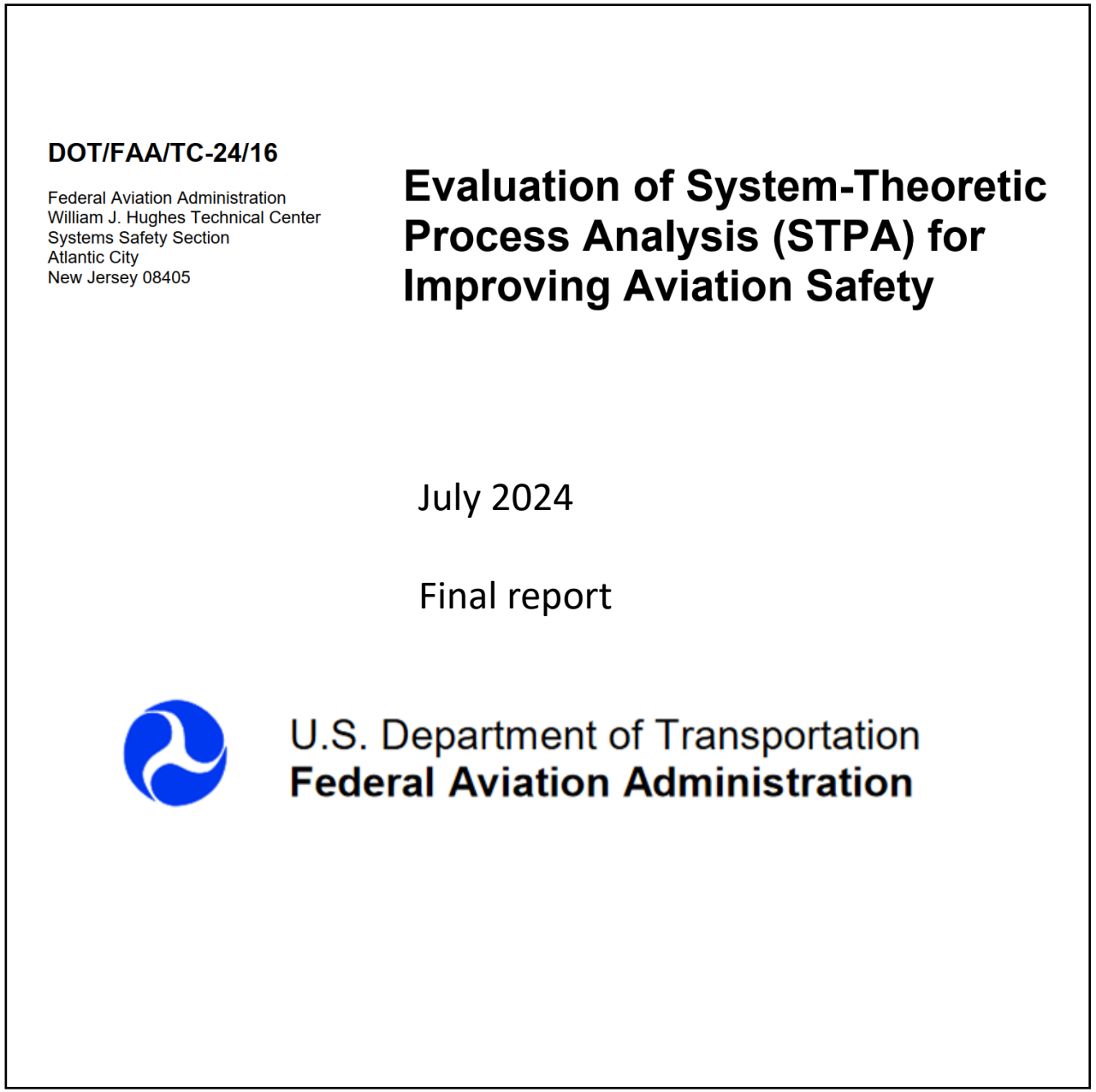
Regulator Evaluations of STPA in Aviation

John Thomas (MIT)

Overview

- FAA-sponsored project
- Goal: Review and evaluate STPA
- Link to Final Report (PDF)



DOT/FAA/TC-24/16

Federal Aviation Administration
William J. Hughes Technical Center
Systems Safety Section
Atlantic City
New Jersey 08405

Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety

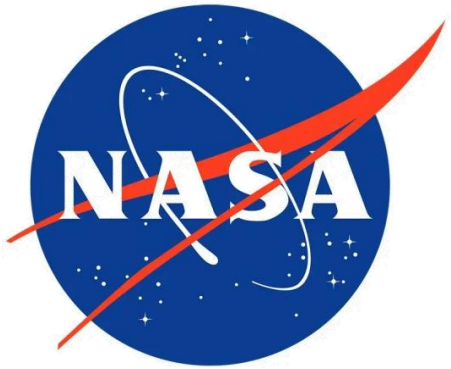
July 2024

Final report

U.S. Department of Transportation
Federal Aviation Administration

Project team that evaluated STPA:











DOT/FAA/TC-24/16

Federal Aviation Administration
William J. Hughes Technical Center
Systems Safety Section
Atlantic City
New Jersey 08405

Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety

July 2024

Final report

U.S. Department of Transportation
Federal Aviation Administration

Who are the Regulator SMEs?

FAA
AIR-600 – Policy and Standards Branch
AIR-620 – Technical Policy Branch
AIR-621 – Flight Test & Human Factors
AIR-627 – System Safety Assessment Group
AIR-640 – Systems Engineering Branch
AIR-700 – Compliance & Airworthiness
AIR-710 – Flight Test & Human Factors Branch

NASA
Aeronautics Research Institute (NARI)

ICAO
- Human Performance Study Group
- Safety Management Section

ANAC
Aeronautical Product Certification Branch (GCPP)

EASA
- Certification Directorate
- Strategy & Safety Management Directorate

SME = Subject Matter Expert

The Plan

Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	
2) Identify key questions that should be asked to evaluate STPA	
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	
5) Answer the key questions from #2	

SME = Subject Matter Expert

The Plan

Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	**Regulator SMEs**
2) Identify key questions that should be asked to evaluate STPA	**Regulator SMEs**
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	- *STPA Class: Taught by John Thomas* - **Apply STPA: Regulator SMEs** - **STPA Projects: Regulator SMEs**
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	**Regulator SMEs**
5) Answer the key questions from #2	**Regulator SMEs**

SME = Subject Matter Expert

The Plan

Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	**Regulator SMEs**
2) Identify key questions that should be asked to evaluate STPA	**Regulator SMEs**
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	- *STPA Class: Taught by John Thomas* - **Apply STPA: Regulator SMEs** - **STPA Projects: Regulator SMEs**
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	**Regulator SMEs**
5) Answer the key questions from #2	**Regulator SMEs**

SME = Subject Matter Expert

SME Analysis of Regulatory Environment

- “The traditional safety approaches that are required today **are heavy and burdensome** for industry.”
- “The regulatory environment has been **inflexible** and has **struggled to adapt** as new technologies and new methods are created.”
- “It is a challenge to keep pace with new developments from industry given the **limited resources on the regulatory side** and the complex processes we use.”
- “There are several constraints: the current approaches that we use require **tremendous work**, the **complexity** of the technologies we must evaluate is increasing, and the **regulatory resources** are not going to be increasing. At least one of these needs to change.”

SME Analysis of Regulatory Environment (3)

- "**New technologies** are a big challenge. Regulatory agencies are in "catch-up" mode, and we are realizing that less is known about VTOL than was generally assumed."

- "The regulatory environment is being challenged by ever-increasing integration levels and an ever-decreasing level of human understanding of automation behaviors. **New approaches are needed to address these challenges.**"

- "The **high cost** and length of today's certification process is a significant barrier."

SME Analysis of Regulatory Environment (2)

- “Some regulatory **gaps are already identified** and have been known for some time, such as lack of human factors integration, but there has **not been enough regulatory effort** to formally recognize practical solutions that address these gaps.”

- “There is **little or no incentive** for industry to share new safety concerns from new, more powerful methods with regulators in the absence of clear regulatory policies or guidance about the new methods.”

The Plan

Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	**Regulator SMEs**
2) Identify key questions that should be asked to evaluate STPA	**Regulator SMEs**
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	- *STPA Class: Taught by John Thomas* - **Apply STPA: Regulator SMEs** - **STPA Projects: Regulator SMEs**
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	**Regulator SMEs**
5) Answer the key questions from #2	**Regulator SMEs**

SME = Subject Matter Expert

Key Questions from Regulator SMEs

- Does STPA provide value beyond what is typically done today?
- Would increased industry use of STPA improve aviation safety?
- Would regulator use of STPA help better achieve regulator safety objectives?
- Does STPA address important gaps that exist in current approaches today?
- Would applying STPA to aviation systems produce important safety insights beyond what our current processes find?
- Does STPA provide a way to identify interactions or scenarios relevant to regulatory safety objectives that can be overlooked today?
- Does STPA provide a stronger way to identify critical automation or software assumptions during a safety assessment?

Key Questions from Regulator SMEs (2)

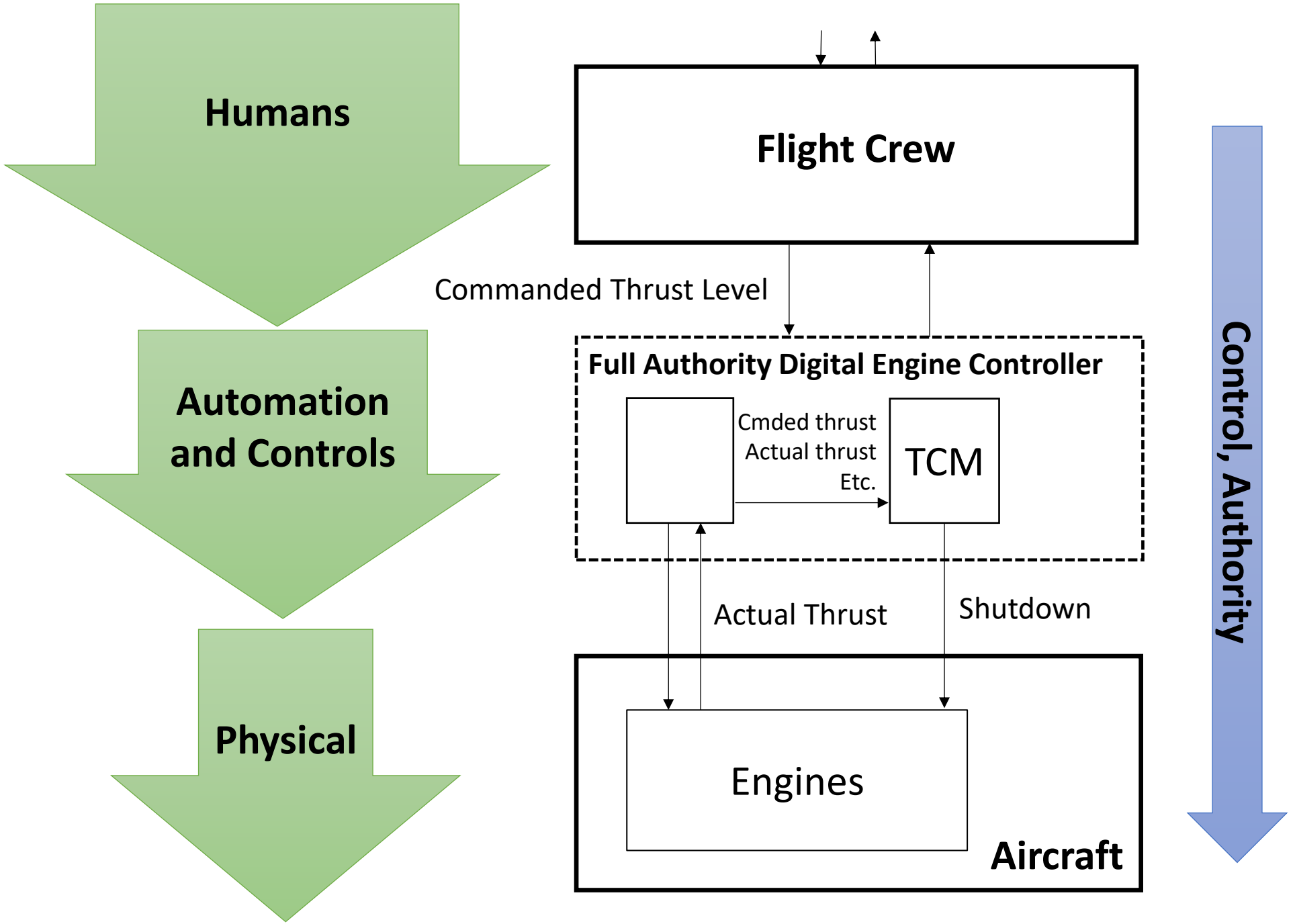
- Does STPA provide a stronger way to identify critical human factors assumptions during a safety assessment?
- Does STPA provide a stronger way to integrate human factors into an overall safety assessment beyond what is done today?
- Would STPA catch the 737MAX automation and human factors issues more reliably than the current practice?
- Future technologies like autonomy, AI, and eVTOL are well known to present new challenges beyond the capability of today's safety processes. Does STPA provide a capability beyond current practices that is applicable to future technologies like increasing autonomy and eVTOL?
- Would regulators benefit from using or adopting STPA in some way?
- Should STPA be incorporated into safety assessment processes?

The Plan

Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	**Regulator SMEs**
2) Identify key questions that should be asked to evaluate STPA	**Regulator SMEs**
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	- *STPA Class: Taught by John Thomas* - **Apply STPA: Regulator SMEs** - **STPA Projects: Regulator SMEs**
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	**Regulator SMEs**
5) Answer the key questions from #2	**Regulator SMEs**

SME = Subject Matter Expert

One example developed from public materials



© Copyright John Thomas 2023

Identify Unsafe Control Actions

All of these UCAs describe an unsafe interaction between functions!

These can occur without individual failures.

	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
TCM Shutdown Cmd	TCM provides shutdown cmd when aircraft is in flight [H-2.1]	TCM provides shutdown cmd too late, when aircraft above V1 [H-6]	TCM stops providing shutdown cmd too soon before engine shutdown (thrust matches TLA) [H-6] (also consider before thrust matches TLA or reset)
	TCM does not provide shutdown cmd when engine stuck at high thrust during RTO [H-6]		
	TCM provides shutdown cmd during RTO when engine not stuck at high thrust (RT needed) [H-6]	TCM provides shutdown cmd too late, more than X seconds after engine stuck high [H-6]	TCM provides shutdown cmd too long after problem is resolved, propulsion/restart is needed [H-2.1,6]
	TCM provides shutdown cmd during landing (RT needed) engine not stuck at high thrust [H-6]		

H2.1: Aircraft has insufficient thrust for sustained flight [L1,L2]
H-6: Aircraft inadvertently leaves taxiway or runway [L1,L2]

Note: additional UCAs not shown

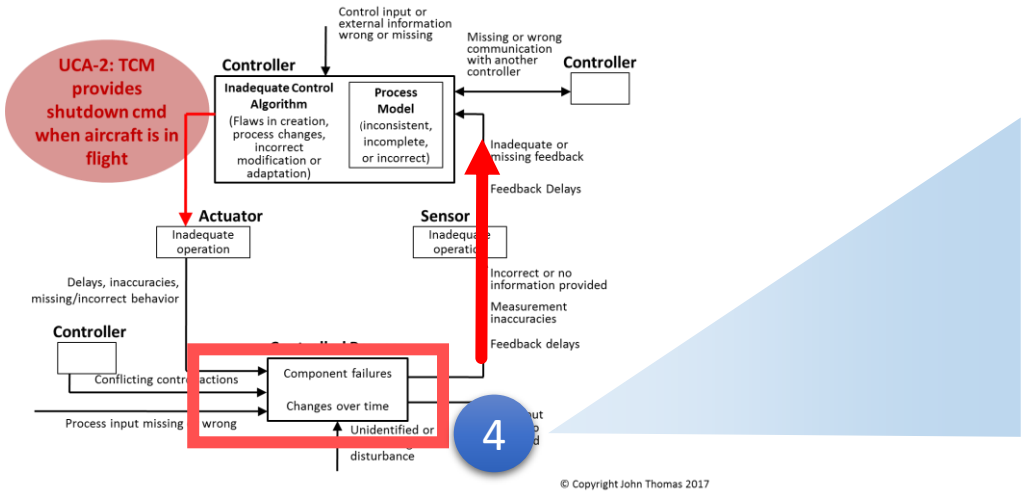
© Copyright John Thomas 2025

STPA Class 2 Scenario Building

UCA-2: TCM provides shutdown cmd when aircraft is in flight

- PM-1: TCM incorrectly believes aircraft on ground
- PM-2: TCM believes engine stuck high
  - Feedback received at TCM:
    - actual thrust input = high
    - commanded thrust input = low

4) How could this unsafe feedback occur without a failure?



Collect all process states so far, convert any feedback to true states (see #4 above):

- **Aircraft is in flight**
- **Engine is stuck high thrust**
- **Actual thrust is high**
- **Commanded thrust is low**

© Copyright John Thomas 2023

STPA Results: Catastrophic Design Flaws Identified

- Example #1: A **combination of two failures** that have a counter-intuitive effect, causing software to command dual engine shutdown in flight, during takeoff, or during landing.
- Example #2: A **single failure** that has a complex effect on multiple software systems, causing software to command dual engine shutdown in flight.
- Example #3: An **interaction between 3 systems**, without any failure, that will cause dual engine shutdown if thrust levers are moved quicker than usual in certain conditions.

These systems were already certified and approved using existing methods

Example Event #1: Dual Engine Flameouts

- 2016: TCM caused dual engine flameouts on aircraft (certified without STPA)
  - Fortunately, no accident—only caused delays
  - Fairly obscure event—not widely known or publicized
  - The TCM flaws exactly match the STPA findings (without any knowledge of the event)

© Copyright John Thomas 2023

Example Event #2: Dual Engine Flameouts

- 2018: TCM caused dual engine flameouts on aircraft (certified without STPA)
  - Fortunately, no accident
  - Aircraft landed and was stuck on runway, crew could not restart engines
  - Maintenance could not locate problem—**no components had failed**
  - Investigation uncovers the TCM flaws
    - The TCM flaws exactly match STPA-identified flaws
    - The design violated regulation, but the flaws were overlooked

© Copyright John Thomas 2023

The Plan

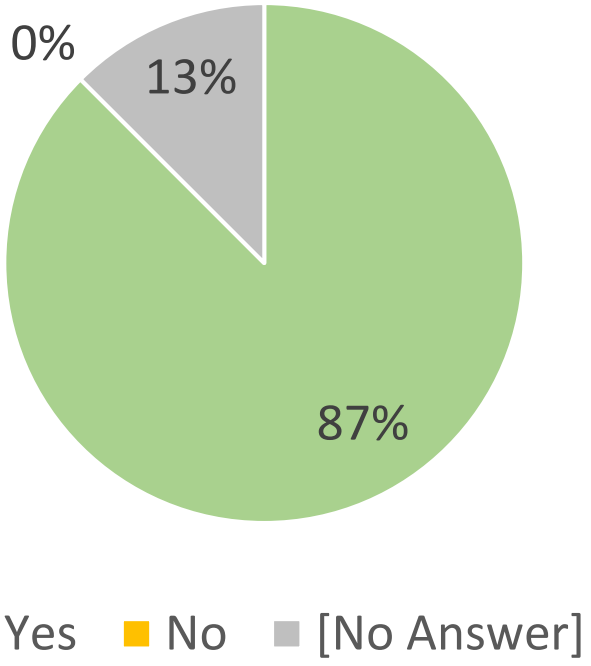
Task	Assigned to:
1) Review the regulatory environment - Identify urgent challenges or gaps that need to be addressed	**Regulator SMEs**
2) Identify key questions that should be asked to evaluate STPA	**Regulator SMEs**
3) Learn STPA - Short training class - Hands-on application of STPA - Complete projects to apply STPA to real systems	- *STPA Class: Taught by John Thomas* - **Apply STPA: Regulator SMEs** - **STPA Projects: Regulator SMEs**
4) Evaluate STPA results compared to - Actual results from standard processes - Actual events in operation	**Regulator SMEs**
5) Answer the key questions from #2	**Regulator SMEs**

SME = Subject Matter Expert

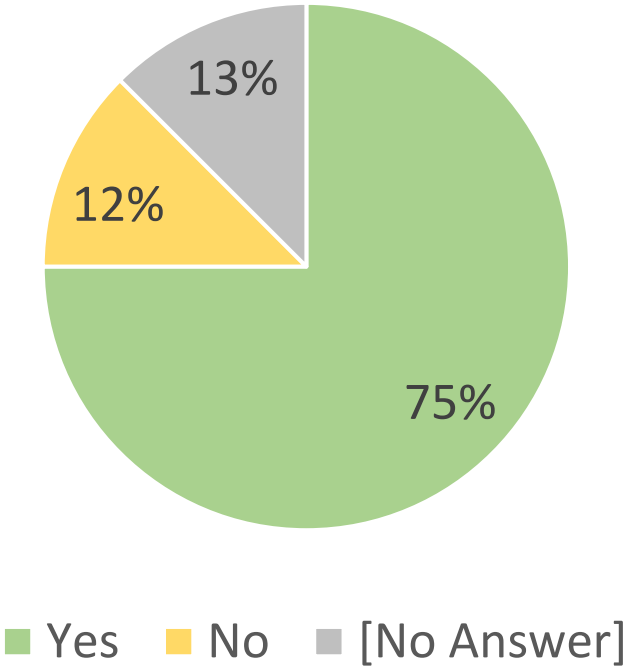
Do you believe STPA *should* be incorporated into safety assessment processes?

Do you believe STPA *will* be incorporated into safety assessment processes in the future?

Do you believe STPA *should* be incorporated into safety assessment processes?



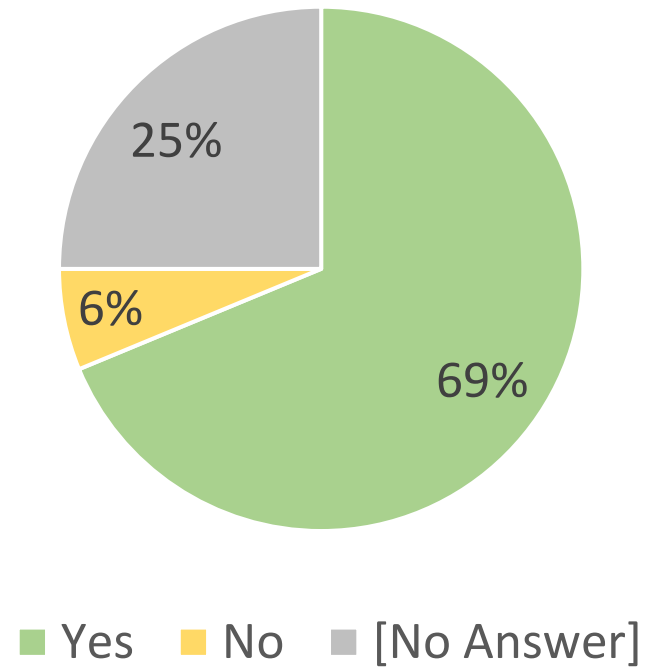
Do you believe STPA *will* be incorporated into safety assessment processes in the future?



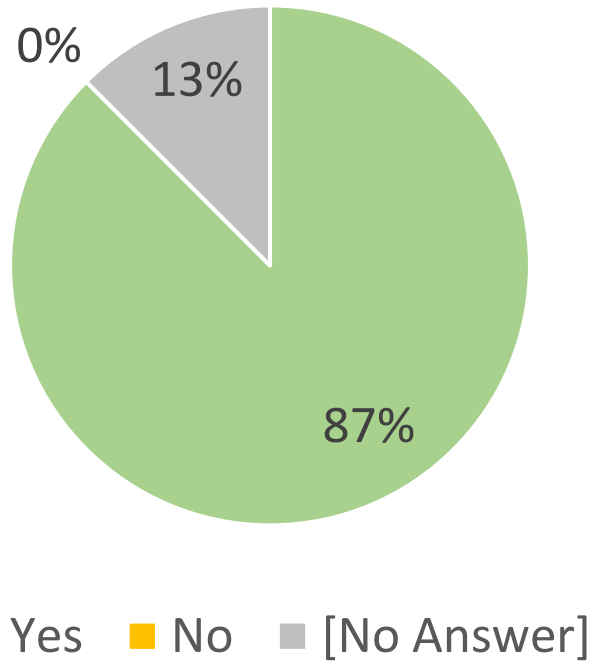
In your view, would STPA catch the 737MAX automation and human factors issues more reliably than the current practice?

Does STPA provide a capability beyond current practices that is applicable to future technologies like increasing autonomy and eVTOL?

In your view, would STPA catch the 737MAX automation and human factors issues more reliably than the current practice?



Does STPA provide a capability beyond current practices that is applicable to future technologies like increasing autonomy and eVTOL?



What were the key insights and “AHA” moments you encountered as you used STPA?

- “The overall STPA method. Thinking of "why would the controller believe it's a good idea to command that action in that context" has a wide field of application.”
- “The possibility to assess a software problem, not a component failure, through STPA. It was not possible with fault tree analysis (FTA), for example.”
- “A certified system (in the case of aviation), working as intended, without any failure, can behave in an unsafe way.”

What were the key insights and “AHA” moments you encountered as you used STPA?

- “That we may be missing key paths to failure by using traditional hazard analysis practices, especially when applied to new and novel technology with high levels of automation.”

SME-Identified Next Steps

- “Pilot programs in coming applications, where STPA will be formally adopted, disclosed, and discussed with us authorities.”
- “Evaluate what could be changed in guidance material and even regulations.”
- “Make STPA a standard part of evaluating new designs and evaluating significant changes to existing designs.”
- “Apply STPA as a part of reviews of designs and changes even if not officially part of the review process.

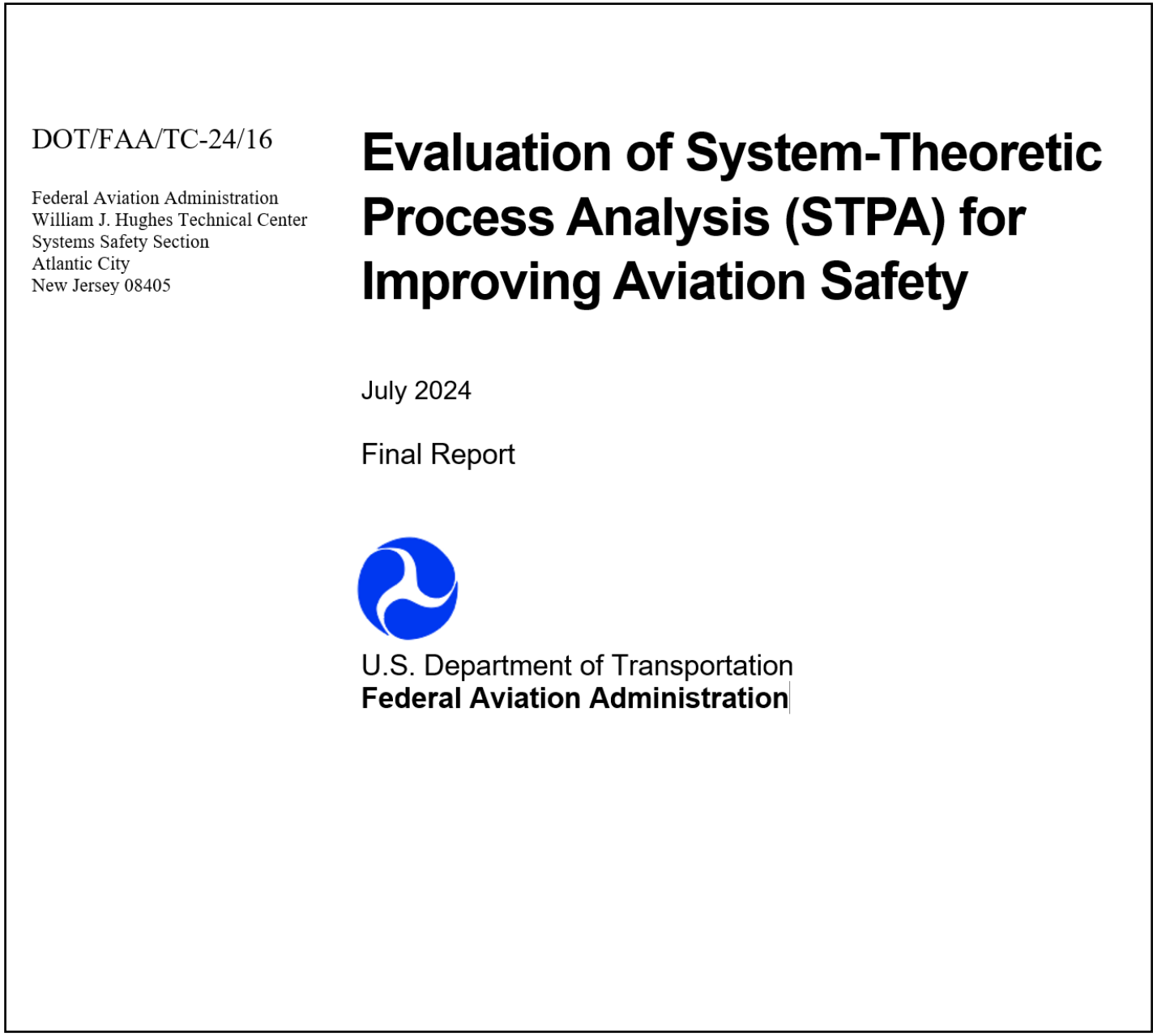
What happens now?

- Forming an Industry Advisory Committee on STPA in aviation
  - Email jthomas4@mit.edu if you'd like to join

- Collaborative STPA project with industry to explore value of STPA and opportunities for certification credit
  - Email jthomas4@mit.edu if you'd like to join

More Information

- FAA Final Report:
- https://rosap.ntl.bts.gov/view/dot/78914/dot_78914_DS1.pdf



DOT/FAA/TC-24/16

Federal Aviation Administration
William J. Hughes Technical Center
Systems Safety Section
Atlantic City
New Jersey 08405

Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety

July 2024

Final Report

U.S. Department of Transportation
Federal Aviation Administration