STPA Applied to Air Force Acquisition Technical Requirements Development

MIT STAMP Conference
27 Mar 2018

Sarah Summers
MIT SDM

Disclaimer

The views expressed in this document are those of the author and do not reflect the official position or policies of the United States Air Force, Department of Defense, or U.S. Government.

Agenda

- UAV Analysis
- STPA Implementation within Acquisitions
- STPA Application to Airworthiness

System Description

- General aviation (GA) aircraft that has been converted to a UAV
  - Controlled by ground stations
  - Autopilot in Vehicle Management System (VMS) controls actuators connected to elevator, ailerons, rudder and engine throttle

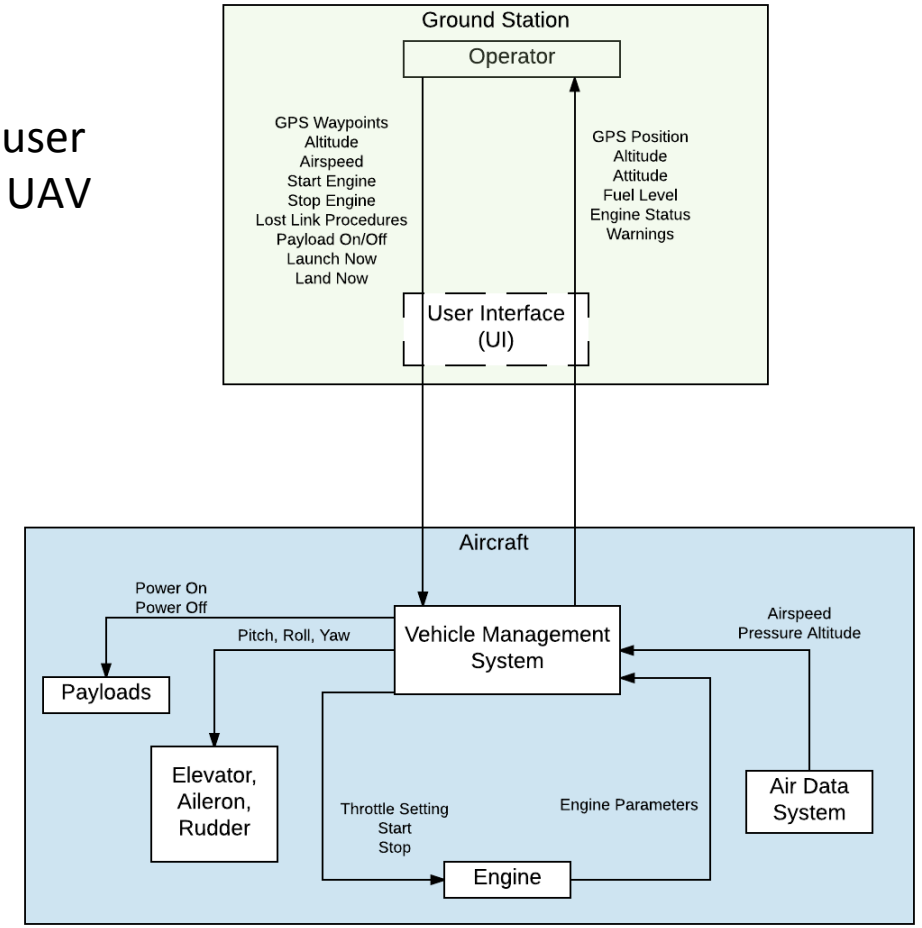
Accidents and Hazards

Designator	Accident Description
A1	Loss of life/injury
A2	Loss of or damage to UAV aircraft
A3	Loss of mission

Hazard	Assoc. Accident	Description of Hazard
H1	A1, A2	UAV too close to ground/building/person
H2	A1, A2	UAV violates minimum separation requirements
H3	A3	UAV does not complete mission
H4	A1, A2	UAV departs controlled flight
H5	A1, A2	UAV departs apron, taxiway, or runway during ground operations
H6	A1, A2	Loss of UAV airframe integrity

Safety Control Structure

- Ground station contains a laptop with a user interface (UI) and radios to link with the UAV
- VMS includes autopilot, and power distribution



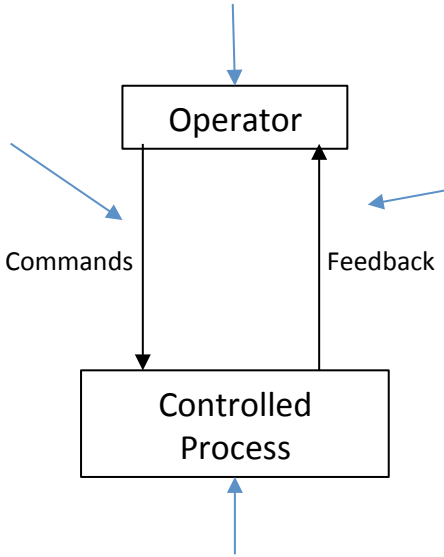
Vehicle Management System UCAs

Vehicle Management System	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Roll, Pitch, Yaw	…when the UAV is off course (H1, H2, H3)	…when the roll, yaw, or pitch command exceeds aircraft attitude limits (H4) …when the roll, pitch, yaw command steers the UAV off course (H1, H2, H3)	…when the throttle is reduced in order to descend, but the subsequent pitch down command is delayed (H4) …when the throttle is increased for a climb, but the subsequent nose up command is delayed (H4)	…the actuator displacement is not brought back to neutral when the aircraft reaches the target heading/descent/ ascent (H1, H2, H3) …the actuator displacement is brought back to neutral before the UAV reaches the target heading/descent/ascent (H1, H2, H3)

Step 2 Process: 4 Types of Scenarios

2. Inappropriate decision
   - Receives accurate feedback
   - Makes unsafe decision

1. Command not followed or followed inadequately
   - Provides command
   - Command either not followed or not followed as commanded



3. Inadequate feedback or other inputs
   - Receives inaccurate feedback
   - Leads to an unsafe command

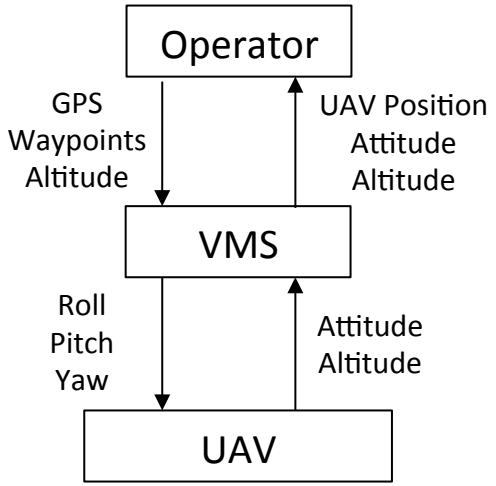
4. Inadequate process behavior
   - Process receives command
   - Process does not act as expected

UCA Scenario – Type 1

Command not followed or followed inadequately

UCA: The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits

The VMS does not provide the roll, pitch, or yaw command. A **shorted wire provides power to the actuator** causing the aileron, elevator, or rudder to move. **The aileron, elevator, and rudder receive the command even though the VMS did not command it.**

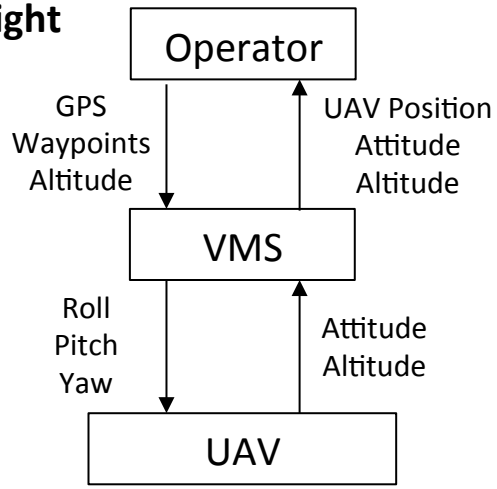


UCA Scenario – Type 2
Inappropriate decision

UCA: The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits

The VMS provides the roll, pitch, or yaw command and exceed limits for the current flight condition. **The VMS was programmed with one set of attitude limits, rather than a set of attitude limits for different flight conditions** (altitude & speed). The command **did not exceed the programmed limits**, but it **did exceed actual limits for that particular flight condition**.

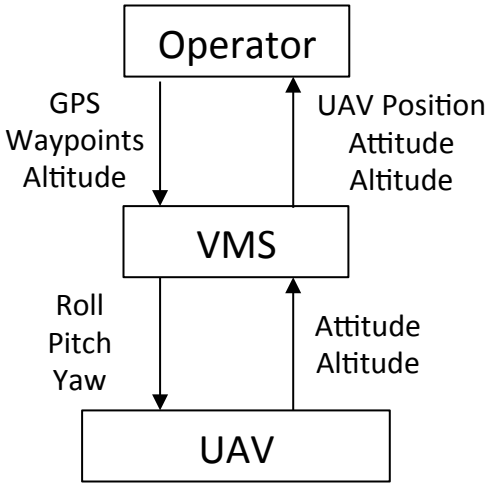
The VMS provides a roll, pitch, or yaw command that it believes will result in an attitude within limits. **The aeromodeling of the system was not validated**, and the magnitude of the command is too large. The commanded attitude is actually out of limits.



UCA Scenario – Type 3

Inadequate feedback or other inputs

UCA: The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits

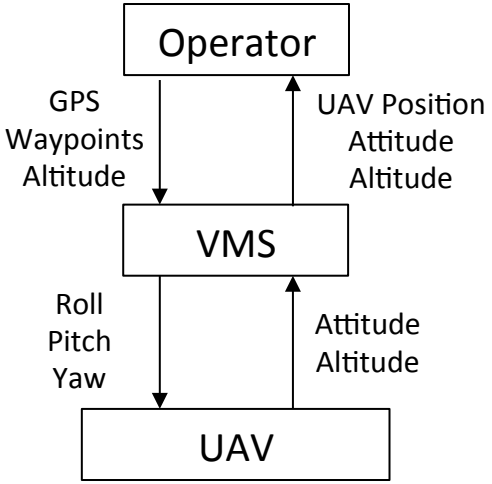


The **VMS provides a roll, yaw, or pitch input to correct an invalid attitude indication** it is receiving. The invalid feedback is due to a **vacuum pump failure** that renders the attitude indicator inoperative. **The command exceeds attitude limits, but the VMS does not recognize the exceedence** due to the invalid attitude indication.

UCA Scenario – Type 4

Inadequate process behavior

UCA: The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits



The VMS provides a roll, pitch, or yaw command that is appropriate for staying within the UAV attitude limits. **The actuator was connected to the cables backwards, and the VMS input has the opposite effect** (roll left input rolls UAV right). The VMS continues to command in the appropriate direction in an attempt to correct the attitude eventually exceeding aircraft limits.

Safety Constraints/Requirements

The VMS does not provide the roll, pitch, or yaw command, but the aileron, elevator, and rudder receive the command. A shorted wire provides power to the actuator causing the aileron, elevator, or rudder to move. The aileron, elevator, and rudder receive the command even though the VMS did not command it.	**Wiring must be designed to withstand the flight environment, and inspected before flight.**
The VMS provides the roll, pitch, or yaw command and exceed limits for the current flight condition. The VMS was programmed with one set of attitude limits, rather than a set of attitude limits for different flight conditions (altitude & speed). The command did not exceed the programmed limits, but it did exceed actual limits for that particular flight condition	**The VMS must be programmed with limits at all flight conditions**
The VMS provides a roll, pitch, or yaw command that it believes will result in an attitude within limits, however the attitude is actually out of limits. The aeromodelling of the system was not validated, and the magnitude of the command is too large. The commanded attitude is actually out of limits.	**The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations**
The VMS provides a roll, yaw, or pitch input to correct an invalid attitude indication it is receiving and exceeds attitude limits. The invalid feedback is due to a vacuum pump failure that renders the attitude indicator inoperative. The command exceeds attitude limits, but the VMS does not recognize the exceedence due to the invalid attitude indication.	**A secondary attitude indicator must be included in the UAV design as a backup to the main attitude indicator. The VMS must receive feedback of a vacuum pump failure so that it can switch to the secondary attitude feedback**
The VMS provides a roll, pitch, or yaw command that is appropriate for staying within the UAV attitude limits. The actuator was connected to the cables backwards, and the VMS input has the opposite effect (roll left input rolls UAV right). The VMS continues to command in the same direction in an attempt to correct the attitude eventually exceeding aircraft limits.	**After any control surface related maintenance, a controls check must be accomplished. A controls check must also be accomplished during preflight. Consider different connectors for the different directions so that it cannot physically be connected backwards.**

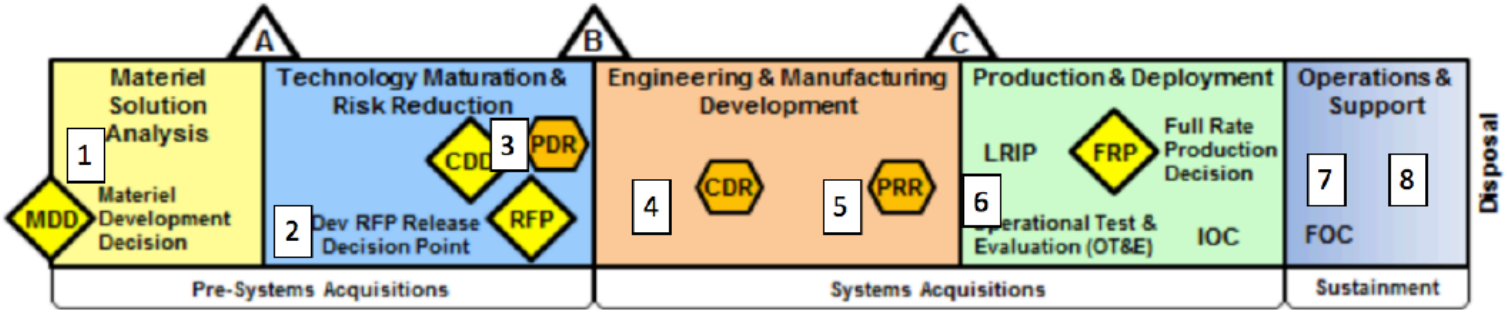
How to Deal with 100s of Constraints

- Found 487 scenarios & associated constraints!
- How do we deal with that?
  - Find duplicate constraints
  - Constraints that already exist in current guidance
  - Some scenarios have multiple potential constraints
  - Organize the remaining in a way to help execute them
    - Example: Design, Test, Maintenance, Operations
    - Test Organization: Questions, Deficiencies, Operational procedures

Let’s look at the bigger picture.

STPA Implementation within AF Acquisitions

1. Concept evaluations during MSA
2. Technical requirement definition
3. Analysis of preliminary design
4. Analysis during EMD
5. Analysis of manufacturing
6. DT & OT may find deficiencies
7. O&S – updates during life of system
8. Mishap investigations

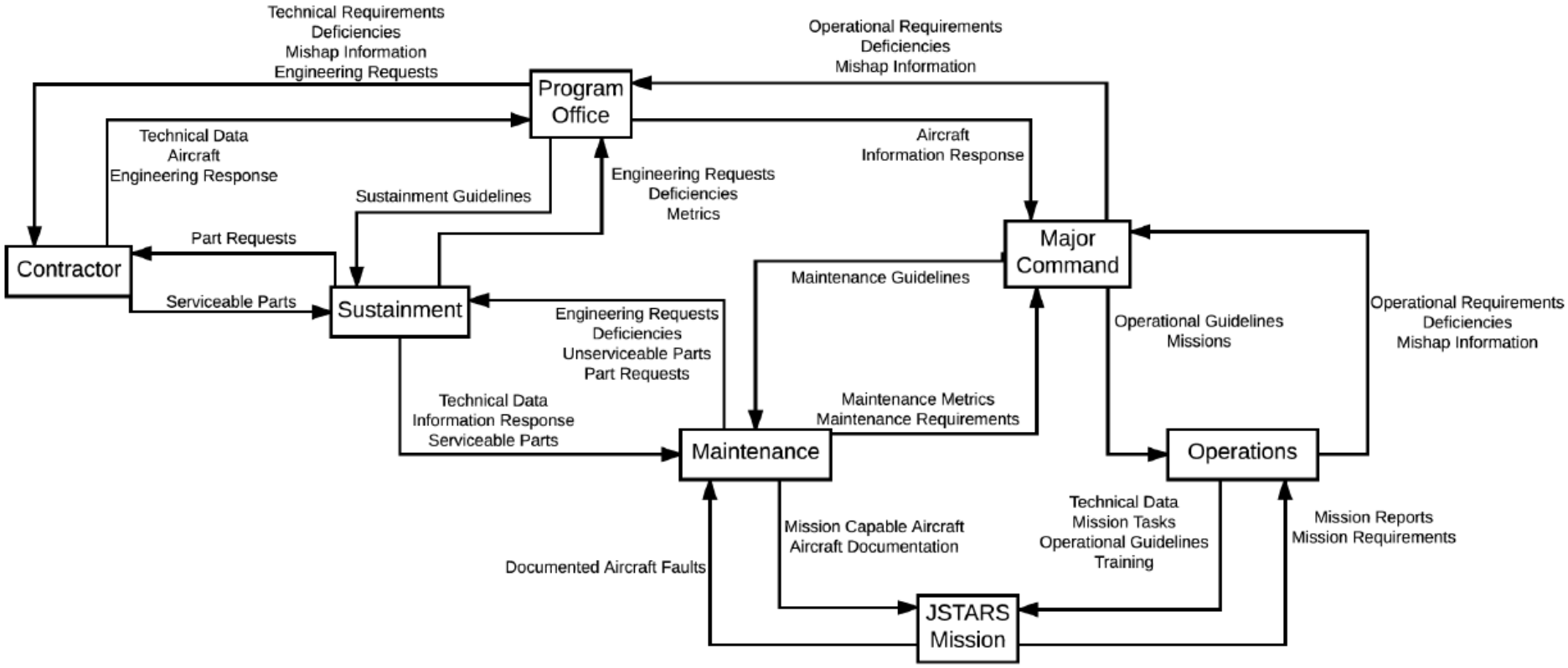


STPA is an iterative process that flows with the design and is utilized throughout the lifecycle of the system.

STPA Application to Airworthiness

- STPA Compliance with MIL-HDBK-516C
  - Aids inspection of documentation
  - Identifies flight critical components
  - Considers more than component failure
  - Will be updated throughout lifecycle (modifications, support & operational changes)
  - Analysis may be scoped as appropriate (aircraft system only, logistics, operations, etc)

Support System



Final Thoughts

- Step 2 process leads to more complete scenario list
- STPA should be used throughout the acquisition lifecycle to incorporate safety from the outset through decommissioning
- STPA supports airworthiness & enables documentation inspection
- STPA can help the program office define support structure

Questions?

Thank you for your time!