Massachusetts Institute of Technology

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Using System Theoretic Process Analysis (STPA) for a Safety Trade Study

David Horney

MIT/U.S. Air Force

Safety-Guided Design

- Use STPA during the conceptual design process
- Iterate design using the STPA results
- Use STPA to compare hazards between possible architectures
- Use STPA safety requirements to guide design decisions

Background

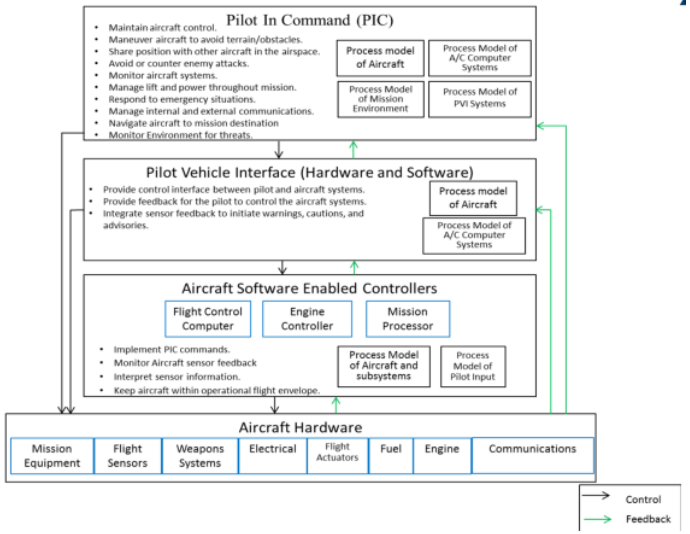
- New light transport for the military
- Capable of carrying 14 soldiers into combat
- Range of 800 nm
- Deliver troops and cargo to remote bases and land on unimproved runways
- Short takeoff and landing capabilities
- Travel in a tethered formation
  - Single crew must control three aircraft from takeoff to landing at improved airports with ILS (Instrument Landing System)

Overall STPA Workflow

1. Define Accidents/ Hazards → 2. Model Control Structure → 3. Identify Unsafe Control Actions → 4. Identify Causal Scenarios → 5. Derive Safety Requirements

High Level Hazards

Hazard	Constraint
H1: Violation of minimum separation standards (M1, M2, M3)[H1] [ICD 216]	The aircraft must maintain minimum separation from potential sources of collision.
H2: Inability to control the aircraft (M1, M2, M3) [ICD 216]	The aircraft must be controllable by the pilot or piloting function in an OPV (optionally piloted vehicle) at all times.
H3: Loss of airframe integrity (M1, M2, M3) [ICD 216-217]	There must not be a loss of airframe integrity during flight.



Unsafe Control Actions (UCAs)

PIC to Flight Controls

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Incorrect Order	Stopped Too Soon/ Applied Too Long
1.Set Aircraft Attitude	UCA 1.1: The PIC does not set aircraft attitude when the trimmed aircraft state is causing the aircraft to deviate from its flight plan. (H1)	UCA 1.2: The PIC sets an incorrect aircraft attitude causing the aircraft to violate separation minimums. (H1, H2) UCA 1.3: The PIC sets an aircraft attitude that is not achievable. (H2)	UCA 1.4: The PIC changes aircraft attitude at a rate that will damage the airframe. (H3)	UCA 1.5: The PIC changes the aircraft attitude at too high or too small a magnitude when there is an obstacle nearby. (H1) UCA 1.6: The PIC changes aircraft attitude too much or too little when the aircraft is close to its flight limits. (H2)

Derive Safety Requirements

Example requirements derived from the above scenarios:

a. Navigation systems and interfaces shall allow for navigation with error less than TBD miles in manual flight mode

Causal Scenarios

UCA 1.1: *The PIC does not set aircraft attitude when the trimmed aircraft state is causing the aircraft to deviate from its flight plan.* (H1)

Example Causal Scenarios for UCA 1.1a: The PIC does not set aircraft attitude when the trimmed aircraft state is causing the aircraft to deviate from its flight path because the PIC believes that the aircraft is on the desired flight path. This could occur if:

1. The PIC does not receive detailed enough feedback through the PVI to detect small deviations from the flight plan. These small deviations become greater over time and the aircraft could violate separation with an obstacle. This problem can be compounded in tethered scenarios where the PIC is responsible for multiple vehicles and cannot easily check clearances for the tethered vehicles.

Define Mishaps

Mishap 1: Loss of or damage to the aircraft or equipment on the aircraft

Mishap 2: Serious injury or fatality to personnel

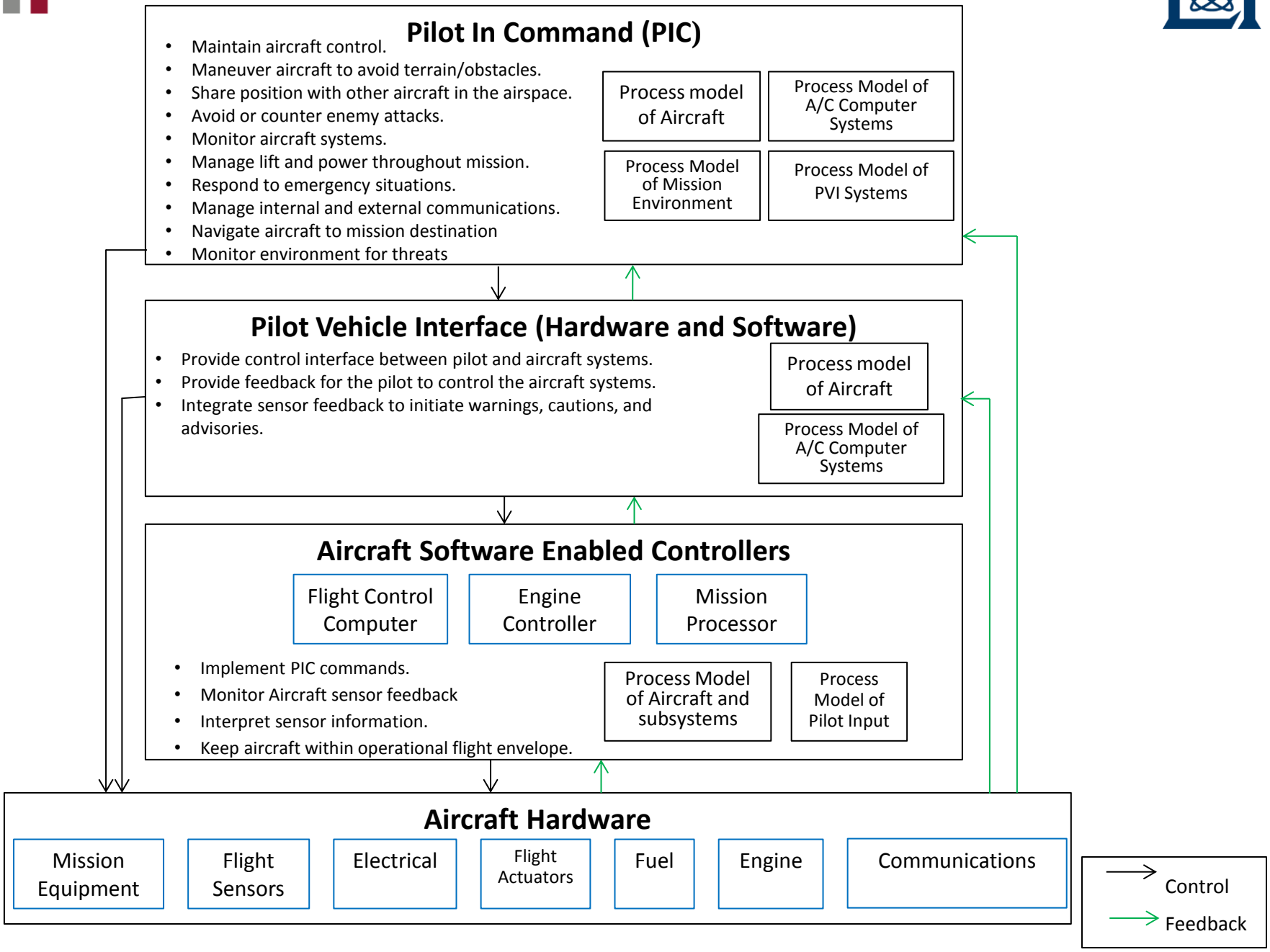
Mishap 3: Inability to complete the mission

* Not listed in order of criticality

Define Hazards

Hazard	Constraint
H1: Violation of minimum separation standards (M1, M2, M3)	The aircraft must maintain minimum separation from potential sources of collision.
H2: Inability to control the aircraft (M1, M2, M3)	The aircraft must be controllable by the pilot or piloting function in an OPV (optionally piloted vehicle) at all times.
H3: Loss of airframe integrity (M1, M2, M3)	Airframe integrity must not be lost during flight.

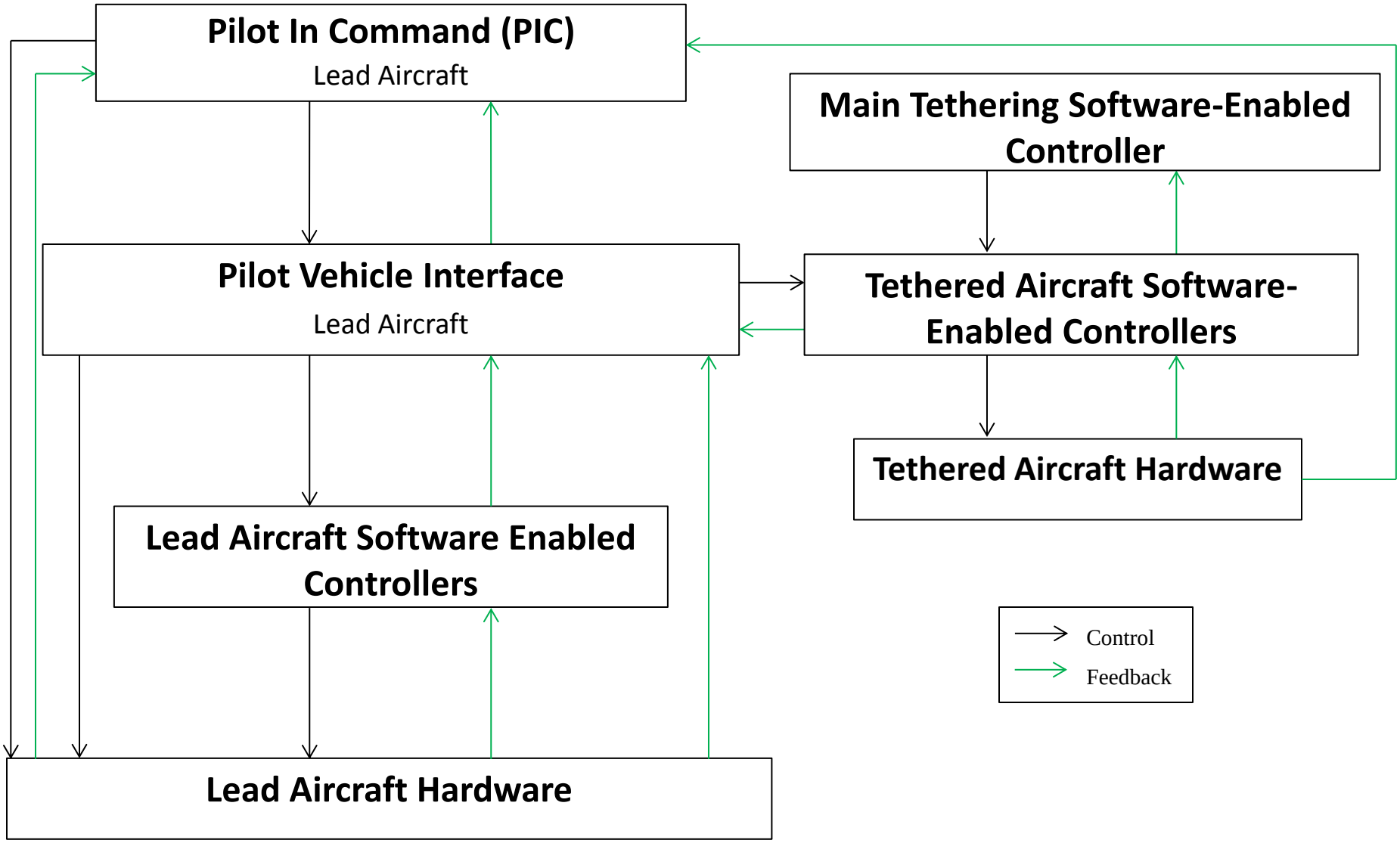
Model Control Structure



General Tethering Requirements

- Tethered aircraft must fly together in a formation
- The lead PIC must know where all of the aircraft are
- Formation must be appropriate for environment and phase of flight

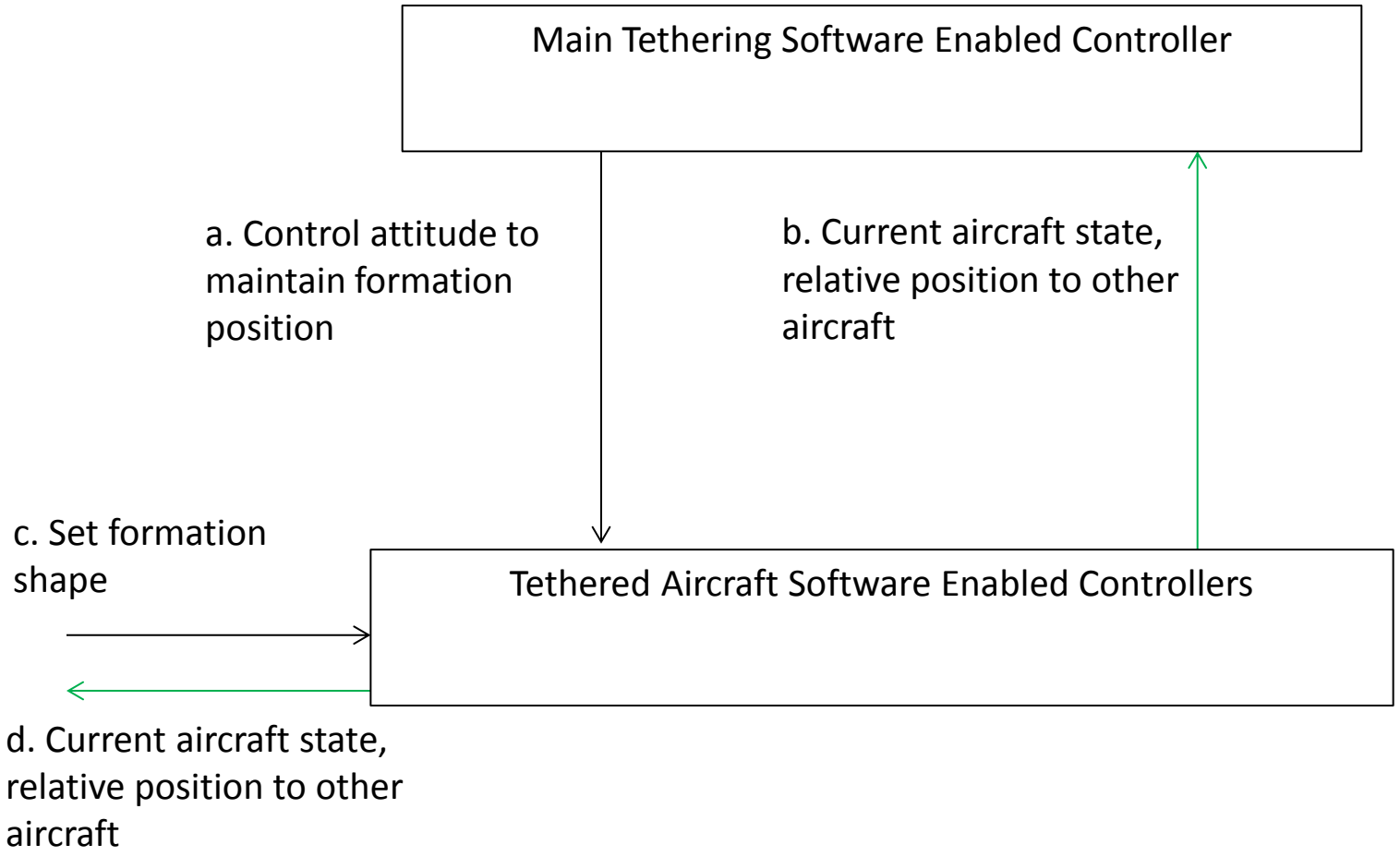
Control Structure Focused on Tethering



Potential Architecture 1

- Human lead PIC determines formation shape
- There are preset formations to choose from
- Tethered aircraft conform to the formation specified by the lead

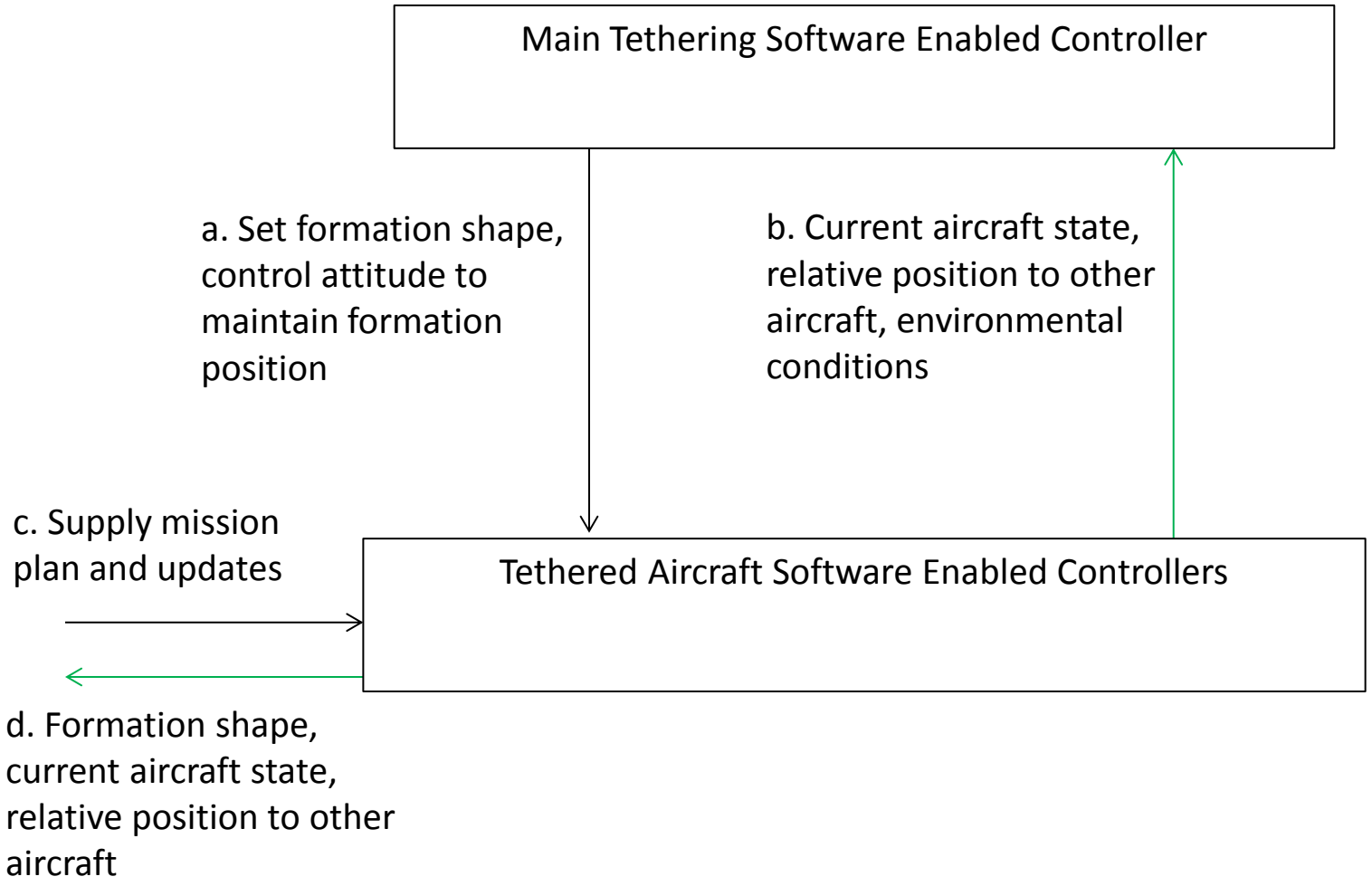
Control Structure for A1



Potential Architecture 2

- Tethered aircraft determine the best formation
- Tethered aircraft agree on a formation and maintain formation shape
- Formation is communicated to lead PIC
- Formation based on shared sensor information

Control Structure for A2



Identify Unsafe Control Actions (UCAs): A1

Controller: Lead A/C PIC
Controlled Process: Tethered A/C

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Incorrect Order	Stopped Too Soon/ Applied Too Long
Set Formation Shape	**UCA 1.1: The lead aircraft PIC does not set a new formation shape when needed. (H1, 2)**	**UCA 1.2: The lead aircraft PIC sets an unsafe formation shape for the current environment. (H1, 2)**	N/A	N/A

Define UCAs: A2

Controller: Main Tethering Software Enabled Controllers
Controlled Process: Tethered Aircraft Software Enabled Controllers

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Incorrect Order	Stopped Too Soon/ Applied Too Long
Set Formation Shape	UCA 2.1: The tethered A/C are unable to agree on a formation shape and none is set. (H1, 2) UCA 2.2: The tethered A/C do not provide the formation shape to the lead PIC. (H1, H2)	UCA 2.3: The tethered aircraft set an unsafe formation shape for the current environment. (H1, 2) UCA 2.4: Multiple tethered aircraft set different formation shapes in unison and maneuver into the disparate formations. (H1, H2)	UCA 2.5: The tethered A/C respond to the new formation shape at different times. (H1, 2) UCA 2.6: The tethered A/C do not have an accurate mission plan and set a formation for the incorrect phase of flight. (H1, 2) UCA 2.7: The tethered aircraft change formation shape too frequently making it difficult for the lead PIC to keep an up to date process model of the formation. (H1, H2)	N/A

Comparison

- A2 has more UCAs than A1 due to coordination and communication requirements
- Must communicate with PIC who is ultimately responsible
- More UCAs does not necessarily mean more dangerous

Identify Causal Scenarios: A1

UCA 1.1: Lead aircraft PIC does not set a new formation shape when needed. (H1,2)

Causal Scenario 1.1a: Lead aircraft PIC does not set a new formation shape when needed because the PIC believes current formation shape is sufficient:

1. Lead aircraft PIC is not able to predict future states of the formation and therefore does not know that a new formation shape is needed to avoid a conflict or unsafe flight configuration.
2. Lead aircraft PIC is task saturated and cannot generate an accurate process model of the entire tethered formation and the environment they are operating in.
3. Insufficient feedback from the tethered aircraft for lead aircraft PIC to determine best formation shape.
4. Malformed feedback from tethered aircraft misleads aircraft PIC. This may be in the form of incorrect position information, dropped feedback, communication with tethered aircraft has been lost, or malformed data that is not displayable by system.

Identify Safety Requirements: A1

Example Requirements:

a. The lead aircraft PIC shall be provided with feedback to predict future states of the formation. Because predicting future states of multiple vehicles is a difficult cognitive task, predictive aids will likely be required.

b. Studies shall be performed to determine how pilots will respond while flying a formation with tethered aircraft. The system shall be designed to keep the workload within the PIC's capabilities even during emergency situations.

c. The tethered aircraft shall supply feedback indicating position and velocity as well as relative position to other aircraft to the lead PIC to allow the lead PIC to make informed decisions about the formation.

d. System shall indicate to PIC current communication status between lead aircraft and tethered aircraft.

e. The system shall indicate the last known good information, and corresponding age of information to the PIC in the lead aircraft.

Identify Causal Scenarios: A1

Causal Scenario 1B: The PIC sets a safe formation shape for the tethered formation but it is not correctly implemented or followed. This could occur if:

1. There is a failure of the flight controls or their connection to the software based PVI.
2. There is a miscommunication between the software based PVI and the mission computer which is responsible for communicating with the tethered vehicles.
3. There is a hardware failure in the communication link between the lead aircraft and the tethered vehicles.
4. There is a malfunction in one or more of the tethered vehicles that does not allow them to reach the desired formation shape.
5. There is a delay in the control path causing the new formation shape to be implemented too late.
6. Malfunction in the communications between the PIC and tethered aircraft.
7. Compromised control path drops, interferes with, or manipulates the PIC commands to the mission system and/or tethered aircraft, despite receiving feedback that a new formation was commanded.

Identify Requirements: A1

Example Requirements:

a. The WCAAS shall alert the PIC if one of the tethered vehicles is operating in a degraded condition.

b. There shall be independent backup communication systems that can be used to maintain communication within the formation in case the primary communication channels are lost.

c. Each aircraft shall have an independent loss of link plan that corresponds to its position in the formation and allows it to exit the formation safely.

d. There shall be adequate sensors on each aircraft to allow them to safely navigate the airspace to a safe landing position without control by the lead aircraft.

e. Each tethered aircraft shall have a loss of link plan that is updated throughout the mission, which allows for the aircraft to safely land as soon as possible.

f. All aircraft shall be able to autonomously coordinate with other air traffic to avoid conflict.

g. All aircraft shall be able to find a suitable landing spot in unfamiliar areas.

h. The tethered vehicles shall send a message to the lead aircraft when they receive and act on commands. If a confirmation message isn't received within TBD seconds, the PIC must be alerted.

Identify Causal Scenarios: A2

UCA 2.1: The tethered A/C are unable to agree on a formation shape and none is set. (H1, 2)

Causal Scenario 2.1a: The tethered A/C are unable to agree on a formation shape because they have different process models of the environment. This could occur if:

1. The tethered A/C each rely on their individual sensor information to create a model of the environment and determine the best shape for the formation.
2. The tethered A/C do not send feedback to the other A/C about formation priority rankings.
3. The feedback from the aircraft cannot be compiled into a coherent model of the formation due to missing information because of failed sensors, bad weather, or improperly calibrated instruments.

Identify Safety Requirements: A2

Example Requirements:

a. Sensor data from all aircraft in the formation shall be compiled to create a more complete model of the formation.
b. Tethered aircraft shall include in the feedback the formation priority rankings.
c. A/C shall have sensors that can determine precise position and velocity in degraded conditions.
d. There shall be backup methods of determining position and velocity and communicating state data between A/C.
e. Instruments shall be checked for proper calibration before flight.

Component	Comparison
Lead PIC Process Model	Architecture 1 (A1) involves the PIC more and thus their process model is more likely to be updated if the formation changes. Requiring the PIC to choose the shape invests them more in the tethering activity, likely increasing situational awareness. (SA)
Tethered A/C Process Models	Both architectures should have the same general process model for the tethered A/C. It is possible that requiring the tethered A/C to make piloting decisions would result in a more robust sensor system and process model as design plays out.
Lead PIC Workload	A2 would not require the lead PIC to perform as many tasks but the number of tasks assigned is not necessarily the cause of high workload. Experiments should be done to compare workload between the architectures.
Hardware	The hardware should be the same. As stated above, requiring tethered A/C to perform processing tasks could affect the hardware choices.
Software Design	Certifying tethered A/C to make piloting decisions would require more stringent software development. As seen in the analysis, A1 would still require the tethered A/C to make individual piloting decisions in case of an emergency.
Airspace Certification	Agencies such as the FAA should be consulted to determine if there would be differences in the certification processes for A1 and A2.

Conclusions

- STPA can be used for safety in architecture trade studies
- The time required is minimal; approximately one day for a single person
- Results can be used to create test/simulation studies to learn more about human behavior in these architectures
- Provides more utility than PHL/PHA – demonstrates safety impact of design decisions