

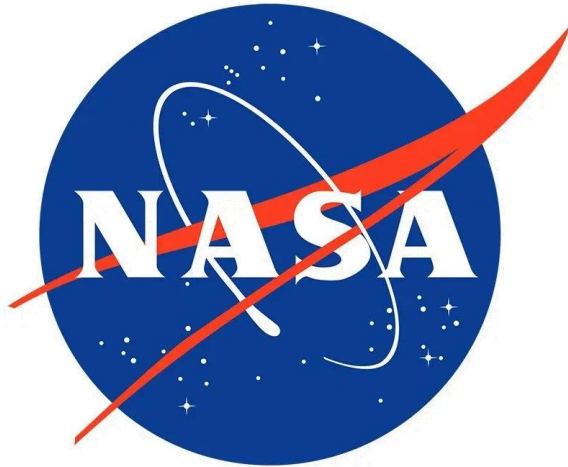
# Regulator Evaluations of STPA in Aviation

Johannes vanHoudt (FAA)

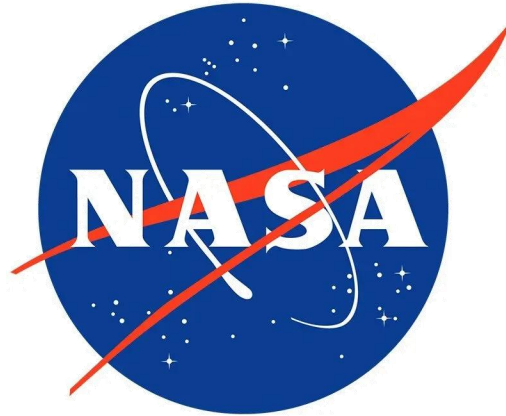
John Thomas (MIT)

# Overview

- FAA-sponsored project to review and evaluate STPA
- Project Team (Regulator SMEs)



# Who are the Regulator SMEs?



ICAO



ANAC  
AGÊNCIA NACIONAL  
DE AVIAÇÃO CIVIL



## 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

# The Plan

1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

# The Plan

1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

# 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)

- “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 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.”
- “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.”

# SME Analysis of Regulatory Environment (2)

- “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.”
- “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.”
- “The high cost and length of today’s certification process is a significant barrier.”

# SME Analysis of Regulatory Environment (3)

“What is most concerning about the regulatory environment is its ignorance and unwillingness to consider the benefits of STPA until now.”

# The Plan

1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

# Key Questions from Regulator SMEs

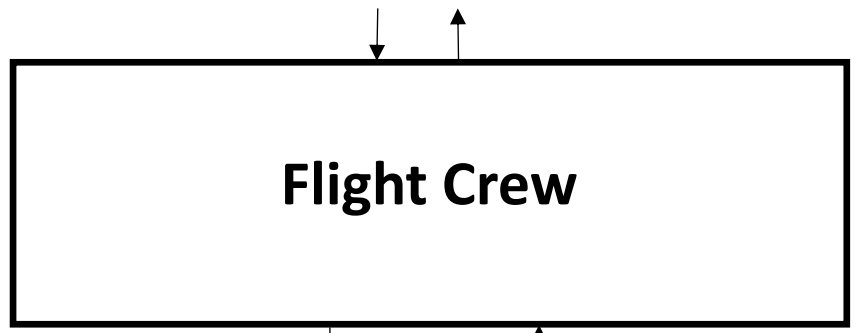
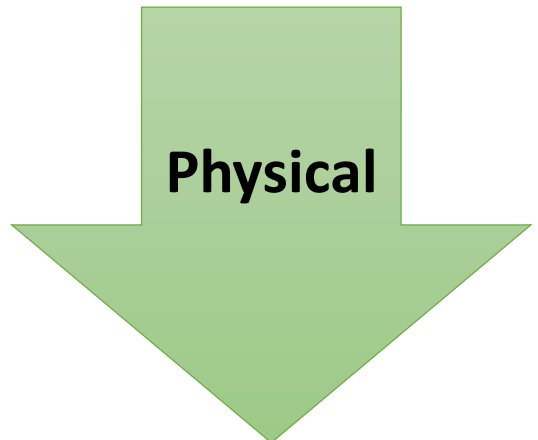
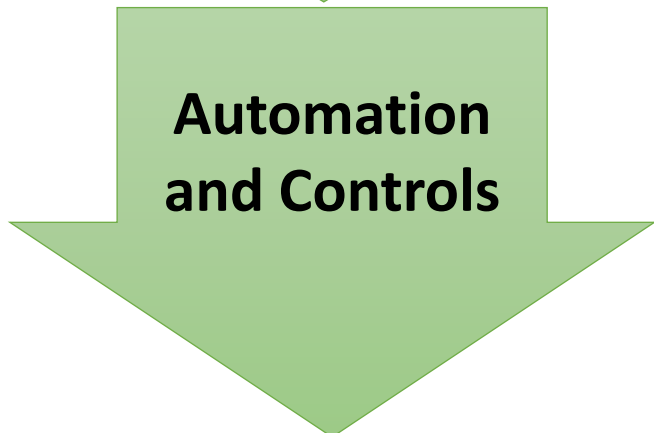
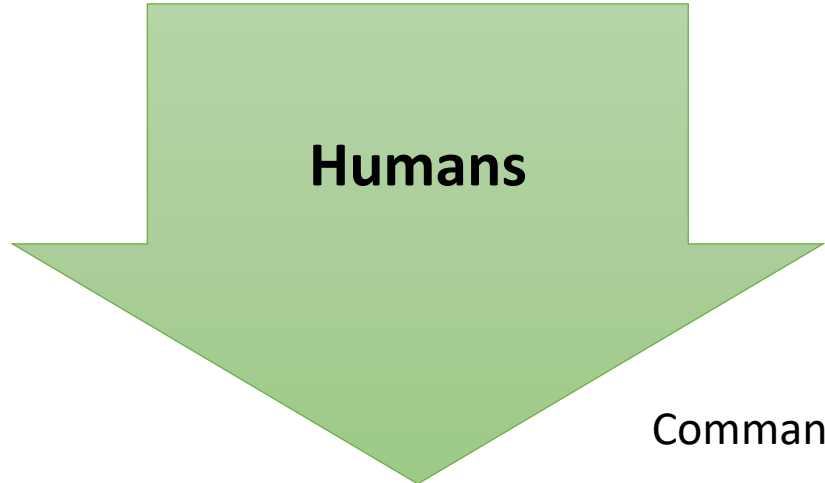
- Does STPA provide value beyond what is typically done today?
- Would increased industry use of STPA improve aviation safety?
- Would regulator use of STPA help better achieve regulator safety objectives?
- Does STPA address important gaps that exist in current approaches today?
- Would applying STPA 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)

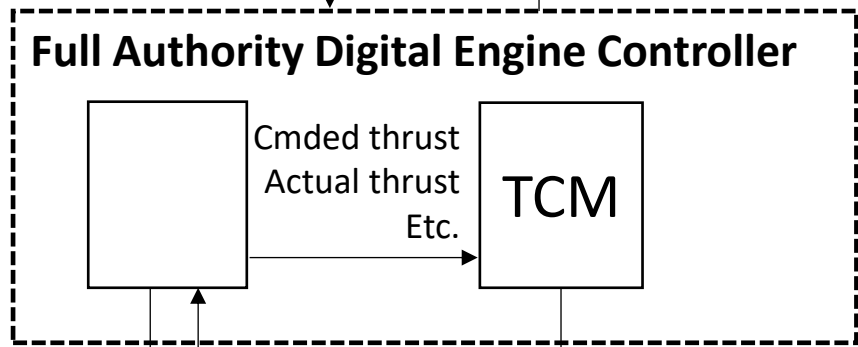
- Does STPA provide a stronger way to identify critical human factors assumptions during a safety assessment?
- Does STPA provide a stronger way to integrate human factors into an overall safety assessment beyond what is done today?
- Would STPA catch the 737MAX automation and human factors issues more 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

1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

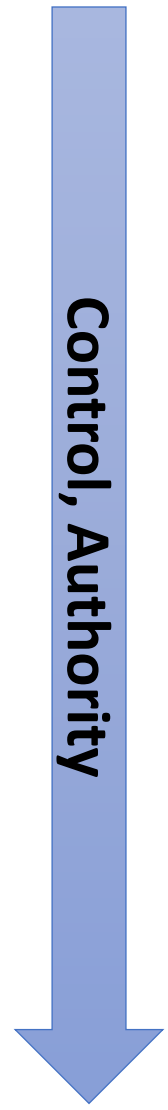
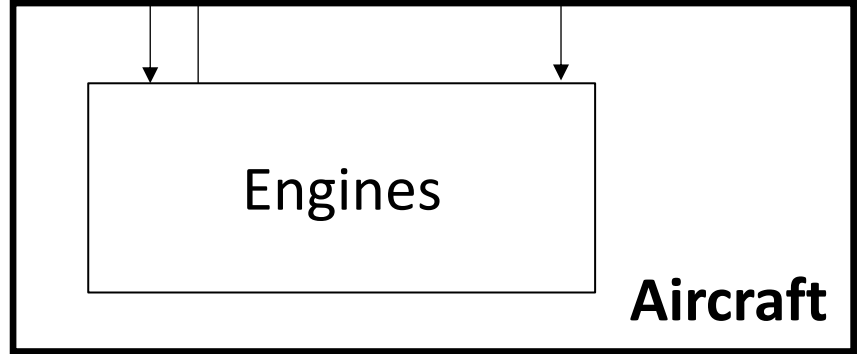


Commanded Thrust Level



Actual Thrust

Shutdown



# Identify Unsafe Control Actions

All of these UCAs describe an unsafe interaction between functions!

These can occur without individual failures.

**TCM Shutdown Cmd**

TCM does not provide shutdown cmd when engine stuck at high thrust during RTO [H-6]

TCM provides shutdown cmd when aircraft is in flight [H-2.1]

TCM provides shutdown cmd during RTO when engine not stuck at high thrust (RT needed) [H-6]

TCM provides shutdown cmd during landing (RT needed) engine not stuck at high thrust [H-6]

Providing causes hazard  
Too early, too late, out of order

TCM provides shutdown cmd too late, when aircraft above V1 [H-6]

TCM provides shutdown cmd too late, more than X seconds after engine stuck high [H-6]

Stopped too soon, applied too long

TCM stops providing shutdown cmd too soon before engine shutdown (thrust matches TLA) [H-6] (also consider before thrust matches TLA or reset)

TCM provides shutdown cmd too long after problem is resolved, propulsion/restart is needed [H-2.1,6]

H2.1: Aircraft has insufficient thrust for sustained flight [L1,L2]

H-6: Aircraft inadvertently leaves taxiway or runway [L1,L2]

Note: additional UCAs are excluded in the interest of time

© Copyright John Thomas 2025

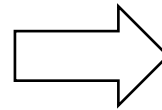
# Class 2 Scenario Building

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

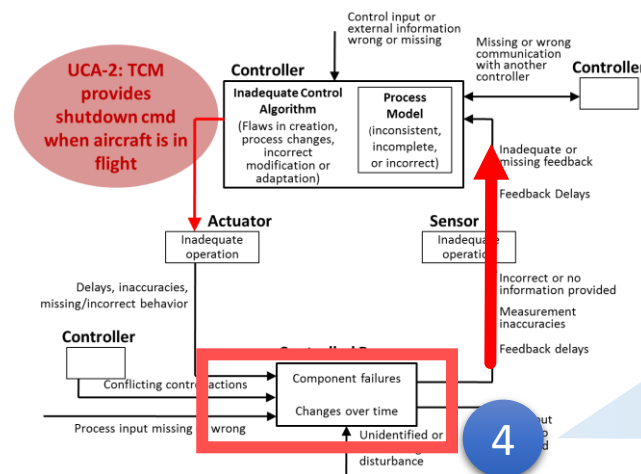
PM-1: TCM incorrectly believes aircraft on ground

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

# 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! They are flying right now!

# The Plan

1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

# 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)

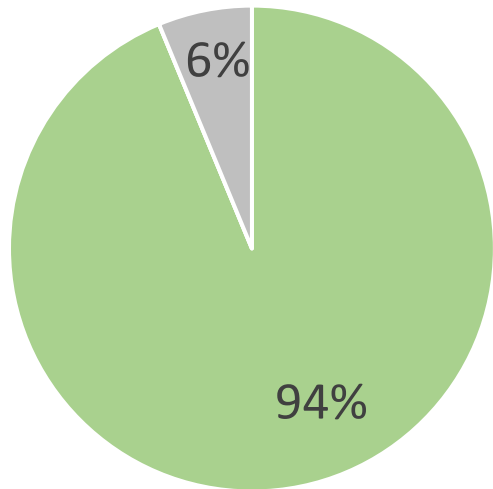
# Example Event #2: Dual Engine Flameouts

- 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

# The Plan

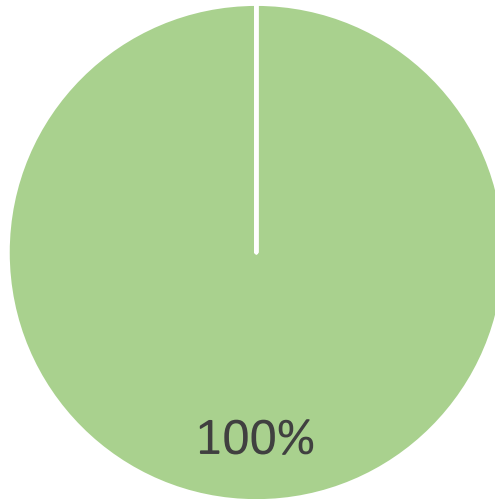
1. Regulator SMEs review the regulatory environment to identify urgent challenges or gaps that need to be addressed.
2. Based on #1, SMEs identify key questions that should be asked to evaluate STPA
3. SMEs learn STPA
  - Short training class
  - Hands-on application of STPA
  - Projects to apply STPA to real systems
    - (... that were already approved using standard processes)
4. Another team collects data about actual operational events involving these systems
  - Then, SMEs compare: STPA results, standard processes, and actual events
5. Regulator SMEs evaluate STPA in terms of the key questions from #2

Does STPA address important gaps that exist in current approaches today?



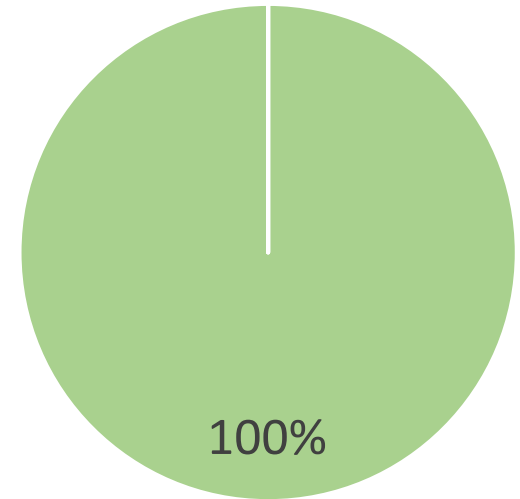
■ Yes ■ No ■ [No Answer]

Do you believe that applying STPA to aviation systems will produce important safety insights beyond what our current processes find?



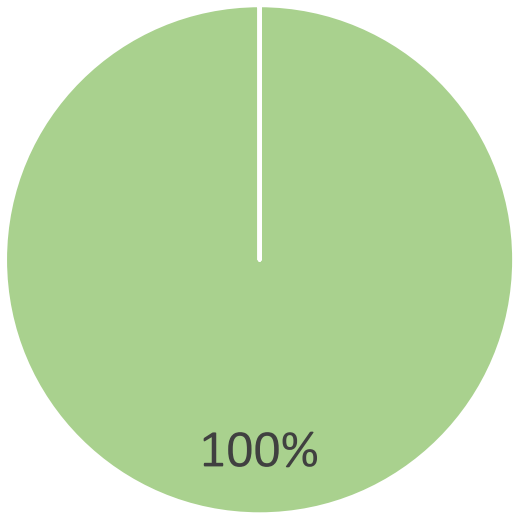
■ Yes ■ No ■ [No Answer]

Does STPA provide a way to identify interactions or scenarios relevant to regulatory safety objectives that can be overlooked today?



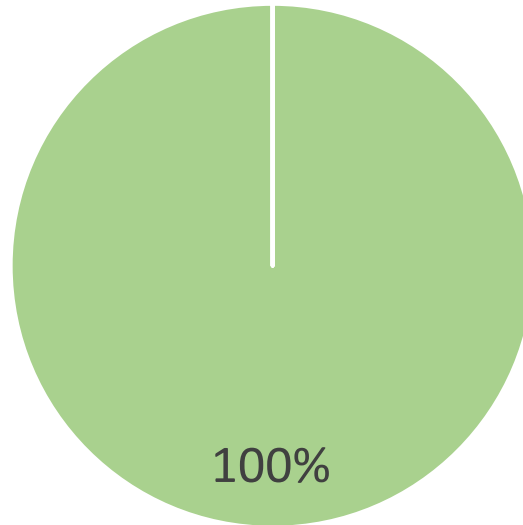
■ Yes ■ No ■ [No Answer]

Does STPA provide a stronger way to identify critical automation or software assumptions during a safety assessment?



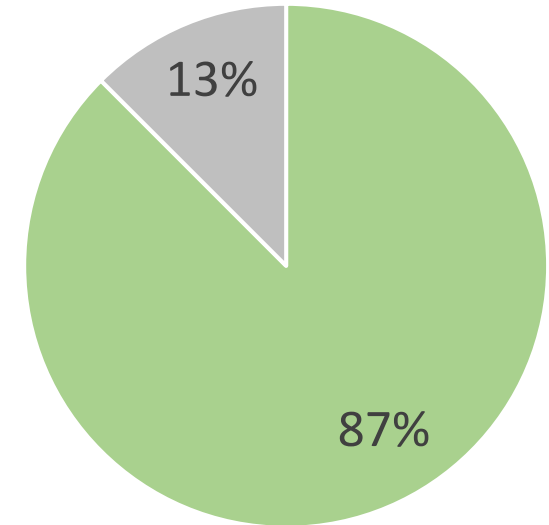
■ Yes ■ No ■ [No Answer]

Does STPA provide a stronger way to identify critical human factors assumptions during a safety assessment?



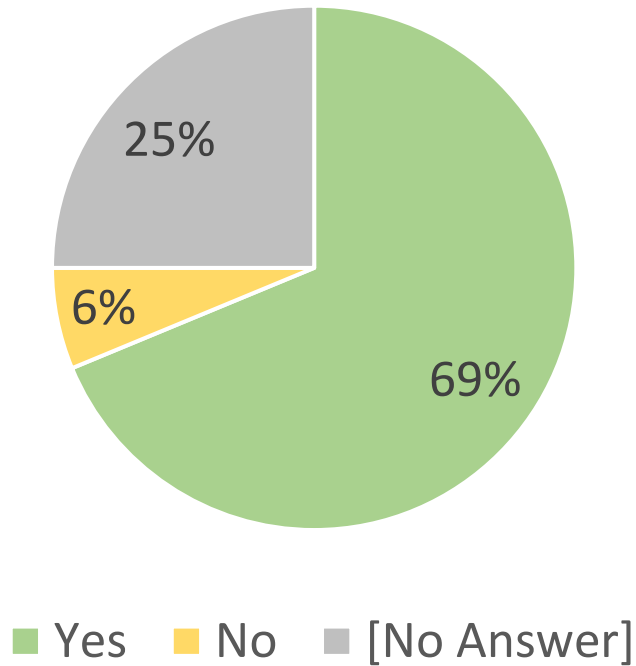
■ Yes ■ No ■ [No Answer]

Does STPA provide a stronger way to integrate human factors into an overall safety assessment beyond what is done today?

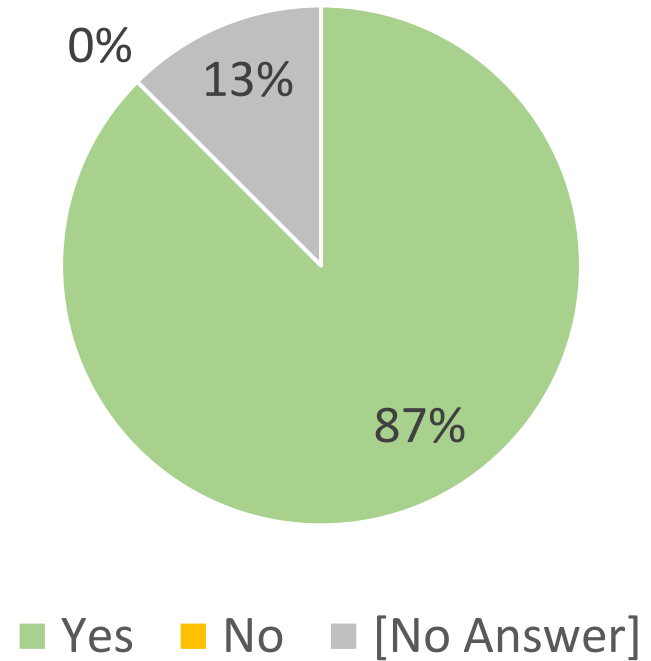


■ Yes ■ No ■ [No Answer]

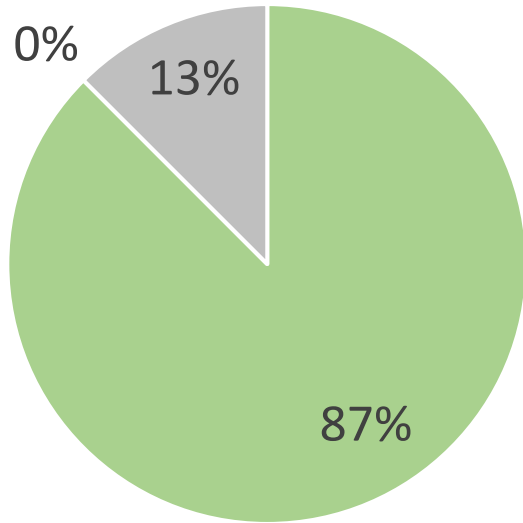
In your view, would STPA catch the 737MAX automation and human factors issues more reliably than the current practice?



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

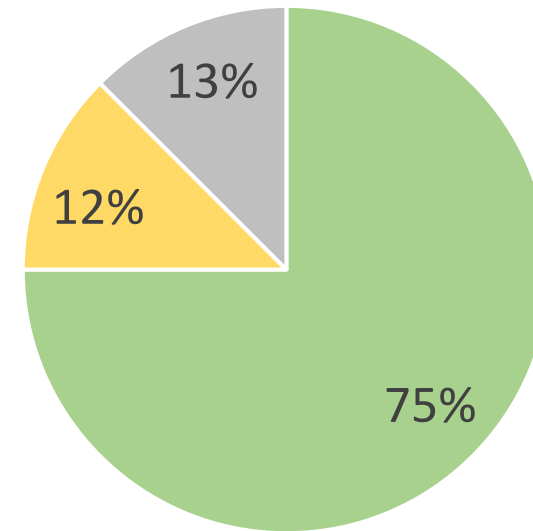


Do you believe STPA \*should\* be incorporated into safety assessment processes?



■ Yes ■ No ■ [No Answer]

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



■ Yes ■ No ■ [No Answer]

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

- “Ability to capture ‘no failure’ scenarios and develop constraints.”
- “Ability to identify other scenarios not captured by the established methods.”
- “STPA strengths to overcome our current challenges in managing safety.”
- “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?

- “The possibility to assess a software problem, not a component failure, through STPA. It was not possible with fault tree analysis (FTA), for example.”
- “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 STPA method brings the analyst to ask given questions and forces thinking of the overall problem, not just the numbers.”

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

- “Using traditional techniques based on probability, we can “what if” everything into oblivion. Using STPA will allow concepts and architectures that will lead to the next big leap in aviation automation and safety.”
- “STPA is especially important to identify losses that occur without any system failure and is possibly the only method capable of doing it systematically.”
- “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.”
- “Require a more robust analysis of system behavior losses that may occur without failures, as STPA does.”
- “Apply STPA as a part of reviews of designs and changes even if not officially part of the review process.

# More Information

- FAA Final Report:
- [https://rosap.ntl.bts.gov/view/dot/78914/dot\\_78914\\_DS1.pdf](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**