System-Theoretic Process Analysis (STPA) Evaluation of Boeing's Automated Test Maneuvers (ATM) System

Dulnath Wijayratne
Jordan Stringfield
Shannon Clark, Technical Fellow
Darren McDonald, Technical Fellow

MIT STAMP Workshop
June 2022

Overview

- **Background**
  - Dutch roll primer
  - Boeing's Automated Test Maneuver (ATM) System
  - Why did we pick the Dutch roll maneuver?
- **STPA Details and Interesting Finds**
  - ATM Control Structure
  - Overview of losses, hazards, UCAs, causal scenarios, flight test preparation
- **Communicating STPA**
  - Introducing STPA into the flight test organization
  - Facilitating STPA
- **Results, Recommendations and Next Steps**

Background

What is a Dutch roll maneuver?

- Part 25 Aircraft Requirement: Dutch roll must be positively damped across the flight envelope
- Lateral dynamic phenomenon characterized by oscillatory response involving lateral and directional modes (bank angle and heading)
- All swept-wing aircraft require active yaw damping

Background

Boeing's Automated Test Maneuver (ATM) Dutch Roll Initiator (DRI) System

- System sends signals to command flight control surfaces without the pilot making the input
- Performs precise test maneuvers, consistently and error free
- Iterative process developed from desktop simulation, then moved to piloted simulations before finally flying on modified flight test aircraft
- This is the next phase in Boeing's Model Based Test and Automation to validate models rather than simply show compliance

Why did we pick the Dutch roll maneuver?

- Maneuver requires inputs to only one control surface (rudder in this case)
- Predictable enough to allow for pilot abort and recovery if necessary
- Beginning of building a library of maneuvers that will grow over time

STPA Details and Interesting Finds

Goals of this Project

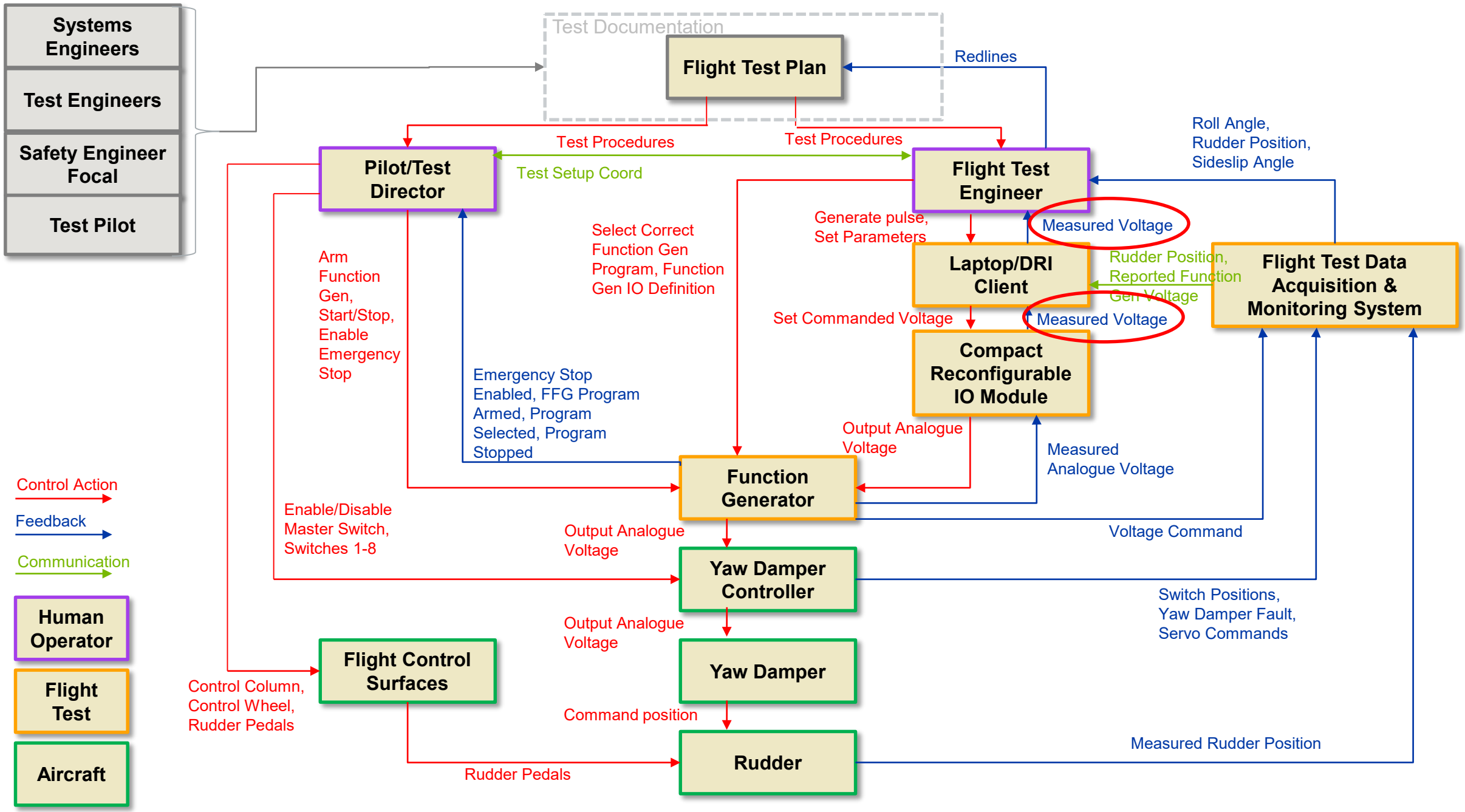
- Perform a structured analysis on a previously designed, built and partially tested system
- Use STPA results to obtain the necessary data going into a Safety Review Board
- Answer the Chief Pilot's Question: "How can you prove to me that you've thought of all the ways this thing can go wrong?"
- Introduce STPA to the Flight Test Engineering Analysis group

Setting up the Analysis – Captured High Level Assumptions to Limit the Scope

- Did not include normal operational flying concerns (weather, bird strikes, terrain avoidance, etc.) nor any Cyber Security
- Defined System Boundaries around the Automated Test Maneuvering System
- 5 Losses
- 3 Hazards

L1: Loss of life or injury to personnel
L2: Loss of or damage to aircraft
L3 Loss of customer satisfaction
L4: Loss of data quality
L5: Loss of flight test productivity

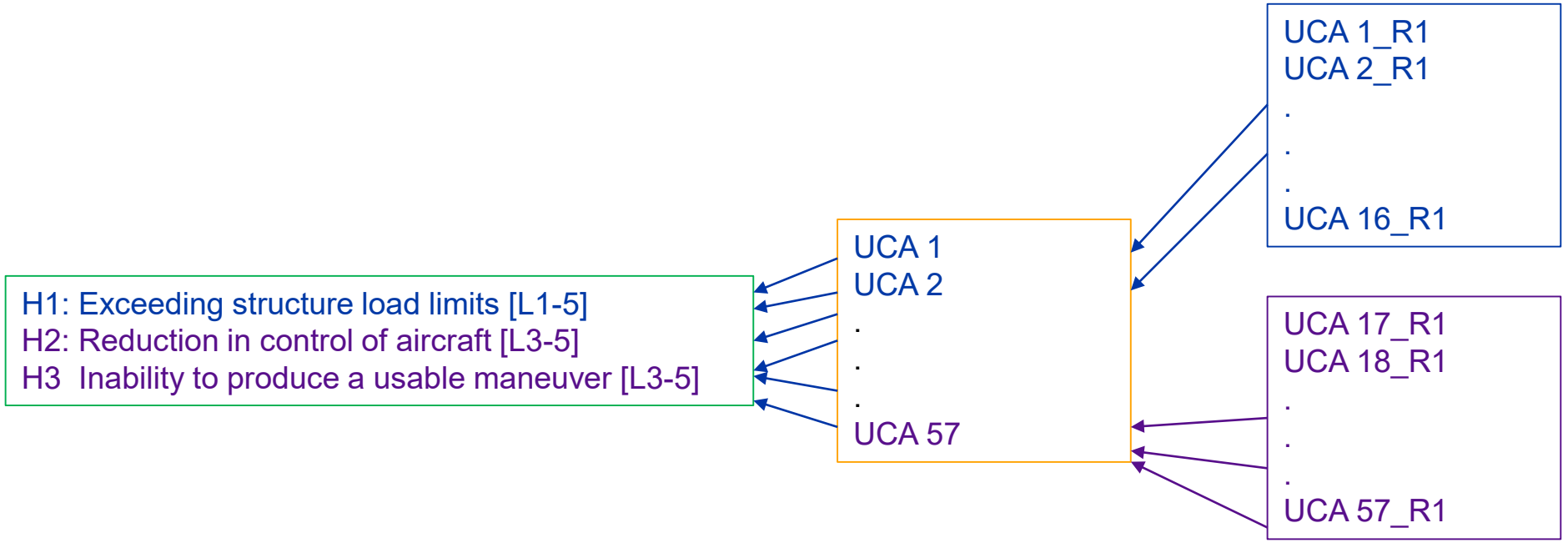
H1: Exceeding structure load limits [L1-5]
H2: Reduction in control of aircraft [L3-5]
H3 Inability to produce a usable maneuver [L3-5]



STPA Details and Interesting Finds

Unsafe Control Actions (UCAs)

- STPA found 16 of 57 UCAs were satisfied by an *existing* system requirement
  - "Ensure that the system cannot exceed the maximum rudder deflection limitation to protect vertical fin structure."
- Although this was a critical requirement, 41 ***additional*** unsafe control actions were uncovered which generated new requirements and new verification activities



STPA Details and Interesting Finds

Example UCAs:

- FTEA changes and/or Sets Natural Frequency out of sequence in the laptop DRI client while DRI Client is executing program and hits "generate pulse“
- FTEA provides set bias that is too small to the DRI client prior to start of testing
- FTEA does not provide set natural frequency input to the DRI client when the Function Generator is executing and the signal is generated
- Pilot enables emergency stop too early when program is running
- FTEA shall monitor and compare DRI Client out signal to Function Generator output signal in user interface (UI) to detect discrepancy

STPA Details and Interesting Finds

Overview of losses, hazards, UCAs, causal scenarios, flight test preparation

- 57 Undesirable Control Actions identified in a relatively small system
- 39 Causal Scenarios > 27 Requirements
- 11 Requirements were Verified by Demonstration/Test in simulator or on aircraft during ground test
  - 4 UCA Level Requirements, 23 Causal Scenario Level Requirements

What we found in our Causal Scenarios

- “I don’t think we would have caught that without STPA”
  - 8 Requirements that drove software updates to LabView code in Special Test Equipment
  - 14 Requirements that updated the Test Procedure and/or Checklist and created new Test Procedures
- This was a system previously designed and used for other similar types of tests
- All together, the effort drove the need for the entire Test Team to update software, tests procedures, flight simulations and go through additional training prior to first flight

Communicating STPA

Introducing STPA into the organization

- Initial STPA discussions were fostered through Boeing Tech Fellowship members
- STPA was used to improve an already built/designed/tested system
- Test Organization initially struggled with performing STPA but saw the benefits in the end

Facilitating STPA

- The STPA analysis was performed by a new team that was facilitated by three facilitators with moderate experience having performed STPA on previous programs.
- STPA analysis better informed the Test Team on requirements for Special Test Equipment and Test Documentation
- Ideally done with 2 facilitators in each meeting
  - One is focused on capturing thoughts, driving tools, etc.
  - Other is facilitating STPA principles in abstract thought and coaching

Results, Recommendations and Next Steps

Safety Review Board

- First time STPA results were used to inform a Safety Review Board
- STPA was incredibly helpful and provided powerful, confident results to test team

Flight Results

- 2 Flights were successfully completed in Nov 2021
- Notable Crew Resource Management (CRM) improvements made to Flight Test Plan
- Comments from the pilots included:
  - “That input felt incredibly smooth. It seemed like it was timed perfectly right on the natural frequency”
  - “The DRI worked really well! It produced nice, crisp inputs that resulted in clean conditions. Automation of flight test maneuvers is a big deal!”

Future Vision, Questions and Answers

Future Vision

- Generated foundational requirements for future programs
- We had a positive culture change instead of: "We've used this system before. It's safe. Why do we need STPA?“

Questions?

Recently featured in Boeing News Now and Innovation Quarterly Magazine