Very short example: DC-10 engine out

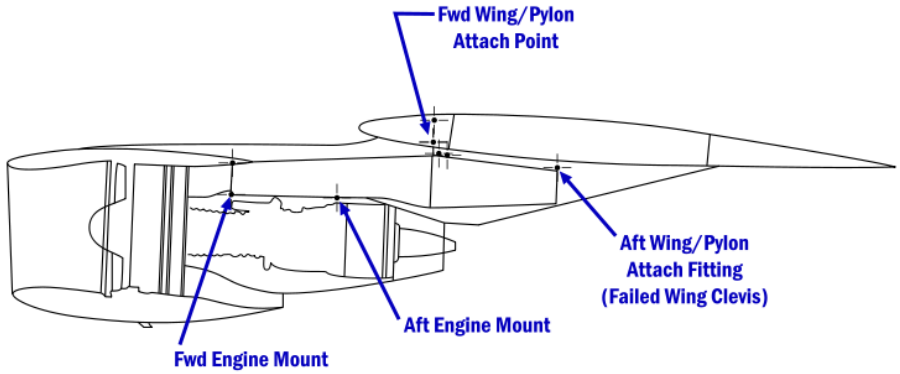
Disclaimer

These exercises are not meant to represent a complete analysis, and they are not meant to exhaustively demonstrate STPA.

The exercises are only meant to introduce a few core concepts.

American Airlines 191: DC-10

- Left engine (#1) separates from aircraft on takeoff
- Pilot follows standard procedure for engine out. Raises nose to 14°, slows to takeoff safety airspeed (V_2) of 153 knots
  - This the specified speed at which the aircraft can safely climb after sustaining an engine failure
- Aircraft suddenly rolls left 120° (uncommanded), crashes
- Killed all 271 people on board. Deadliest aviation accident on US soil to this day.
- Post-accident simulator recreations done with 12 other pilots. None could prevent the crash.



American Airlines 191: DC-10

- Left engine (#1) separates from aircraft on takeoff
- Pilot follows standard procedure for engine out. Raises nose to 14°, slows to takeoff safety airspeed (V_2) of 153 knots
  - This the specified speed at which the aircraft can safely climb after sustaining an engine failure
- Aircraft suddenly rolls left 120° (uncommanded), crashes
- Killed all 271 people on board. Deadliest aviation accident on US soil to this day.
- Post-accident simulator recreations done with 12 other pilots. None could prevent the crash.

- Damaged hydraulic lines, left slats retracted
- Stall speed of left wing increased from 124 knots to 159 knots
- Cockpit indication incorrectly confirmed slats still in extended position (not visible from cockpit)
- Slat disagreement warning light inoperative (powered by #1 engine)
- Captain stick shaker inoperative (powered by #1 engine)
- First officer stick shaker never installed (offered as optional feature, not purchased by AA)

John Thomas, 2019

Using STPA to ask questions

System Hazard: Aircraft uncontrolled flight

Question: What Pilot control actions can cause aircraft to stall?

UCA: Pilot decreases speed below stall speed

Question: What Pilot beliefs would cause Pilot to decrease speed below stall speed?

- Incorrectly believes speed is higher than it is
- Incorrectly believes stall speed is lower than it is

Pilot

Control algorithm

Process Model (beliefs)

Question: What Pilot inputs would cause Pilot to believe stall speed lower than it is?

- No stick shaker during stall
- No slat disagreement ind. during slat retract

Control Actions

Feedback

Question: What process behavior would cause slats to retract without slat disagreement indication?

Controlled Process

Loss #1 engine/power
Hydraulic rupture near slats