A Safety-Driven Framework for Developing System Architectures

2025 MIT Virtual STAMP Workshop

Justin Poh

22 September 2025

The Evolution of Complex Systems

More Components,
More Connections,
More Software

Increasing Emphasis on Desired Properties

Safety

Cybersecurity

Sustainability

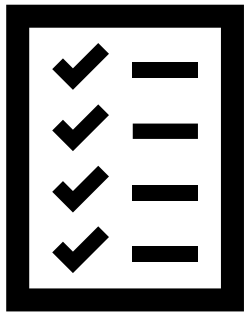
Need to design desired properties into the system architecture

[1] Image from: https://www.wired.com/2016/12/googles-latest-self-driving-car-minivan/
[2] Image from: https://www.aurora.aero/urban-air-mobility/
[3] Image from: https://www.nats.aero/news/london-city-is-first-major-airport-controlled-by-remote-digital-tower
[4] Image from: https://www.theguardian.com/technology/2023/aug/01/uber-self-driving-arizona-deadly-crash
[5] Image from: https://onboard.thalesgroup.com/connected-cybersecure-aircraft-tackle-challenge/
[6] Image from: https://www.cnn.com/2024/02/21/climate/space-debris-solution-climate-scn/index.html

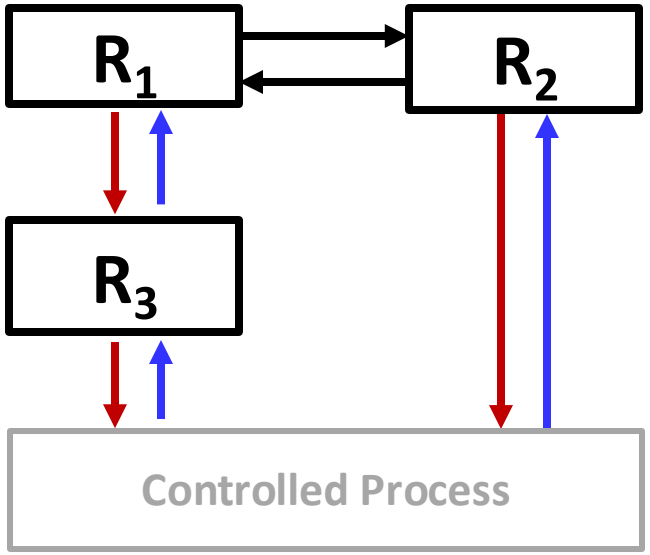
Types of Design Decisions in Architecture Development

System Architecture: Description of system entities and relationships between them

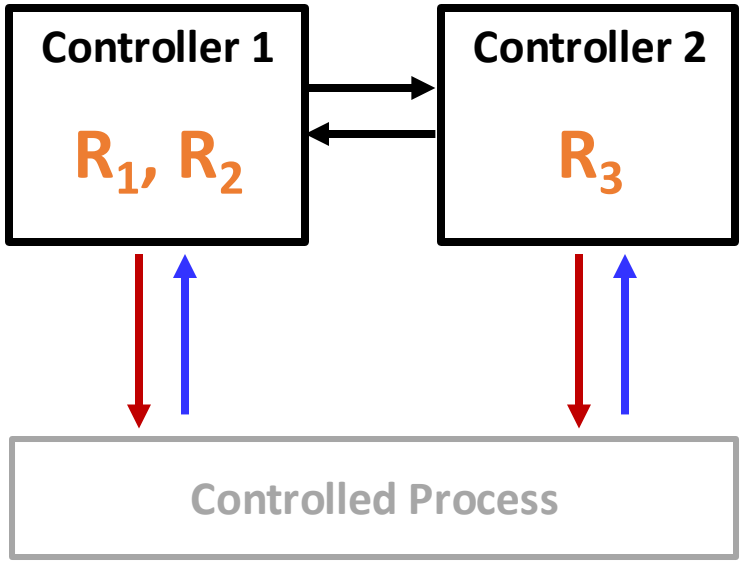
1 **Identify System Requirements**



2 **Define Responsibilities (Functions) & Relationships**



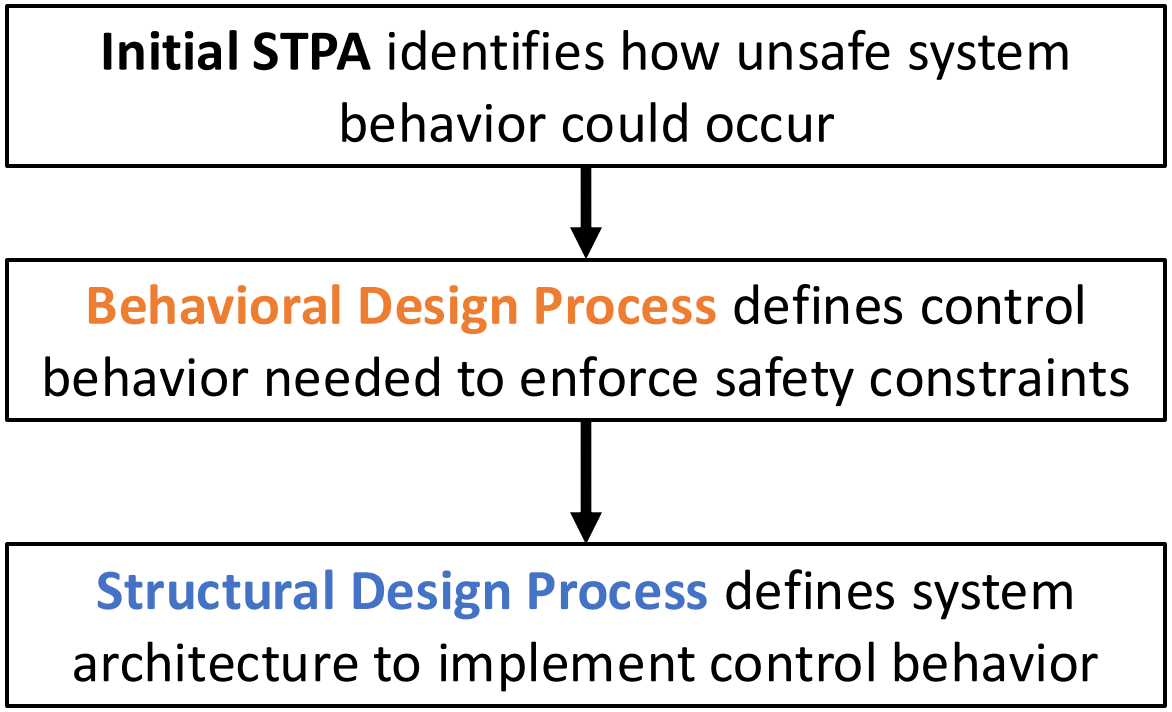
3 **Allocate Responsibilities to System Elements**



Research Objective: Develop a framework for considering safety upfront when making these design decisions

Overview of Framework

Approach: STPA drives design decisions



Key Output: Conceptual Architecture
Functional control structure of desired control behavior

Key Output: Benefits & Tradeoffs
Used to inform decisions about the preferred system architecture

Result: Safety designed into the system architecture from the beginning

Case Study: Urban Air Mobility

- **Urban Air Mobility (UAM)**: On-demand cargo or passenger flights within a metropolitan area
- Today's air traffic management system not designed to handle UAM air traffic characteristics


[7]

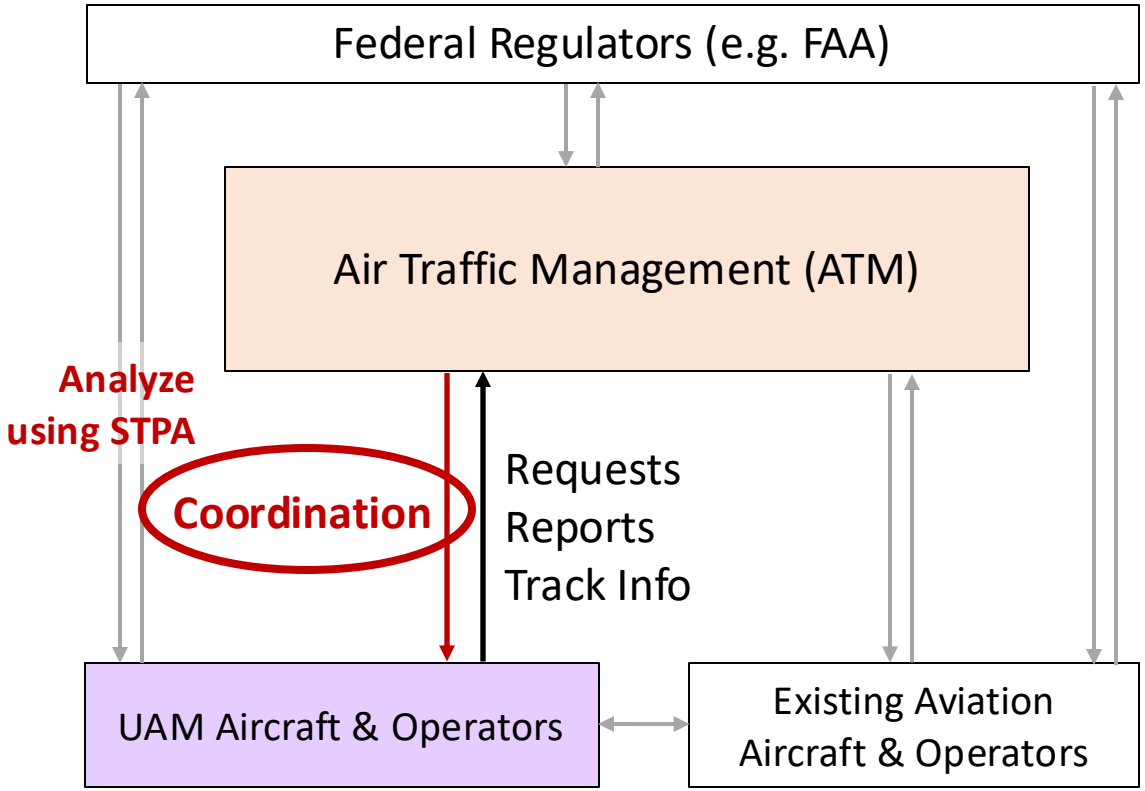
Case Study Goal:

Develop an alternative air traffic management architecture to safely manage UAM air traffic (prevent collisions)


[8]

[7] Image from: *NASA, Urban Air Mobility OpsCon: Passenger-Carrying Operations, May 2020*
[8] Image from: UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4, Version 1.0, NASA (2020)

Part 1: Early-Stage STPA Analysis of ATM System



Start: Abstract ATM control structure

Unsafe Control Action: Air Traffic Management (ATM) does not **Coordinate Aircraft Movements** when a collision between two aircraft is imminent

Causal Scenario: ATM receives feedback about a conflict (potential collision) but is preoccupied addressing other conflicts and does not address this one

Part 2: Deriving Desired Control Behavior From STPA Scenarios

Input: STPA Scenarios

1. **Derive System Requirements:** Safety constraints to mitigate or prevent unsafe behavior

2. **Define Control Elements & Relationships:** Responsibilities, control actions and feedback needed to meet system requirements

Output: Conceptual Architecture

Functional control structure representing desired control behavior

Example: Deriving Collision Avoidance Requirements

Causal Scenario (from STPA): ATM receives feedback about a conflict (potential collision) but is preoccupied addressing other conflicts and does not address this one

Req-1: ATM system must coordinate the movement of aircraft to resolve any identified conflicts

---

System Requirements

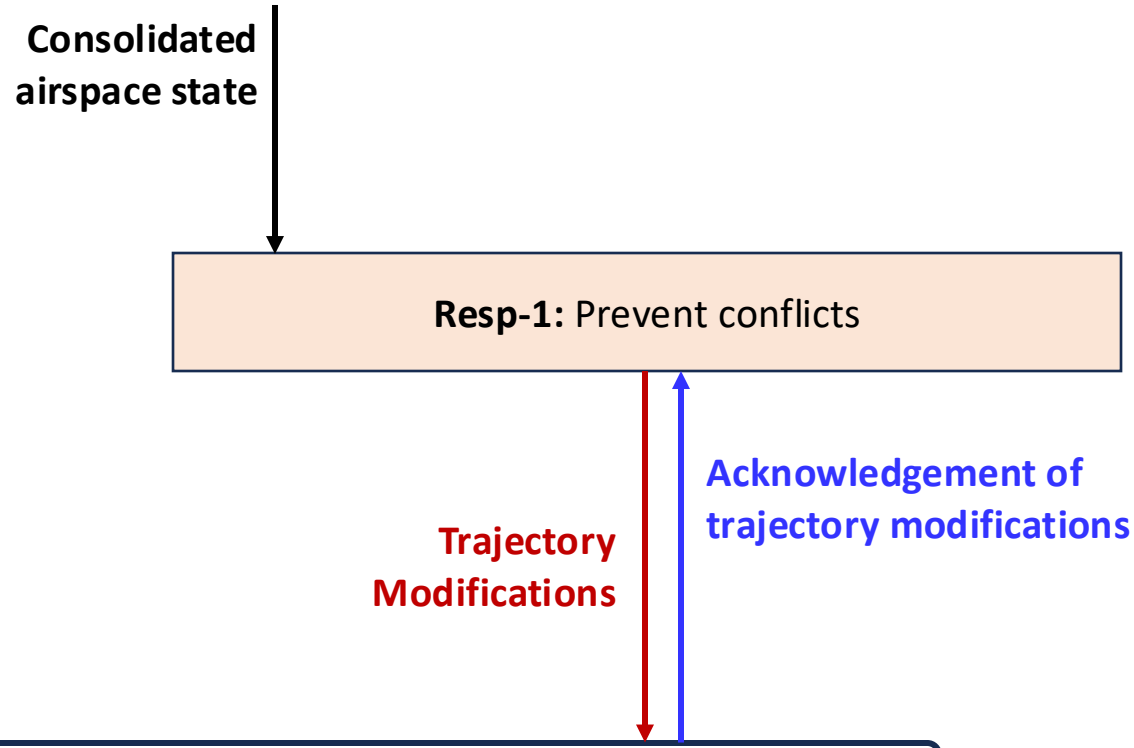
Req-1: ATM system must coordinate the movement of aircraft to resolve any identified conflicts

Req-3: ATM system must only allow as many aircraft to access the airspace as it is capable of managing

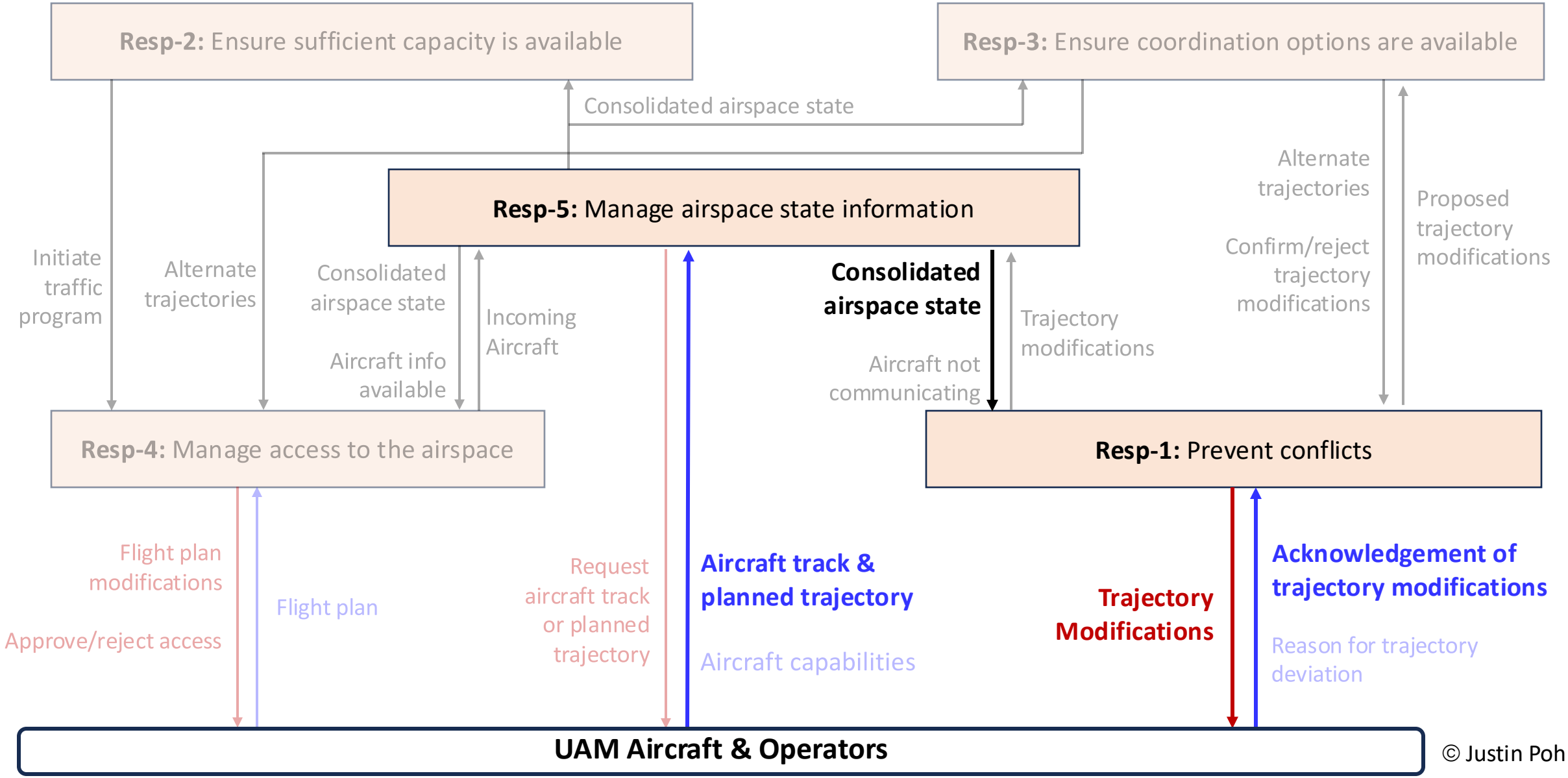
⋮

Deriving Control Elements From Requirements

Req-1: ATM system must coordinate the movement of aircraft to resolve any identified conflicts



Creating the Conceptual Architecture for Collision Avoidance



Part 3: Creating and Comparing Architecture Options

Input: Conceptual Architecture

1. **Create Architecture Options:** Ways to assign responsibilities to system controllers
2. **Analyze & Compare Options:** Comparing STPA scenarios identified for each option highlights qualitative differences in control behavior

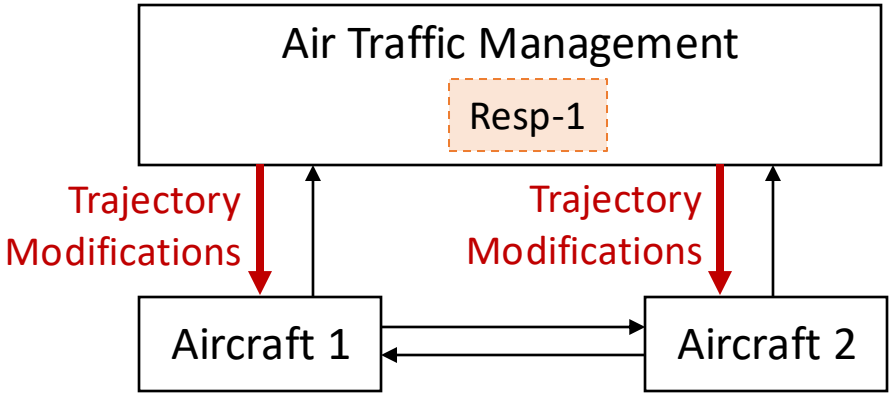
Output: Control-Related Benefits and Tradeoffs

Used to select responsibility assignments that best achieve emergent properties

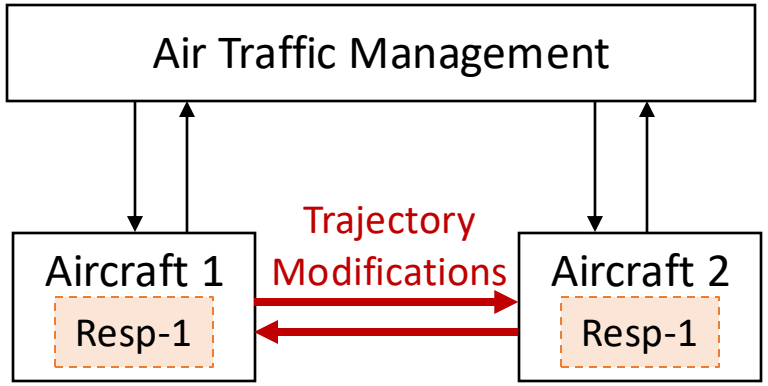
Creating Potential Collision Avoidance Architecture Options

Case Study Scope:
Focus on assignment of Resp-1 to develop a collision avoidance architecture for UAM

	A1: Centralized Collision Avoidance	**A2:** Decentralized Collision Avoidance
Resp-1: Prevent conflicts	**ATM**	**Aircraft**
Resp-2: Ensure sufficient capacity	ATM	ATM
Resp-3: Generate alternate trajectories	ATM	ATM
Resp-4: Manage access to the airspace	ATM	ATM
Resp-5: Maintain consolidated airspace state	ATM	ATM



A1: Centralized Collision Avoidance



A2: Decentralized Collision Avoidance

Analyzing and Comparing Architecture Options

1

STPA Analysis of Architecture Options

Architecture Option	Identified Scenarios
A_1	SC-1, SC-4
A_2	SC-2, SC-3, SC-4

Consolidate to create master set

Evaluation Criteria: Qualitative description of differences in control behavior

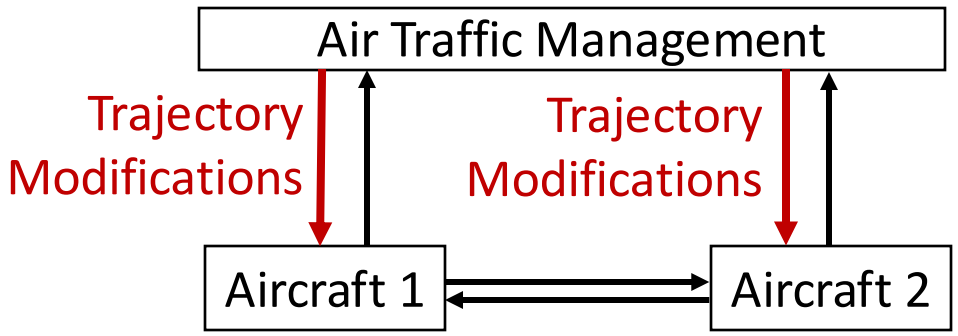
2

Create Architecture Comparison Table

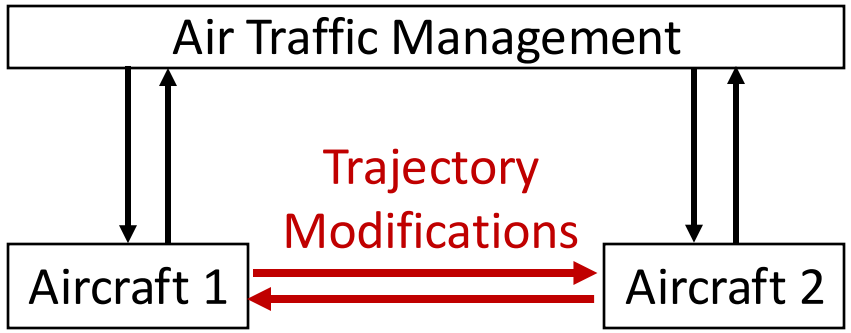
Identified Scenarios	Scenario Occurs?		Evaluation Criteria
	A_1	A_2	
SC-1	YES	NO	EC-1
SC-2	NO	YES	EC-2
SC-3	NO	YES	EC-3
SC-4	YES	YES	N/A

Comparing Centralized v.s. Decentralized ATM Architectures

Centralized Architecture



Decentralized Architecture



Evaluation Criteria	**Centralized Architecture**	**Decentralized Architecture**
Responsiveness of decisions in densely populated airspace	⊕	⊖
Ability to make appropriate decisions when multiple conflicts occur	⊕	⊖
Vulnerability of trajectory modifications when communications errors occur	⊖	⊕

⊕ Benefit ⊖ Tradeoff

Full details published in [Poh, Leveson, Neogi '24]

Evaluating Identified Evaluation Criteria

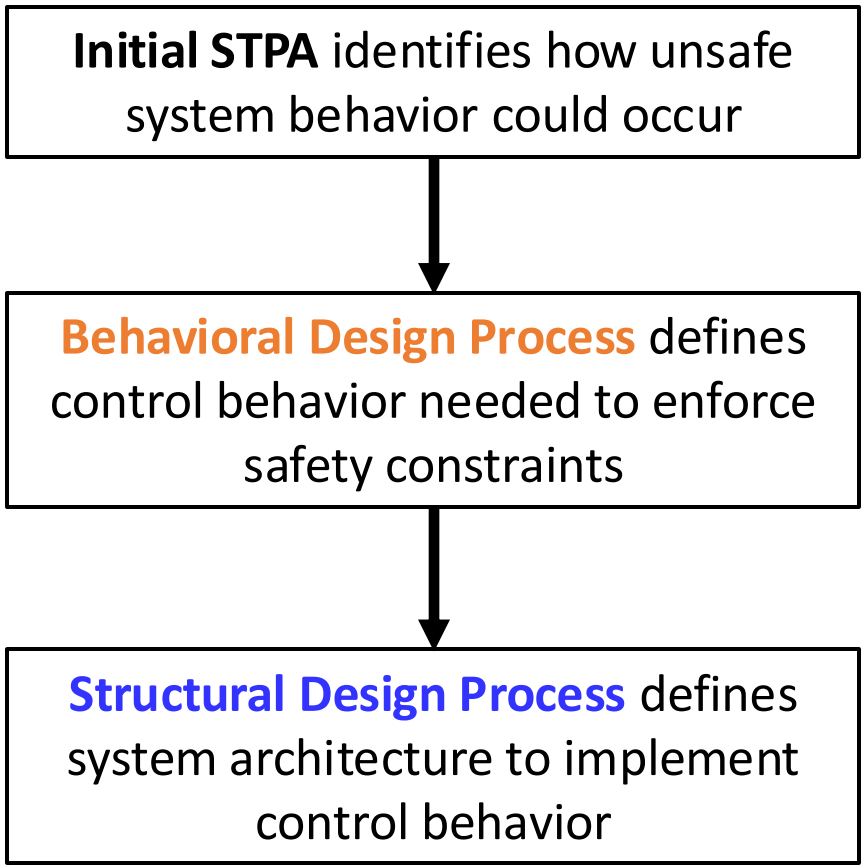
Compare benefits and tradeoffs found using this framework with those found in existing literature
[Xue '20], [Mondoloni et al '03]

Benefits/tradeoffs found using this framework: **19**
Benefits/tradeoffs found in existing literature: **9**

Control Aspect	Found In Existing Literature	Found Using This Framework
Decision Making	5	8
Process Models	1	3
Feedback and External Inputs	0	5
Control Path	3	3

- **More benefits and tradeoffs that cover more aspects of control**
- **STPA-based comparison is more focused on control-related differences and why they occur**

Summary



Research Objective: Develop a framework for developing system architectures that considers safety upfront

- Framework provides structured processes to enable **more informed early design decisions** driven by safety considerations
- STPA-based comparison of architecture options **focuses on control-related benefits and tradeoffs**

Questions?

justin@justinpoh.com

References

- Hill, Brian, Dwight DeCarme, Matt Metcalfe, Christine Griffin, Sterling Wiggins, Chris Metts, Bill Bastedo, Michael Paterson, and Nancy Mendoca. “UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4.” NASA, December 2, 2020.
- Leveson, Nancy. *Engineering a Safer World: Systems Thinking Applied to Safety*. Engineering Systems. Cambridge, Mass: MIT Press, 2011.
- N. Leveson and J. P. Thomas, “STPA Handbook.” Mar. 2018. [Online]. Available: psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- C. H. Fleming, “Safety-Driven Early Concept Analysis and Development,” MIT Department of Aeronautics and Astronautics, PhD Dissertation, Feb. 2015.
- N. Leveson, “An Improved Design Process for Complex Control-Based Systems Using STPA and a Conceptual Architecture,” MIT, White Paper, 2019.
- Poh, Justin. “A Systems-Theoretic Framework for Safety-Driven Development of System Architectures.” PhD Thesis, Massachusetts Institute of Technology, 2024.
- Xue, Min. “Urban Air Mobility Conflict Resolution: Centralized or Decentralized?,” 2020.
- Mondoloni, Stephane, Tamara Breunig, Steven Green, and Dan Kozarsky. “Distributed Air/Ground Traffic Management (DAG-TM) Benefit Mechanisms.” In *AIAA’s 3rd Annual Aviation Technology, Integration, and Operations (ATIO) Forum*. Denver, Colorado: American Institute of Aeronautics and Astronautics, 2003.
- Poh, Leveson, Neogi, "A Safety-Driven Approach to Exploring and Comparing Air Traffic Management Concepts for Enabling Urban Air Mobility", Proceedings of the International Conference on Research in Air Transportation (ICRAT), July 2024