Quality Assurance Standards for Commercial Flight Safety Analysis

THE OHIO STATE UNIVERSITY
BATTELLE CENTER FOR SCIENCE, ENGINEERING, AND PUBLIC POLICY

FEDERAL AVIATION ADMINISTRATION

To: Cameron Gude, Aerospace Engineer
Paul Wilde, Chief Engineer
FAA Office of Commercial Space Transportation

From: Samantha Burmeister, Kelly DeRees, Jacob Keller, Andrew Noonan
Battelle Center, The Ohio State University

Contact:
Samantha Burmeister, burmeister.32@osu.edu
Kelly DeRees, derees.1@osu.edu
Jacob Keller, keller.974@osu.edu
Andrew Noonan, noonan.83@osu.edu

Issue:

The Federal Aviation Administration (FAA) Office of Commercial Space Transportation holds a valuable role in the newly developing commercial space sector, tasked with promoting public safety and encouraging industry growth. Their oversight of the launch license application process is a key interaction between the FAA and space launch providers. Currently, the FAA struggles to review an application within the mandated 180 day limit. This problem is compounded by new technologies and the FAA's relationship to the United States Space Force (USSF) (previously the United States Air Force). Due to their historic involvement in space, Air Force methodologies for range safety and other processes are woven into the fabric of commercial space operations today.

The FAA's struggle to keep pace with a rapidly growing commercial space industry shows no signs of abating, especially in the face of disruptive technologies challenging the technical expertise and resourcefulness of regulators. The increasing use of autonomous flight safety systems (AFSS) has begun to raise questions surrounding the launch license application process of the FAA's technical ability to evaluate these systems (See Appendix A for more background and discussion surrounding AFSS). Moreover, AFSS requires more extensive flight safety analysis since automation effectively shifts flight termination decision making to the front of the process. Since existing workflows require the FAA perform an independent flight safety analysis for each applicant, and AFSS increases the breadth and depth of required analyses by 2-3 times [1], it is clear that current FAA approaches to certify flight safety are unsustainable for the future.

Due to the problems surrounding the FAA's system for flight safety analysis in the face of rising demands, the FAA must expedite the process in a controlled way that prioritizes public safety. Such a method already exists, expediting the flight safety component of the launch license application process; launch providers can pay the Space Force to perform their analysis, which the FAA will accept in lieu of their own. This speeds up the process by several months [2].With technologies like AFSS reducing industry reliance on the federal ranges, it's clear that the FAA needs a process for trusting third party analysis similarly to how analyses from the Space Force are treated. This will broaden the ways that the analysis component can be satisfied.

With the introduction of AFSS, commercial space is in a transition period where services previously held by the government will be democratized. For this transition to occur gracefully, and satisfy the objectives of FAA AST, well-planned action must occur to make sure regulators and launch providers can ensure a thriving and safe commercial space sector. Failure to do so may result in an industry hindered by red-tape from inadequate policy and overreliance on underfunded federal entities.

Recommendation:

We propose the development of a comprehensive industry consensus standard for flight safety analysis that the FAA may leverage to incorporate performance-based application evaluation and better focus agency resources. Developing the standard will require 1) roundtable discussions co-sponsored by the FAA and the Commercial Spaceflight Federation (CSF); 2) adoption of the standard by an independent, ANAB-accredited quality assurance organization; and 3) FAA safety approval of the quality assurance process developed by the independent certifying body.

Roundtable: Four quarterly roundtable discussions will occur over one year. Participants will include, but are not limited to, the following:

- FAA and Commercial Spaceflight Federation as co-hosts
- Representatives from the Department of Defense, such as the Space Enterprise Operations Division of the Space Force, and 30th Space Wing and 45th Space Wing range operators
- Commercial space industry participants, including launch/reentry operators and flight safety analysis software developers
- Space insurers, such as Allianz Global Corporate and AXA XL

Agenda items will include acceptable non-vehicle dependent inputs, methods for developing trajectories, acceptable software tools, environmental analysis, and other topics as determined by the FAA and CSF co-hosts. Critical interests of major stakeholder groups include public safety for the FAA, mission assurance for industry, and critical asset protection for the Space Force. Roundtable discussions should be centered around establishing standard methods that address these interests, which were revealed through interviews with representatives from each stakeholder group, including Jennifer Bailey of the FAA [3], Eric Stallmer of the CSF [4], Christopher Allison of Sierra Nevada Corporation [5], Burton Catledge of Launch On Demand [2], and Tim Leroy of the U.S. Space Force [6].

Other relevant topics include addressing environmental concerns and local public interests. Given the FAA’s role in National Environmental Policy Act (NEPA) compliance, we expect the FAA can offer expertise during the roundtables to influence the environmental analysis portion of the industry standard. We also recommend the roundtable co-hosts 1) conduct a public comment period to gather input from interested parties and 2) establish prerequisites for participation prior to the roundtables. Such prerequisites may include reports developed by participating organizations on their current practices for addressing environmental and local concerns.

Industry Standard: At the conclusion of the roundtable series, an industry standard will be developed through SAE International, recommended for its previous experience in developing widely-adopted aerospace standards. The new standard will include ISO 9001:2015 requirements for quality management systems with additional requirements for flight safety analysis. The publication process for a new SAE standard will include the Systems Development and Safety, Component Process, and Management Systems Group of the SAE Aerospace Council [11], [12].

During interviews conducted by the team, members of the space community have expressed strong interest in developing industry standards for flight safety analysis. The FAA Handbook for Flight Safety Analysis may serve as a starting point for such a standard [8]. Interviewed members of the space community included Eric Stallmer [4], Christopher Allison [5], Burton Catledge [2], Tim Leroy [6], and Kevin Hatton [7].

Independent certification body and FAA safety approval: An independent quality assurance organization accredited by the ANSI National Accreditation Board (ANAB) will certify organizations in the new industry standard. The proposed process is modeled after processes used for AS9100D certifications for aerospace manufacturers [9]. The independent certification body will apply for an FAA Safety Approval of their flight safety analysis certification process. The independent body will then certify companies in the new industry standard. Launch license applicants may use their certified flight safety analysis processes to show acceptable means of compliance.

FAA Workflow Changes: Appendix B includes figures and details summarizing the current workflow, proposed workflow, and comparison of both. Anticipated overall changes include shorter pre-application phases and shorter launch license application review times. These changes will equip the FAA with a new workflow that is more easily scaled with industry growth.

Schedule: Appendix C includes the implementation timeline. Total anticipated implementation time is 6-8 years.

Costs:

Though we do not have estimates of costs for each component of this solution, we foresee costs incurred for preparatory activities in advance of roundtable discussions; coordination between organizations in government and industry; and personnel costs for time spent participating in the roundtables, industry standard development, and safety approval for independent certification organization.

Benefits:

This solution provides significant benefits for regulators and other stakeholders alike, holding the potential to shift the commercial space economy towards self-sufficiency and market diversity. The creation of industry standards surrounding flight safety analysis are currently positioned within an industry climate desperately in need of cooperation, with the impending end of a regulatory moratorium surrounding human spaceflight set to end in 2023.

Our recommendation provides quality assurance to the commercial space market and relieves both applicant and FAA analysts from reconsidering an already-certified flight safety analysis process used in a launch license application [10]. Rather than the FAA flight safety analysts dedicating the majority of their time to guiding applicants in the pre-application process, this solution will allow FAA flight safety analysts to focus their workload on submitted applications. In doing so, the FAA is able to streamline the launch licensing process with performance based evaluation. By providing launch license applicants the option to use their certified flight safety analysis processes to show acceptable means of compliance, this will also help to alleviate the Air Force's flight safety analysis workload.

The success of commercial space hinges on the ability of stakeholders and regulators to cooperate to formulate industry standards. An important incentive for standardization lies in launch vehicle insurance; the more standardized an industry (meaning, the more measured quality assurance exists), the more accessible launch vehicle insurance is. Insurance companies have significant influence in the choices of commercial space companies, and this solution incentivizes the best interests of each organization. A more standardized industry means that the FAA and Space Force can redistribute tasks to certified entities, opening up a new era of capabilities and innovation to increase safety and facilitate the evolution of commercial space.

Risks:

The most significant risk of the proposed solution is the changing nature of interplay between regulators and other stakeholders as they navigate the launch licensing process. Through integrating third party service providers to streamline the responsibilities of regulators, the risk of giving too much power to these entities is introduced. To mitigate this risk, we included the utilization of a third party quality assurance organization, as is typical for more developed industries. This solution mitigates the aforementioned risk by verifying an organization's compliance with industry standards, therefore assuring the FAA that their approach is valid, and an independent analysis is redundant, since equally rigorous methods were employed.

The risks associated with our solution are primarily concentrated within its initial stages. Curating a list of participants who should be involved in early roundtable discussions is an outlying risk, with potential cons including a less diverse industry perspective surrounding flight safety analysis. Keeping initial roundtable discussion on topic and impressing the need for the development of industry standards is another significant risk, mitigated through clear and concise communication surrounding the nature of the roundtable. After the development of several industry standards, risk diminishes as stakeholders and regulators alike see the benefits of moving commercial space towards standards that promote quality assurance.

Note: The technical risks introduced by AFSS are discussed in Appendix A.

Conclusion:

The new age of AFSS marks the beginning of significant growth in the space industry. Regulators and stakeholders must cooperate to develop a more self-sufficient and self-regulated industry through the creation of standards, or risk falling behind and threatening the so-far perfect record for public safety in commercial spaceflight.

References

[1] K. Cranor, National Aeronautics and Space Administration, personal communication. 7 February, 2020.

[2] B. Catledge, Launch On Demand, personal communication. 21-22 April, 2020.

[3] J. Bailey, Federal Aviation Administration, personal communication. 2 April, 2020.

[4] E. Stallmer, Commercial Spaceflight Federation, personal communication. 9 April, 2020.

[5] C. Allison, Sierra Nevada Corporation, personal communication. 10 April, 2020.

[6] T. Leroy, United States Space Force, Space Enterprise Operations Division, personal communication. 22 April, 2020.

[7] K. Hatton, ACTA Inc., personal communication, 21 April, 2020.

[8] Federal Aviation Administration. (2011). Flight Safety Analysis Handbook, Version 1.0. Washington, D.C.: Federal Aviation Administration. Retrieved from https://www.faa.gov/about/office_org/headquarters_offices/ast/media/Flight_Safety_Analysis_Handbook_final_9_2011v1.pdf

[9] AS9100 Certification - What Is the AS9100 Standard?. NQA.com. (2020). Retrieved 25 April 2020, from https://www.nqa.com/en-us/certification/standards/as9100.

[10] Federal Aviation Administration. (2012). Safety Approval Guide for Applicants, Version 1.1. Washington, D.C.: Federal Aviation Administration. Retrieved from https://www.faa.gov/about/office_org/headquarters_offices/ast/licenses_permits/safety_approvals/media/Safety_Approval_Guide_1.1.pdf

[11] Standards Development Process. SAE.org. (2020). Retrieved 24 April 2020, from https://www.sae.org/standards/development/process.

[12] SAE Aerospace Council Organization Chart. SAE.org. (2020). Retrieved 24 April 2020, from https://www.sae.org/binaries/content/assets/cm/content/standards/aerospace_standards_org_chart.

Appendix A: Technical Background of AFSS, Discussion of Potential Issues

Background

Flight termination systems (equivalent to flight safety systems, FSS) act as a method to terminate off-nominal rocket launches which threaten public safety. Traditional flight termination systems incorporate a trained decision maker observing telemetry data to make a decision based on preconceived mission rules. This system requires significant ground infrastructure and personnel to ensure this safety capability. The development of Autonomous Flight Safety Systems opens the doorway to eliminating some costs and risks associated with traditional systems, but may open up new gaps in the process.

With AFSS, the organizational complexity of the system is significantly reduced through the introduction of an automated system. That is, the network of range infrastructure requiring certification and maintenance becomes far simpler. In traditional FSS, most infrastructure is required to transmit commands to the vehicle in real time. AFSS eliminates this infrastructure system, as flight termination decision-making is centralized onboard the rocket itself via configurable, software-based redundant flight processors using data from redundant GPS/IMU navigation sensors. This allows the dismantling of infrastructure systems which require regular maintenance, inspection, and operational personnel.

Many individuals within the expert community referred to autonomous flight termination systems as contrary to the “Human-In-The-Loop” system, exposing a particular assumption that automation can replace human capabilities. In actuality, the introduction of an autonomous agent (in this case, a pre-programmed software suite) actually constitutes a shift in work system architecture, pushing the requirement of human expertise and creative problem solving to the front of the launch process in the flight safety analysis phase. This phase involves the development of mission rules, the guiding elements which determine nominal flight conditions based on factors such as payload, vehicle, trajectory, and more. Mission rules are essentially the parameters which define nominal flight status, derived from careful hazard analysis and debris profiling for a particular launch in order to adequately weigh safety concerns in the event of a flight termination. In traditional FSS, the MFCO (or Range Safety Officer) studies mission rules prior to a launch, as their rigorous training and certification process has prepared them to do. During a launch, multiple MFCOs observe key telemetry data, ensuring the vehicle remains within the parameters defined by mission rules.

Mission rules play an integral part in AFSS as well. Since the decision-making agent is a software suite, mission rules must be transposed into a language intelligible to the software, then dubbed a mission data load, or MDL. The evaluation of MDL’s for error is a lengthy task, as AFSS boasts a rather complicated software and hardware configuration, with most systems including three major components: the Core Autonomous Software Suite (CASS), developed by NASA, wrapper software, usually developed proprietarily by launch provider, and hardware, the autonomous flight termination unit as well as its associated sensor array and GPS/IMU navigation sensors onboard the vehicle. The evaluation of MDL's has proved difficult for regulators and the FAA, responsible for providing commercial launch licenses for space, struggles to keep up with demand and technical knowledge required to ensure compliance with the risk standards for public safety.

The creation of mission rules and MDLs which define flight termination decisions create a new set of challenges associated with flight terminations. Some subject matter experts have voiced concerns surrounding the ability of AFSS to provide flexibility and adaptive capacity of an experienced MFCOs, who possess rich domain expertise allowing them to make decisions in context. Astronauts notoriously dislike these systems, and have been known to make a point to introduce MFCOs and Range Safety Officers (RSOs) to their families before launches. Concern surrounding AFSS is warranted, and the nature of subverting real-time decision-making capability to the front end of the launch process is part of a larger decision to sacrifice resilience for optimality. The centralized, onboard nature of an AFTU preloaded with a MDL boasts significant advantages, including reducing range expenses by as much as 50%, amounting to billions of dollars a year saved on maintaining and certifying equipment (based on information from our array of interviews). Other benefits include more rapid decision-making capabilities, global coverage (rather than being bound to ranges which have the proper infrastructure), and the elimination of latency. The tradeoff between optimality and resilience seen in AFSS seems to be justified through the series of unlikely events necessary for a failure. Off-nominal flight conditions would be required for the activation or failure of AFSS to be of concern, and from there, the likelihood that off-nominal flight conditions are significantly novel or contextually rich enough to break the pre-ordained boundaries of the MDL rules or system capabilities affords the system high likelihood to avoid failure in the form of an errant termination (false positive) or missed termination (false negative).

This assumption places heavy credence on independent verification and validation (IV&V) processes intended to ensure the automated system performs as envisioned and has an adequate model of the world. But, these methods, while the best we have at the moment, are by no means ironclad. Low observability is a hallmark trait of automation in highly complex domains, and the software making flight termination decisions in AFSS is no outlier. The tradeoff here is wagering that the upfront capital gains from a significant reduction in range infrastructure costs, coupled with reduced latency increasing flight termination windows (thereby increasing range for destruct line drawing), will outpace the likelihood of an errant flight termination. The potential for an errant or missed flight termination exists, and despite our best efforts for IV&V, and we may pay the price for reaping the benefits of AFSS. Since resilience has been sacrificed as a method of approach, proactively managing the weaknesses introduced through taking measures to increase the robustness of the new system is the next best path to minimize the likelihood of a major error.

Discussion

The elimination of real-time input for flight termination decisions mandates pre-flight safety analysis and mission rule creation as paramount for successful flight termination systems. Automation increases the complexity of the system, changing role dependencies and shifting work system architecture. It's clear that the redistribution of key human responsibilities has occurred with AFSS, pushing responsibilities for termination decision-making

An area of concern for AFSS is that of the lack of uniform qualifications and methods for flight safety analysts, whom the majority of decision making responsibility falls upon with the introduction of automation in this domain.

When considering the implications of an AFSS, it's crucial to highlight the shift of decision-making responsibility for flight terminations. Human flight termination decision makers undergo an extensive training and certification process, including regular skill assessments once certified. Flight safety analysts have no such process, and the title itself bears no specific pedigree or methodology. Many companies hire analysts with various backgrounds, utilize entirely different methods and software tools. It's important to note that a FSA's task while operating under traditional systems includes the development of mission rules to be a guide for termination decisions by the MFCO or RSO. These mission rules possess a level of flexibility, as the decision maker leverages experience against contextual evidence and telemetry data to arrive at a decision which may conflict with pre-ordained mission rules. The introduction of AFSS has eliminated that flexibility, creating more binary mission rules (MDL's) executed by software to terminate flights upon crossing a threshold for off-nominal conditions as detected by sensors and GPS/IMUs.

While flight safety analysis practice is currently 2-3x more extensive with AFSS than in traditional systems, it appears that the lack of analyst training and certification process to ensure expert termination decision making is a major pitfall of the work architecture shifts incurred with the introduction of AFSS. This lack of role training equivalency between MFCOs/RSOs and flight safety analysts threatens the technical validity of the system, and introduces risk for an errant termination to occur in contextually rich flight conditions.

The development of mission rules and mission data loads should entail the expertise of a trained human decision maker to mitigate risk introduced from eliminating the flexibility, or resilience, afforded by a human decision maker. A new paradigm is required to bridge the expertise of trained MFCOs/RSOs and the flight safety analysts now tasked with creating rigid termination criteria for software execution.

Appendix B: Updates to FAA Flight Safety Analysis Workflow

The current FAA flight safety analysis workflow involves an extensive pre-application phase in which FAA flight safety analysts consult with the applicant. This consultation period helps the applicant develop a thorough application that meets FAA expectations, allowing FAA personnel to process the application more efficiently upon receipt. However, flight safety analysts must balance the workload of pre-application and evaluating completed applications. The pre-application phase has no established duration limit, so it may extend into years of FAA consultation. Once received, evaluation requires 2-3 weeks of work per application [5]. This workflow places pressure on FAA resources that is unsustainable with expected growth of commercial space launches.

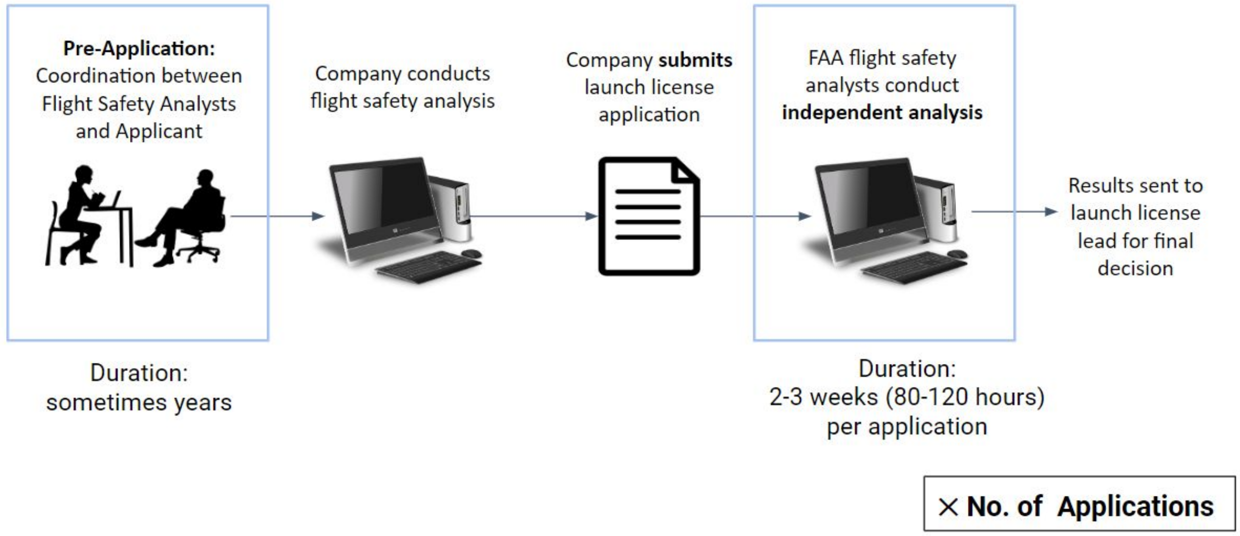
Pre-Application: Coordination between Flight Safety Analysts and Applicant
Company conducts flight safety analysis
Company submits launch license application
FAA flight safety analysts conduct independent analysis
Results sent to launch license lead for final decision
Duration: sometimes years
Duration: 2-3 weeks (80-120 hours) per application
× No. of Applications

Figure B1: Overview of current FAA flight safety analysis workflow.

Following implementation of the proposed solution, the flight safety analysis procedure will follow the workflow shown in Figure A2. In the updated workflow, pre-application flight safety analysis consultation is still an option applicants may choose, but if the applicant is certified in the industry standard, shorter pre-application periods can be expected. Even applicants not yet certified should see shorter pre-application periods due to the existence of an industry standard they may use as guidance.

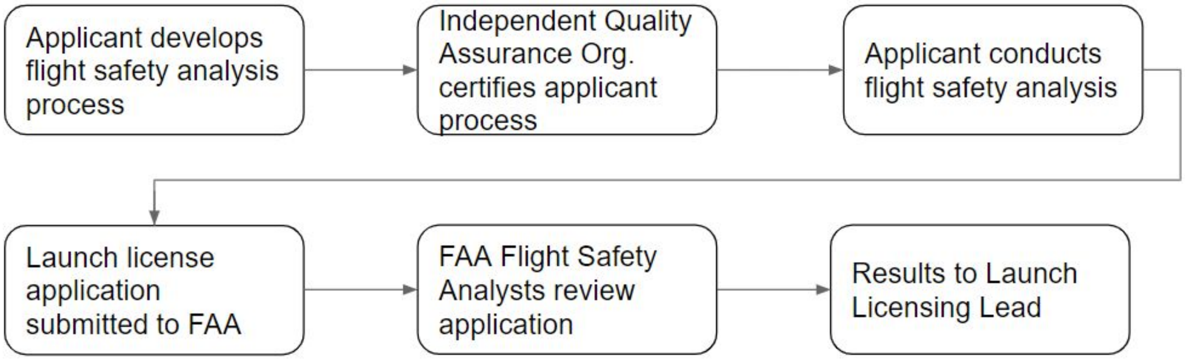
Applicant develops flight safety analysis process
Independent Quality Assurance Org. certifies applicant process
Applicant conducts flight safety analysis
Launch license application submitted to FAA
FAA Flight Safety Analysts review application
Results to Launch Licensing Lead

Figure B2: Workflow after implementation of industry standard and independent certification body for flight safety analysis.

Differences between the current workflow and new workflow are shown in yellow in Figure A3. Consistent with the Streamlined Launch and Reentry Licensing Requirements in 14 CFR proposed Part 450, implementation of the industry standard recommendation will allow FAA flight safety analysts to apply a performance-based evaluation approach to submitted applications.

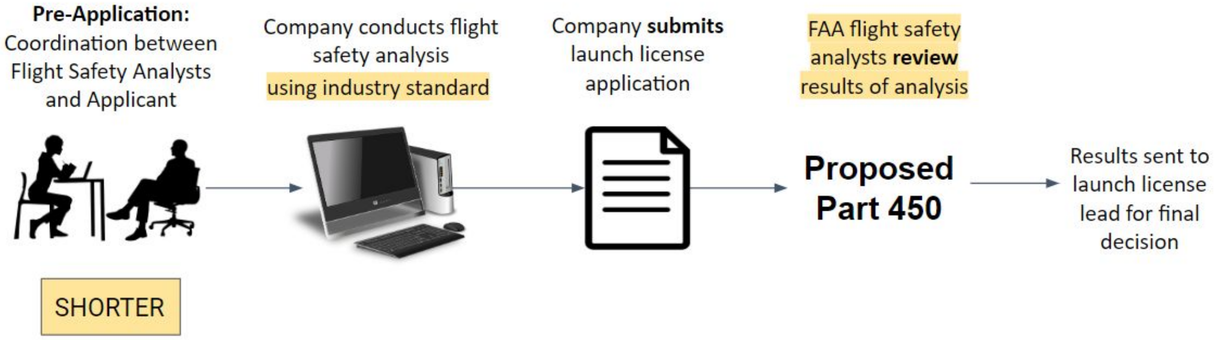
Pre-Application:
Coordination between Flight Safety Analysts and Applicant
Company conducts flight safety analysis using industry standard
Company submits launch license application
FAA flight safety analysts review results of analysis
Proposed Part 450
Results sent to launch license lead for final decision
SHORTER

Figure B3: FAA flight safety analysis workflow following implementation of proposed solution.

Appendix C: Implementation Schedule

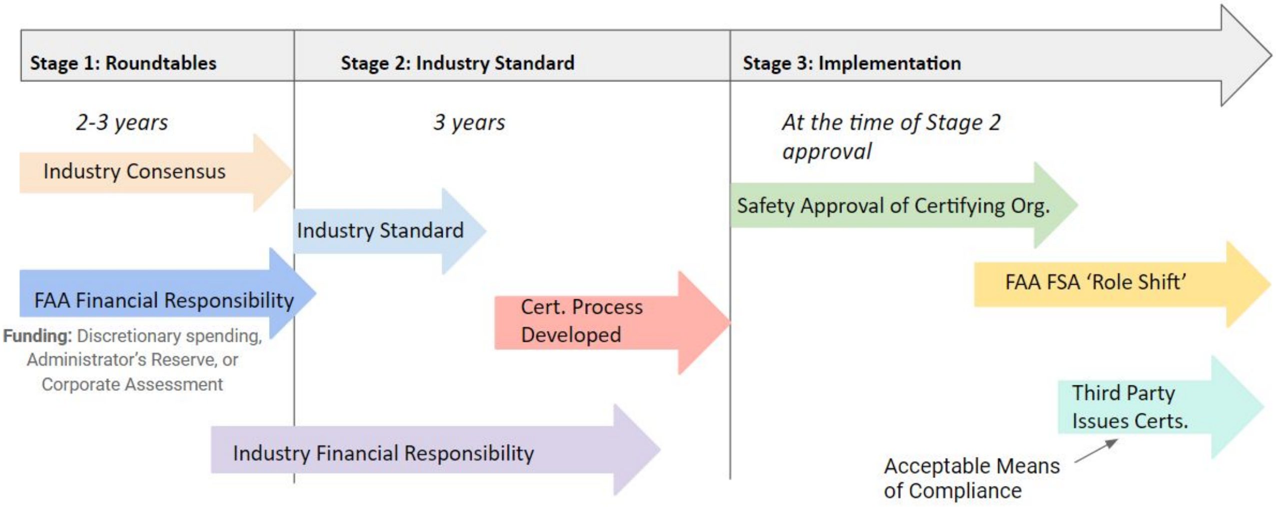
Stage 1: Roundtables
Stage 2: Industry Standard
Stage 3: Implementation
2-3 years
3 years
At the time of Stage 2 approval
Industry Consensus
Industry Standard
FAA Financial Responsibility
Funding: Discretionary spending, Administrator's Reserve, or Corporate Assessment
Cert. Process Developed
Industry Financial Responsibility
Safety Approval of Certifying Org.
FAA FSA 'Role Shift'
Third Party Issues Certs.
Acceptable Means of Compliance

Figure C1: Schedule to develop industry standard and implement safety approval of certifying body.