Adopting STPA within the FAA - an eVTOL test case

2026 MIT STAMP Workshop proposal

Michael Bartron & Johannes vanHoudt

U.S. Federal Aviation Administration

24 March 2026

Acknowledgement and Disclaimer

The views expressed in this presentation are those of the presenters and do not reflect the official policy or position of the Federal Aviation Administration or the United States Government

Project Overview

1. Follow-on from recommendations in the 2024 FAA Report "*Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety*"
2. FAA team applied STPA to an eVTOL concept, representative of emerging technologies and certification challenges
   - Used high-level system descriptions (battery, BMS, propulsion, navigation, pilot)
   - Focused on system-level control structures and interactions. Didn't consider component failure rates or quantitative risk
3. Intended to "stress-test" the STPA method among multiple learning curves
   - STPA novices (not experts) conducted the project
   - Organization early in adoption of STPA
   - Support/facilitation provide by MIT

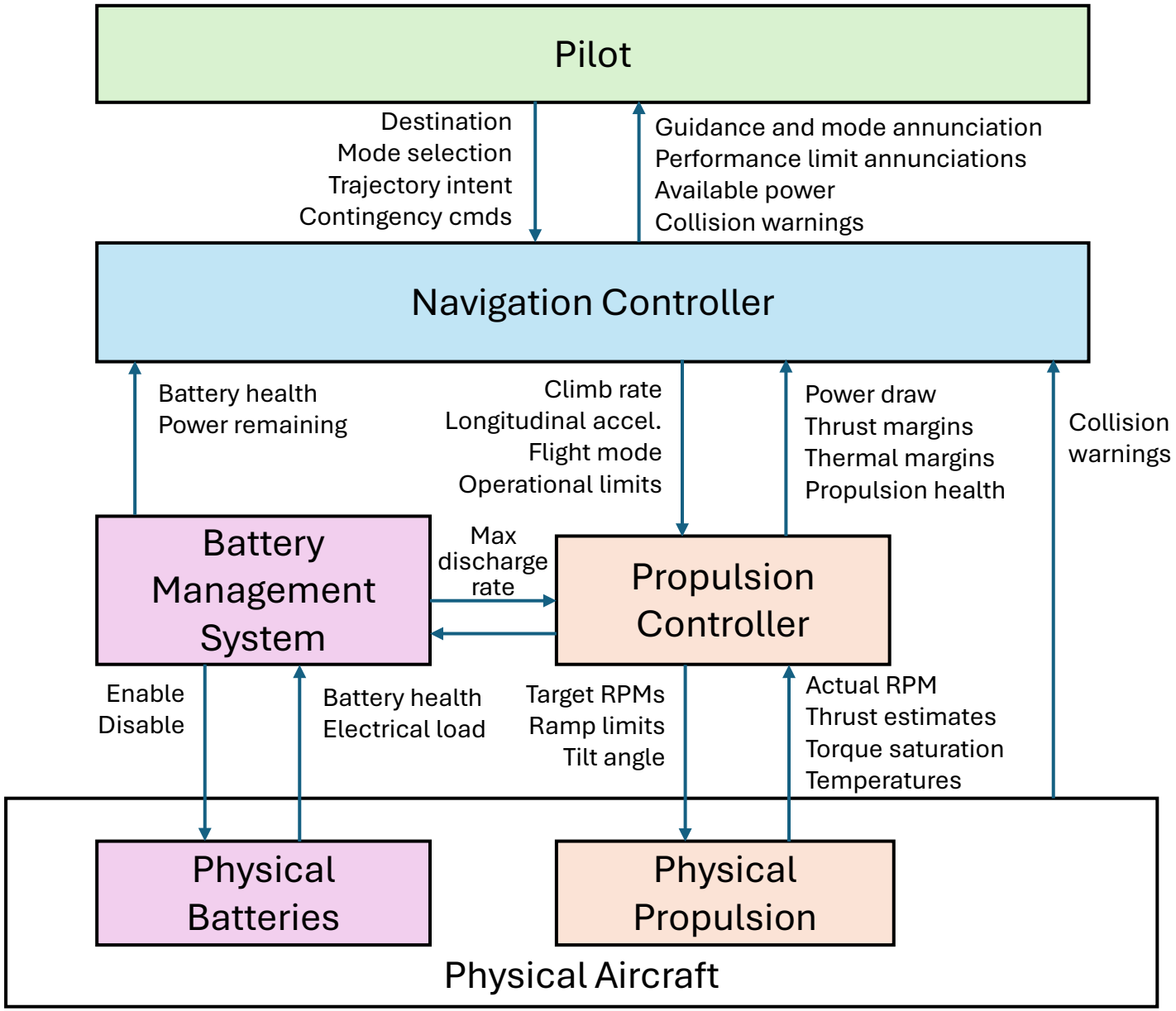
How to prepare for successful adoption of STPA into a regulator's operations?

Project Objectives

1. Assess application of STPA early in the product lifecycle (design and certification)
2. Explore the ability of STPA to address novel, highly-integrated systems (eVTOL)
3. Understand how STPA can reveal cross-domain safety issues (energy, automation, human factors)
4. Understand the type and quality of questions and insights generated through STPA
5. Evaluate practicality of STPA during early learning curves and under time-constraints

How can STPA identify new areas of concern or topics to consider?

STPA Control Structure



This is only a representative example only and is incomplete

Before STPA:

- **Siloed** regulatory teams
- **Piecemeal** approach focusing on detailed requirements in each domain
- Insufficient consideration of the **overall system-level design**

Team 1: Battery

Team 2: Propulsion

Team 3: Autonomy

Team 4: Human Factors

STPA emphasized the **interactions** between multiple domains

Examples of questions raised by STPA

Temporal mismatches

- How long does the navigation controller believe a battery limit will persist? How can this assumption be violated by future BMS feedback?
- Can short-duration battery alarms (transient current spike) cause longer-lasting automation mode changes that outlive the actual hazard?
- When the BMS reports “reserve energy remaining,” what assumptions are made about future propulsion states? (e.g., steady cruise, hover, or emergency maneuvering)

Examples of questions raised by STPA

Controller-authority conflicts

- Under what conditions can the BMS correctly declare a power-limited state while the navigation controller still assumes sufficient control authority to execute collision-avoidance maneuvers?
- Can propulsion response to a BMS-imposed power cap unintentionally reduce control authority below what navigation assumes is available?
- How can “available thrust” be interpreted differently by different controllers, given that battery limits are time-dependent (e.g., peak power possible for 5 seconds but not 10)?

Examples of questions raised by STPA

Human factors

- What if the battery alarm is technically correct but operationally misleading? (e.g., reaching conservative threshold during momentary aggressive maneuvering)
- Could pilots misinterpret battery-protective behavior as a propulsion fault or flight-control anomaly?
- When an anomaly is detected, new limits are immediately imposed. Can these hard limits introduce new human factors vulnerabilities? Should the technology follow a gradual performance degradation as battery limits approach?
- If BMS conflicts with collision avoidance autonomy, can the pilot realistically diagnose the problem immediately and provide safe overrides?

Project Observations

1. Overall Conclusions
2. Limitations Observed
3. Strengths Observed
4. Takeaways – STPA
5. Takeaways – Effort and Practicality
6. Alignment with Industry Experience

Overall Conclusions

1. Applying STPA to an eVTOL concept meaningfully improved system understanding, even with limited time and novice analysts
2. STPA consistently surfaced important cross-domain questions (battery–propulsion–automation–pilot) that can be overlooked
3. Many of the issues identified by STPA involved no component failure. Issue arose from:
   - correct system behavior that proves unsafe in a new context,
   - conservative protections that can backfire,
   - human responses to system feedback
4. STPA proved particularly effective at identifying safety-critical interactions early
5. The project demonstrated that STPA was practical, in the presence of multiple learning curves

Limitations Observed

1. STPA does not:
   - Calculate probabilities or failure rates
   - Decide how much redundancy is “enough” (e.g., 2 vs. 3 sensors)
2. STPA is not focused on purely physical damage mechanisms, such as:
   - structural integrity losses
   - material selection (e.g., flammability)

Strengths Observed

1. STPA explicitly evaluates how automation and equipment influence human behavior
2. STPA captures cases where software behaves as designed, but the resulting system behavior is unsafe
3. STPA addresses safety-critical scenarios outside the scope of ARP4761, including:
   - authority conflicts
   - mode confusion
   - autonomy timing and prioritization
4. STPA forces consideration of humans, software, and hardware together, rather than in isolation

Takeaways – STPA

1. STPA is well suited for:
   - highly integrated, software-intensive systems
   - novel architectures with limited historical data (e.g., eVTOL)
   - early design and certification phases
2. STPA addresses different classes of hazards, especially those involving human–automation interaction and controls
3. STPA is particularly strong at identifying:
   - unsafe control actions
   - unintended consequences of protection logic
   - “zero-point failures” where nothing has failed in the traditional sense

Takeaways – Effort and Practicality

1. The STPA effort required **far less time** than traditional hazard approaches
2. Most effort was spent on:
   - understanding the control structure
   - clarifying assumptions between domains
3. The analysis did not require detailed failure rates, architectures, or redundancy models to be useful
4. Value was realized early, without having a mature design

Alignment with Industry Experience

1. Findings are consistent with public industry results, including:
   - Rolls-Royce's application of STPA to FADEC thrust control
   - STPA identifying conditions leading to dual-engine shutdowns that were later observed in service and not captured by ARP4761
2. Previous FAA and industry empirical studies have shown similar outcomes
3. Appendix D of the FAA STPA report summarizes 60 other aviation STPA applications by industry and the results

Next Steps for the FAA

1. Continue exploring STPA in context of aviation safety, including -
   - eVTOL
   - Autonomy
   - Remote piloting operations
   - Urban Air Mobility
   - Other novel applications

2. Encourage early use of STPA to inform:
   - System requirements
   - Automation development
   - Human factors integration into safety assessments

Recommendations for Industry

1. Consider using STPA:
   - early in design, before detailed design decisions are fixed
   - to examine interactions across disciplines, not just within them
2. Use STPA results to:
   - inform design decisions
   - strengthen safety assessments
   - identify human–automation risks early
3. Engage FAA early in your project. Current certification projects are using STPA applications, particularly for eVTOL and other emerging technologies.

Industry engagement is welcome and encouraged.