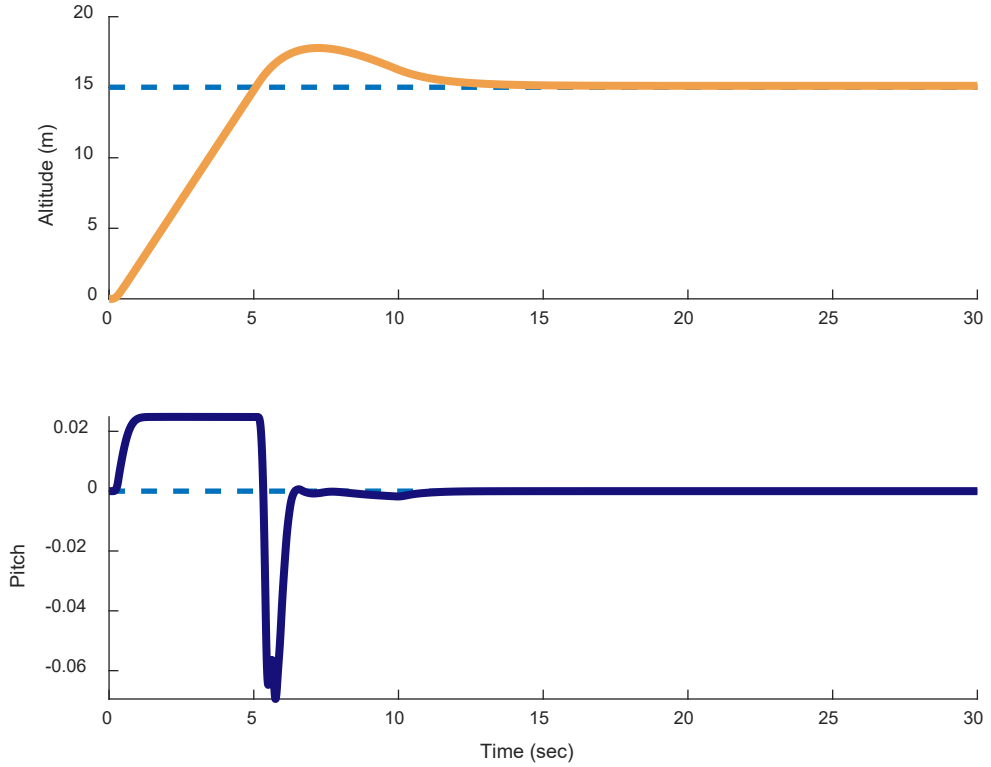
Control Loop of Multirotor Controller (MC)

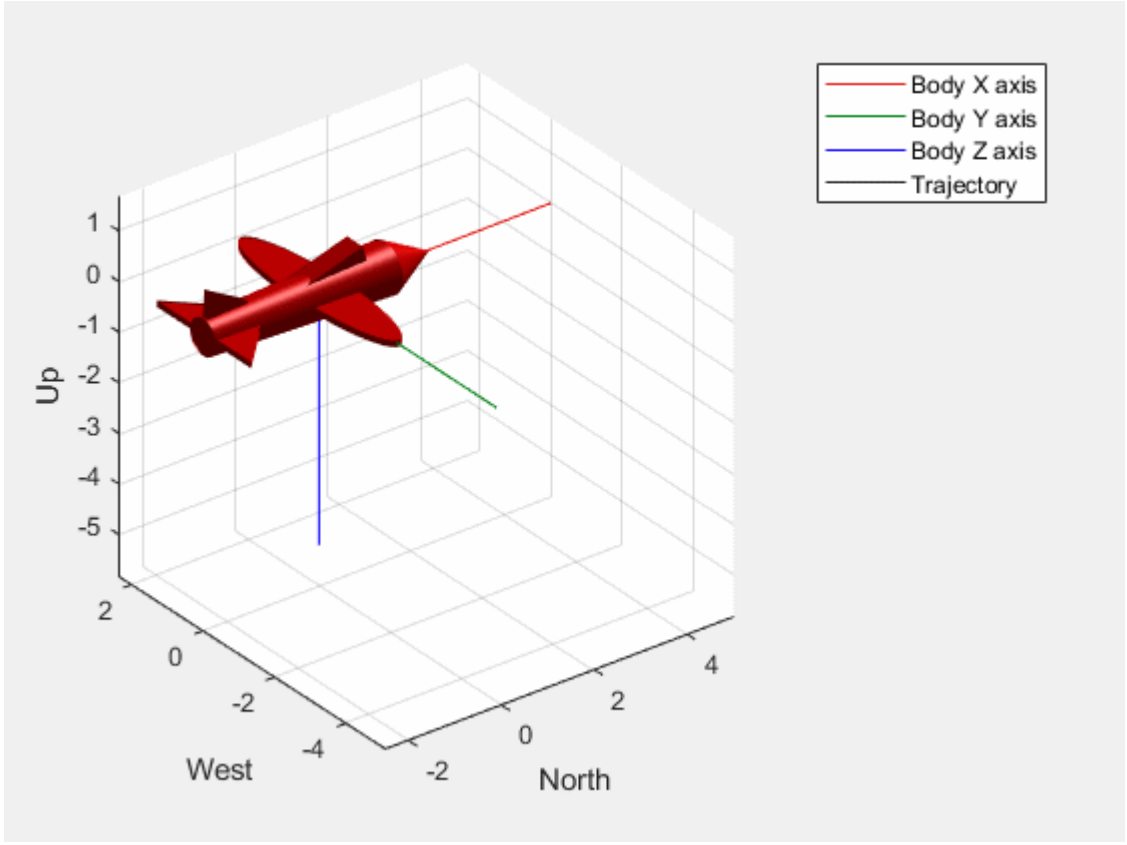


Phases of Flight

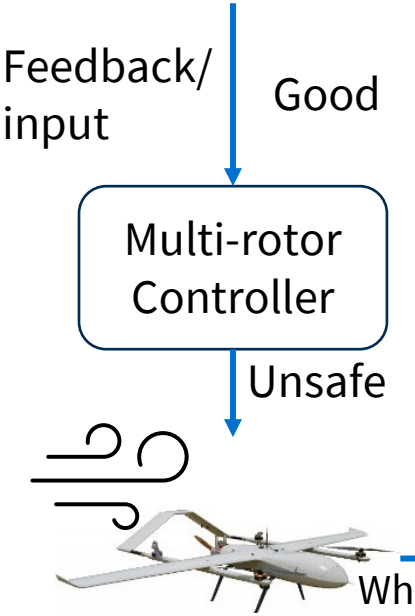


Nominal Operation : Take-off





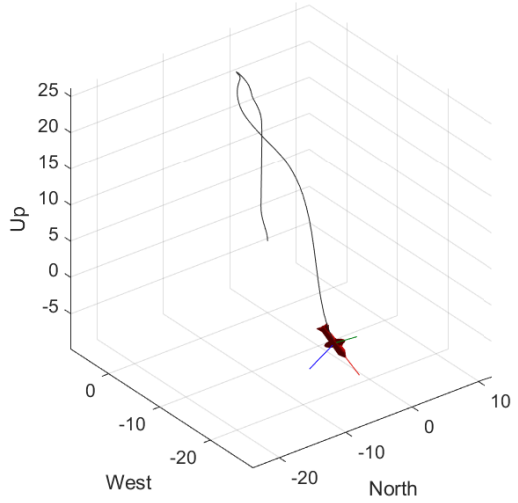
Class 1 Loss Scenario: Take-off



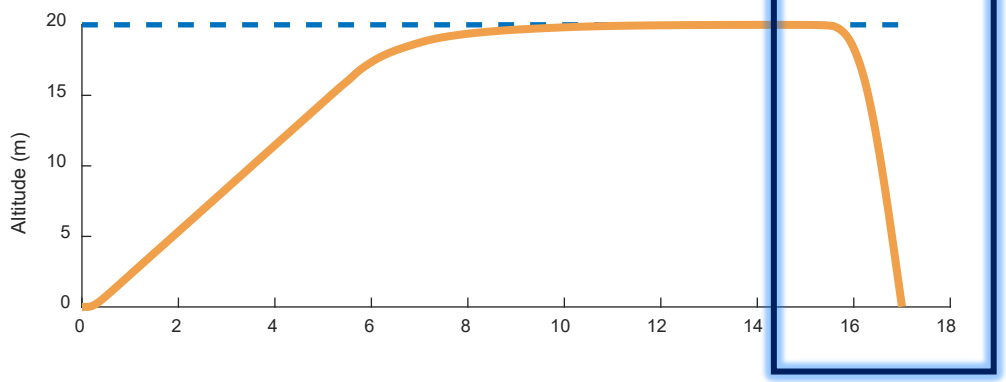
When wind conditions change

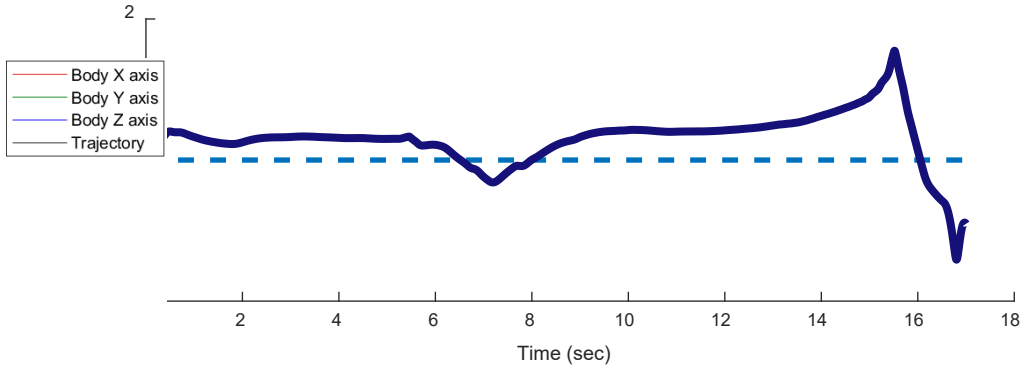
Not providing causes hazards

UCA-5: MC does not provide motor actuation [H-1, H-3 H-6]



Crash





Scenario

The MC controller tuned for trim conditions are inefficient due to change in wind conditions.

Class 1 Loss Scenario: Transition / Back transition

Transition/back transition



Scenario

The VTOL doesn't reach a steady-state for the tuned gains (hold TBD sec before transition)

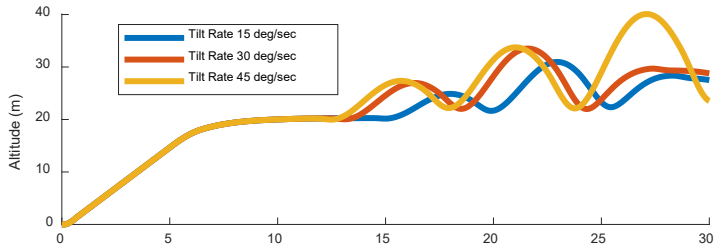


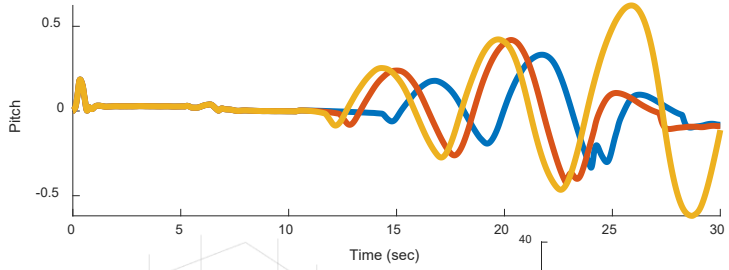
https://www.cs.cmu.edu/~mmousaei/highlights/2022/05/20/vtol/

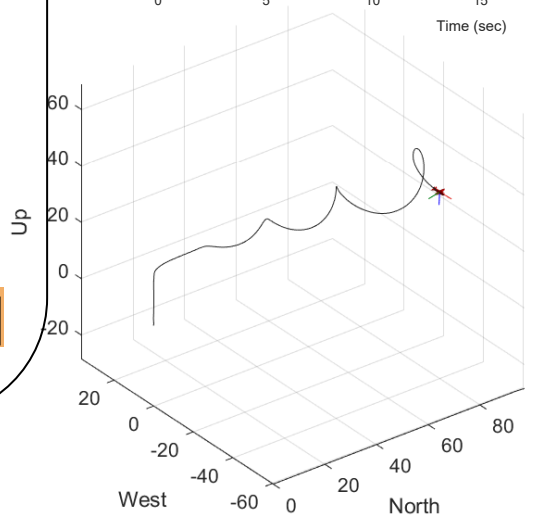
Not providing causes hazards

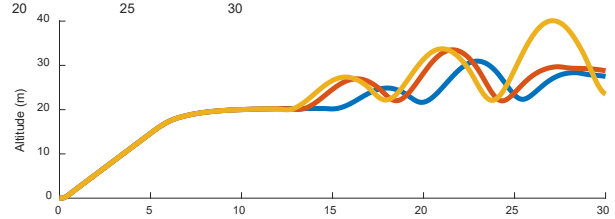
UCA-9/10: Multirotor Controller (MC) does not provide correct tilt rate and critical tilt angle when trim conditions are mismatched for tuned controller [H-3 H-6]

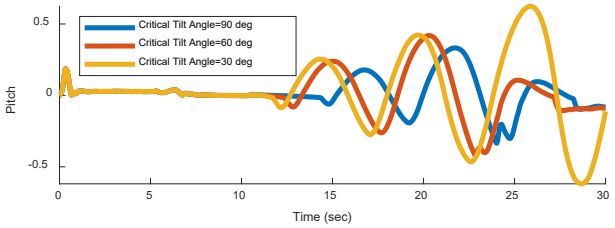
UCA-11: Multirotor Controller (MC) does not provide thrust when the flight is oscillating [H-3 H-6]







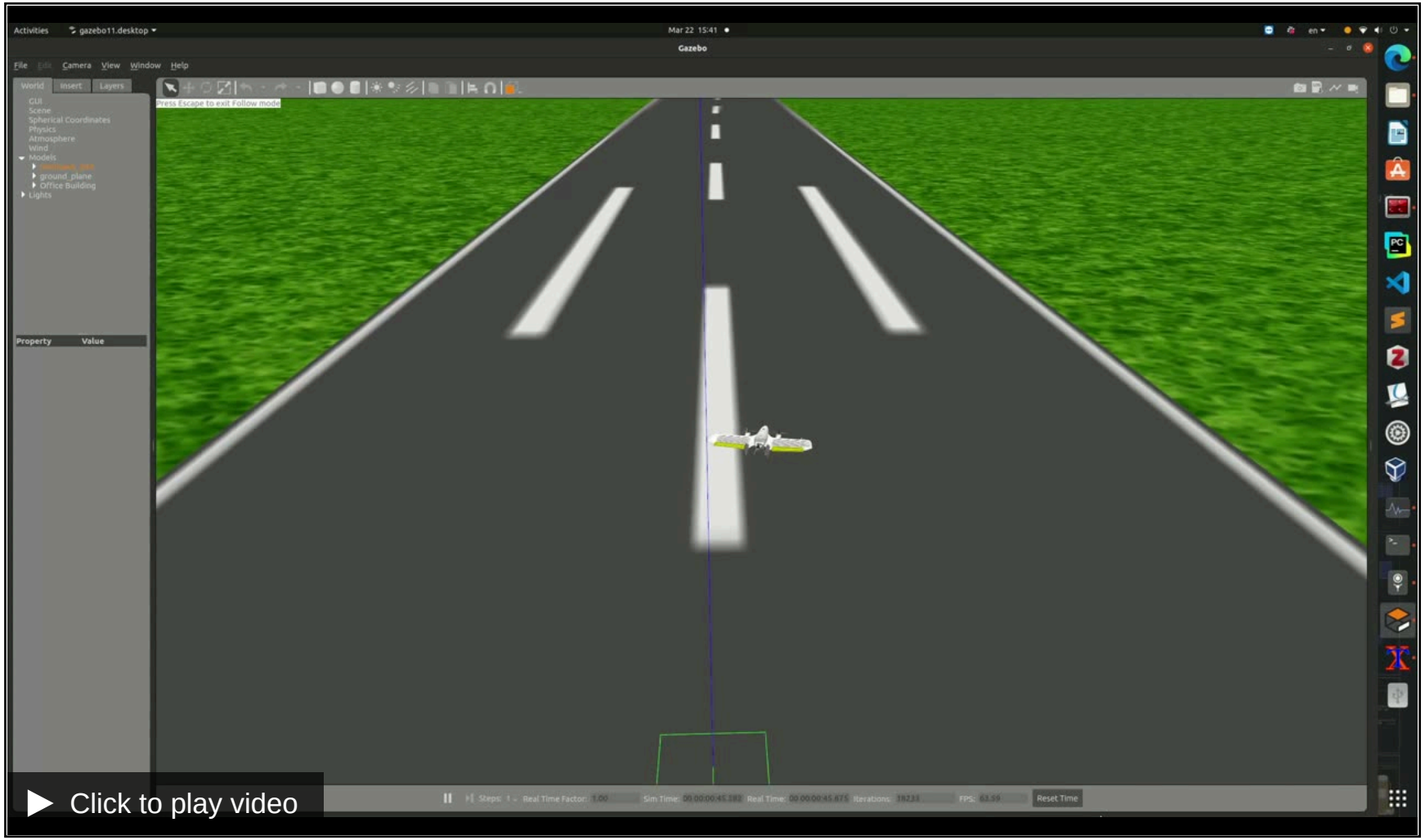




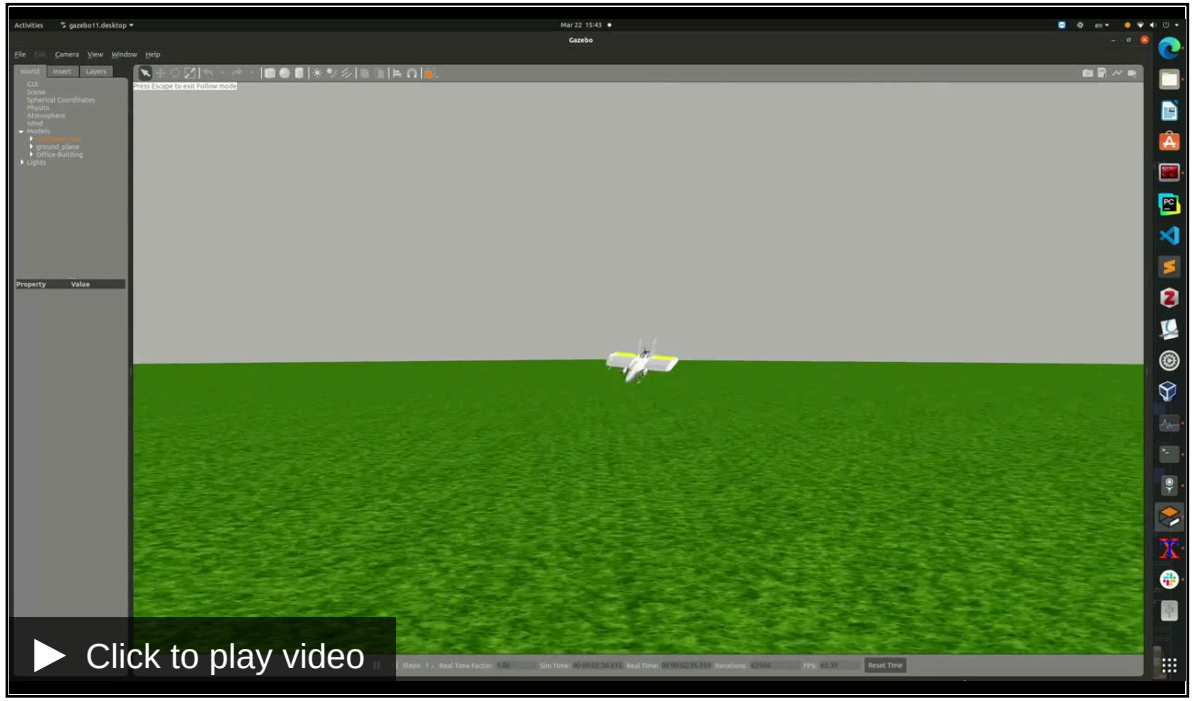
Class 1 Loss Scenario: Transition

GUAM model

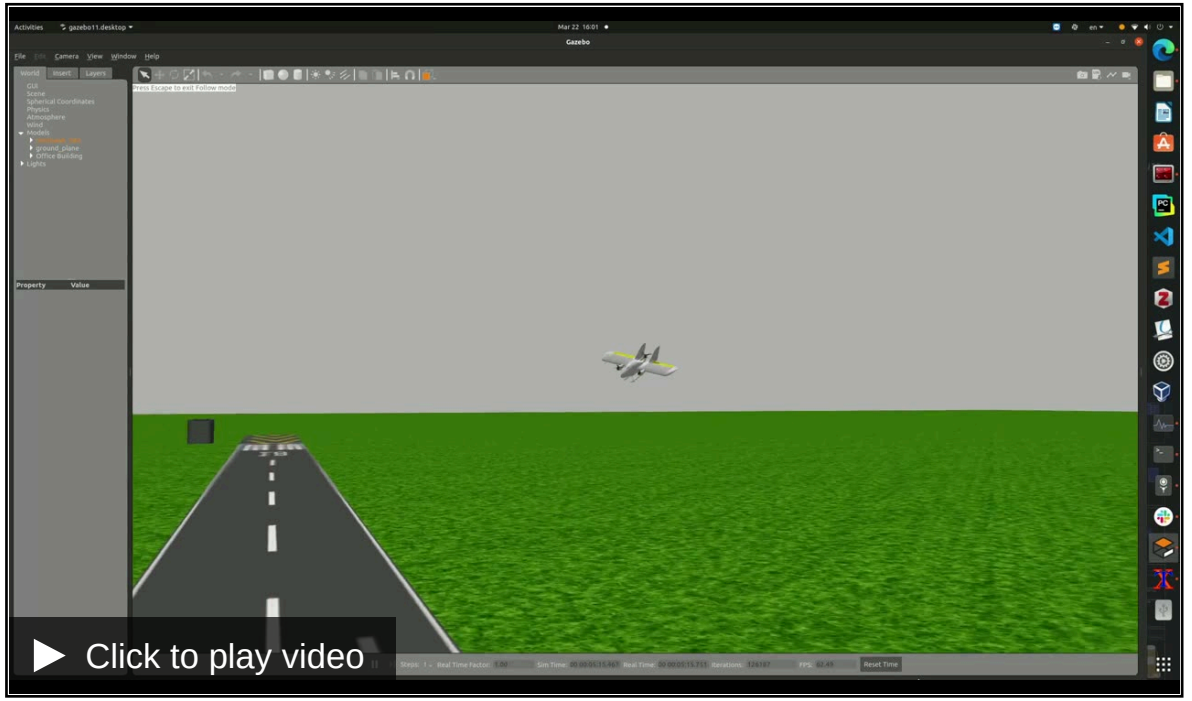
Quad to Cruise – Leading to reduced altitude



Class 1 Loss Scenario: Back transition



Cruise to Quad - Unstable



Cruise to Quad - Crash

Class 1 Loss Scenario: Take-off and transition



When the aircraft has reached desired altitude

Providing causes hazards

UCA-6: MC provides undesired motor thrust [H-3]



when the commanded thrust is amplifying oscillations during a transition

Providing causes hazards

UCA-9: MC provides motor thrust [H-3, H-6]

Scenario
The MC receives RC commands which override or append existing thrust commands



Scenario
The VTOL is unable to maintain altitude.

Class 1 Loss Scenarios

Not providing causes hazards

UCA-1: ATS does not provide landing pad position - [H-3,H-4,H-6]

Scenario
ATS believes the altitude is below the threshold altitude

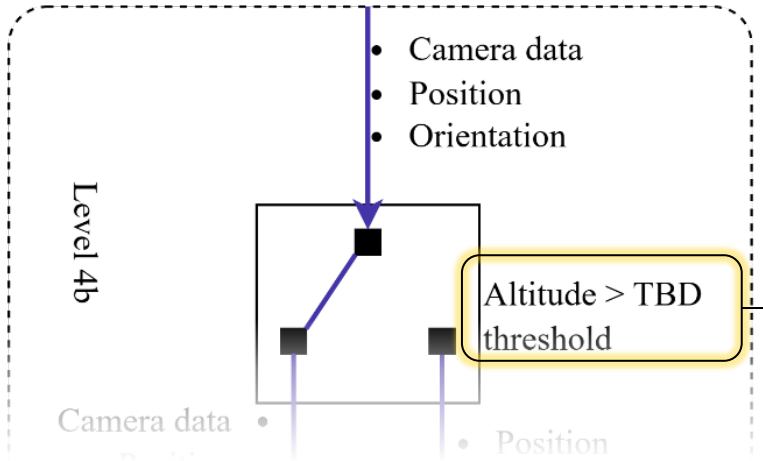
When fiducial marker is visible during the take-off and landing phase

Providing causes hazards

UCA-2: ATS provides vision-based landing pad position [H-3, H-4, H-6]

Scenario
ATS believes the altitude is above the threshold altitude

When fiducial marker is out of sight (not completely visible) during the take-off and landing phase

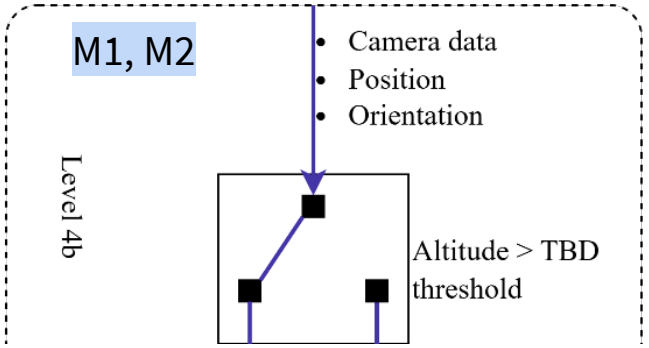


AprilTag System - ATS

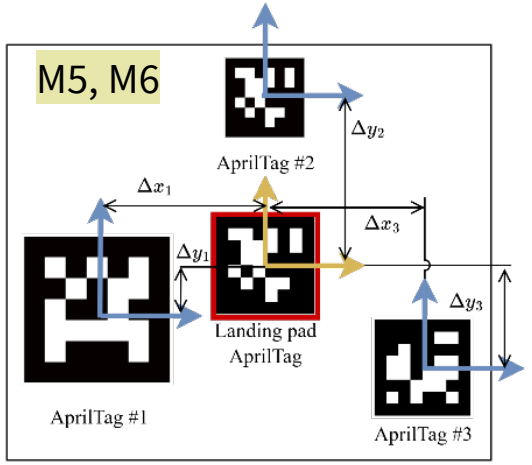
Mitigation Strategies - 1

- M1 - Introduce a secondary altitude measurement - AprilTag system. (UCA-1, UCA-2, UCA-4, UCA-5).
- M2 - Optimize the camera's image capture rate (UCA-3).
- M3 - Performs an occlusion check on the fiducial marker (UCA-1).
- M4 - Conduct the mission only under predefined (TBD) lighting conditions - low visibility (UCA-1).
- M5 - Deploy multiple fiducial markers (UCA-2, UCA-4).
- M6 - Integrate a tagging system - AprilTag (UCA-2, UCA-4).

M1, M2



M5, M6



M3, M4



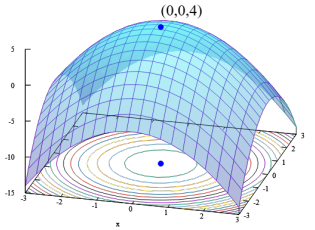
Mitigation Strategies - 2

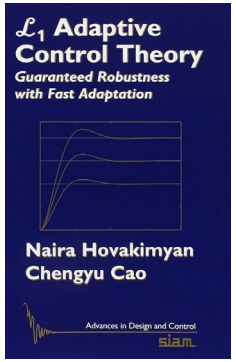
- M7 – Create a gain-transition angle-wind map (UCA-5, UCA-8, UCA-9, UCA-10, UCA-11).
- M8 – Software lock to ignore RC commands during transition (UCA-6, UCA-13).
- M9 - Introduce a secondary altitude measurement (UCA-7).
- M10 – Tune the steady state time end of flight conditions (UCA-5, UCA-14, UCA-12).
- M11 – Add adaptive control in existing control policy (UCA-5—UCA--12).
- M12 – Develop a hybrid mode for transition between quad and fixed-wing mode (UCA-5, UCA-8, UCA-9)



M7,M8,M9

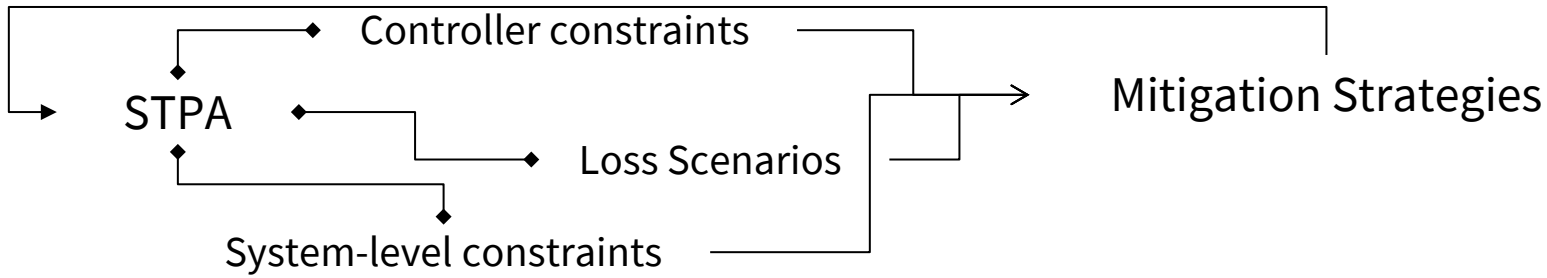
M11, M12





Conclusion

- ❑ Performed STPA on VTOL with vision during take-off and landing
- ❑ Multi-level control structure
- ❑ 16 Unsafe control actions
- ❑ 2 classes of loss scenarios – 13 total scenarios
- ❑ 12 mitigation strategies



Future Work

- ❑ Create the worse-scenario with hardware-in-the-loop (experiments)
- ❑ Connect the STPA with gang of six (transfer function analysis)

Acknowledgement

Jinrae Kim Naira Hovakimyan Luca Carlone John P Thomas Nancy G. Leveson







NASA ULI UNIVERSITY LEADERSHIP INITIATIVE

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH UNITED STATES AIR FORCE AFOSR

NSF CAREER AWARDS



Mikael Yeghiazaryan, Research Assistant, UIUC

Thank You

Questions ?