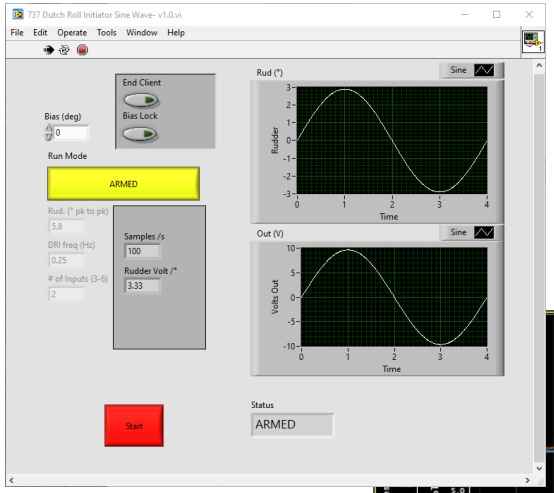
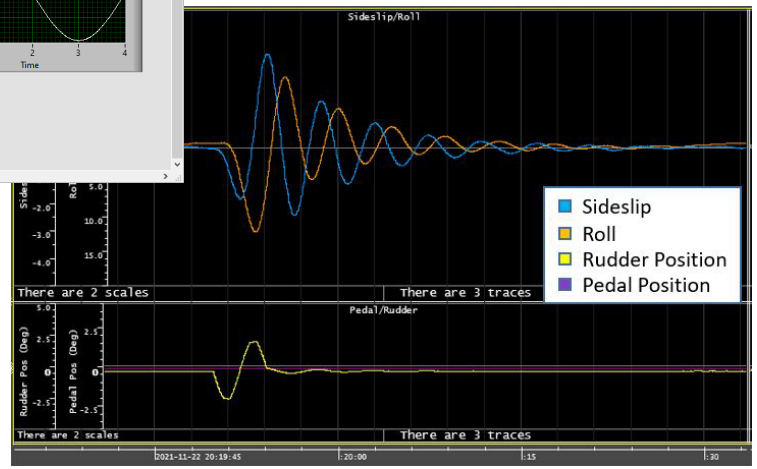
Unsafe Control Actions in the Time Domain

A technique for visualizing UCA problem space

STPA in Commercial Experimental Flight Test

- Boeing Projects
  - New test hardware
    - Dutch Roll Initiator
  - Existing hardware
- Industry exploring aids to Test Hazards and Analyses





We saw the value in STPA, but each time developing the UCAs felt grueling

Pretest Brief

- The Problem Statement
- UCA Breakthrough
- Using Timing Diagrams
- Auto Generating UCAs
- Creating Causal Scenarios
- Post Test Conclusions

STPA Handbook Steps 1 and 2

What went smoothly

- Losses and Hazards
  - Analogous to Effects and Hazards in Test Hazards and Analyses (THAs)
- Control Structure
  - We like flow diagrams

Risk	Risk Description
H H1	***Situation*** Flight up to and beyond maximum wing lift (stall) while at load factors near 2g ***Hazard(s)*** a ***Hazard*** Un-commanded roll oscillations or asymmetric departure during post stall maneuvering and stall recovery. ***Effect(s)*** Loss of control Roll off, spin Exceeding structural limits; Structural damage ***Alleviation(s)*** • Testing will be conducted no less than 10,000 ft above hard deck in order to allow for a recovery from the maneuver. If an undercast is present, it will be treated as a hard deck for risk alleviation purposes.

Losses

- L-1: Loss of life or injury to personnel
- L-2: Loss of or damage to aircraft
- L-3: Loss of mission

Hazards

- H-1: Aircraft exceeds structural limits [L1, L2]
- H-2: Unable to maintain controlled flight [L1, L2, L3]
- H-3: Unable to produce a usable maneuver [L4]

The Struggle

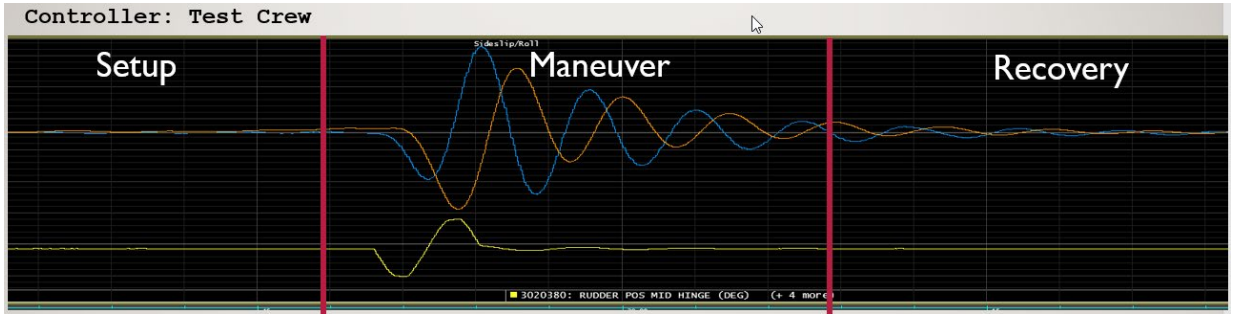
Where we struggled

- UCAs and Causal Scenarios
  - Didn’t know where to start
  - Struggled to get agreement
  - Group brainstorming wasn’t consistent
  - Took an excessively long time
    - Resulted in disinterest
  - Are we done?

The Problem Statement

Why do our UCAs feel weak?

- Control actions can be different depending on use case
  - Same controller, different maneuvers
- UCAs can be argued into multiple categories
  - Example: Did an action occur too early for Recovery or stop too soon for the Maneuver?
- Control actions are different depending on the phase of the maneuver
  - We kept missing the timing context in our UCAs



How do you create a complete set of UCAs for controller that has varying time dependent control actions

Examples

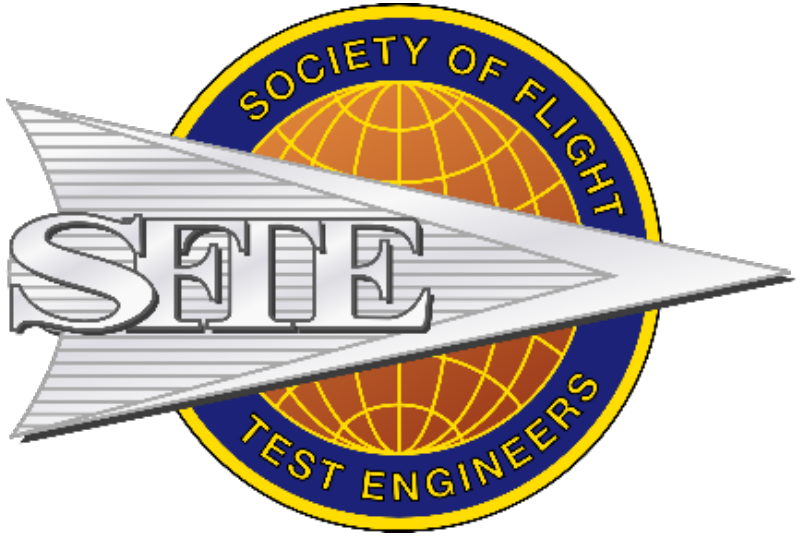
- Equip Operator Providing FSB Power OFF as a method of terminating a sweep resulting in an abrupt change in aircraft control law configuration
  - *Wait a minute, in some cases this is a good thing*
  - *Seems like we're missing context*

- Pilot provides control input too early before fault insertion program has completed
  - *Well…..we want them to interfere if the program has a fault*
  - *Seems like we're missing context*

The Breakthrough

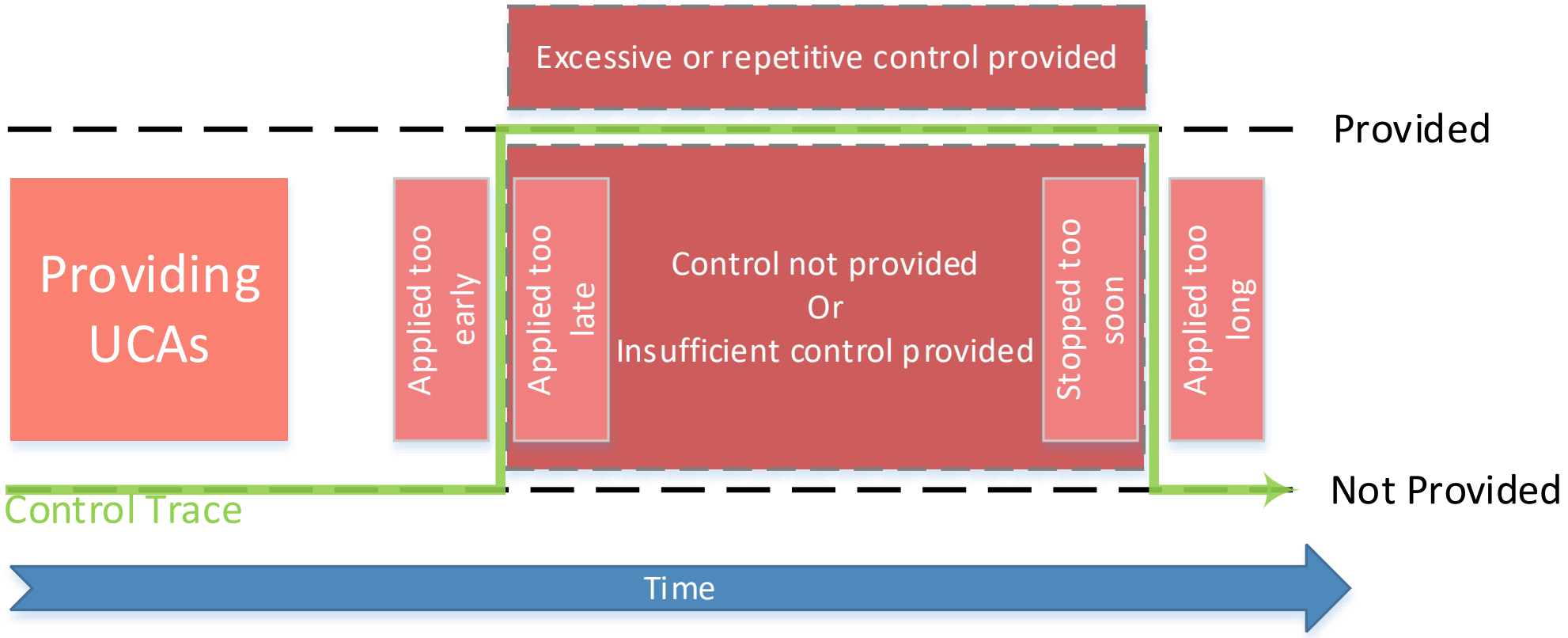
The Breakthrough

- STPA workshop at 2023 symposium for the Society of Flight Test Engineers
  - Collaborated with Dr. Thomas
  - Workshop goal to introduce STPA to flight test engineers across the industry



- Timing diagrams are always encouraged.
- Breakthrough occurred when Dr. Thomas provided an illustration

It’s in the time domain!

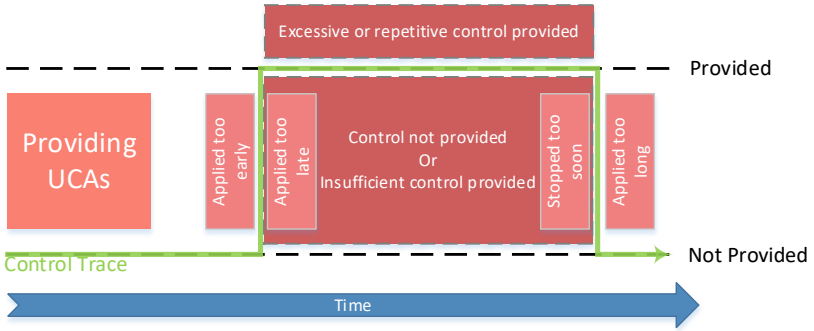


What if we could illustrate the controller actions in this format?

Example UCA Syntax

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Out of Order	Stopped Too Soon / Applied too long
<control action>	<controller> does not provide <control action> when <context> [<link to hazards>]	<controller> provides <control action> when <context> [<link to hazards>]	<controller> provides <control action> too late after (>TBD s after) <context> [<link to hazards>] <controller> provides <control action> too early before (>TBD s before) <context> [<link to hazards>]	<controller> stops providing <control action> too soon before (>TBD s before) <context> [<link to hazards>] <controller> continues providing <control action> too long after (>TBD s after) <context> [<link to hazards>]

Could UCAs be created with more consistency



+

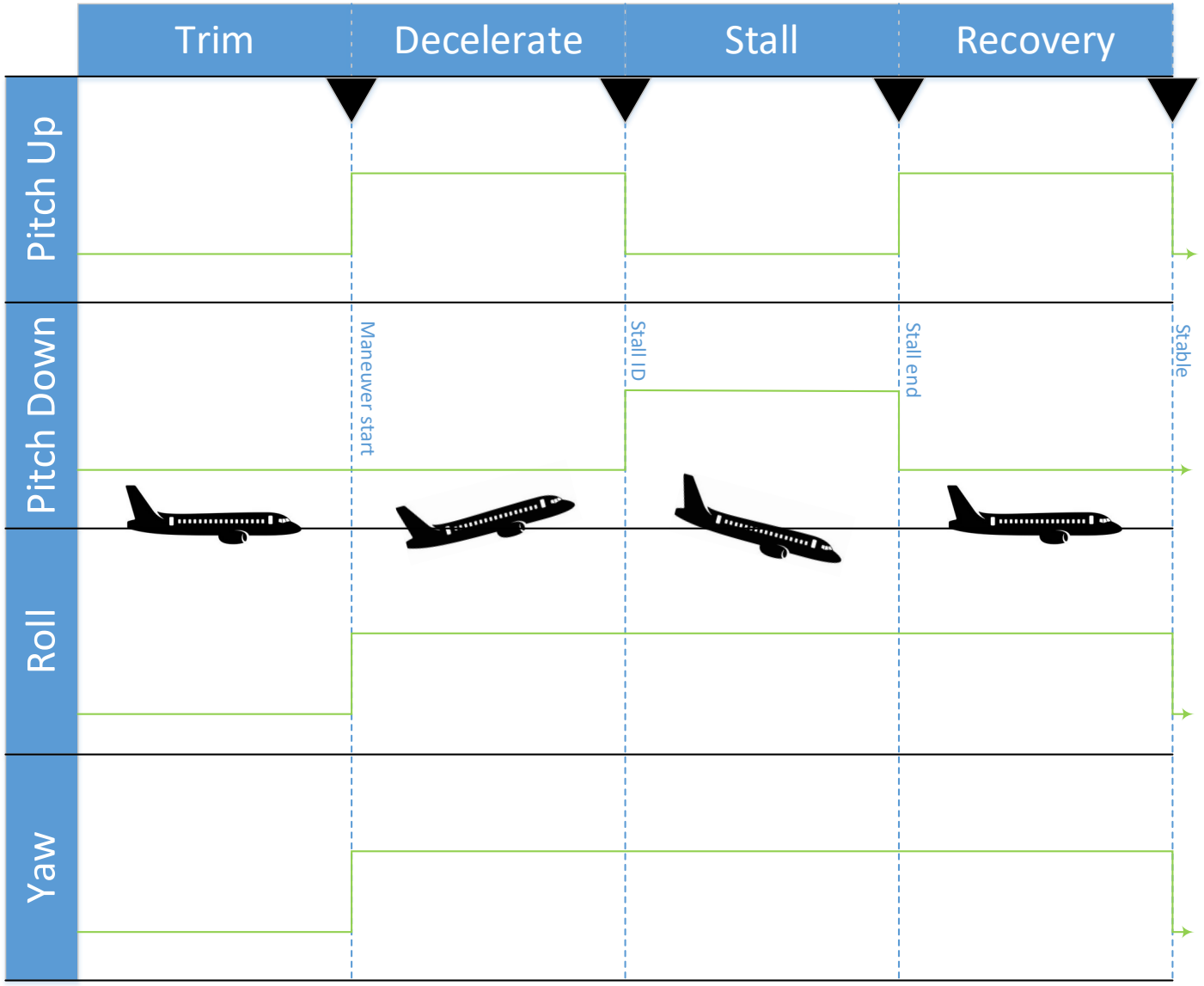
Example UCA Syntax

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Out of Order	Stopped Too Soon / Applied too long
<control action>	<controller> does not provide <control action> when <context> [<link to hazards>]	<controller> provides <control action> when <context> [<link to hazards>]	<controller> provides <control action> too late after (>TBD s after) <context> [<link to hazards>] <controller> provides <control action> too early before (>TBD s before) <context> [<link to hazards>]	<controller> stops providing <control action> too soon before (>TBD s before) <context> [<link to hazards>] <controller> continues providing <control action> too long after (>TBD s after) <context> [<link to hazards>]

=

UCA

Diagram of a stall maneuver

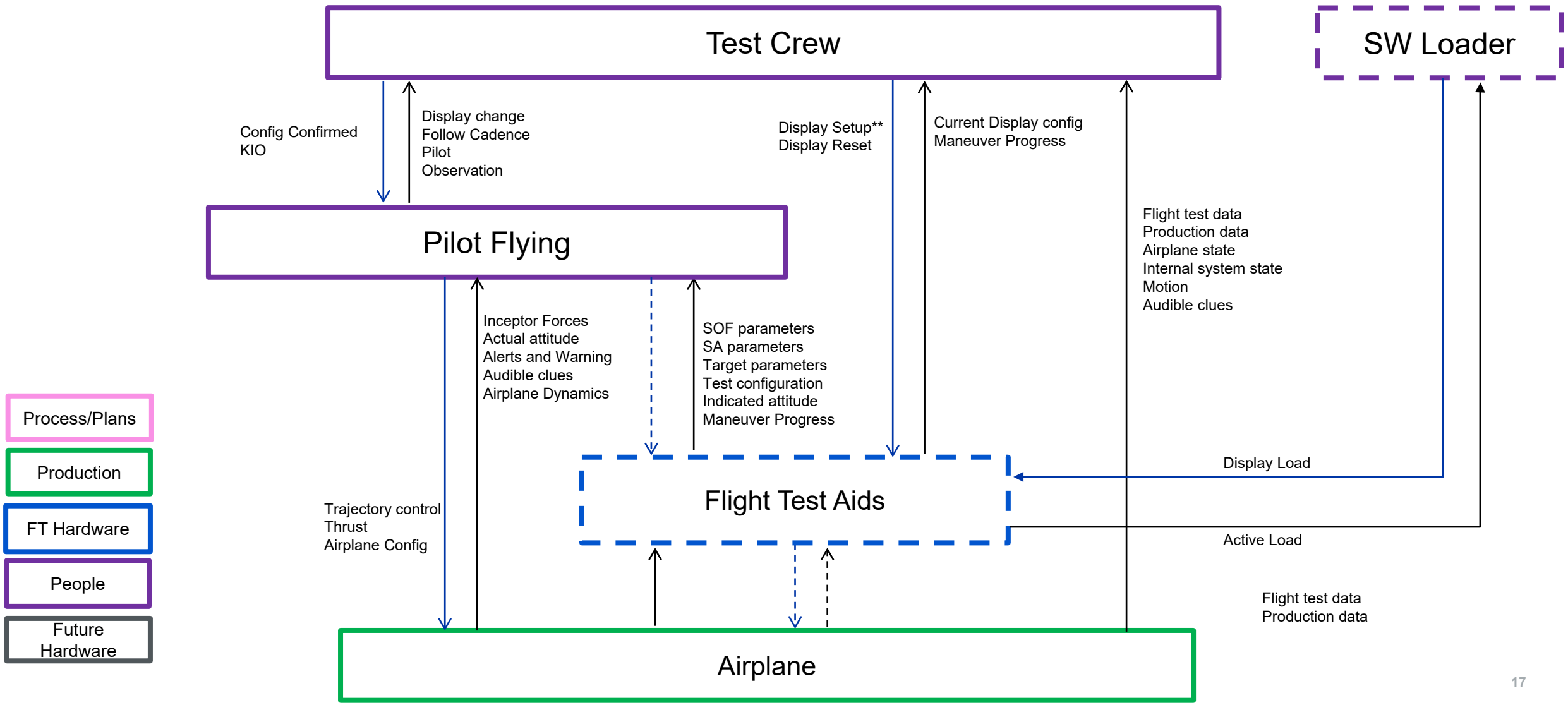


Control Action	Not providing causes hazard	Providing causes hazard (excessive, insufficient, repetitive)	Too early, too late, out of order	Stopped too soon, applied too long
Pitch UP [Decel Phase] [Recovery Phase]	Pilot does not provide pitch up when decelerating [H3]		Pilot provides pitch up too late after stall end [H1.3]	
Pitch Down				
Roll		Providing insufficient roll input during stall recovery [H1.2, H1.3, H2.1]		
Yaw				

Control Action	Not providing causes hazard	Providing causes hazard (excessive, insufficient, repetitive)	Too early, too late, out of order	Stopped too soon, applied too long
Pitch Up [Decel Phase] [Recovery Phase]	Pilot does not provide pitch up when decelerating [H3] Pilot does not provide pitch up during recovery to stabilize [H1.3]	Pilot provides excessive pitch up during decel [H2, H3] Provides insufficient when decelerating to initiate stall [H3] Pilot provides excessive pitch up during recovery [H1.1, H1.2, H2] Pilot provides insufficient pitch up during recovery [H1.3]	Pilot provides pitch up too early before decel [H3] Pilot provides pitch up too late after stall ID[H1.3] Pilot provides pitch up too early before stall recovery [H2, H3] Pilot provides pitch up too late after stall recovery [H1.3]	Pilot stops providing pitch up too soon before stall ID [H3] Pilot continues providing pitch up too long after stall ID [H2] Pilot stopped providing pitch up too soon before airplane is stable [H1.3] Pilot continues providing pitch up too long after airplane is stable [H2]
Pitch Down	Pilot does not provide pitch down after stall ID [H2]	Pilot provides excessive pitch down after stall ID [H1.3]	Pilot provides pitch down too early before stall ID [H3] Pilot provides pitch down too late after stall ID [H2]	Pilot stops providing pitch down before airplane recovers from stall [H2] Pilot continues providing pitch down too long after airplane recovers [H1.3]
Roll	Pilot does not provide roll input during recovery [H2.1, H3]	Pilot provides excessive roll during recovery [H2.1, H3] Providing insufficient roll input during stall recovery [H1.2, H1.3, H2.1]	Pilot provides roll input prior to stall ID [H3] Pilot provides roll input too late after stall ID [H2.1]	Pilot stopped providing roll before aircraft is stable [H2.1, H3] Pilot continues providing roll too long after airplane is stable [H2.1]
Yaw	Pilot does not provide yaw input during recovery [H2.1, H3]	Pilot provides excessive yaw during recovery [H2.1, H3] Providing insufficient yaw input during stall recovery [H1.2, H1.3, H2.1]	Pilot provides yaw input prior to stall ID [H3] Pilot provides yaw input too late after stall ID [H2.1]	Pilot stopped providing yaw before aircraft is stable [H2.1, H3] Pilot continues providing yaw too long after airplane is stable [H2.1]

Using Timing Diagrams

Flight Test Hardware Development

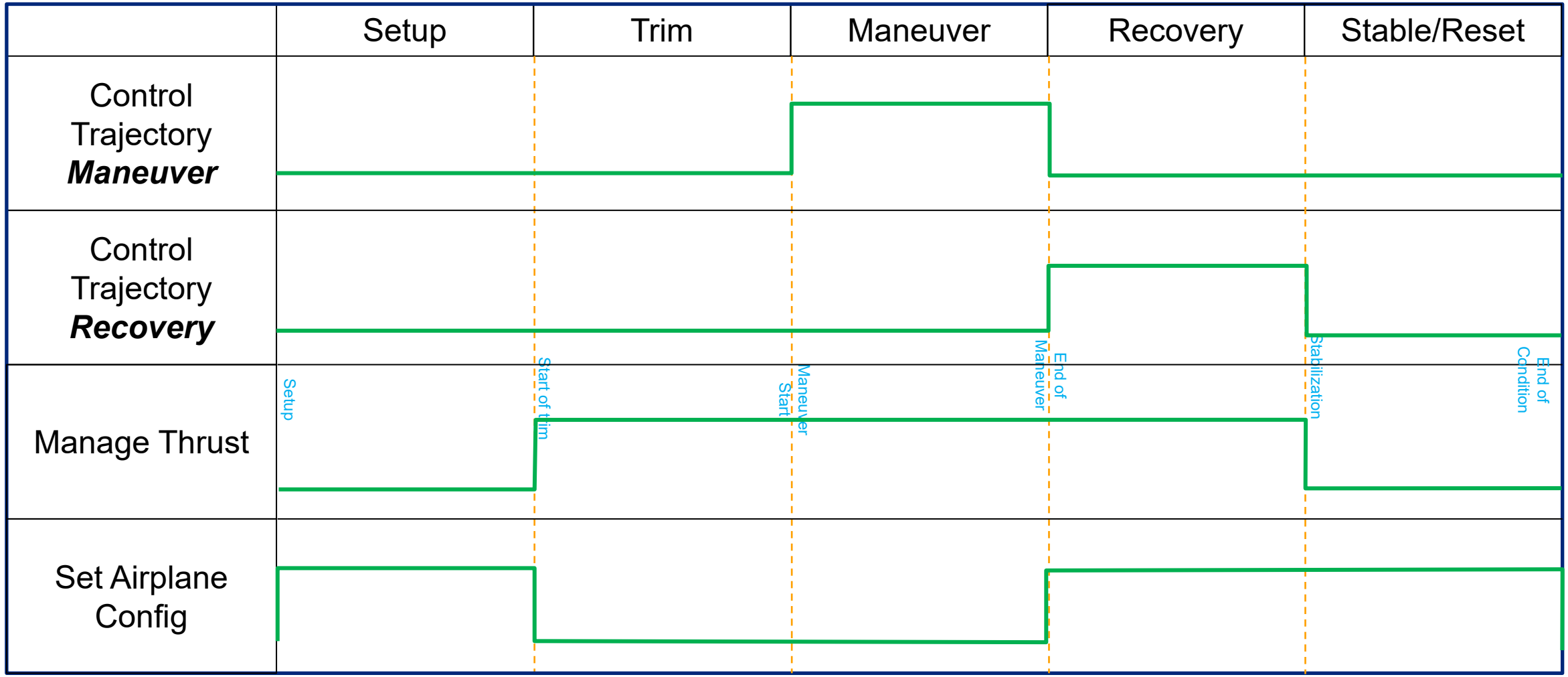


Decompose the Maneuver (or timeline)

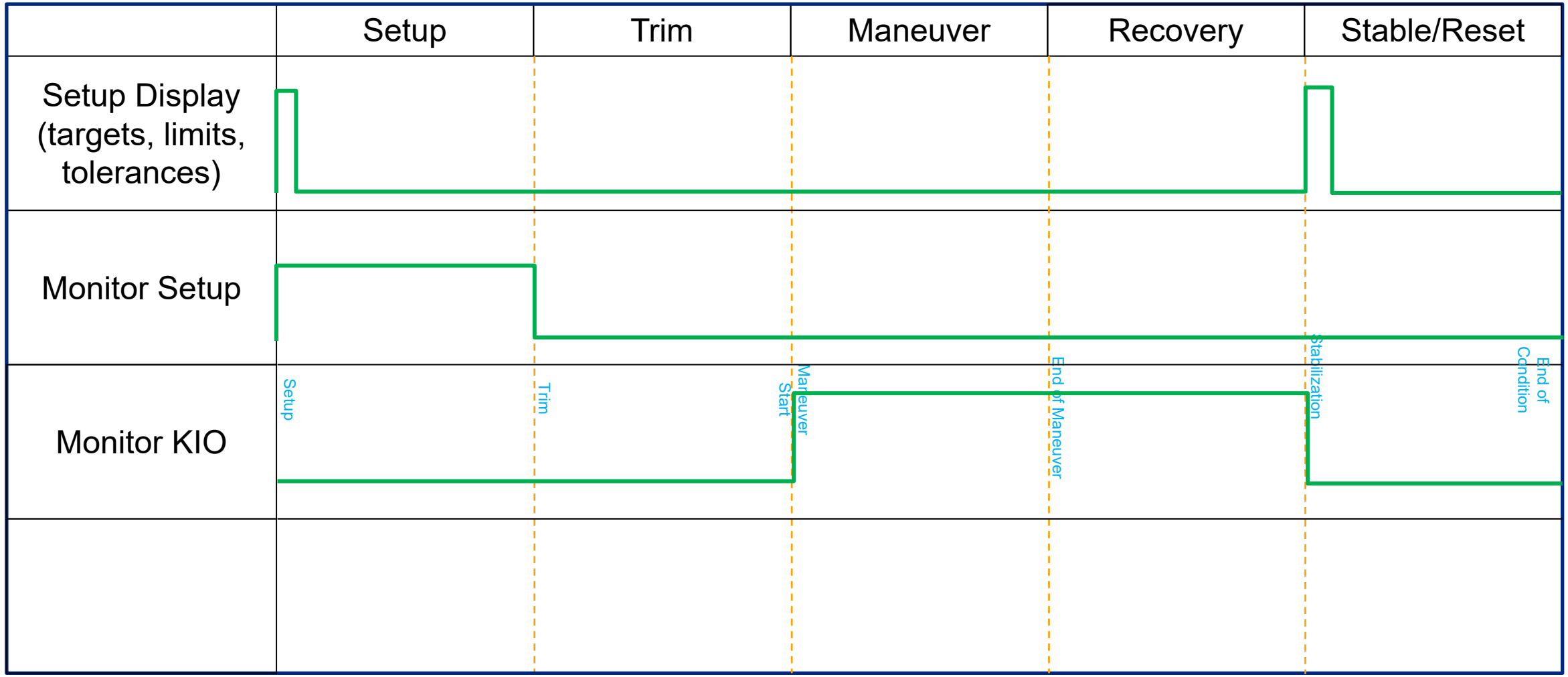
	Setup	Trim	Maneuver	Recovery	Stable/Reset
Control Action 1					
Control Action 2					
Control Action 3					
Control Action 4					

Setup
Start of trim
Maneuver Start
End of Maneuver
Stabilization
End of Condition

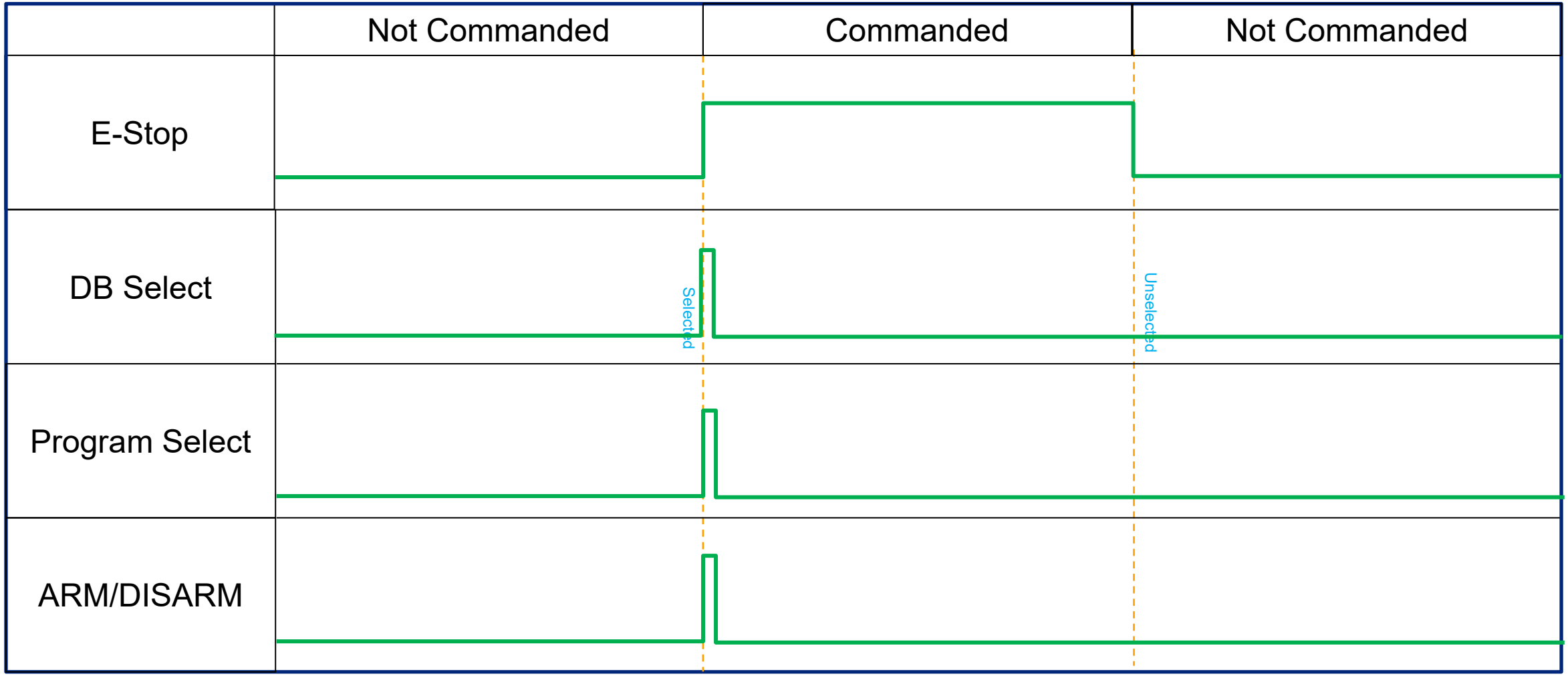
Controller: Pilot



Controller: Test Crew



Hardware controller



Auto Generating UCAs

UCA Assembly

- Controller
- UCA Type
- Control Action
- Timing Context
- Phase or Event

Controller	UCA Action	Control Action (Function or Responsibility)	Context	Phase or Event	Full UCA
Pilot	does not provide	maneuver control	during	maneuver	Pilot does not provide maneuver c
Pilot	provides	maneuver control	during	setup or trim	Pilot provides maneuver control d
Pilot	starts providing	maneuver control	too late after	maneuver start	Pilot starts providing maneuver co
Pilot	starts providing	maneuver control	too early before	maneuver start	Pilot starts providing maneuver co
Pilot	stops providing	maneuver control	too soon before	end of maneuver	Pilot stops providing maneuver co
Pilot	continues providing	maneuver control	too long after	end of maneuver	Pilot continues providing maneuve
Pilot	does not provide	recovery control	during	recovery	Pilot does not provide recovery co
Pilot	provides	recovery control	during	setup or trim	Pilot provides recovery control du
Pilot	starts providing	recovery control	too late after	end of maneuver	Pilot starts providing recovery con
Pilot	starts providing	recovery control	too early before	end of maneuver	Pilot starts providing recovery con
Pilot	stops providing	recovery control	too soon before	stablization	Pilot stops providing recovery con
Pilot	continues providing	recovery control	too long after	stablization	Pilot continues providing recovery
Pilot	does not provide	trim thrust management	during	trim	Pilot does not provide trim thrust
Pilot	provides	trim thrust management	during	setup	Pilot provides trim thrust manage
Pilot	starts providing	trim thrust management	too late after	start of trim	Pilot starts providing trim thrust m
Pilot	starts providing	trim thrust management	too early before	start of trim	Pilot starts providing trim thrust m
Pilot	stops providing	trim thrust management	too soon before	maneuver start	Pilot stops providing trim thrust m
Pilot	continues providing	trim thrust management	too long after	maneuver start	Pilot continues providing trim thru
Pilot	does not provide	maneuver thrust management	during	maneuver	Pilot does not provide maneuver t
Pilot	provides	maneuver thrust management	during	setup	Pilot provides maneuver thrust ma
Pilot	starts providing	maneuver thrust management	too late after	maneuver start	Pilot starts providing maneuver th
Pilot	starts providing	maneuver thrust management	too early before	maneuver start	Pilot starts providing maneuver th
Pilot	stops providing	maneuver thrust management	too soon before	end of maneuver	Pilot stops providing maneuver th
Pilot	continues providing	maneuver thrust management	too long after	end of maneuver	Pilot continues providing maneuve

Assembly of Full UCA Statement

Concatenated Statement

Hazard Assignment

Eliminating unnecessary UCAs

Context	Phase or Event	Full UCA	Hazards
during	maneuver	Pilot does not provide maneuver control during maneuver	H1, H2.1, H3
during	setup or trim	Pilot provides maneuver control during setup or trim	H1, H3
too late after	maneuver start	Pilot starts providing maneuver control too late after maneuver start	H3
too early before	maneuver start	Pilot starts providing maneuver control too early before maneuver start	H3
too soon before	end of maneuver	Pilot stops providing maneuver control too soon before end of maneuver	H1, H2.1, H3
too long after	end of maneuver	Pilot continues providing maneuver control too long after end of maneuver	H1, H2.1
during	recovery	Pilot does not provide recovery control during recovery	H1, H2.1
during	setup or trim	Pilot provides recovery control during setup or trim	H3
too late after	end of maneuver	Pilot starts providing recovery control too late after end of maneuver	H1, H2.1
too early before	end of maneuver	Pilot starts providing recovery control too early before end of maneuver	H3
too soon before	stablization	Pilot stops providing recovery control too soon before stablization	H1, H2.1
too long after	stablization	Pilot continues providing recovery control too long after stablization	H1, H2.1
during	trim	Pilot does not provide trim thrust management during trim	H3
during	setup	Pilot provides trim thrust management during setup	NA
too late after	start of trim	Pilot starts providing trim thrust management too late after start of trim	NA
too early before	start of trim	Pilot starts providing trim thrust management too early before start of trim	NA
too soon before	maneuver start	Pilot stops providing trim thrust management too soon before maneuver start	NA
too long after	maneuver start	Pilot continues providing trim thrust management too long after maneuver start	NA
during	maneuver	Pilot does not provide maneuver thrust management during maneuver	H1, H2.1, H3
during	setup	Pilot provides maneuver thrust management during setup	NA
too late after	maneuver start	Pilot starts providing maneuver thrust management too late after maneuver start	H1, H2.1, H2.4, H3
too early before	maneuver start	Pilot starts providing maneuver thrust management too early before maneuver start	H2.4, H3
too soon before	end of maneuver	Pilot stops providing maneuver thrust management too soon before end of maneuver	H1, H2.1, H3
too long after	end of maneuver	Pilot continues providing maneuver thrust management too long after end of maneuver	NA

Creating Causal (Loss) Scenarios

- Continued STPA per handbook guidelines
- Macro used to generate tables

Pilot_UCA01	**Pilot does not provide maneuver control during maneuver**	**H1, H2.1, H3**
Pilot_UCA01_CS01	Pilot believed maneuver control was not necessary because they where not briefed or trained on how to use the FTA. As a result the correct manuever is not controlled.	
Pilot_UCA01_CS02	Pilot believed they were maneuvering correctly but the incorrect FTA configuration was selected. As a result the correct maneuver is not controlled.	
Pilot_UCA01_CS03	Pilot believed attitude control was sufficient due to confusing or masked primary flight display. As a result the correct maneuver control was not provided.	
Pilot_UCA01_CS04	Pilot believed maneuvering was sufficient due to FTA providing incorrect targets. As a result the correct maneuver control was not provided.	
Pilot_UCA01_CS05	Pilot believed maneuvering was sufficient due to incorrect measurement inputs. As a result the correct maneuver control was not provided.	
Pilot_UCA01_CS06	Pilot believed critical measurements are accurate and on time even though they are lagging. As a result the correct maneuver control was not provided.	H1, H2.1
Pilot_UCA01_CS07	Pilot believed they were flying to one type of measurement (KEAS vs KCAS, Cone vs. Co-pilot static), however FTA was providing a different value. As a result the correct maneuver control was not provided.	
Pilot_UCA01_CS08	Pilot believed that the autopilot was going to control the aircraft. However the AP was disengaged or in another mode. As such pilot does not provide maneuver control.	
Pilot_UCA01_CS09	Pilot believed that the FTA are incorrect due to external input (buffet, noise, out the window, etc.). As a result they maneuvered in conflict with the FTA.	
Pilot_UCA01_CS10	Pilot believed that FTA was missing. However FTE selected it to be on a different part of the PFD (Aux panel vs. Minimap)	
Pilot_UCA02	**Pilot provides maneuver control during setup or trim**	**H1, H3**
Pilot_UCA02_CS01	Pilot believed that the condition had already started due to unexpected FTA cueing. As a result maneuver control is provided when not on condition.	
Pilot_UCA02_CS02		
Pilot_UCA02_CS03		
Pilot_UCA03	**Pilot starts providing maneuver control too late after maneuver start**	**H3**
Pilot_UCA03_CS01	Pilot follows FTA guidance but the display information is delayed (late measurement, frozen screen, etc).	
Pilot_UCA03_CS02	Pilot delays maneuver input because they believes a FTA parameter is incohorent or confusing (conflict with other input)	
Pilot_UCA03_CS03	Pilot does not believe that the condition started because FTA correct cuing information was not provided. As a result they did not start the maneuver on time.	
Pilot_UCA03_CS04	Pilot does not believe that the condition started because they were expecting a different cue. As a result they responded late and did not start the maneuver on time.	
Pilot_UCA03_CS05	Pilot could not close the loop on all required parameters because the required scan takes too long between parameters. As a result maneuver control may be late.	
Pilot_UCA03_CS06	FTA cueing is provided without lead in. As a result the pilot does not provide maneuver soon enough.	

Conclusions

Cautionary Notes

- This method does not replace common sense and a healthy understanding of the system being evaluated
  - Particularly useful for flight testers who may not have been involved in the design
- May need to have multiple timing diagrams for different scenarios
  - *E.g. Pilot response for normal operation vs. non-normal*

Post Test Conclusions

- Timing diagrams are useful for understanding context of UCAs
- Forces users to identify systems actions in the time domain first
  - Separates the decomposition of the system's actions from the assembly of the UCAs
- Benefits realized from this UCA method
  - Consistency
  - Time savings (less time in meetings)
  - Sense of completeness
  - Effectively deferred the "creative brainstorming" part of STPA to the last step

The presenter continued providing speech too long resulting in no time for questions

Post Test Conclusions

- Timing diagrams are useful for understanding context of UCAs
- Benefits realized from this UCA method
  - Consistency
  - Time savings (less time in meetings)
  - Sense of completeness
  - Effectively deferred the “creative brainstorming” part of STPA to the last step

~~The presenter continued providing speech too long resulting in no time for questions~~

Questions