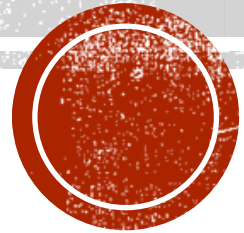
STPA APPLIED TO ROTORCRAFT FLIGHT CONTROLS



MIT STAMP WORKSHOP 2024

Presented by:

Dr John Thomas (MIT)
Rodrigo Rose (MIT)
Dave Cummins (Bell Textron Inc)

ROTORCRAFT FLIGHT CONTROL

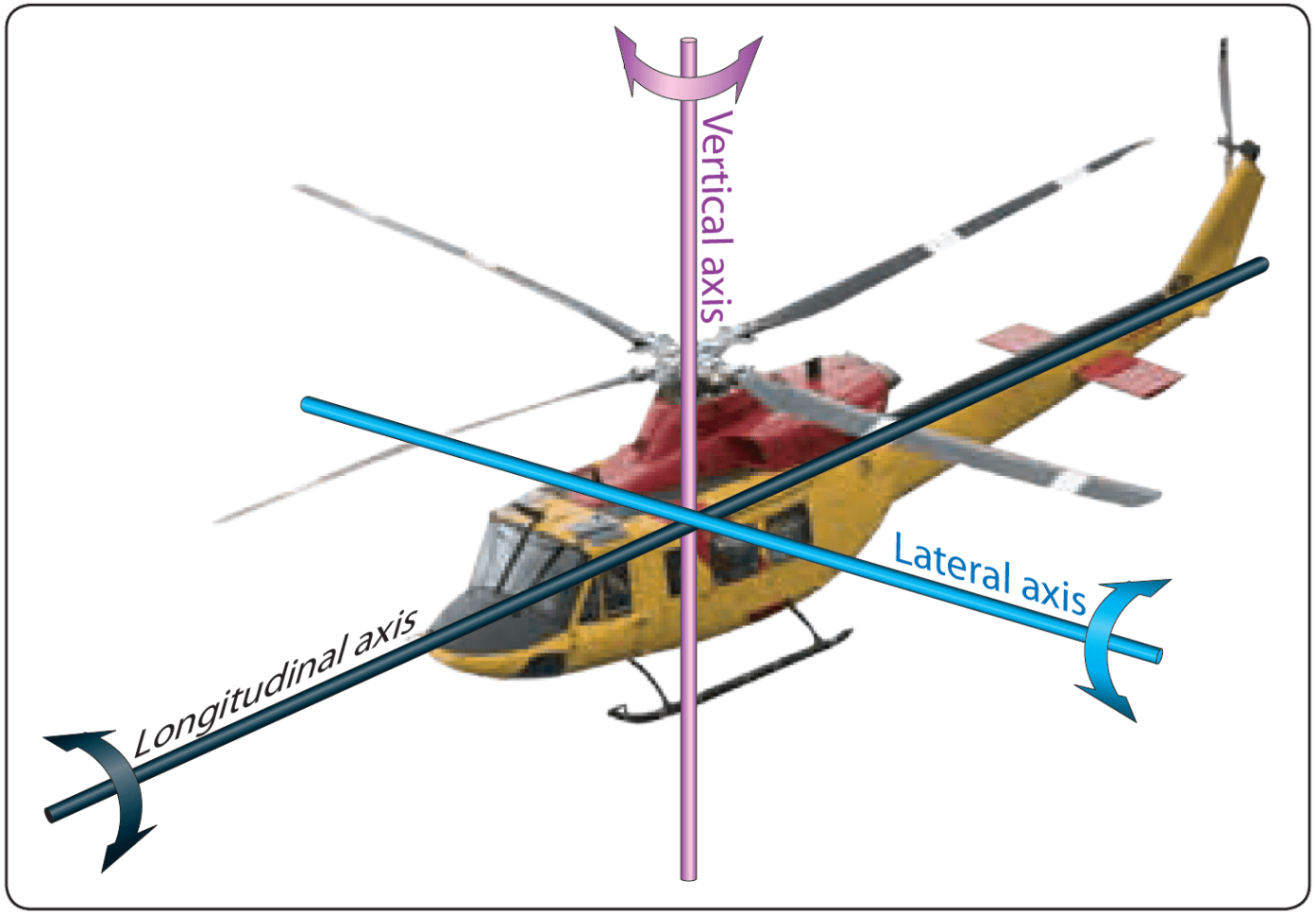


Image ref: Aviation Maintenance, Helicopter Aerodynamics – Aircraft Theory of Flight

Translational movement

CLIMB / DESCENT = translation in the vertical axis

FWD FLIGHT / REARWARD FLIGHT = translation in the longitudinal axis

SIDESLIP = translation in the lateral axis

Rotational movement

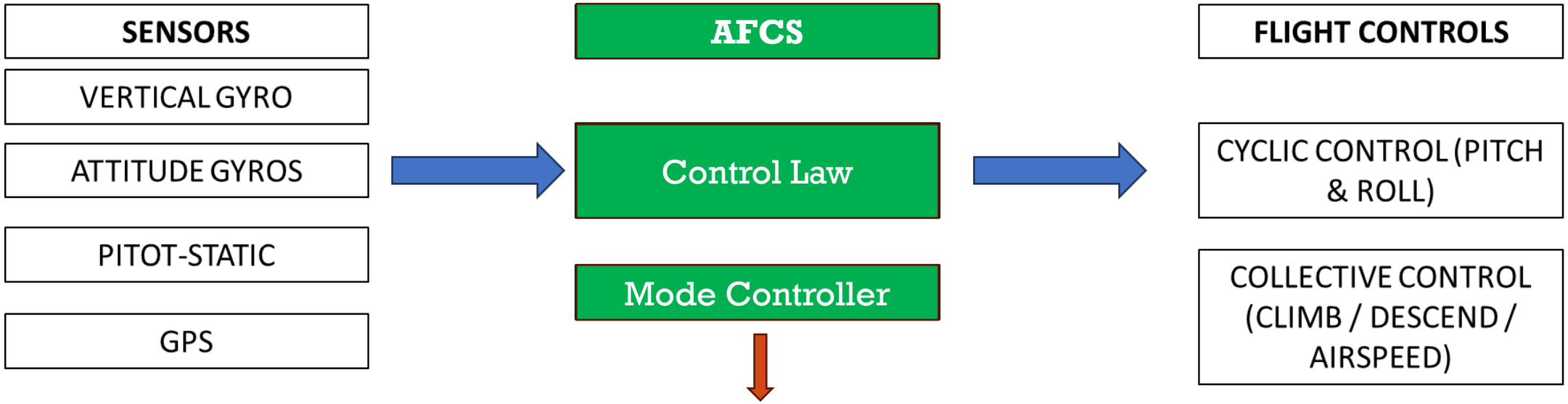
YAW = rotation about vertical axis

PITCH = rotation about lateral axis

ROLL = rotation about longitudinal axis

HELICOPTER AFCS

AUTOMATIC FLIGHT CONTROL SYSTEM (AFCS)



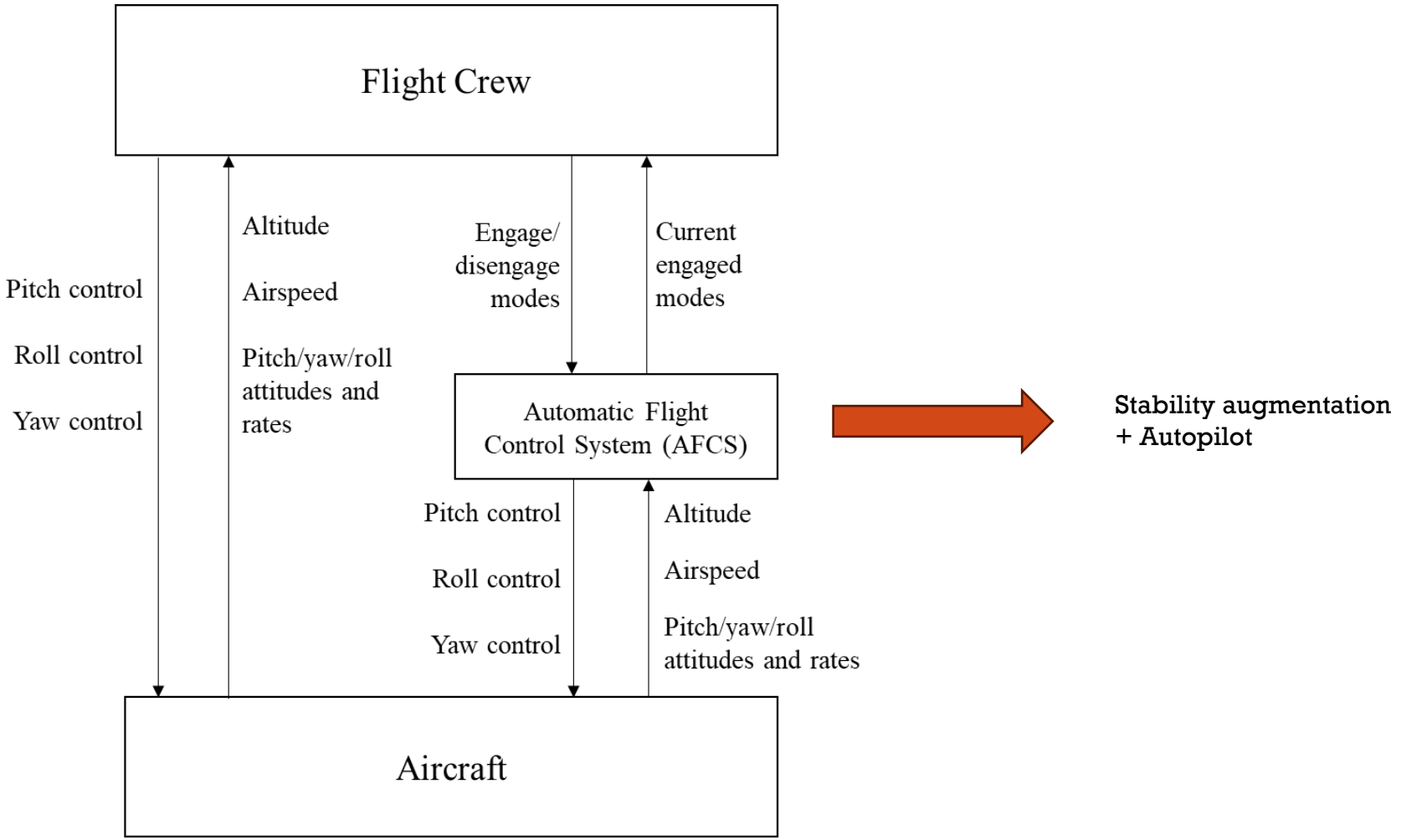
Some Basic Autopilot Modes:

- Hold Airspeed (IAS Hold) - pitch and collective trim
- Hold BarAlt (BarAlt Hold) - pitch and collective trim
- Heading Hold – rudder trim
- Transition up – collective trim
- Transition down – collective trim
- Flight Director – follow preset course, and holds

STPA STEP 1

- Loss L1 - Loss of life or serious injury to aircraft occupants
- Loss L2 - Destruction or physical damage to aircraft structure
- Hazard H1 - Aircraft is uncontrollable [L1, L2]
- Hazard H2 - Aircraft does not maintain adequate separation from terrain and other objects [L1, L2]

STPA STEP 2: HIGH-LEVEL CONTROL STRUCTURE



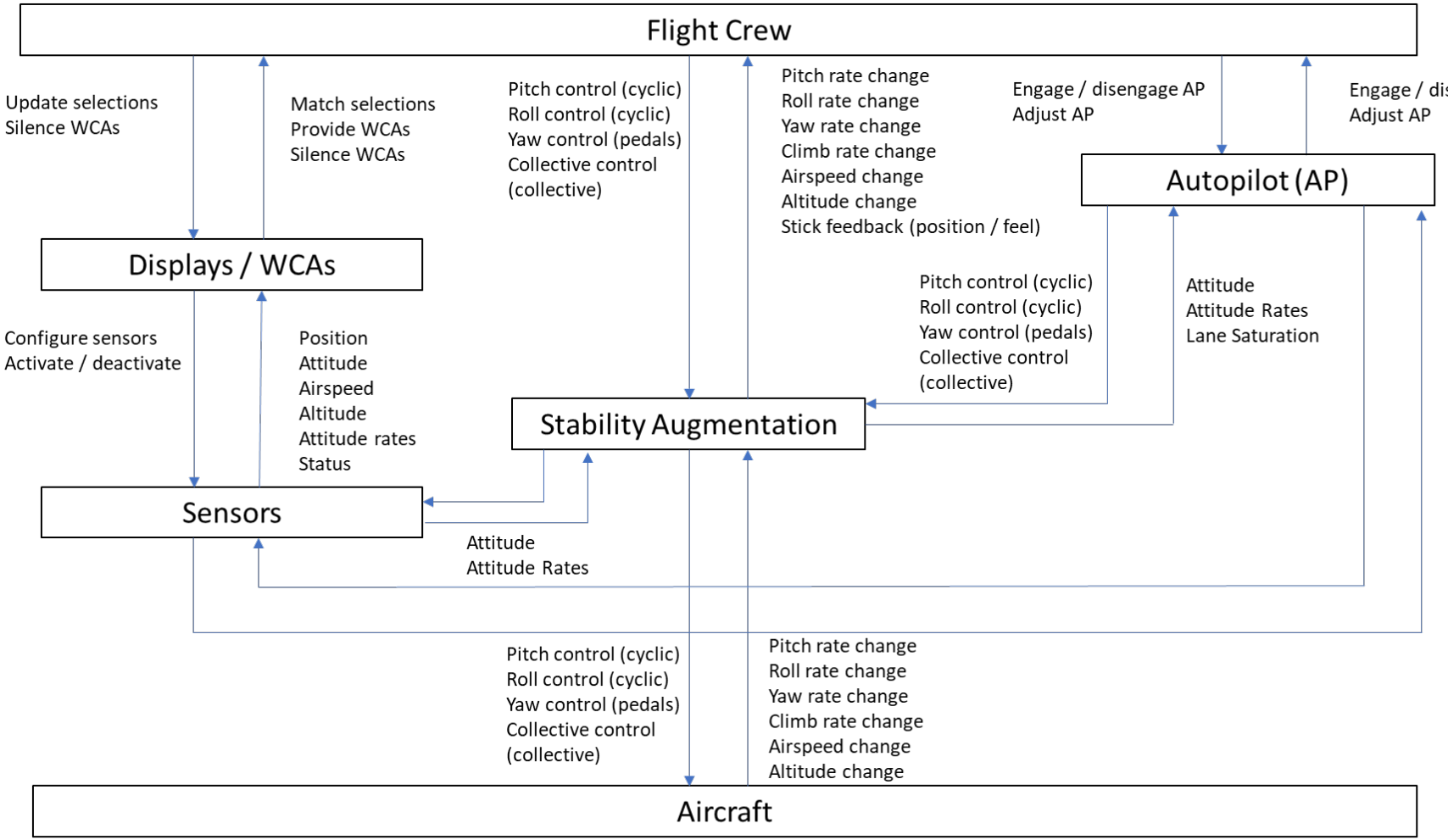
STPA STEP 2A: DETAILED CONTROL STRUCTURE

Could the AFCS commands conflict with those of the crew and reduce authority at a critical time?

Will the AFCS disengage a mode when the flight crew make selections / control input?

How could the flight crew not provide sufficient control input?

Are the flight crew sufficiently aware of the AP modes engaged or the level of control authority that they have at any point in time during flight?



AFCS UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	…	**UCA-1:** AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, Etc.]	**…**	…
Disengage IAS Hold mode	**UCA-2:** AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]	…	…	…

Flight Crew UCAs

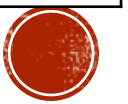
Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	**UCA-3:** Flight crew does not provide sufficient positive pitch commands when aircraft pitch is insufficient to maintain flight. [H1, H2, etc.]	…	…	…
Disengage IAS Hold mode	**UCA-4:** Flight crew does not disengage an AFCS Basic FD Mode when the constraints enforced by that mode interfere with crew flight control inputs [H1, H2, etc.]	…	…	…
Provide sensor calibration	...	**UCA-5:** Flight crew provides incorrect sensor calibration to aircraft forcing unexpected control res ponse through AFCS [H1, H2, etc].	...	...

AFCS UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	…	**UCA-1:** AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, Etc.]	…	…
Disengage IAS Hold mode	**UCA-2:** AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]	…	…	…

Flight Crew UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	**UCA-3:** Flight crew does not provide sufficient positive pitch commands when aircraft pitch is insufficient to maintain flight. [H1, H2, etc.]	…	…	…
Disengage IAS Hold mode	**UCA-4:** Flight crew does not disengage an AFCS Basic FD Mode when the constraints enforced by that mode interfere with crew flight control inputs [H1, H2, etc.]	…	…	…
Provide sensor calibration	...	**UCA-5:** Flight crew provides incorrect sensor calibration to aircraft forcing inadequate control response through AFCS [H1, H2, etc].	...	...



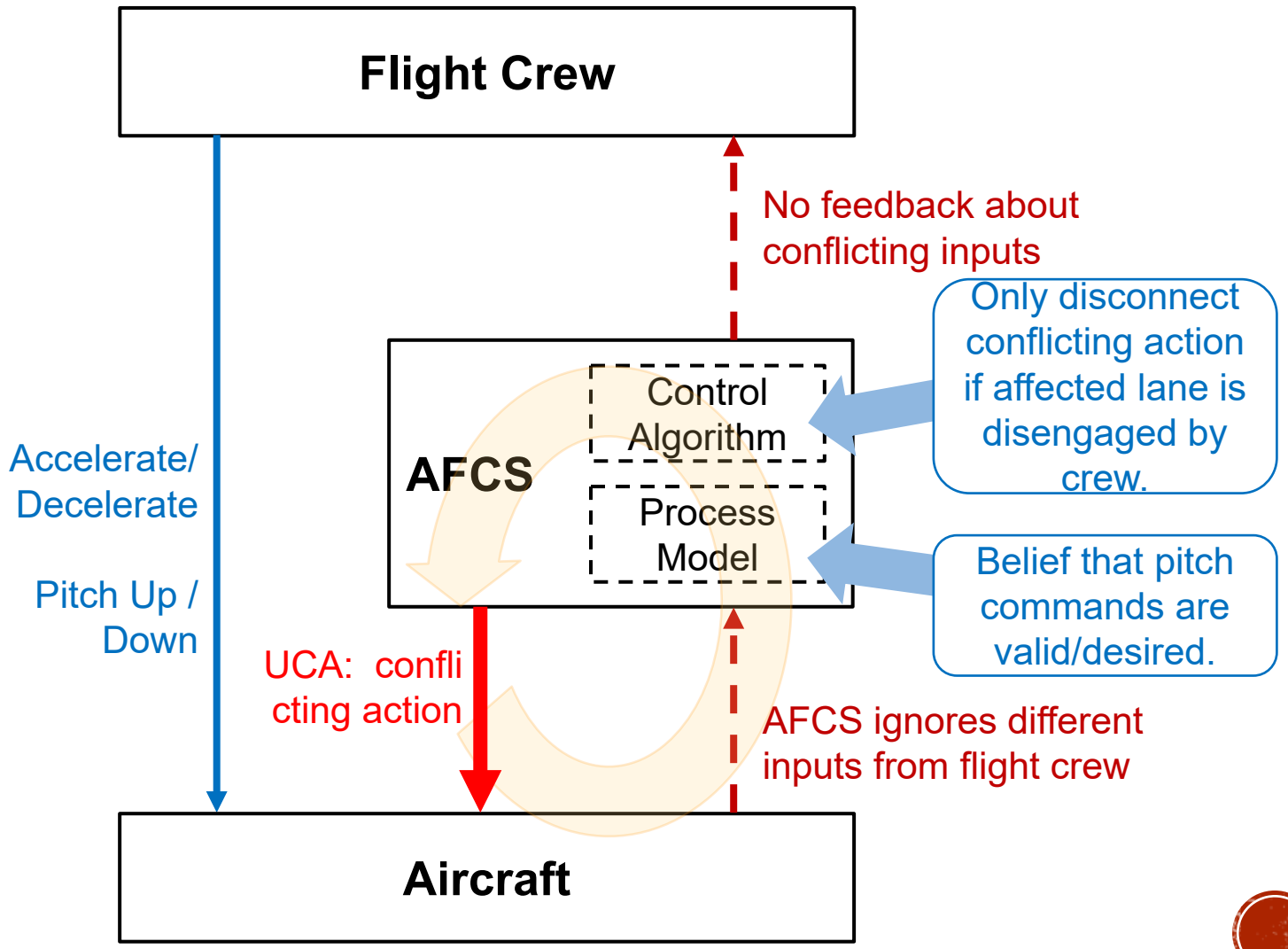
STPA STEP 4: UCA-1 SCENARIOS (1 OF 2)

UCA-1: AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, etc.]

Scenario 1.1: AFCS may provide pitch commands due to a failure or malfunction of the AFCS IAS Hold function.

Scenario 1.2: AFCS may believe that conflicting pitch commands are necessary due to the selected flight mode.

Scenario 1.3: AFCS may believe that conflicting pitch commands are necessary in response to other manual flight control inputs (e.g., pitch, roll, yaw).



STPA STEP 4: UCA-1 SCENARIOS (2 OF 2)

UCA-1: AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, etc.]

Scenario 1.1: AFCS may provide pitch commands due to a failure or malfunction of the AFCS IAS Hold function.

Requirement 1.1.1: The AFCS shall audibly and visually alert flight crew to any detected failure scenario or malfunction.

Requirement 1.1.2: The AFCS shall automatically disengage a failed lane and alert the flight crew to its disengagement.

Scenario 1.2: AFCS may believe that conflicting pitch commands are necessary due to the selected flight mode.

Requirement 1.2.1: AFCS shall automatically stop enforcing airspeed constraint in response to flight control input from flight crew that opposes the constraint by TBD.

Requirement 1.2.2: AFCS shall audibly and visually alert non-enforcement of airspeed constraint.

Scenario 1.3: AFCS may believe that conflicting pitch commands are necessary in response to other manual flight control inputs (e.g., pitch, roll, yaw).

Requirement 1.3.1: AFCS-commanded pitch adjustments shall not exceed TBD at any time.

Requirement 1.3.2: AFCS shall limit pitch adjustments to TBD when manual pitch commands above TBD are provided.

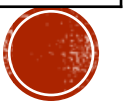
Requirement (all!) The flight manual shall include a complete and full description of AFCS functionality, stability augmentation, and hold mode engagement and disengagement criteria. The flight crew shall be routinely trained in the use of the AFCS and AFCS emergencies in the simulator.

AFCS UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	…	**UCA-1:** AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, Etc.]	**…**	…
Disengage IAS Hold mode	**UCA-2:** AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]	…	…	…

Flight Crew UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	**UCA-3:** Flight crew does not provide sufficient positive pitch commands when aircraft pitch is insufficient to maintain flight. [H1, H2, etc.]	…	…	…
Disengage IAS Hold mode	**UCA-4:** Flight crew does not disengage an AFCS Basic FD Mode when the constraints enforced by that mode interfere with crew flight control inputs [H1, H2, etc.]	…	…	…
Provide sensor calibration	...	**UCA-5:** Flight crew provides incorrect sensor calibration to aircraft forcing inadequate control response through AFCS [H1, H2, etc].	...	...



STPA STEP 4: UCA-2 SCENARIOS

UCA-2: AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]

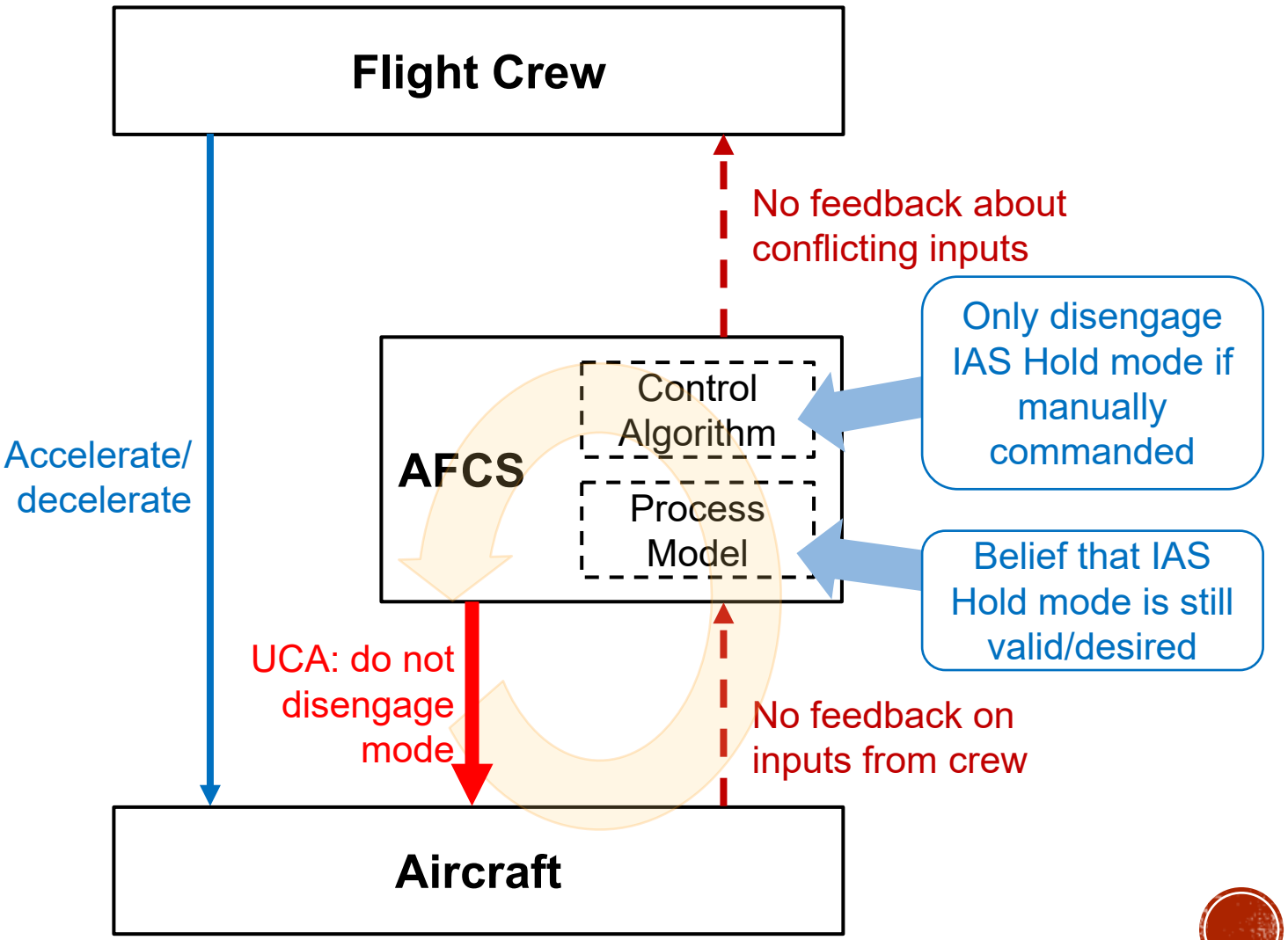
Scenario 2.1: AFCS believes the previously selected flight mode (e.g., IAS Hold) is still valid (PM-2.1.1). The AFCS does not consider flight control inputs from crew (CA-2.1.2) when determining mode transitions (e.g., disengage IAS Hold).

Requirement 2.1.1: AFCS shall automatically disengage IAS Hold in response to >TBD rapid rate primary flight control input from crew.

Requirement 2.1.2: AFCS shall automatically disengage IAS Hold in response to >TBD large primary flight control input from crew.

Requirement 2.1.3: AFCS shall automatically disengage IAS Hold in response to >TBD conflicting primary flight control input from crew.

Requirement 2.1.4: AFCS shall audibly and visually alert flight crew of >TBD conflicting primary flight control inputs.



STPA STEP 4: UCA-2 SCENARIOS

UCA-2: AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]

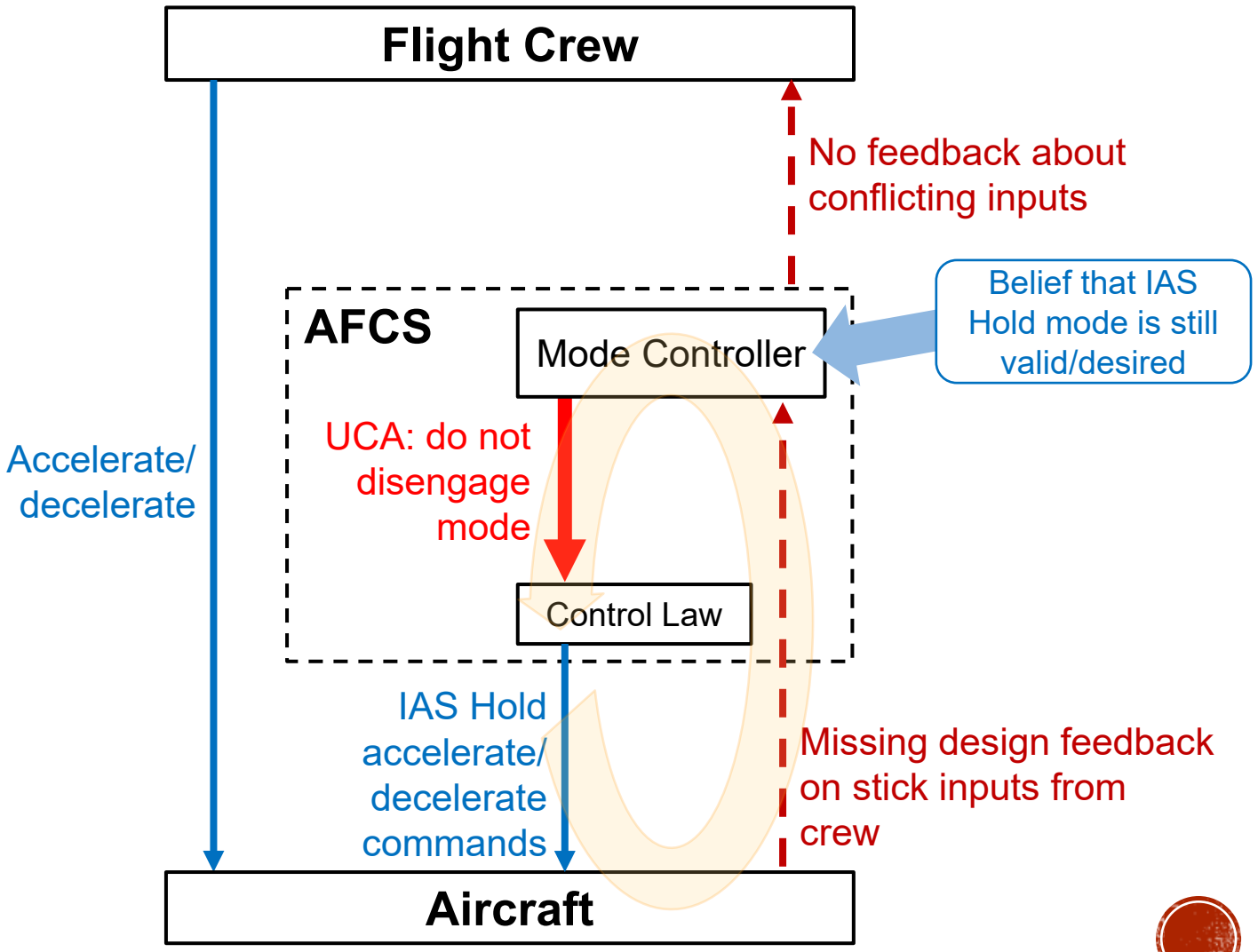
Scenario 2.1: AFCS believes the previously selected flight mode (e.g., IAS Hold) is still valid (PM-2.1.1). The AFCS does not consider flight control inputs from crew (CA-2.1.2) when determining mode transitions (e.g., disengage IAS Hold).

Requirement 2.1.1: AFCS shall automatically disengage IAS Hold in response to >TBD rapid rate primary flight control input from crew.

Requirement 2.1.2: AFCS shall automatically disengage IAS Hold in response to >TBD large primary flight control input from crew.

Requirement 2.1.3: AFCS shall automatically disengage IAS Hold in response to >TBD conflicting primary flight control input from crew.

Requirement 2.1.4: AFCS shall audibly and visually alert flight crew of >TBD conflicting primary flight control inputs.



AFCS UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	…	**UCA-1:** AFCS provides pitch commands when the pitch commands conflict with manual flight control inputs from the flight crew. [H1, H2, Etc.]	**…**	…
Disengage IAS Hold mode	**UCA-2:** AFCS does not disengage IAS Hold mode when flight crew attempts to overcome IAS Hold mode commands. [H1, H2, etc.]	…	…	…

Flight Crew UCAs

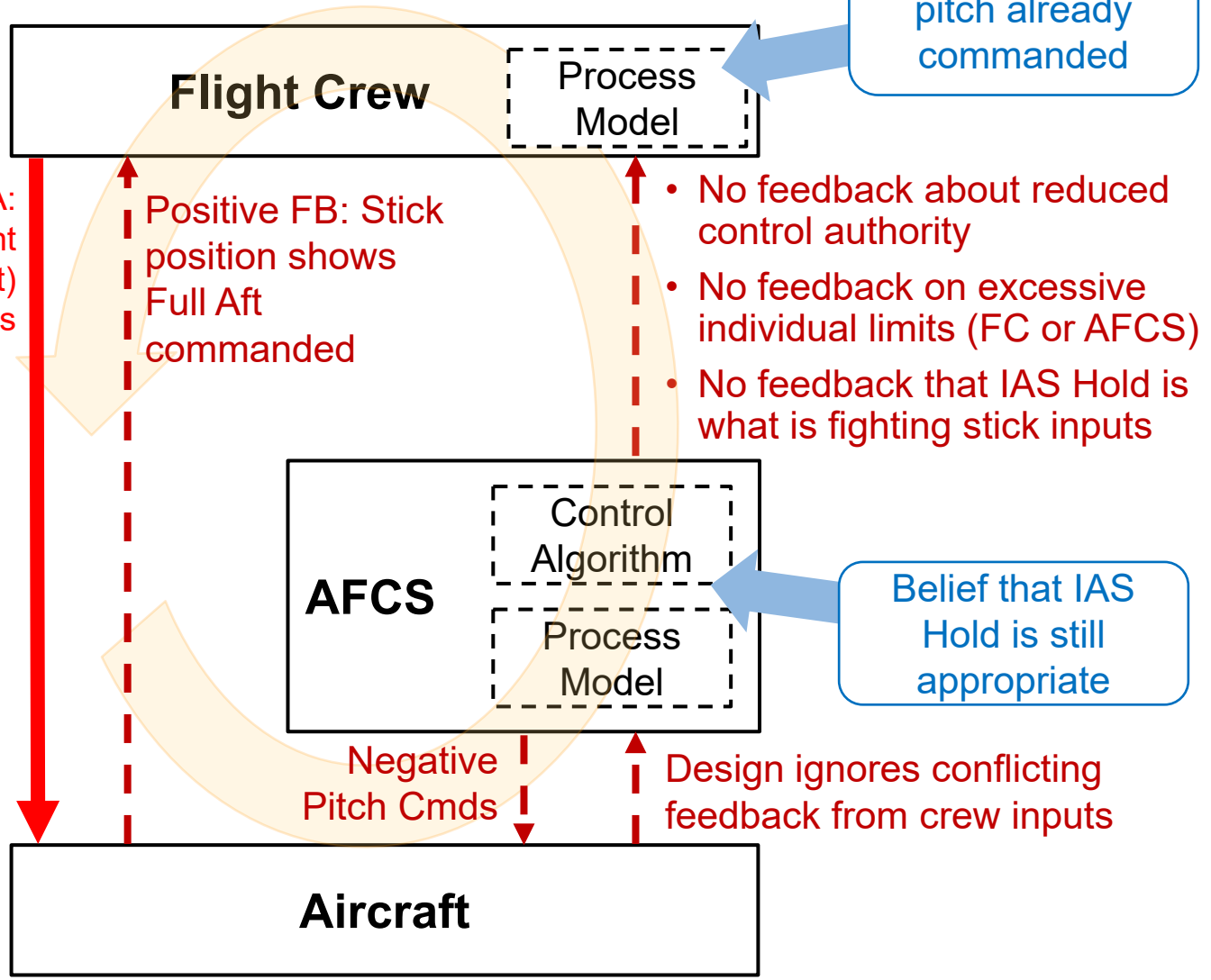
Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide pitch commands	**UCA-3:** Flight crew does not provide sufficient positive pitch commands when aircraft pitch is insufficient to maintain flight. [H1, H2, etc.]	…	…	…
Disengage IAS Hold mode	**UCA-4:** Flight crew does not disengage an AFCS Basic FD Mode when the constraints enforced by that mode interfere with crew flight control inputs [H1, H2, etc.]	…	…	…
Provide sensor calibration	...	**UCA-5:** Flight crew provides incorrect sensor calibration to aircraft forcing inadequate control response through AFCS [H1, H2, etc].	...	...

STPA STEP 4: UCA-3 SCENARIOS

- **UCA-3:** Flight crew does not provide sufficient positive pitch commands when aircraft pitch is insufficient to maintain flight. [H1, H2, etc.]

Scenario 3.1: Crew believe they are already commanding maximum positive pitch (PM-3.1.1). Why?

- FB: The crew's beliefs are informed by the position of the manual controls as well as audible/visual warnings (FB-3.1.2).
- Positive FB: The manual controls may be in the full aft (pitch up) position, confirming the crew's belief.
- Missing FB: Audible and visual warnings regarding control authority will not sound if the total commanded pitch (AFCS plus Crew) does not exceed TBD (DM-3.1.3).
- Missing FB: There are no audible or visual warnings associated with conflicting AFCS IAS Hold pitch commands (missing functionality)
- Missing FB: There is no indication of a significantly diminished manual control authority due to AFCS IAS Hold behavior (missing functionality).



FINDINGS FROM STPA

Key Finding:

STPA provides a simplistic methodology for active discussion with SMEs.

In doing so, we can really bring the rest of the Engineering and operator community into the safety discussion.

The language and paperwork barrier is much reduced!

Traditional Failure-based Requirements

- **Independence Requirements**: Use independent AFCS collective, pitch, roll, yaw lanes. Use triple redundant AFCS computers.
- **Probability**: Probability of AFCS runaway shall be 1E-9 failures per hour or less.
- **Software:** AFCS computer software and programmable hardware shall be developed to DAL A.
- **Weakest link**: failure of redundant AFCS computers and inability to disengage affected control lanes.
  - Solution: monitoring and voting between AFCS computers.

- **Conclusion:** AFCS loss and malfunction is extremely improbable.

Results from FHA, FTA, FMEA, Etc.

Requirements from STPA

- **Requirement 3.1.3**: AFCS shall ensure that a minimum of TBD control authority is allocated to manual pitch controls at all times.
- **Requirement 3.1.4:** AFCS shall automatically disengage IAS Hold in response to rapid rate primary flight control input from crew.
- **Requirement 3.1.5:** AFCS shall automatically disengage IAS Hold in response to large scale primary flight control input from crew.
- **Requirement 3.3.1:** AFCS shall automatically disconnect IAS Hold when manual pitch controls >TBD conflict with IAS Hold pitch controls >TBD.
- **Requirement 3.2.1:** AFCS shall audibly and visually alert any disarm of IAS Hold mode.
- **Requirement 3.2.2:** AFCS shall audibly and visually alert any failure of IAS Hold mode.

New functionality needed

Conclusion: AFCS is missing critical functionality to mitigate UCAs and hazards.

New feedback needed

CONCLUSIONS

- STPA enabled quick identification of intended and unintended functionality that was unsafe
  - Not just examine failures of intended functions.
- While not complete in this example, time to perform STPA on some critical functions was substantially lower than traditional analysis.
  - Time to perform typical FHA on these elements may be very substantial – of the order weeks-months.
- These kinds of insights are typically found during flight test, which is late and expensive to fix
- A common approach is to increase the level of engineering rigor to deal with possible errors
  - This approach (STPA) identified exact flaws so they can be prevented