ERRATA

Report No. DOT/FAA/TC-24/16 Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety

May 2025

Prepared for

Department of Transportation
Federal Aviation Administration
William J. Hughes Technical Center for Advanced Aerospace
Atlantic City International Airport, NJ 08405

Updated to add Sponsoring Agency Code in Block 14 of the Technical Documentation Page. Please replace file tc24-16.pdf, dated 8/1/2024 with the attached file tc24-16.pdf, dated 5/2/2025.

Released May 2025

1 Attachment: tc24-16.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

NOTICE

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-24/16		

4. Title and Subtitle	5. Report Date
Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety	July 2024
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
John P. Thomas and John G. Van Houdt	DOT/FAA/TC-24/16
9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Center for Aviation Safety Advanced Engineering Services 39B W Brookfield Rd N Brookfield, MA 01535	11. Contract or Grant No.
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Aviation Administration William J. Hughes Technical Center Building 300, Fourth Floor Atlantic City International Airport Atlantic City NJ 08405	14. Sponsoring Agency Code ANG-E27

15. Supplementary Notes

This research and development effort was jointly sponsored between AIR 62B (Product Policy Management Section) and AIR 714 (Flight Test Branch, Policy and Standards Section). John Van Houdt and David Sizoo were the sponsors.

16. Abstract

This report summarizes the results of a joint effort by civil aviation authorities to learn System-Theoretic Process Analysis (STPA) and evaluate its applicability to aviation safety including safety management, aircraft development, safety assessment, and certification. Subject matter experts (SMEs) from FAA, EASA, ANAC, ICAO, and NASA participated to investigate STPA's capabilities, existing STPA uses in industry, STPA results and findings that have been produced by industry, and how the STPA method and its capabilities compare to current approaches and recent accidents, including 737MAX. The SMEs explored STPA during a series of technical interchange meetings, workshops, and hands-on projects where participants reviewed STPA and applied the methodology to real systems. The SMEs from these agencies identified STPA benefits, limitations, and applicability for use by both regulatory authorities and industry. The findings are summarized in this report.

17. Key Words	18. Distribution Statement
STPA, development, safety assessment, safety management systems, aircraft certification, 737MAX, eVTOL, emerging technologies, human factors	No restrictions. This document is available through the National Technical Information Service. 5285 Port Royal Road Springfield, VA 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	70	

Contents

Executive summary

This report summarizes a joint effort by civil aviation authorities to evaluate System-Theoretic Process Analysis (STPA) and its applicability to aviation safety including safety management, aircraft development, safety assessment, and certification. Subject Matter Experts (SMEs) from FAA, EASA, ANAC, ICAO, and NASA participated in this FAA-sponsored project.

The interagency SMEs explored STPA during a series of technical interchange meetings, workshops, and hands-on projects where participants applied the methodology themselves to real systems. The SME participants reviewed and evaluated the STPA method, including STPA's capabilities, regulatory challenges with respect to STPA, existing STPA results and findings from industry, STPA use as an alternative stand-alone or a complementary approach, and how the STPA method compares to current approaches. Participants developed recommendations for future STPA use by authorities and by industry.

This report does not attempt to duplicate the existing literature that explains each step of the STPA method in detail (Leveson & Thomas, 2018). This report focuses on the findings from the collaborative, international effort to learn STPA and to evaluate its capabilities, uses, and other findings as they relate to aviation safety.

The key findings from SME participants at FAA, EASA, ANAC, ICAO, and NASA include:

1. SME participants demonstrated the ability to effectively use STPA to discover real flaws in design, requirements, human interactions, and operations that were overlooked by independent teams using existing methods.
2. SME participants identified gaps, barriers, and other concerns regarding the ability of the current regulatory environment to handle increasingly complex modern technologies, future technologies, and future operational concepts that are being created.
3. SME participants found that STPA addresses important gaps that exist in standard approaches to safety that are used today.
4. SME participants found that STPA provides a way to identify interactions and scenarios relevant to regulatory safety objectives that can be overlooked by current methods.
5. SME participants found that applying STPA to aviation systems produces important safety insights beyond what current processes find.
6. SME participants found that STPA provides a stronger way to identify critical automation or software assumptions during a safety assessment.

7. SME participants found that STPA provides a stronger way to identify critical human factors assumptions during a safety assessment.
8. SME participants found that STPA provides a stronger way to integrate human factors into an overall safety assessment beyond what is done today.
9. Most SME participants believed that STPA would catch the 737MAX automation and human factors issues more reliably than the current practices. See Appendix A.
10. SME participants found that STPA provides a capability beyond current practices that is applicable to future technologies like increasing autonomy and eVTOL.
11. SME participants found that their organizations would benefit from using or adopting STPA and recommended that STPA should be incorporated into modern safety assessment processes.

All findings came directly from the SME participants, as summarized in Appendices A, B, and C.

1 Introduction

1.1 Background

In this project, SMEs examined the STPA method, including the regulatory barriers and opportunities related to STPA, STPA's capabilities, STPA uses in industry, the findings that have been produced by STPA. They also examined how the STPA method and its capabilities compare to current approaches. STPA is a development and safety assessment method based on systems theory and an extended model of accident causation called System-Theoretic Accident Model and Process (STAMP). STAMP includes traditional failure-related causes as well as more complex causes of accidents, such as:

- Unsafe human interactions (with or without a failure)
- Unsafe automation behaviors (with or without a failure)
- Advanced autonomy
- Systems with Artificial Intelligence (AI)
- Complex functions that create hazards by operating as intended
- Non-failure-related common causes that defeat diversity and independence
- Independence claims with hidden or undocumented assumptions
- Dysfunctional interactions between non-failed functions or components
- Complex flaws in design or requirements
- Missing test cases
- Nontrivial human errors such as automation-induced mode confusion
- Nontrivial human decision-making
- Complex causes that emerge only from a combination of factors, such as automation behavior, human behavior, and operational contexts
- Causes rooted in social and organizational design and culture
- New technologies like electric vertical takeoff and landing (eVTOL)
- Etc.

STPA has been used in industry for approximately 10-20 years to overcome these challenges in development, safety assessment, operations, and in safety management systems. Appendix D provides more information about aviation industry adoption and published industry findings regarding STPA over the last decade, including cases where STPA was used in a complementary or a stand-alone fashion.

1.2 Participants

SME participants from FAA, EASA, ANAC, ICAO, and NASA participated in this effort by:

- Identifying key questions that should be asked to evaluate STPA
- Learning STPA
- Attending technical interchange meetings, workshops, and performing hands-on projects
- Applying the STPA methodology to real applications that had already followed the standard development and safety assessment methods
- Discussing, evaluating, and comparing STPA findings with respect to actual operational and safety-related events, which included hidden flaws and vulnerabilities that were not previously known to the teams applying STPA or the standard safety assessment and development methods
- Documenting insights and conclusions regarding regulatory needs and challenges and whether or how STPA would address them.
- Identifying practical recommendations for regulators and the aviation industry moving forward.

The participants included the following departments in each organization:

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

EASA

- Certification Directorate
- Strategy & Safety Management Directorate

ANAC

- Aeronautical Product Certification Branch (GCPP)

ICAO

- Human Performance Study Group
- Safety Management Section

NASA

- Aeronautics Research Institute (NARI)

The participants were surveyed to identify their backgrounds, which included:

- Aircraft certification
- System safety
- Aircraft safety assessment processes (ARP4761)
- Continuing Airworthiness (Service Difficulties, Airworthiness Directives, Scheduled Maintenance Programs, etc.)
- Safety Management
- Safety management systems
- International standards development
- Avionics Certification
- Safety assessment
- Systems Engineering

- Human factors
- Human factors policy and innovation
- Development and certification of new technology
- Automation and complex system/controls certification
- Use of AI/ML in aviation for certifiable applications
- Civil aviation regulations
- Engineering
- Project Management
- Aircraft systems integration
- Flight Test Engineer
- Certification of rotary/fixed wing aircraft
- Certification of Powered-lift aircraft
- Certification of new & novel (e.g. eVTOL) aircraft
- Emerging aircraft design approval

Many participants had overlapping backgrounds. For example, more than 80% of participants worked (either currently or previously) in aircraft certification and safety assessment.

1.3 Project plan

The project plan included:

- Initial participant surveys and evaluations
- Identification of STPA questions the participants believe should be answered
- Kickoff meeting
- Technical interchange meetings
- STPA introduction
- Review of industry adoption and use of STPA

- Review of published industry STPA applications and findings
- Review of STPA differences from standard approaches to development, safety assessment, and safety management
- STPA workshops
- STPA hands-on projects performed by participants
- Review of STPA findings and results generated by participants
- Comparison of STPA findings to the accepted findings from standard approaches
- Review of actual safety events and vulnerabilities (not known or available to teams before this point)
- Comparison between real vulnerabilities, STPA findings, and conclusions from standard approaches
- Review, discussions, and surveys to identify and document the SME insights and findings from the project

SME participants were asked to identify and describe regulatory challenges, gaps, needs, opportunities, and solutions throughout the project. Meetings were held to review and discuss the views and perspectives from SME participants regarding the regulatory environment and new methods like STPA. A series of technical interchange meetings was conducted to provide a basic familiarity with STPA and to review industry STPA uses and documented STPA applications and findings.

STPA workshops were held to enable participants to work individually and in groups to apply STPA to real applications. Participants were also asked to complete individual STPA projects on their own and submit the results for review and discussion. The STPA findings were compared to existing conclusions from industry and regulatory professionals following standard approaches to development, safety assessment, and safety management. The STPA findings and the existing conclusions from standard approaches were compared to actual safety events and vulnerabilities that were found during operational use for these real systems—events and vulnerabilities that had not been known or available to the teams using STPA or the teams following the standard approaches.

The SME participants identified and discussed the insights and lessons learned throughout this effort, and formal surveys, evaluations, and internal interviews were conducted to document the findings, conclusions, and recommendations for regulatory authorities and the aviation industry.

2 Participant findings

Findings in four principal areas were collected:

1. Analysis of regulatory environment
2. The STPA method and existing uses
3. Evaluation of STPA
4. Recommendations for civil aviation regulators and industry

2.1 Analysis of regulatory environment

The SME participants from FAA, EASA, ANAC, ICAO, and NASA were asked to identify and evaluate regulatory challenges, barriers, gaps, and opportunities that exist today given modern complex technologies, future technologies, and new operational concepts that are being introduced in the aviation industry. These were reviewed to identify whether there is a need for a safety assessment process like STPA. A portion of the results are summarized below. Additional results are provided in Appendix A and B.

The SME participants identified that the traditional safety approaches that are required today are heavy and burdensome for industry. 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.

The regulatory environment does not provide clear enough guidance to determine when to accept new methods, when to reject old methods that are no longer suitable for modern technologies, how to ensure the right methods are accepted, and how to respond within the appropriate time to new innovations and industry approaches. It also typically lags behind industry best practices and new technologies. Meanwhile, 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.

In addition, 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 lack of regulatory experience with new methods is a barrier. Industry may try new methods, but if it works and finds new weaknesses or new concerns in their application, then they will have no reason to share the results with regulators. We need another path for regulators to gain experience with new methods.

One of the biggest concerns is systems that are highly integrated into critical safety functions. Currently accepted requirements and standards leave many gaps, and sometimes, poor assumptions. In addition, the increasing complexity of systems and the reliance of software is one of the most concerning aspects of today's regulatory environment. Many unexperienced companies are joining new markets, and they lack internal resources to learn and properly apply the very complex traditional methods that we require today. There is a need to simplify and streamline the process with new methods.

Gaps exist today related to Human Factors considerations in Safety Assessments and losses that can occur with zero failures. These gaps are already known, but there is not yet a clear, recognized solution or effective guidance from regulators.

There is a strong reluctance for industry to bring new or more effective methodologies to regulators who have not yet adopted the same processes due to the possibility of increasing the certification schedules and raising new concerns that otherwise would not face the same level of scrutiny.

The SME participants identified the following general regulatory opportunities to help address the challenges above.

There is an opportunity to use methods like STPA:

- To simplify and streamline the safety process with new methods.
- To improve consideration of human behaviors and human-automation interactions.
- To improve consideration of fully autonomous software.
- To create a more streamlined and more efficient process for smaller applications.
- To provide results that are easier to understand and review, especially by SMEs outside safety (e.g., engineers, pilots, flight testers, etc.).

- To provide alternative ways to evaluate new technologies that cannot provide a historical data basis for failure rates with sufficient confidence before deployment.
- To handle more complex systems and software than is possible today.
- To better consider operational contexts in a safety assessment.
- To reduce cost.
- To make organizations fully aware—at all levels from technical to management—that "0 failure losses" are an important safety issue that STPA can help identify and prevent.
- Opportunity for regulators to push and evaluate new methods like STPA for new/novel technologies like eVTOL.

2.2 The STPA method and existing uses

The STPA method and existing uses were discussed and reviewed by participants. Appendix D provides information and references regarding industry adoption and published industry findings related to STPA over the last decade. Introductory STPA materials and literature are also available from MIT (MIT Partnership for Systems Approaches to Safety and Security (PSASS), n.d.). Several industry standards (Thomas, Overview of STPA in Industry Standards, 2020) that have been produced for STPA were reviewed.

Participants also discussed additional uses, such as:

- The FAA's internal certification training classes that have recognized STPA for six years
- EASA's successful use of STPA on aviation projects and rule-making activity
- The regulators and industry groups that used STPA to accurately identify 737MAX vulnerabilities either before receiving the findings from accident investigations or to evaluate the new mitigations that were proposed
- The use of STAMP/STPA by the National Academy of Sciences, commissioned by the U.S. Congress to ensure the FAA is identifying emerging risks to commercial aviation in the aftermath of the 737MAX accidents
- Other uses

2.3 Evaluation of STPA

At the start of this effort, participants discussed a set of general questions that should be answered to evaluate a new method like STPA. During the project, STPA was applied, discussed, and reviewed by the participants. Participants reviewed existing STPA materials, performed STPA on real systems, and compared the results to the conclusions from standard processes that had already been applied and reviewed. At the end of the project, the original questions were presented to participants to evaluate STPA. Appendix A contains additional information about these questions and answers.

The SME participants from FAA, EASA, ANAC, ICAO, and NASA found that:

- STPA addresses important gaps that exist in current approaches today.
- STPA produces important insights beyond what our current processes find.
- STPA identifies interactions and scenarios relevant to regulatory safety objectives that can be overlooked today.
- STPA provides a stronger way to identify and document critical assumptions related to human factors.
- STPA provides a stronger way to identify and document critical assumptions related to automation and software.
- STPA provides a stronger way to integrate human factors considerations into the safety assessment compared to current approaches.
- STPA would catch the 737MAX automation and human factors issues more reliably than the current hazard analysis methods (See Appendix A).
- STPA provides a capability beyond current practices when analyzing future technologies like increasing autonomy and eVTOL.
- STPA should be incorporated into safety assessment processes.
- Regulator use of STPA would help better achieve regulator safety objectives.
- Increased industry use of STPA would improve aviation safety.
- Their specific organizations (see the list of organizations and offices in Section 1.2) would benefit from using or adopting STPA.
- STPA provides value beyond what is typically done today.

Additional information about these findings is provided in Appendix A and B.

2.4 Recommendations for civil aviation regulators and industry

SME participants identified many regulatory or international groups that would benefit from STPA, including aircraft certification offices, continuing airworthiness, rulemaking, policy groups, human factors groups, and groups involved in safety management systems. Appendix B provides the full list of groups identified by the SMEs.

SME participants identified, discussed, and reviewed potential recommendations for regulators and industry groups as part of the STPA evaluation. The recommendations include initiating pilot programs involving STPA for certification and safety management, developing and releasing guidance material on STPA, more training on STPA for certification authorities worldwide, and creating requirements for more effective approaches like STPA.

The SME participants from FAA, EASA, ANAC, ICAO, and NASA produced the following recommendations:

- Create pilot programs in upcoming applications, where STPA would be formally adopted, disclosed, and discussed with us authorities.
- Evaluate what could be changed in guidance material and even regulations.
- Develop guidance material linking STPA to safety management.
- Include STPA as an option to demonstrate safety requirements.
- Boost STPA training for our staff.
- Provide in-depth STPA training for specialists responsible for reviewing applicant safety assessments.
- Communicate more strongly about our interest in STPA to the industry.
- Make an initial proposal on how to integrate STPA.
- 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.

- Invite other regulatory authorities to a formal working group, with industry collaboration, to evaluate and recognize STPA as part of an acceptable approach to system safety assessment and development.
- Request that the applicants use STPA.
- Require that the STPA approach is part of the risk assessment process for new technology.
- Develop and release STPA guidance and/or policy within the FAA.
- Propose the STPA method to companies (as they are free to propose to us different means of compliance).
- Apply STPA as a part of reviews of designs and changes, even if it is not officially part of the review process.
- Apply STPA to address the concern that always exists that "escapes" will open the door for incidents and accidents.
- Ask applicants questions about potential unsafe system behavior of their proposed architectures using the mental model of STPA.
- Use STPA for any outstanding concerns.
- Use STPA at the aircraft-level hazard identification process as a review element before functional allocation.
- Recommend STPA for application, even if out of a formal certification context, for supporting safer designs.
- Start mandating STPA outcomes.

Additional participant recommendations are provided in Appendix B.

3 Other observations and findings

3.1 Limitations

Some limitations of this effort have been recognized.

The STPA engagements were limited to approximately 20 FAA SMEs and EASA, ANAC, ICAO, and NASA experts who were available and able to participate in an environment of

competing priorities. Appendix C summarizes similar findings from approximately 70 additional FAA SMEs in previous years. The agencies invited to participate were not asked to develop official agency positions on STPA as part of this effort. The findings in this report were produced from surveys and evaluations directly by the SMEs from each agency, which may serve as an input to future agency positions.

The participants were from the organizations and offices listed in Section 1.2. Additional applicable groups and organizations that would also benefit were identified during this project and are listed in Appendix B. Participants represented a broad array of backgrounds and SME focus areas, but not every possible background was represented. Section 1.2 also lists the backgrounds of the participants. Participants also recommended additional STPA efforts to further explore STPA benefits and limitations and to produce further findings.

The questions in Appendix A were asked of all participants, with the option to not answer specific questions if unable to. Every question was answered by a majority of participants, although not every participant was able to answer every question. Additional information is available in Appendix A.

The STPA evaluation included case studies, workshops, and participant projects to apply STPA to real systems. However, these were necessarily limited in scope and by participant availability. This evaluation was not designed to apply STPA on a full certification project or safety management system, and it was not designed to produce experienced STPA facilitators to lead STPA projects.

As with other approaches, STPA proficiency requires STPA education and training as well as practice on real projects. STPA teams typically must include an experienced and qualified STPA facilitator. If these criteria are not met, success is limited.

There is a need for future work and regulatory guidance to define how and to what extent STPA may satisfy existing regulatory requirements.

3.2 STPA best practices

Additional STPA observations and best practices have been documented in past work and during previous STPA industry adoption. The following observations summarized from Leveson and Thomas (2018) were found to be relevant.

Learning STPA requires practice and a “learning by doing” approach, such as hands-on projects applying STPA to real and complex systems together with an STPA expert. Reading papers and

attending public conferences and workshops, such as the annual STAMP/STPA workshops[1], may provide a minimum familiarity with STPA but does not provide a full understanding of the process. STPA requires a different mindset than other methods, and experienced practitioners often report that this was the biggest hurdle. Specialized transition training is often, but not always, required for practitioners to successfully transition between methods, especially when learning STPA after becoming proficient in other methods. System engineers, software and digital system engineers, human factors, and operations specialists tend to learn STPA quickly.

To be successful, STPA projects should include a qualified expert STPA facilitator on the team. The facilitator role typically requires years of experience leading large, successful STPA projects. The STPA facilitator provides method expertise, guidance, and oversight. They must be qualified to provide STPA guidance and answer any STPA-related questions that arise during the project. They generally review the results during and at the end of the process to ensure that the method is being followed correctly and that no gaps are overlooked. The most effective way to produce STPA experts who can serve as future trainers and facilitators is to immerse candidates in real projects where STPA is actively used. Having a basic awareness and familiarity of STPA for many years is not enough to produce STPA experts. Those who have been immersed in large, successful STPA projects are candidates for future trainers and facilitators. The facilitators-in-training learn a great deal by seeing firsthand the challenges encountered in different projects and the questions that are raised.

STPA is best performed by an interdisciplinary team that includes expertise across the relevant areas and with access to SMEs as needed. Personalities and biases matter when forming an STPA team. The best STPA teams include knowledgeable experts who are open to new approaches and can become comfortable with discovering holes and gaps in their knowledge.

4 FAA capabilities needed

Additional steps were identified to further build the FAA's capability to evaluate STPA:

- FAA staff do not yet have enough experience in the effective use of STPA in terms of satisfying regulatory objectives.

[1]For example, the five international STAMP/STPA conferences and workshops that are organized by different groups in the US, Europe, Japan, Korea, and Latin America.

    - Because any safety analysis depends on the competence of the performers or performing team, FAA staff need significant hands-on experience with the STPA method to understand the competencies needed.
    - To understand the factors influencing the quality of the safety analysis, FAA staff need to exercise the STPA method on a real project, facilitated by a qualified method expert.
    - The FAA would benefit from having a small number of in-house certified STPA facilitators who can facilitate STPA activities and are qualified to serve as STPA SMEs when reviewing STPA findings and results.
- The FAA does not yet have regulatory guidance for an applicant to use in preparing an STPA-based submission.
- The FAA does not yet have specific-enough internal guidance and technical criteria to review and evaluate STPA-based submissions. Experience from hands-on, real-world projects would help FAA staff to create such review guidance.
- The STPA competencies needed, mentioned above, also apply through the applicants or operators to their supply chains, including performers, verifiers, and auditors. However, the FAA does not have sufficiently specific criteria and guidance to evaluate whether these controls are adequate and the personnel adequately qualified in STPA.

In summary, the FAA's capabilities must be improved, as identified above, to obtain the safety insights needed during a safety evaluation, especially when following existing guidance that was not created with an awareness of STPA and the differences in the approach.

5 Conclusions

The following are the principal findings developed by SMEs from FAA, EASA, ANAC, ICAO, and NASA:

- STPA systematically analyzes safety-related areas that are not well represented in the current regulatory oversight process.
- STPA addresses critical safety gaps that exist in current approaches today, including human factors assumptions and complex system interactions.
- STPA provides a capability beyond current practices when analyzing future technologies like increasing autonomy and eVTOL.

- There is an opportunity to reduce cost and streamline safety assessments and reviews by using STPA, whether or not STPA was used by the applicant.
- Regulator use of STPA would help better achieve safety objectives.
- Increased industry use of STPA would improve aviation safety.
- STPA has been successfully used in industry to discover critical safety deficiencies that were overlooked by professional industry teams and regulatory representatives following standard approaches.
- The participants from FAA, EASA, ANAC, ICAO, and NASA were able to use STPA to discover safety-critical flaws in real aircraft systems that were overlooked by professional teams using current methods.
- The current regulatory guidance materials do not provide adequate guidance regarding the suitability and potential for STPA to satisfy regulatory objectives.
- STPA can satisfy existing regulatory objectives and would be beneficial in regulatory reviews and oversight.

Some regulatory challenges and concerns that could be addressed by STPA were identified by the SMEs, including:

- 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.
- Gaps exist today related to human factors considerations in safety assessments and losses that can occur with zero failures. These gaps are already known, but there is not yet a clear, recognized solution or effective guidance from regulators. STPA can address these challenges.
- The current practice of waiting for industry to submit results from new methods is too restrictive. If a new method works and finds new weaknesses or raises new concerns in their application that are otherwise overlooked, then they will have little reason to share those results with regulators.
- Regulatory bodies need to be prepared to review submissions in which the applicant's safety analysis or development process is based on STPA.
- The use of STPA can improve safety management systems defined by ICAO Annex 19.

- The use of STPA can streamline and improve the effectiveness of aircraft and system development processes.
- Regulatory bodies could review traditional submissions (e.g., means of compliance, safety analysis reports, design certification documents) more effectively by using STPA to identify the information needed for reasonable assurance and to formulate requests for additional information more quickly and with less effort.

6 Next steps

The participants found that additional STPA collaboration and experience on real projects would enable regulators and industry partners to identify specific opportunities to achieve the benefits of STPA. A larger scale effort, representative of modern real-world concerns and challenges, would further develop the level of STPA competence across the FAA and other organizations. In parallel, recommendations, guidance material, and other means must be established to communicate the findings of this investigation and to reduce the uncertainty regarding STPA use in formal safety assessments and safety management systems.

The FAA staff has recommended the following next steps:

- FAA will select candidate applications that would benefit from STPA.
- FAA will identify a core team to apply STPA, consisting of both FAA and industry practitioners, and a qualified STPA expert facilitator.

STPA will be applied by the core team to the candidate application. The STPA results will be evaluated in terms of regulatory objectives as an input to official decisions related to regulatory rules, policies, and STPA.

7 References

Abrecht, B., Arterburn, D., Horney, D., Schneider, J., Abel, B., & Leveson, N. (2016, March 22). Hazard Analysis for Rotorcraft. *5th STAMP/STPA Workshop*.

Allsop, D., & Xu, X. (2014). The Use of STAMP in Aircraft Evaluation, Test and Research. *3rd STAMP/STPA Workshop*.

Allsop, D., & Xu, X. (2015). STAMP/STPA Analysis of Remote Flight Testing. *4th STAMP/STPA Workshop*.

Almalik, N. (2013). System Theoretic Process Analysis Application (STPA) in a Service Safety Environment. *3rd STAMP/STPA Workshop*.

Archibald, R. (2020, March 23). Introduction and Training of STPA at L3HARRIS Technologies. *9th STAMP/STPA Workshop*.

Aust, M., Pennington, E., & Young, W. (2021). STPA Results from Agility Prime. *10th STAMP/STPA Workshop*.

Berry, K., & Sawyer, M. (2014). Proactively Examining NextGen Human Performance and System Safety: An Application of a Modified STPA in Air Traffic Control. *3rd STAMP/STPA Workshop*.

Castilho, D. (2017, March 30). Scenarios of Over-Automation in Flight Testing of Manned Aircraft. *6th STAMP/STPA Workshop*.

Castilho, D. S. (2019). Active STPA – A Systems-based Hazard Analysis for Safety Management Systems (SMS). *8th STAMP/STPA Workshop*.

Castilho, D. S., Urbina, L. M., & de Andrade, D. (2015, March). Application of STPA for Hazard Analysis on Light Aircraft Crosswind Takeoffs. *4th STAMP/STPA Workshop*.

de Boer, R. J. (2013, March 26-27). Cognitive Resilience Applied to STAMP. *2nd STAMP/STPA Workshop*. Boston, Massachusetts.

de Boer, R. J. (2014, March 27). Using STAMP to Improve Platform Safety. *3rd STAMP/STPA Workshop*.

Deming, X. Z. (2012). STAMP Based Safety Analysis for Navigation Software Development Management.

Dewalt, M., & Skaves, P. (2012). Applicability/Compatibility of STPA with FAA Regulations and Guidance.

Federal Aviation Administration (FAA). (2017, May 2). Grant of Exemption. *Regulatory Docket No. FAA-2016-8059*.

Fleming, C. (2013, March 28). Improving Hazard Analysis and Certification of Integrated Modular Avionics.

Fleming, C. (2014, March 26). Hazard Analysis of NextGen Arrival Phase of Flight Concepts: Interval Management – Spacing. *3rd STAMP/STPA Workshop*.

Fleming, C., & Wilkinson, C. (2014). ARP 4761 and STPA. *3rd STAMP/STPA Workshop*.

Fletcher, W. S. (2014, March). Application of System Theoretic Process analysis to requirements and algorithms for a thrust control malfunction protection system. *3rd STAMP/STPA Workshop*.

Garcia, J., & Mtlokwa, B. (2022). ICAO Safety Management Panel and the Need for Improved Safety Risk Management Methodology and Tools. *11th STAMP/STPA Workshop*.

Helfer, J. (2015). Cyber Security in Aircraft Networks Control Systems. *4th STAMP/STPA Workshop*.

Horney, D. (2017). Using System Theoretic Process Analysis (STPA) for a Safety Trade Study. *6th STAMP/STPA Workshop*.

Howard, E., & Smith, L. (2016, March 21). STAMP Applied to Workplace Safety. *5th STAMP/STPA Workshop*.

Hurley, M., & Wankel, J. (2019). Safety Guided Design Using STPA and Model Based System Engineering. *8th STAMP/STPA Workshop*.

International Air Transport Association. (2019). Issue Review Meeting Summary Bulletin. *(26)*.

Johnson, E. (2020, July 31). Early Conceptual Design of Future Manned and Unmanned Aerial Vehicles. *9th STAMP/STPA Workshop*.

Johnson, K. (2017, March 29). Extending Systems-Theoretic Safety Analyses for Coordination. *6th STAMP/STPA Workshop*.

Johnson, K., & Leveson, N. (2015, March 24). Unmanned Aircraft Integration into the National Airspace: A Cognitive Systems Engineering Framework for Safety Model Development. *4th STAMP/STPA Workshop*.

Juhnke, L. (2017). The Human Element of STPA. *6th STAMP/STPA Workshop*.

Karanikas, N., & Abrini, M. (2016, March 21-24). Using STPA for Evaluating Aviation Safety Management Systems (SMS). *5th STAMP/STPA Workshop*.

Koglbauer, I. (2017). STPA-based Model of Threat and Error Management in Dual Flight Instruction. *6th STAMP/STPA Workshop*.

Koglbauer, I., & Leveson, N. (2016). Using STAMP to Address Causes and Preventive Measures of Mid-Air Collisions in Visual Flight. *5th STAMP/STPA Workshop*.

Larard, G. (2020). Importance of Organizational Culture in Effective Safety Management. *9th STAMP/STPA Workshop*.

Larard, G. (2021). Industrialization Panel. *10th STAMP/STPA Workshop*.

Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook.* MIT Partnership for Systems Approaches to Safety and Security.

Leveson, N. G., & Young, W. E. (2013). Systems thinking for safety and security. *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13)*.

Lima, I., Schwienhorst, M., & Reichmuth, J. (2020, August 4). STPA for Safety, Security and Privacy in Smart Airport Terminal New Concepts. *9th STAMP/STPA Workshop*.

Malloy, N. H. (2017, March 30). Integrating STAMP-based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis. *6th STAMP/STPA Workshop*.

Mendes, P., & Sousa, M. (2022). Use of the STPA Technique in the Requirements Definition of a Drone Power Generation System. *11th STAMP/STPA Workshop*.

Merladet, A., Lahoz, C., & Silveira, R. (2020). STPA Applied to Military Certification Process. *9th STAMP/STPA Workshop*.

MIT Partnership for Systems Approaches to Safety and Security (PSASS). (n.d.). Retrieved from MIT Partnership for Systems Approaches to Safety and Security (PSASS): http://mit.edu/psas

Moraes, R. (2020). STAMP: The Strategy of Organization as a System. *9th STAMP/STPA Workshop*.

Mutuel, L. H. (2022, June 9). A Structured and Comprehensive Air Vehicle Risk Assessment. *11th STAMP/STPA Workshop*.

Nance, M. (2019). Overview of STAMP and STPA for Product and Production Systems Engineering. *8th STAMP/STPA Workshop*.

Neogi, N. A. (2012, April 19). Integrating Uninhabited Aerial Systems in to the NAS. *1st STAMP/STPA Workshop*.

Palyok, S. (2023). Implementing STAMP at the World's Largest Airline. *12th STAMP/STPA Workshop*.

Pereira, D. P., Hirata, C. M., Pagliares, R. M., & de Lemos, F. L. (2017). STPA-Sec for Security of Flight Management System. *6th STAMP/STPA Workshop*.

Plioutsias, A., Karanikas, N., & Chatzimichailidou, M. M. (2016). Application of STPA on Small Drone Operation. *5th STAMP/STPA Workshop*.

Quilici, A. I., & de Oliveira, G. L. (2022). Application of STPA-Sec in Military Systems. *11th STAMP/STPA Workshop*.

Reeves, S. (2020). STAMP at FedEx Air Operations. *9th STAMP/STPA Workshop*.

Reiser, C., Martinez, C. E., Lahoz, C. H., & Villani, E. (2019, March). STPA Analysis of Aircraft Landing Phase with Focus on Runway Excursion. *8th STAMP/STPA Workshop*.

Ribeiro, D. d. (2016, March). A Systems Approach to the Development of an Aircraft Smoke Control System. *5th STAMP/STPA Workshop*.

Scarinci, A., & Gusti, A. (2016, March 21-24). A STAMP-based Hazard Log for Use during Development and Operations. *5th STAMP/STPA Workshop*.

Scarinci, A., Quilici, A., Ribeiro, D., Oliveira, F., Moraes, R., & Pereira, D. (2017). A complete STPA Application to the Air Management System of Embraer Regional Jets family. *6th STAMP/STPA Workshop*.

Scarinci, A., Quilici, A., Ribeiro, D., Oliveira, F., Moraes, R., & Pereira, D. (2017). STPA in the Aeronautical Industry. *6th STAMP/STPA Workshop*.

Silva, C. C., Filho, C. M., & Pinto, A. M. (2022). A Systematic Approach to Aircraft System Supportability. *11th STAMP/STPA Workshop*.

Span, M., Mailloux, L. O., & Young, W. (2018, March 27). STPA-Sec Aerial Refueling Case Study. *7th STAMP/STPA Workshop*.

Stanley, P., & Barraquero, V. A. (2021). STPA Evaluation of Potential Conflicts between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace. *10th STAMP/STPA Workshop*.

Stephane, L. (2015, March 24). MH 370: STPA Supporting Possible Improvements in Air-Ground Tracking &. *4th STAMP/STPA Workshop*.

Summers, S. (2018, March 27). STPA Applied to Air Force Acquisition Technical Requirements Development. *7th STAMP/STPA Workshop*.

Summers, S., & Folse, S. (2017). STAMP applied to SUAS at Edwards AFB. *6th STAMP/STPA Workshop*.

Tavares, M. A. (2018, March 27). Challenges and Plans for Introducing STAMP/STPA. *7th STAMP/STPA Workshop*.

Thomas, J. (2020). Overview of STPA in Industry Standards. *9th STAMP/STPA Workshop*.

Thomas, J. (2020). When STPA Results Surprise You: An Industry Case Study Employing STPA. *9th STAMP/STPA Workshop*.

Thomas, J. (2023). Empirical Evaluations of STPA in the Aviation Industry. *12th STAMP/STPA Workshop*.

Weller-Fahy, D. J. (2019, March 28). Systems Theoretic Process Analysis for Security of Aircraft Systems (STPA-Sec). *8th STAMP/STPA Workshop*.

Wijayratne, D., Stringfield, J., Clark, S., & McDonald, D. (2022, June). STPA Evaluation of Boeing's Automated Test Maneuvers (ATM) System. *11th STAMP/STPA Workshop*.

Yi, L. (2013, March 28). A Systematic Safety Control Approach and Practice on Flight Tests of A Low-cost Blended-wing-body Demonstrator. *2nd STAMP/STPA Workshop*.

A Subject matter expert close-ended answers

This appendix summarizes the quantitative results from the FAA, EASA, ANAC, ICAO, and NASA subject matter experts (SMEs). The SMEs from each agency answered these questions directly, and they were not asked to create an official agency position. Appendix B provides additional qualitative results from participants. The questions in this appendix were identified by early participants before System-Theoretic Process Analysis (STPA) was reviewed. At the end, all participants were asked to evaluate these questions after they had learned and applied STPA themselves. Participants had the option to not answer specific questions if unable to reach a conclusion (e.g., outside their area of expertise). Every question was answered by a majority of participants, and every question resulted in a supermajority (greater than two-thirds) consensus.

Figure A-1 summarizes participant responses when asked if STPA addresses important gaps that exist in current approaches today, if STPA will produce important insights beyond what our current processes find, and if STPA identifies relevant interactions and scenarios that can be overlooked today.

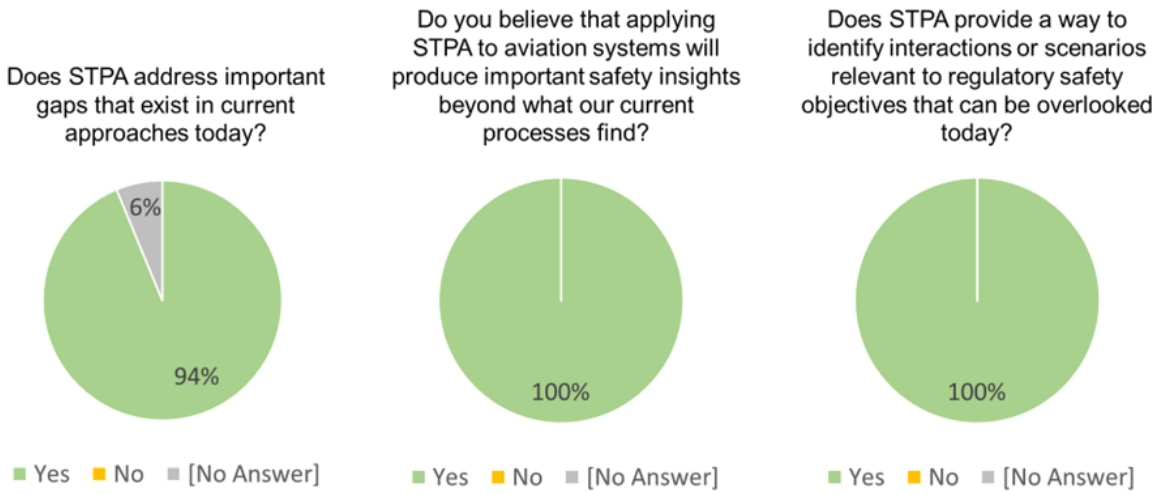

Figure A-1. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's ability to produce relevant findings that may be missed today

All participants reported that STPA provides a stronger way to identify and document critical assumptions related to human factors and automation, which are two major challenges in modern safety assessments and new emerging technologies. These findings are summarized in Figure A-2.

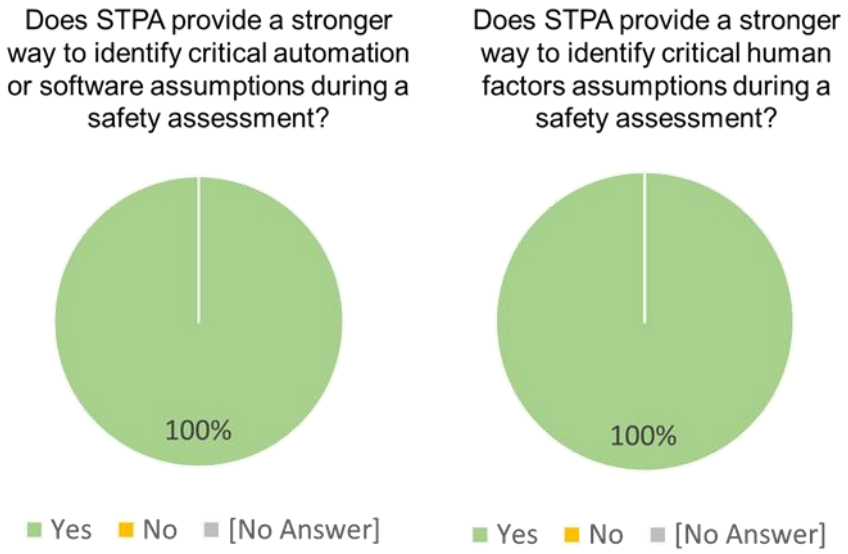

Figure A-2. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's ability to improve identification of critical assumptions in safety assessments

One concern identified in recent accident investigations and in the certification of new technologies is the need for stronger integration of human factors considerations during development assurance and safety assessment processes. Figure A-3 summarizes participant responses when asked if STPA provides a stronger way to integrate human factors considerations into the safety assessment compared to current approaches.

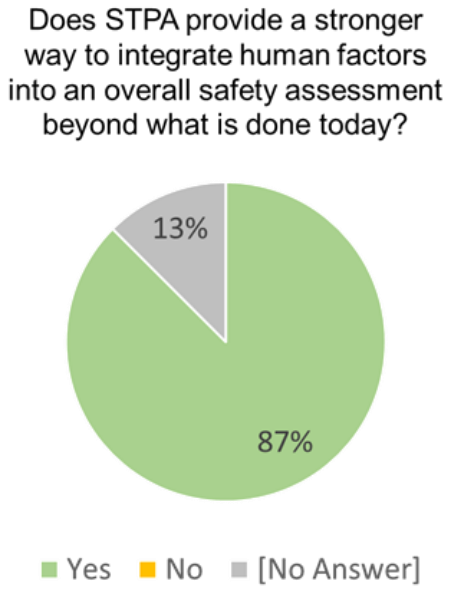

Figure A-3. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's integration of human factors into the safety assessment

The project included dedicated discussions of the 737MAX accident, the flaws involved, how they were overlooked during development and safety assessment, the relationship to STPA, and STPA efforts post-737MAX. These discussions produced valuable insights and continued longer than originally planned, resulting in some participants unable to fully attend these discussions. All participants, including those unable to fully attend, were asked if STPA would catch the 737MAX automation and human factors issues more reliably than the current practice. Figure A-4 summarizes participant responses.

Figure A-4. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's ability to more reliably capture the 737MAX flaws compared to current practices

Figure A-5 summarizes participant responses when asked whether STPA provides a capability beyond current practices for future technologies like increasing autonomy and eVTOL.

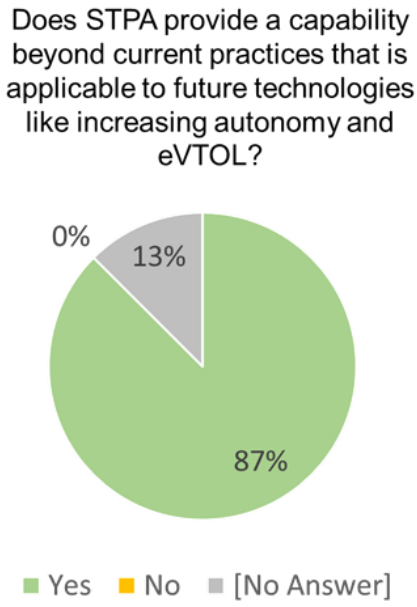

Figure A-5. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's capability to handle future technologies like autonomy and eVTOL more effectively

Figure A-6 summarizes participant responses when asked whether STPA should or will be incorporated into safety assessment processes.

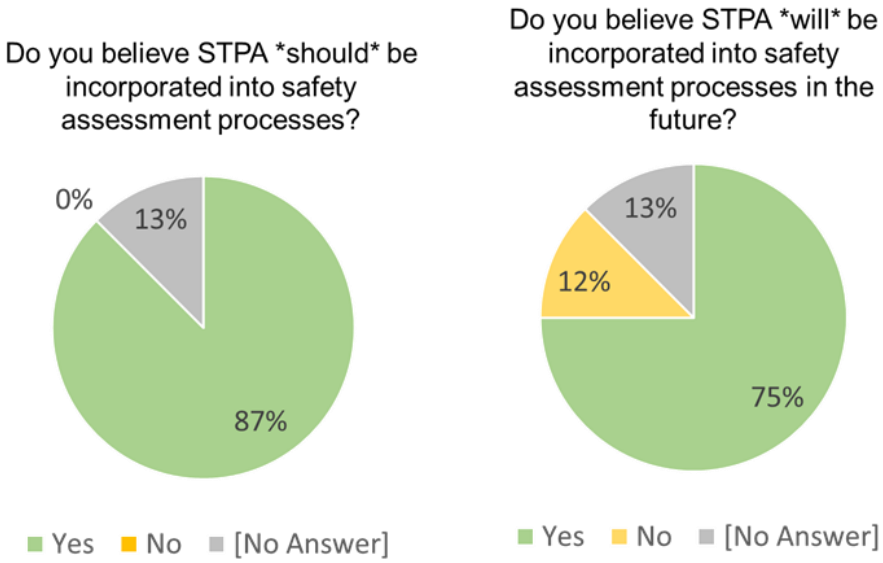

Figure A-6. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's incorporation into standard safety assessment processes

Figure A-7 summarizes participant responses when asked whether industry and regulatory use of STPA would improve aviation safety and better achieve regulator safety objectives.

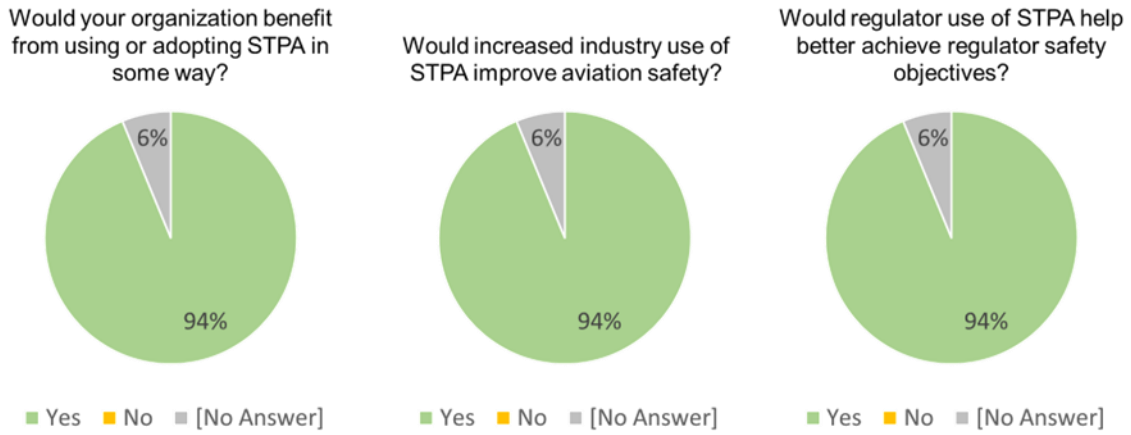

Figure A-7. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to whether industry or regulatory use would improve safety or provide other benefits

All participants reported that STPA provides value beyond what is typically done today. These findings are summarized in Figure A-8.

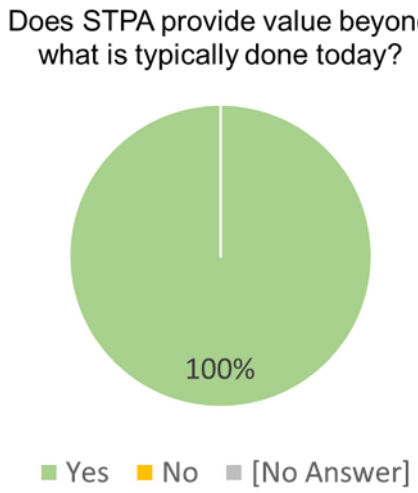

Figure A-8. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to whether STPA provides value beyond what is done today

B Subject matter expert open-ended answers

This appendix provides open-ended results from the surveys, evaluations, and interviews performed by the SMEs from FAA, EASA, ANAC, ICAO, and NASA.

B.1 Regulatory considerations

Participants were asked to identify and evaluate regulatory challenges, barriers, gaps, and opportunities that exist today given modern complex technologies, future technologies, and new operational concepts that are being introduced in the aviation industry.

The subject matter experts (SMEs) observed that:

- 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.
- The current regulatory environment was developed for controlled and slow changes. It has not been nimble enough to keep up with changing threats and new environments.
- 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.
- The regulatory environment does not provide clear enough guidance to determine when to accept new methods, when to reject old methods that are no longer suitable for modern technologies, how to ensure the right methods are accepted, and how to respond within the appropriate time to new innovations and industry approaches.
- The regulatory environment typically lags behind industry best practices and new technologies. Meanwhile, 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.

- It is a challenge for regulatory bodies to learn something different, whether a new technology or a new method, and to apply it or accept it within a few years. That has to change because there is also a risk that is created if more effective solutions are delayed.
- The lack of regulatory experience with new methods is a barrier. Industry may try new methods, but if it works and finds new weaknesses or new concerns in their application then they will have no reason to share the results with regulators. We need another path for regulators to gain experience with new methods.
- The regulatory environment is often resistant to change, and there is strong preference for familiar approaches have been used for the last 30 years with older technologies. However, regulatory changes do happen when there are big drivers, and we have big drivers today—new technologies being pushed by industry, smaller aircraft, unmanned aircraft, and autonomy are all coming together to drive big changes. The old thinking has not been enough to tackle these. The current approaches will take more and more effort to apply, so there is also a strong driver to find more efficient approaches.
- Regulators need to build competence in a new method before it can be endorsed or accepted. The FAA has already included STPA in internal training classes, but not all regulators have.
- The high cost and length of today's certification process is a significant barrier.
- It is a challenge to figure out how to scale safety requirements, but there is no reason STPA can't be a solution to that. We do not need a one-size-fits-all answer—STPA could be used in a complementary way on Part 25 aircraft, and it still may be that STPA is more suitable for smaller aircraft with lower risk.
- 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.
- What is most concerning about the regulatory environment is its ignorance and unwillingness to consider the true benefits of STPA until now.
- One of the biggest concerns is systems that are highly integrated into critical safety functions. Currently accepted requirements and standards leave many gaps, and sometimes, poor assumptions.
- New challenges are coming from the increased use of automation. Automation is very difficult to assess while designing it. Many components of a system are developed by

different manufacturers and their integration is a critical challenge that needs to be solved.

- The increasing complexity of systems and the reliance of software is one of the most concerning aspects of today's regulatory environment. Many unexperienced companies are joining new markets, and they lack internal resources to learn and properly apply the very complex traditional methods that we require today. There is a need to simplify and streamline the process with new methods.
- Gaps exist today related to Human Factors considerations in safety assessments and losses that can occur with zero failures. These gaps are already known, but there is not yet a clear, recognized solution or effective guidance from regulators.
- One of the biggest concerns is new novel articles and the large quantity of products coupled with old safety regulations that have not kept pace with new innovations.
- A concern is that some organizations are not willing or able to look at things differently or to try different methods. We have regulated and the industry copies the standard process to get approval, but we need to do more if we want to enable innovation. One example is context driven performance assessment.
- There is a strong reluctance for industry to bring new or more effective methodologies to regulators who have not yet adopted the same processes due to the possibility of increasing the certification schedules and raising new concerns that otherwise would not face the same level of scrutiny.
- 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.
- Additional research and development is needed in new methods to develop effective VTOL certification.

The participants identified the following general regulatory opportunities to help address the challenges above.

There is an opportunity to use new methods like STPA:

- To simplify and streamline the safety process with new methods.
- To improve consideration of human behaviors and human-automation interactions.
- To improve consideration of fully autonomous software.

- To decrease the current siloing with better integration of human factors into the engineering safety assessment.
- To create a more streamlined and efficient process for smaller applications.
- To provide results that are easier to understand and review, especially by SMEs outside safety (e.g., engineers, pilots, flight testers, etc.)
- To provide alternative ways to evaluate new technologies that cannot provide a historical data basis for failure rates with sufficient confidence before deployment.
- To provide formal basis for identifying missing functions and non-trivial missing failure conditions.
- To consider interactions between functions, systems, or components in a more efficient way than brute force.
- To rigorously identify missing, incomplete, or flawed requirements.
- To handle more complex systems and software than is possible today.
- To better consider operational contexts in a safety assessment.
- To systematically challenge or validate assumptions, including engineering, human factors, or environmental assumptions.
- To identify critical missing test scenarios and test cases.
- To identify new questions or concerns in a system that might otherwise be overlooked during review.
- To reduce cost. It is possible that a predominately Development Assurance Level (DAL) C system with level A monitors in place, evaluated extensively by human factors, flight test, systems, and safety engineers using STPA would be superior to systems designed to current standards at DAL A for all components that are flight critical.
- To provide economic advantage with more efficient and effective methods for traditional original equipment manufacturers (OEMs).
- To enable new, streamlined approaches that can be more easily adopted and integrated for younger companies that are still establishing their procedures.

- To make organizations fully aware—at all levels, from technical to management—that "zero failure losses" are an important safety issue that STPA can help identify and prevent.
- To create consensus standards that are more flexible and do not over-specify what is required to demonstrate compliance.
- To push and evaluate new methods like STPA for new/novel technologies like eVTOL by regulators.
- To help identify the hidden assumptions to provide sufficient mitigation.

B.2 Groups that would benefit from STPA

Participants were asked, "What other groups in your organization would benefit from learning STPA?"

They provided the following answers:

- Continuing airworthiness group
- RPAS
- AAM
- Security
- Aerodromes
- CNS
- Emergency Response Planning
- All groups
- Aircraft Certification Office
- PCMs
- Certification experts
- Cybersecurity experts
- Rulemaking officers
- Anyone involved with system design

- R&D
- Airworthiness
- Operational (system wide) safety
- All aircraft systems certification specialists
- Software
- Human Factors Design Certification teams
- System experts
- AIR-1 (Executive Director of the Aircraft Certification Service)
- AIR-2 (Deputy Executive Director for Regulatory Operations)
- AIR-500 (Planning and Program Management Division)
- AIR-600 (Policy and Innovation Division)
- AIR-700 (Compliance and Airworthiness Division)
- Policy
- Systems Engineering
- All of aircraft certification engineering

Participants were asked, “What other regulatory groups would benefit from learning STPA?” They provided the following answers:

- Aircraft certification authorities
- All Civil Aviation Authorities
- All branches could benefit from STPA process
- EASA
- FAA
- Standards Bodies
- Operators working on safety management systems for industry
- Continued Airworthiness

- ATO
- AFS
- AIR
- HF focus groups
- All
- LEADERSHIP

Participants were asked, “What industry groups would benefit from learning STPA?”

They provided the following answers:

- All aircraft design organizations
- All aircraft OEMs, including transport and eVTOL
- Platforms OEMs
- IATA
- ICCAIA
- ACI
- CANSO
- IFALPA
- IFATCA
- ASECNA
- All industry groups that consider system safety concepts
- Safety and security groups
- IT
- Software developers
- Standards bodies
- System design
- Ops safety

- Certification
- Aircraft systems development
- Aircraft integration
- Aircraft safety assessment
- Human factors
- UAS community
- AMM
- Unions / workforce groups
- Most ASTM members
- Most SAE members

B.3 Key insights

Participants were asked, “What were the key insights and "aha moments" you encountered during these STPA TIMs?”

They provided the following answers:

- 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.
- 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.

- Moving away from the component/functional failure viewpoint to the STPA view of analyzing systems, safety risk controls, etc. was one of the most important concepts for future automation.
- 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.
- Following the STPA guidelines when building the control structure of the system and using the correct syntax of STPA items (UCA, etc.) is very important to achieve good results.
- Systems thinking and approaches.
- Benefits of STPA for finding and addressing potential problems with human/machine interfaces.
- STPA identifies potential concerns about system interactions (namely, emerging functions/behaviors and unsafe interactions not related to failures) which seem not to be properly covered in today's regulation.
- STPA discovers hazards beyond those caused by system failures (which is broader than traditional XX.1309 scope).
- The wholistic approach to safety.
- The staffing requirements to do a good STPA.
- How to build STPA scenarios and how to move through the levels of assessment to keep things simple and focused.
- Being able to describe subsystem behavior in sufficient detail without a representative block diagram is difficult (if not impossible); however, decluttering that model to describe the specific inter-control system interaction is essential to 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.

B.4 Next steps

Participants were asked, “What would you choose to do after this to incorporate/implement what you have learned about STPA, if you had the power to do so?”

They provided the following answers:

- Pilot programs in coming applications, where STPA would be formally adopted, disclosed, and discussed with us authorities
- Evaluate what could be changed in guidance material and even regulations
- Develop guidance material linking STPA to safety management
- More training to develop skills to apply/review the concepts as a safety assessment tool recognized by the certification authorities worldwide
- Include STPA as an option to demonstrate safety requirements
- Start using STPA together with an expert
- Boost STPA training for our staff
- Raise STPA awareness and reach "critical mass." The advantages should be clear
- Stronger communication about our interest in STPA to the industry
- An initial proposal on how to integrate STPA should be made
- Make STPA a standard part of evaluating new designs and evaluating significant changes to existing designs
- Require STPA training for all NASA, FAA, and industry designers, certification engineers, etc.
- Require a more robust analysis of system behavior losses that may occur without failures, as STPA does
- Begin using STPA, even for simple situations
- Invite other regulatory authorities to a formal working group, with industry collaboration, to evaluate and recognize STPA as part of an acceptable approach to system safety assessment and development
- Request that the applicants use STPA
- Require that the STPA approach is part of the risk assessment process for new technology

- Challenge the probabilistic/linear methods for human risk, as assigning a number to human performance is misleading and fails to think about context and normal behavior as opposed to STPA
- In-depth STPA training for specialists responsible for reviewing applicant safety assessments
- Add STPA to the appropriate consensus standard so that it's artifacts will be used to demonstrate regulatory compliance

Participants were asked, “What do you intend to actually do (or pursue) in your role in terms of incorporating/implementing what you have learned about STPA?”

They provided the following answers:

- Apply STPA thinking when evaluating in-service occurrences
- An ICAO Strategy for promoting
- Development and release of STPA guidance and/or policy within the FAA
- Attempt to identify which applicants use STPA in any product or product change
- Assess the effectiveness of the safety assessment carried out
- Spread STPA awareness among colleagues, possibly management
- Plan internal STPA training
- Propose the STPA method to companies (as they are free to propose to us different means of compliance)
- Discuss internally the introduction of STPA as a requirement
- Apply STPA as a part of reviews of designs and changes even if not officially part of the review process
- Apply STPA to address the concern always exists that "escapes" will open the door for incidents and accidents
- Continue to gain STPA skills
- Exercise STPA on existing systems
- Participate on standards committees related to STPA
- Become fairly competent with the STPA methodology

- Collaborate with FAA STAMP/STPA research and development project.
- Share these STPA discussions/outcomes within my organization
- Ask applicants questions about potential unsafe system behavior of their proposed architectures, using the mental model of STPA
- Use STPA for any outstanding concerns
- Promote the STPA method
- Use STPA at the aircraft level hazard identification process as a review element before functional allocation

Participants were asked, "What needs to happen next, given what you have learned in the STPA TIMs? (not limited to your specific role)."

The following answers were produced:

- Certification authorities, and possibly ICAO, convene to discuss STPA implementation in current regulatory material
- STPA can be, right now, recommended for application, even if out of a formal certification context, but supporting safer designs
- Work to develop STPA competencies across our industry
- Practical application with a STPA mentor
- Revision of regulatory standards
- Companies need to start using STPA
- Authorities should start mandating STPA outcomes
- The FAA and NASA need to embrace the techniques completely
- Begin using STPA where possible
- Educate DOT management about STPA
- Wider promotion of the STPA method and, importantly, who uses it
- Complete and release ASTM STPA standard

C Previous FAA STPA evaluations

Since 2017, the FAA has hosted internal annual classes and workshops that include STPA alongside standard approaches for FAA certification, policy, and other staff. At the end, evaluations are often conducted by FAA staff to collect insights and gauge the potential value added from STPA. This appendix provides a summary of previous findings from approximately 70 FAA staff during three of these FAA internal classes.

C.1 Class A

Approximately 20 FAA staff were involved in this internal class. The staff reported that the FAA would benefit from using or adopting STPA, and that STPA provides a practical way to address real challenges at the FAA. These findings are summarized in Figure C-1.

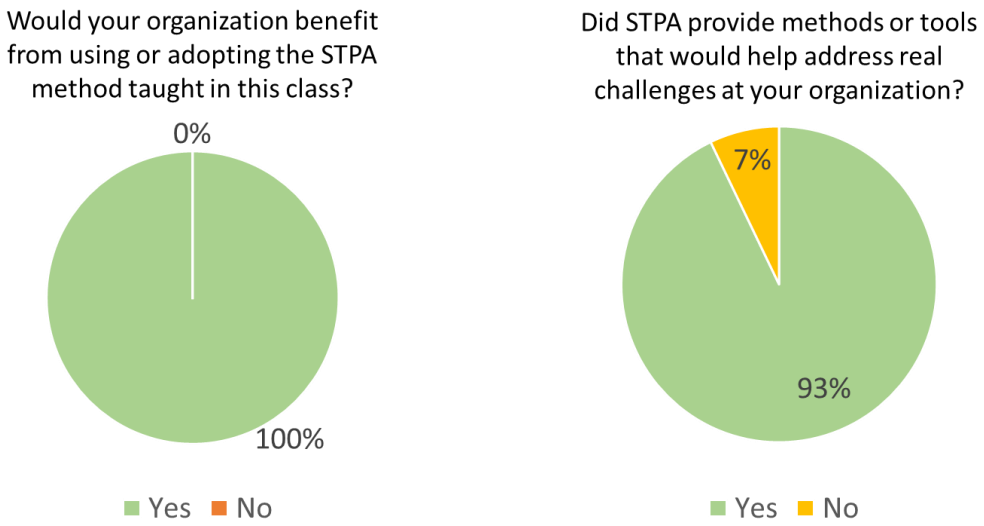

Figure C-1. Findings from FAA certification, policy, and other staff related to whether STPA provides benefit and addresses real challenges the staff encountered

FAA staff were asked which FAA groups would benefit from STPA.

They provided the following answers:

- Systems & Equipment
- Cabin Safety
- Propulsion
- Policy making groups

- Certification
- Standards
- Airports
- MIDO inspectors
- ACOs

FAA staff were asked if they had any additional comments regarding STPA.

They provided the following:

- A better process that should eliminate more omissions
- Definitely helpful with interrogation of applicant's submissions
- Need applicants to embrace
- As a regulator this is not something we would directly use on a project, but general knowledge of the process is helpful
- Not sure how an oversight org would use directly
- Appreciate the concept of human-to machine interface from a systems standpoint
- This needs to be widely available to our applicants, i.e. aircraft manufacturers

C.2 Class B

A separate group of approximately 20 FAA staff were involved in a similar internal class. These FAA staff also reported that the FAA would benefit from using or adopting STPA, and that STPA provides a practical way to address real challenges at the FAA. These findings are summarized in Figure C-2.

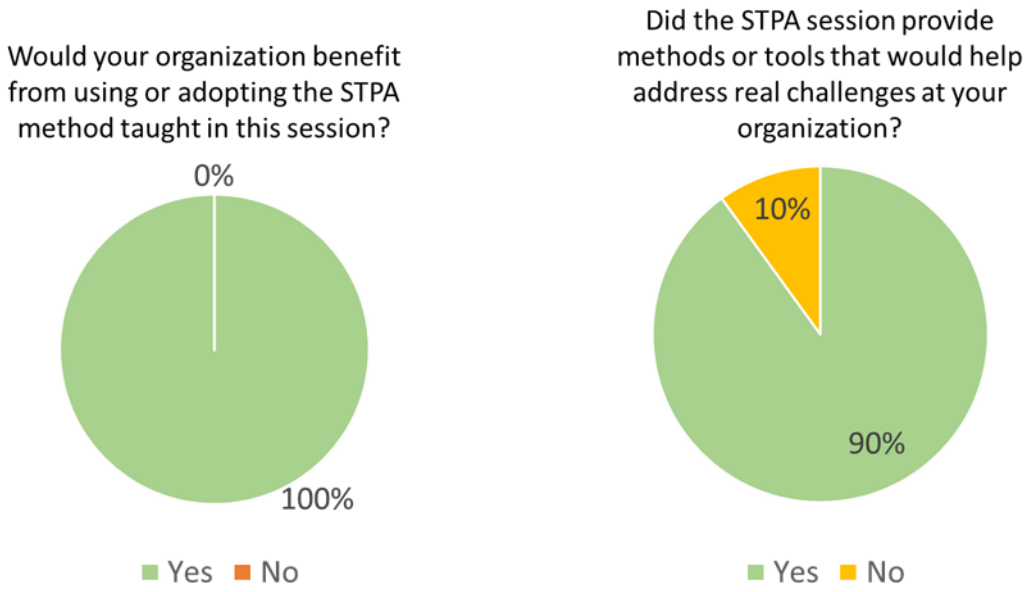

Figure C-2. Findings from FAA certification, policy, and other staff related to whether STPA provides benefit and addresses real challenges the staff encountered

FAA staff were asked which FAA groups would benefit most from STPA.

They provided the following answers:

- Flight Test Engineers
- Pilots
- Human Factors Engineers
- Continued Operational Safety
- AIR-600 (Policy and Innovation Division)
- AIR-700 (Compliance and Airworthiness Division)
- Boeing ODA Engineering Unit Members

FAA staff were asked if they had any additional comments regarding STPA.

They provided the following:

- This [STPA] process seems to fit well into deriving requirements for ARP4754A
- Good info on new approaches to address deficiencies in current processes

- I learned how to identify isolated points between human psychology behavior and machine/autopilot behavior
- I would like more time dedicated to this subject so I can have a better understanding of how to apply it to my job function

C.3 Class C

A longer, in-depth class was held at an FAA office in Seattle after the 737MAX accidents. A group of approximately 30 FAA staff attended, including the FAA Aircraft Certification Office and policy branches. After learning STPA and performing STPA on a variety of aircraft systems, these FAA staff reported that the FAA would benefit from using or adopting STPA, and that STPA provides a practical way to address real challenges at the FAA. These findings are summarized in Figure C-3.

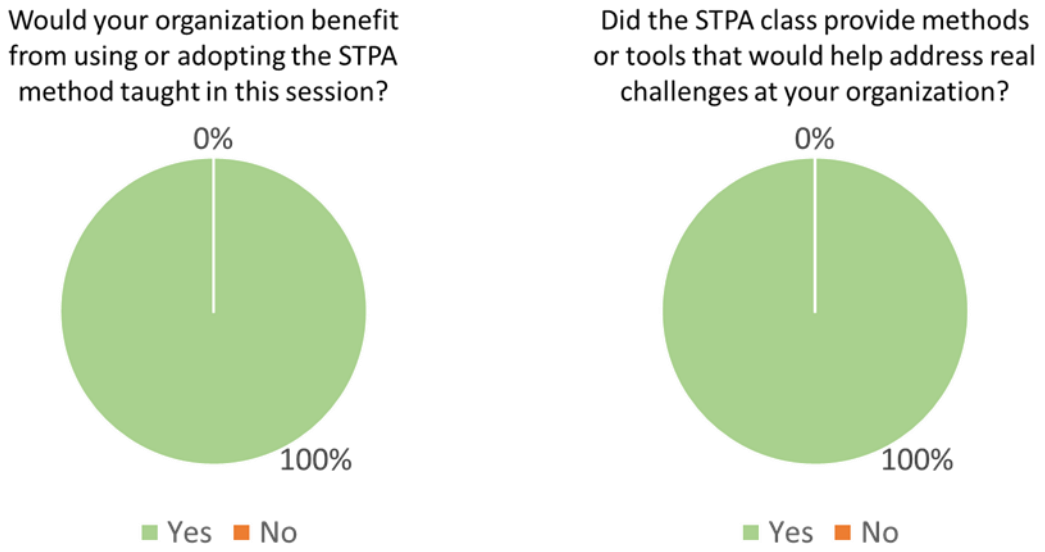

Figure C-3. Findings from FAA certification, policy, and other staff related to whether STPA provides benefit and addresses real challenges the staff encountered

FAA staff were asked which FAA groups would benefit from STPA.

They provided the following answers:

- Transport Standards Branch
- ACO's (Aircraft Certification Offices)

- BASOO (Boeing Aviation Safety Oversight Office)
- Accident/Incident Investigation
- Continued Operational Safety
- FAA Standard Staff
- FAA ACO specialists involved with system safety
- AFS
- ATO
- AEG
- FS
- AEL
- Standards Development - Washington DC
- Hlgtvs
- Standards Development - All directorates
- Compliance enforcement
- Those at ATO that introduce new products or changes in the NAS
- Those at ATO doing Ground-Based Surveillance, Navigation Communication Systems, Airport Design

FAA staff were asked if they had any additional comments regarding STPA.

They provided the following:

- This workshop was great! There is certainly a compelling reason/explanation as to why we may need to change our way! The workshop should be expanded to a broader audience within the FAA.
- The management is a big issue.

D Sample of industry STPA evaluations and uses in aviation

Table 1 contains a brief selection of published STPA industry evaluations and uses in aviation. The full extent of STPA use by industry is not possible to gauge as it is a public method with no requirement to disclose to regulators or any other entity when STPA is used or what additional hazards were identified by STPA.

Some STPA results have been published, as are some results from FHA and other standard approaches. At the time of this writing, thousands of publications exist for both STPA and FHA applied to aircraft systems, although FHA has been standard practice for about two decades longer than STPA. Thousands of publications also exist for STPA applied to safety management.

- 6,380 publications on FHA used to analyze aircraft systems (~30-year period)
- 1,640 publications on STPA used to analyze aircraft systems (~10-year period)
- 4,270 publications on STPA in safety management (~10-year period)

The Annual MIT STAMP/STPA Workshop has included 2,769 aviation participants from 1,389 aviation organizations across 79 countries worldwide. Before attending the workshop, most reported that they had already applied STPA at their organizations. A partial list of organizations is available on the workshop website (Garcia & Mtlokwa, 2022). The STPA Handbook for practitioners has been downloaded 220,000 times worldwide since its release in 2018.

Table 1 summarizes a selection of 60 public-domain and peer-reviewed STPA evaluations and uses in aviation safety. Note that this table is incomplete and represents a subset of thousands of publicly presented or published STPA uses in the aviation industry.

Table 1. Selection of past STPA uses in aviation

Organization	**Year**	**Summary**
FAA (Dewalt & Skaves, 2012)	2012	▪ STPA “proposes an alternative process to current FAA safety assessment methods.” ▪ STPA “extends the safety analysis to include nonlinear, indirect, and feedback relationships among events.” ▪ “Need to identify gaps in existing FAA guidance material that STPA would address (would require review of the new ARP4754A and proposed ARP4761 standards)” ▪ “Recommendations include implementation of STPA on a pilot certification project for fact finding purposes.”

Organization	Year	Summary
NASA (Neogi, 2012)	2012	▪ STPA was applied to safety of new aircraft, including software, hardware, crew, operational planning, and contingency planning and execution.
Amsterdam University (de Boer, 2013)	2013	▪ STAMP/STPA was used to understand unsafe human/pilot behaviors, including scenarios where automation and alerting systems working as designed will negatively influence human performance
Beihang University (Deming, 2012)	2013	▪ STPA was used for safety analysis of aircraft modifications, management, design of flight navigation software, hardware synchronization, and other areas. ▪ STPA results were compared to standard fault tree analysis (FTA) and failure modes and effects analysis (FMEA). FTA and FMEA were found to be ineffective in preventing critical software and hardware unsafe behaviors and other factors that led to 20 serious events that threatened flight safety. STPA identified the gaps and led to more effective system and software designs. ▪ STPA was compared to standard aviation development processes. Standard processes were found to omit critical system, software, and verification and validation requirements that were captured by STPA.
MIT (Fleming, Improving Hazard Analysis and Certification of Integrated Modular Avionics, 2013)	2013	▪ STPA was applied to aircraft designs using integrated modular avionics (IMA) and compared to standard approaches. STPA was found to identify critical cases overlooked by standard approaches.
Beihang University (Yi, 2013)	2013	▪ STPA was applied to novel remote-piloted aircraft with unmanned aerial vehicle (UAV) ground stations and blended wing body designs. ▪ STPA was used in a low-cost environment with “lack of adequate funding,” uncertainty of novel aircraft characteristics, lack of robust reliability data for aircraft

Organization	Year	Summary
		systems, schedule pressure, and low levels of experience in standard system safety assessment approaches. ▪ STPA was quickly learned and applied to safety assessment, including aircraft development (flight control, propulsion, etc.), manufacturing, and flight test. ▪ STPA was found to be more cost effective and more broadly applicable than the standard processes.
Rolls Royce Civil Aerospace (Fletcher, 2014) (Thomas, 2023)	2014	▪ STPA was applied to a Part 25 aircraft engine control system after it had already been designed and analyzed using the standard development and safety assessment processes for certification, including the typical independent reviews, approvals, and two years of flight testing. ▪ STPA was found to readily identify specific causes of a critical flight safety issue that had been overlooked by the standard safety assessment and development processes. ▪ STPA was demonstrated to catch a subtle but catastrophic common-mode failure scenario involving the engine, engine controls, sensors, and environment that had been overlooked by the standard development and safety assessment processes. Design and requirements changes were necessary to bring the design into compliance with regulatory criteria regarding single failures. ▪ STPA identified 30 additional causes of unsafe behavior that necessitated several late design changes. This occurred after the system had been designed, reviewed, approved, built, and flown for two years while the 30 additional causes of unsafe behaviors were overlooked using standard processes for development and safety assessment. ▪ After the original publication, the control system was used as a case study by INTA and others to measure the capability and consistency of STPA across practitioners with standard STPA training and to compare the STPA

Organization	Year	Summary
		results with those from teams that applied standard aircraft safety assessment and development assurance processes on the same system. STPA was found to consistently identify the flaws, including the subtle but catastrophic common-mode failure, as well as flawed requirements and human behavior assumptions that were overlooked by the standard processes (Thomas, 2023). ▪ In parallel, other engine control systems with the same intended functionalities were added in other aircraft and were developed using the standard development and safety processes (not STPA). These systems were independently evaluated by the FAA and others following standard processes (not STPA). These other designs were each approved by the FAA based in part on the conclusion (without STPA) that the control systems would correctly respond to certain discrepancies and that all practicable actions had been taken including appropriate control system logic, system requirements, and human procedures (Federal Aviation Administration (FAA), 2017). These assumptions and approvals contradict the STPA results years earlier that identified significant flaws and corrective actions that were missed in similar systems with the same intended functionalities—including the design flaws, missing requirements, and missing procedures that were consistently overlooked by the standard processes. ▪ A non-fatal event occurred in one of these systems that was approved without STPA. Unexpected dual engine shutdowns occurred during operation due to unsafe commands by the control system in exactly the way STPA predicted years earlier on an equivalent system with the same intended functionalities. The event was caused by the same STPA unsafe control actions, missing requirements, unanticipated pilot actions, omitted

Organization	Year	Summary
		information in operations manuals, inconsistent functionality leading to pilot confusion, and gaps in pilot procedures that were found by STPA before the event. No recommendations or preventative measures were implemented after this event. ▪ Another dual engine shutdown event occurred a second time during operation in a system approved without STPA (International Air Transport Association, 2019), again due to unsafe automation system design, missing requirements, unanticipated pilot actions that violated safety assessment assumptions, omitted information in operations manuals, inconsistent functionality leading to pilot confusion, and other factors in exactly the way STPA predicted before the event. After the second event and the ensuing investigation, a number of changes were implemented including a safety bulletin, updated procedures, new system requirements, and a software modification to the control system. These changes matched the specific solutions and requirements previously generated by STPA years before both events (Thomas, 2023).
Fort Hill Group with support from FAA Human Factors Division (Berry & Sawyer, 2014)	2014	▪ STPA was used to identify human performance hazards and evaluate system safety in NextGen, including flight crew, flight deck automation, air traffic control (ATC), and ATC automation.
MIT (Fleming, Hazard Analysis of NextGen Arrival Phase of Flight Concepts: Interval	2014	▪ STPA was used to analyze safety of NextGen, including flight deck-based automation behaviors, flight crew behaviors, and ground-based automation behaviors. ▪ STPA was found to be an effective approach to identify new unsafe scenarios that had not otherwise been analyzed and mitigated.

Organization	Year	Summary
Management – Spacing, 2014)		▪ STPA was found to identify safety concerns and flawed operational concepts and assumptions earlier, resulting in a more cost-effective and efficient approach.
Boeing (Allsop & Xu, 2014)	2014	▪ STPA was compared to FMEA, failure modes, effects and criticality analysis (FMECA), FTA, and other standard techniques for safety assessment. ▪ Standard techniques were found to be more complex, costly, and overly focused on narrow root causes rather than systemic causes. ▪ STPA was selected to analyze hazards in new NextGen aircraft systems.
BAE (Almalik, 2013)	2014	▪ STPA was applied to aircraft training for Hawk T-165. ▪ Findings: STPA identified secondary safety risks and control behaviors that were otherwise overlooked. STPA could be understood by non-safety experts. STPA did not require extensive training like other techniques. ▪ Conclusions: STPA should be implemented throughout the design phases, beginning with initial design, together with other tools.
MIT and Honeywell (Fleming & Wilkinson, 2014)	2014	▪ STPA was demonstrated and compared to standard aircraft safety assessment processes, including examples from an aircraft wheel braking system. ▪ Gaps were identified in standard safety assessment processes include the lack of integration of human factors considerations, gaps in identifying unsafe automation/software behaviors and their causes, and the continued use of incorrect probabilities in practice.
Amsterdam University (de Boer, Using STAMP to Improve Platform Safety, 2014)	2014	▪ STPA was applied in the context of aviation safety management systems (SMSs).

Organization	Year	Summary
Boeing (Allsop & Xu, 2015)	2015	▪ STPA was applied to safety of novel aircraft and operational considerations, including remote flight-testing capability.
Florida Institute of Technology (Stephane, 2015)	2015	▪ STPA was applied to aircraft, communication, and other technologies after the loss of MH370, including ADS-B and others.
MIT and US Air Force (Johnson & Leveson, Unmanned Aircraft Integration into the National Airspace: A Cognitive Systems Engineering Framework for Safety Model Development, 2015)	2015	▪ STPA was applied to new unmanned aircraft to be integrated into the national airspace, including detect and avoid automation, remote pilot behaviors, and cognitive system engineering considerations.
Institute of Aerospace Technology, Brazil (Castilho, Urbina, & de Andrade, Application of STPA for Hazard Analysis on Light Aircraft Crosswind Takeoffs, 2015)	2015	▪ STPA was applied to safety of light aircraft and crosswind takeoffs, including failure conditions and pilot behaviors.

Organization	Year	Summary
MIT and FAA (Helfer, 2015)	2015	▪ STPA was applied to cyber security of aircraft networks and control systems, including field loadable software.
Boeing (Howard & Smith, 2016)	2016	▪ STPA was applied to workplace safety for aircraft manufacturing.
MIT and University of Alabama (Abrecht, et al., 2016)	2016	▪ STPA was applied to analyze safety of a rotary-wing aircraft, including the warning, caution, and advisory system, flight control system, and electrical systems. ▪ STPA results were compared to standard safety assessment processes for Department of Defense aircraft. STPA found additional hazards not documented in the standard safety assessment and hazards that were incorrectly categorized as low severity before STPA was applied.
Embraer (Ribeiro, 2016)	2016	▪ STPA was used to analyze the safety of an aircraft smoke control system in parallel with standard safety assessment methods. ▪ STPA results were compared to results from standard safety assessment methods. ▪ Conclusions: STPA systematically assessed interfaces at an earlier stage than possible with standard approaches. STPA results are not as dependent on past experience. STPA identified additional component interaction accident scenarios that were not covered by standard approaches. STPA identified additional relevant human interactions and identified hidden engineering assumptions about human behaviors.
Amsterdam University (Karanikas & Abrini, 2016)	2016	▪ STPA was used to evaluate aviation SMSs, identifying weaknesses, developing requirements, and developing efficient auditing strategies to continuously assess performance. ▪ STPA was compared to current SMS tools, including tools from five civil aviation authorities. ▪ Conclusions for current SMS tools: Current SMS tools have notable weaknesses, including lack of systematic

Organization	Year	Summary
		analysis of the SMS, high variation in their coverage of SMS processes, lack of consideration of interconnections and influences between individual SMS processes, focus on compliance and operation rather than the full spectrum of safety, and focus on failures of system components. ▪ Conclusions for STPA-based approach: STPA provides systematic analysis of the SMS, considers individual SMS elements as well as their interactions, provides necessary information on SMS performance, and may reduce the workload of auditors and the duration of audits.
University of Athens, Amsterdam University, and University of Cambridge (Plioutsias, Karanikas, & Chatzimichailidou, 2016)	2016	▪ STPA weas applied to the operation of four small commercial drones, including developing safety requirements for automation/software, the drone operator, the drone manufacturer, and regulators. ▪ Conclusions: STPA can be used for drone design, certification, and safety benchmarking.
MIT and Alitalia Airlines (Scarinci & Gusti, A STAMP-based Hazard Log for Use during Development and Operations, 2016)	2016	▪ STPA was used to bridge gaps between aircraft development and operations, such as assumptions made during development that are inadvertently violated during operations. ▪ STPA was applied to systematically generate a log of potential hazards during development, generate safety requirements and constraints during development, rigorously identify hidden assumptions made about aircraft operations, and generate leading indicators of risk during operation.
Graz University of Technology and MIT (Koglbauer & Leveson, Using	2016	▪ STPA was applied to analyze safety risks in visual flight and develop more effective mitigations.

Organization	Year	Summary
STAMP to Address Causes and Preventive Measures of Mid-Air Collisions in Visual Flight, 2016)		
Embraer, ITA, Federal University of Alfenas, IPEN (Pereira, Hirata, Pagliares, & de Lemos, 2017)	2017	▪ STPA was applied to the safety and security of an aircraft flight management system. ▪ Conclusions: STPA was found to be an effective alternative to current security standards. ▪ Embraer proposed STPA as an alternative means of compliance to ED-202A/DO-326A, which was accepted.
Embraer (Scarinci, et al., A complete STPA Application to the Air Management System of Embraer Regional Jets family, 2017)	2017	▪ STPA was used to analyze safety of the air management systems of the Embraer Regional Jets family of aircraft. ▪ Conclusions: STPA was found to effectively identify scenarios and requirements that were otherwise missed with standard methods.
US Air Force and MIT (Summers & Folse, STAMP applied to SUAS at Edwards AFB, 2017)	2017	▪ STPA was used to analyze safety of small unmanned aerial systems (SUASs) including eVTOL, autonomous UAV technologies, manned/unmanned aircraft, and air traffic control. ▪ STPA was found to identify additional requirements and safety insights that were not found otherwise.
General Dynamics Mission Systems (Malloy, 2017)	2017	▪ STAMP/STPA was demonstrated to satisfy requirements of a functional hazard analysis (FHA), one of the standard foundations of an aircraft safety assessment. ▪ STPA was found to satisfy standard FHA tasks, including function identification, hazard identification, requirements development, function allocation, and traceability between

Organization	Year	Summary
		functions, commands, hazards, requirements, and constraints. ▪ STPA was found to provide additional benefits that are consistent with FHA intent but go beyond standard FHA definitions, such as identification of conflicts between multiple controllers, addressing potential coordination problems and inadequate control schemes, and identification of how unsafe control actions can occur. ▪ STPA was found to be an effective approach to support risk assessment, including classifying severity, making risk acceptance decisions, and planning mitigations. ▪ STPA "provides the needed conceptual rigidity and contextual flexibility to perform accurate and complete functional hazard analysis consistently."
Boeing (Juhnke, 2017)	2017	▪ STPA was applied to flight line work, including lockout tagout (LOTO) activities, supervisors, and management roles. ▪ Conclusion: STPA benefits included improved capture of all possible causal scenarios, faster generation of causal scenarios, production of a stronger business case to implement necessary mitigations, verification that the mitigations and solutions will really work, and improved adoption by end-users of the mitigations.
Embraer and MIT (Scarinci, et al., STPA in the Aeronautical Industry, 2017)	2017	▪ STPA guidance and best practices for the aviation industry were identified and provided following several years of successful STPA applications in industry.
MIT and US Air Force (Horney, 2017)	2017	▪ STPA was applied to light transport aircraft, including aircraft systems, software, hardware, pilot-vehicle interfaces, and flight crew interactions. ▪ STPA was found to be effective for early concept development, architectural trade studies, software and system functionality trade-offs, aircraft and system

Organization	Year	Summary
		requirements identification, and other key aspects of development.
MIT and US Air Force (Johnson K. , 2017)	2017	▪ STPA was applied to improve consideration of unsafe coordination behaviors in novel aircraft with complex control schemes and multiple controllers. ▪ An unmanned aircraft system (UAS) with detect and avoid (DAA) automation was analyzed separately using both STPA and FHA applied by separate teams of expert practitioners. The STPA results were compared to actual FHA results. ▪ STPA was demonstrated to provide coverage over nine critical types of unsafe coordination that are overlooked by standard techniques. ▪ FHA was found to provide no coverage of five categories of unsafe coordination. About 45% of all known hazardous coordination scenarios are represented by these categories. These scenarios were identified by STPA but overlooked by FHA. ▪ FHA was found to provide partial coverage for four out of nine categories of unsafe coordination. Within these four categories, FHA overlooked 55% of all hazardous coordination scenarios identified by STPA. ▪ STPA-identified safety requirements for unmanned aircraft. These were compared to safety requirements produced by standard techniques that had been performed and reviewed by expert practitioners. Standard techniques were found to miss critical safety requirements that were found by STPA.
Graz University of Technology (Koglbauer, STPA-based Model of Threat and Error	2017	▪ STPA was applied to expected and unexpected events during flight and the flight crew's ability to recognize and respond appropriately to recover. STPA was used to develop improved requirements and recommendations. ▪ STPA was found to be more comprehensive for flight crew behaviors, including threat and error management

Organization	Year	Summary
Management in Dual Flight Instruction, 2017)		(TEM). STPA was found to improve the quality of flight instruction and training.
MIT and Brazil Air Force (Castilho D. , 2017)	2017	▪ STPA was applied to flight testing, including in-cockpit automation systems and artificial intelligence (AI).
US Air Force Institute of Technology (Span, Mailloux, & Young, 2018)	2018	▪ STPA was applied to a Next Generation refueling aircraft.
MIT and US Air Force (Summers, 2018)	2018	▪ STPA was applied to a general aviation aircraft that is being converted to a UAV, including ground station control, autonomy, vehicle management system (VMS) controls, and other aspects. ▪ STPA was demonstrated to identify additional scenarios that were originally missed using standard techniques. ▪ STPA was found to comply with and support existing Department of Defense airworthiness requirements.
Embraer (Tavares, 2018)	2018	▪ Experiences over many years using STPA in the context of aircraft development, safety assessment, and cybersecurity were discussed. ▪ "It is important to influence the certification authorities to include STAMP/STPA as a complementary and/or alternative means of compliance."
BAE (Hurley & Wankel, 2019)	2019	▪ STPA was found to provide an effective model-based systems engineering (MBSE) approach to design safety into a system, as opposed to standard safety methods that provide safety assessment rather than safety design. ▪ BAE describes an MBSE tool based on SysML that captures the results from each step of STPA, including formal requirements and executable state machine logic

Organization	Year	Summary
		generated by the STPA process for systems with automation. ▪ STPA was found to improve safety by influencing key early decisions that system designers would otherwise have to revise later with more difficulty.
MIT and Brazil Air Force (Castilho D. S., 2019)	2019	▪ STPA was demonstrated to satisfy key parts of the standardized ICAO SMS framework, including hazard identification, safety risk management, risk mitigation, and safety performance monitoring and measurement. ▪ STPA was used by an international commercial airline to analyze flight operations quality assurance (FOQA) data and develop safety performance indicators, which identified additional hidden operational events and risks that were otherwise overlooked.
Boeing (Nance, 2019)	2019	▪ STPA was demonstrated and evaluated on a limited range of commercial and military products, which "uncovered numerous product, production system, and automation design anomalies that were previously unknown" and were overlooked by the standard techniques. ▪ STPA was applied to a new aircraft in development. STPA identified numerous design flaws that were overlooked by industry standard development and safety assessment techniques, including: o Design flaws in pilot/flight management o Design flaws in the avionics system o Design flaws causing flight control computing system (FCCS) unsafe actions o Design flaws in flight control actuation ▪ STPA was applied to factory automation, including robot and automated ground vehicles. STPA identified previously unknown system design flaws that were missed with standard techniques.

Organization	Year	Summary
		▪ STPA was applied to hot fire test (HFT) safety and identified additional scenarios and safety mitigations that improved the test configuration. ▪ STPA was applied to aircraft work management. STPA identified significant challenges that led to new compelling mitigations and unified production and delivery teams on safety improvements. ▪ STPA was applied to a production system and identified many additional safety requirements. ▪ In all cases, STPA was found to provide key improvements over existing processes: ▪ STPA "analyzes systems hardware, software, human, and environment interfaces and interactions." ▪ STPA was "proven to be more efficient and effective than traditional methods." ▪ STPA provided the "greatest benefits with complex systems with hardware, software, and human interaction." ▪ STPA "provides a different perspective than industry standard tools, e.g. failure modes and effects analysis." ▪ STPA was found to be "relatively simple and straightforward to use."
Lincoln Laboratory and FAA (Weller-Fahy, 2019)	2019	▪ STPA was applied to aircraft safety, security, and risk assessment.
Embraer and ITA (Reiser, Martinez, Lahoz, & Villani, 2019)	2019	▪ STPA was used to analyze an aircraft approach/landing procedure and find additional vulnerabilities related to runway excursions. ▪ STPA was found to be an effective approach to analyze complex behaviors and interactions between aircraft mechanical systems, aircraft automation, flight crew behaviors, and airline operations and procedures.

Organization	Year	Summary
L3HARRIS (Archibald, 2020)	2020	▪ STPA was found to provide a systematic approach that identifies relevant hazards at a rate six times faster than standard techniques. ▪ STPA benefits were recognized by engineers, and STPA was found to be more efficient. ▪ Challenges exist related to organizational inertia. There is management reluctance to drive change given the lack of government rules, policy, or guidance on STPA. ▪ Effective STPA training was found to be difficult without experienced expert STPA instructors.
Embraer (Moraes, 2020)	2020	▪ STPA use for aircraft system engineering and safety over the last nine years was summarized, including safety, security, and novel applications like Urban Air Mobility (UAM).
Air Hong Kong (Larard, 2020)	2020	▪ STPA adoption to improve an airline's SMS was summarized, including FOQA data analysis, Aviation Safety Action Program (ASAP), and safety culture.
MIT (Thomas, 2020)	2020	▪ STPA, FTA, and FMEA were compared empirically. Each method was applied independently by teams of expert professional practitioners to a cooling system with associated automation and human interactions. ▪ The results from each method were compared to each other and to real operational incidents that occurred after the real design was put into operation. The real incidents were not known to any practitioners in this study—they had to discover the flaws by performing their own safety assessment. ▪ STPA was the only method found to identify the critical design flaws that existed in the real system and that lead to actual catastrophic events. These flaws included unsafe automation behavior in certain operational contexts, undocumented assumptions about the human operators and the environment, unanticipated human behaviors, and flawed human procedures.

Organization	Year	Summary
MIT and US Air Force (Johnson E. , 2020)	2020	▪ STPA was used to develop and evaluate conceptual designs of future manned and unmanned aircraft. ▪ Conclusions: STPA advantages include additional insights possible during early design phases before detailed architectures and other information is available, critical requirements and responsibilities that can be identified earlier using STPA, the ability to quickly compare alternative concepts, and the ability to identify gaps in a concept earlier than is otherwise possible.
RWTH Aachen University (Lima, Schwienhorst, & Reichmuth, 2020)	2020	▪ STPA was used to evaluate safety and security of future airport designs and concepts. ▪ STPA was found to effectively identify common causes, generate clear requirements, identify paths and opportunities for the legal framework to improve, and identify critical scenarios that can be easily simulated.
Brazilian Air Force (Merladet, Lahoz, & Silveira, 2020)	2020	▪ STPA was applied to certification of military aircraft, including design approvals, production approvals, certificate management, and continued airworthiness. ▪ STPA identified gaps in the certification process and led to improvements at the certification authority.
FedEx Air Operations (Reeves, 2020)	2020	▪ STPA was used for safety of airline flight operations.
US Air Force (Aust, Pennington, & Young, 2021)	2021	▪ STPA was applied to development and safety assessment of electric vertical takeoff and landing (eVTOL) aircraft in order to accelerate the commercial industry in partnership with the FAA. ▪ STPA results are being used by airworthiness teams, and one company already received airworthiness certification.
Boeing (Stanley & Barraquero, 2021)	2021	▪ STPA was applied to small UAS (sUAS) and emerging hazards, including UAS air vehicles, UAS ground stations, UAS operators, UAS flight approval providers, and air traffic control (ATC). ▪ Conclusions:

Organization	Year	Summary
		○ STPA provided an effective way to evaluate alternate requirement proposals. ○ STPA provided traceability with documented rationale for each scenario and requirement. ○ STPA enabled evaluation of alternate hazard mitigation strategies. ○ STPA effectively managed complex interactions. ○ STPA generated insight and solid analytical basis for recommendations to stakeholders. ○ STPA provided a pictorial depiction of hazards that aided organization and communication. ○ STPA proved to be an effective analysis tool.
Cathay Pacific (Larard, Industrialization Panel, 2021)	2021	▪ STPA was used to improve airline operational safety.
Embraer (Silva, Filho, & Pinto, 2022)	2022	▪ STPA was applied to aircraft concept and development phases with a focus on ground operations, including providing system updates, preparing and configuring aircraft systems for missions, loading and unloading, repairing and maintaining systems, towing, and accident recovery. ▪ STPA results included insights about inadequate lifting points, flaws in fault detection and monitoring, system diagnostic errors, gaps in human procedures, and cybersecurity vulnerabilities related to system updates. ▪ Conclusions: STPA structured the development and safety assessment process in a way that made the problem easier to study compared to standard approaches, and STPA provided an improved requirements definition process.
ICAO Safety Management Panel [62]	2022	▪ An overview of STAMP/STPA was provided as a solution to improve current safety risk management methods and tools.

Organization	Year	Summary
Boeing (Wijayratne, Stringfield, Clark, & McDonald, 2022)	2022	▪ STPA was applied to safety of an automated test maneuver (ATM) Dutch roll initiator (DRI) system that commands flight control surfaces without pilot inputs. ▪ STPA was used in the context of model-based test automation to validate models rather than simply show compliance. ▪ STPA was performed in part to 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?" ▪ The STPA results included many new scenarios that had not been previously considered, even though the system was already previously designed and used for other similar types of tests. STPA results included new scenarios that would change the natural frequency settings, inputs that would confuse or otherwise would not be handled properly by the DRI system, pilot interactions with the system, and potential discrepancies between critical signals that would disrupt safe DRI behavior. ▪ The STPA results generated many additional requirements, mitigations, new verification activities, software updates, and new procedures to ensure safe DRI operation. ▪ Conclusions: o Team members found that the STPA results would not have been caught without STPA. o STPA was effective and improved an already built, designed, and tested system by identifying previously unknown safety concerns. o STPA results were accepted by the Safety Review Board. o STPA was found to be "incredibly helpful and provided powerful, confident results."

Organization	Year	Summary
		○ STPA created "a positive culture change instead of, 'We've used this system before. It's safe. Why do we need STPA?'"
AEL Sistemas (Quilici & de Oliveira, 2022)	2022	▪ STPA was applied to aircraft security/cybersecurity in a certification context. ▪ Conclusions: STPA produced a robust requirements basis in a short period of time, made the complex systems easier to analyze, and lead to the company recommendation to execute STPA on future applications.
Xmobots and UNIFEI (Mendes & Sousa, 2022)	2022	▪ STPA was applied to small electric propulsion aircraft, including control systems and electrical power systems. ▪ Conclusions: STPA led to new requirements, provided a robust methodology that led to a more robust product, and resulted in overall development cost reduction compared to other standard processes.
Bell / Textron (Mutuel, 2022)	2022	▪ STPA was applied to development and safety assessment of a future rotary-wing aircraft with advanced autonomy and "optionally manned" flight. ▪ A blended approach was adopted for development and safety assessment with STPA used alongside standard civil and Department of Defense processes, including ARP4754, ARP4761, and MIL-STD-882E. ▪ Conclusions: ○ STPA was effective in extending the standard system safety framework to strengthen human factors considerations. ○ STPA was applied and useful at both the aircraft level and system level. ○ STPA integration provided key benefits, including improved hazard identification, risk assessment, risk mitigation, requirements identification, safety verification, and identification of critical test cases. ○ STPA both extends and integrates with system safety activities.

Organization	Year	Summary
		○ STPA was found to be most powerful where traditional practices were weakened by context (e.g. lack of established design maturity, complexity of interactions). ○ The new results that were discovered by STPA were initially intended to be added to the existing standard approaches. However, the team of expert practitioners found that some complex unsafe behaviors identified by STPA could not be represented by standard processes like FHA even after they were discovered by STPA because of the rigid types of causal factors modeled by standard processes.
American Airlines (Palyok, 2023)	2023	▪ STPA was used extensively in all areas of airline safety, including engineering, aircraft technical modifications, human factors, flight crew operations, equipment, and other areas.