AEROSPACE REPORT NO.
ATR-2022-02101

Commercial Human Spaceflight Safety Regulatory Framework

September 28, 2022

Josef S. Koller[1], Samira Patel[1], Angie Bukley[2], Stephanie E. Barr[3], Lee D. Graham[4], Robert W. Seibold[5], Catrina A. Melograna[6]

[1]Policy and Regulatory Support, Center for Space Policy and Strategy
[2]Center for Space Policy and Strategy, Defense Systems Operations
[3]JSC Engineering and Safety Department, EVA Programs and JSC Engineering Subdivision
[4]KSC Programs Department, MSFC/KSC Programs Subdivision
[5]Commercial Launch Projects Department, Civil and Commercial Launch Projects Subdivision
[6]Civil Aerospace Operations, Federal and Commercial Programs Directorate

and

Paul A. Masson, StarNet, LLC

Prepared for:

Office of Commercial Space Transportation (AST)
Federal Aviation Administration (FAA)
U.S. Department of Transportation
800 Independence Avenue SW (AST)
Washington, DC 20591

Contract No. 693KA9-20-T-00004

Authorized by: Civil Systems Group

Abstract

This report presents a recommended framework for commercial human spaceflight safety based on an analysis of other transportation sectors, identification of common safety components, and a roadmap that leads to an ideal future where human spaceflight is a common practice. This takes into consideration current and future commercial activities regardless of the development status of individual spaceflight companies. The developed safety framework is flexible in order to recognize new developments, new transportation mechanisms, and new spaceflight destinations as they emerge.

Through case studies of other transportation sectors, we identified three themes or common components in all effective safety frameworks, regardless of the individual structure or maturity level of a particular sector:

1. People
2. Safety Culture
3. Data Collection and Analytics

The report describes activities promoting these three common components and provides additional aspects for an effective and comprehensive safety framework, including a safety management system, safety case approaches, and other long-term considerations. The report concludes with a roadmap and a recommended timeline for implementation.

Contents

Figures

Tables

1. Executive Summary

To develop a comprehensive and future-proof safety framework for commercial human spaceflight, we analyzed case studies and interviewed stakeholders from several other transportation and leisure sectors with strong safety interests in their passengers and participants. While recognizing that human spaceflight is unique, these case studies have some elements that are relevant and similar to commercial human spaceflight safety. Analysis of the case studies showed emerging common themes that are applicable to commercial human spaceflight safety. We identified that an effective safety framework for commercial human spaceflight likely includes several building blocks that can be implemented on varying time scales depending on the maturity level of the industry.

We identified that all sectors have three themes or common components in their safety framework, regardless of the individual structure or maturity level of a particular sector:

1. People
2. Safety Culture
3. Data Collection and Analytics

The most fundamental common element of any safety framework is (1) people. As human beings, we need to recognize that mistakes will be made. People are always involved throughout the design process or operations, and nobody is infallible. While risks can be mitigated through engineering and technology, there is always a human component and potential for unanticipated hazards. People can recognize such hazards and mistakes, and need to feel empowered to speak up. That is where a positive (2) safety culture comes into play. A positive safety culture allows for people to make mistakes, and for companies to learn from such mistakes and mitigate them as the nascent industry develops and evolves. A positive safety culture allows people to report the issue without fear of punishment or retribution, recognizing that safety is a key concern and requires cooperation and communication across all stakeholders, internally and externally, between regulators and commercial operators. The third component involves (3) data collection and analytics. Without collecting data on hazards, risks, materials, and processes, and the subsequent analyses, any reaction to mishaps or accidents will be retroactive. However, economic damage will already have been done, affecting the entire industry. The paradigm of "failing early and often" still applies, and learning from failures becomes increasingly important before humans are put at risk. To be proactive and even predictive, data needs to be collected and analyzed in a systematic way.

Additional components of a safety framework certainly should include industry consensus standards, best practices, and regulation (as appropriate). Further, methods like safety case approaches, audits, inspections, compliance monitoring, safety management systems, certifications, licensing, accident investigations, and even international agreements should be considered on a timeline that is appropriate to the state of the industry.

To develop a commercial human spaceflight safety framework that recognizes the transition from now to a future where human spaceflight is a common practice, it must be developed into something that is future proof. This means the implementation of the recommended safety components should follow a roadmap that takes into consideration current and future commercial activities, regardless of the development status of individual spaceflight companies. The framework should also be flexible enough to recognize new developments as they emerge.

Our approach to developing the safety framework was to imagine a most optimal future of commercial spaceflight. We asked what space travel would look like from a safety and regulatory perspective, and what the framework enables. Choosing an arbitrary time of 50 years in the future, far enough to create a separation from current trends, we imagined commercial human space travel covering a much broader domain than today, including orbital, cislunar, and even interplanetary destinations.

We concluded that the future of human spaceflight is dynamic and evolving, and the safety framework should reflect that. It should evolve with the needs of the specific times, drawing on best practices from other sectors. While spaceflight risks will never be completely extinguished to zero, and space is inherently risky, such risks should be mitigated and addressed proactively. The safety framework should account for risk management practices that recognize the shifting nature of this sector, and with it, an evolving set of risks.

In summary, our recommendations include a variety of safety components that can be implemented on different timescales. Because some safety components could be implemented even before an expiration of the learning period, our recommendations are divided into near-, mid-, and far-term initiatives. This approach strongly considers the current status of the industry and, while making small steps toward a comprehensive safety framework, our framework implements regulatory safety activities in small but sensible steps to limit any impedance to this nascent and developing industry.

Summary Recommendations on "People and Safety Culture"

- Implement a scalable safety management system requirement that builds on the existing System Safety Program, Advisory Circular (AC) 450.103-1.
- Establish memoranda of understanding (MOUs) with individual spaceflight providers on data sharing, data protection, and nonretribution.
- Affirm FAA Compliance Philosophy, Order 8000.373, to include space more prominently.
- Promote a positive and just safety culture with activities such as non-attribution safety workshops.

Summary Recommendations on "Data Collection and Analysis"

- Develop a system to collect safety-related data, enabling technical analyses on hazards and risk mitigations.
- Develop a program to share safety-related data, as appropriate, among industry and FAA.
- Update and improve FAA Compliance Philosophy to cover commercial space transportation deliberately.

Summary of Recommendations on "Hazards and Risk Mitigations"

- Implement industry consensus standards, together with audit and enforcement mechanisms, through recommended practices, advisory circulars, and, as appropriate, regulation.
- Establish a safety case approach, together with independent review functions.

Summary of Recommendations on "Policy and Strategy"

- Establish a whole-of-government strategy for in-space astronaut rescue.
- Obtain a "selective" on-orbit authority, specific to commercial human spaceflight safety, to establish the whole chain of custody during all phases of flight.
- Lead international discussion to promote standards and best practices to commercial human spaceflight safety.

The following sections describe the details on how the safety framework was developed, its components, and a roadmap for implementation.

2. Approach to Developing a Safety Framework

2.1 Assumptions

The goal of a human spaceflight safety framework is to promote commercial human spaceflight by providing an industry-driven and predictable regulatory environment. To develop a safety framework, we identified the following list of assumptions for an ideal future of commercial human spaceflight:

1. Commercial human spaceflight (cHSF) is growing.

2. The regulatory learning period will expire at some point, as soon as October 1, 2023.

3. Space is inherently risky and accidents will happen. However, risk can be lowered to an acceptable level through technology and engineering solutions.

4. Spaceflight will go beyond suborbital and include a variety of destinations. Hazards exists along all phases of flight, regardless of regulatory authorities.

5. New missions will include commercial space walks (extravehicular activity, or EVA), cislunar destinations, and space habitats.

6. Human spaceflight launch will develop into different types, dubbed as a "launch triad," including horizontal, vertical, and balloon-type launches. See Table 1 and note that launch technology, effectiveness, and cost will define the suitability of HSF destinations. Table 1 is notional.

7. Various larger, medium, and smaller companies compete for cHSF customers, with diverse levels of safety expertise.

The success of a safety framework depends upon an understanding of what the future of cHSF might be. Setting a list of assumptions upfront will enable a proactive approach to safety.

Table 1. Various Launch Methods Supporting Different Destinations for cHSF with a Notional Assessment

	Point to Point	Suborbital	LEO	GEO	Cislunar	Interplanetary
Vertical Launch	Yes (likely)	Yes (Blue Origin)	Yes (SpaceX)	Yes (likely soon)	Yes (likely soon)	Yes (longer-term goal)
Horizontal Launch	Yes (possible)	Yes (Virgin Galactic)	Not in the near term	No	No	No
High-altitude Balloons	No	Yes (in development)	No	No	No	No

LEO = Low Earth orbit, GEO = Geosynchronous Earth orbit

2.2 A Future-Back Approach for Principles of a Safety Framework

Our approach to developing the safety framework was to imagine a most optimal future of commercial spaceflight. This is known as a future-back approach, mapping out steps and components of a framework with the destination in mind. Throughout, we asked ourselves what space travel would look like from a safety and regulatory perspective, and what the framework would enable. Choosing an arbitrary time of 50 years in the future, far enough to create a separation from current trends, we imagined commercial human space travel covering a much broader domain operating in the following environment:

- Commercial space travel has developed beyond suborbital and orbital and includes point-to-point transportation, geosynchronous, cislunar and (perhaps) even interplanetary.

- A few larger companies dominate with smaller companies filling niche demands.

- Human commercial spaceflight includes transportation, exploration, and leisure/adventure.

- Spaceflight has grown beyond the national domain of the U.S. and includes international partners and destinations.

- Human spaceflight safety is viewed as proactive, collaborative, and engrained into the culture of all stakeholders.

The future of human spaceflight is dynamic and evolving, and the safety framework should reflect that. It should evolve with the needs of the specific times, drawing on best practices from other sectors. While spaceflight risks will never be completely eliminated, and space is inherently risky, such risks should be mitigated and addressed proactively as opposed to reactively. The safety framework should account for risk management practices that recognize the shifting nature of this sector, and with it an evolving set of risks.

Based on the future "destination" or the envisioned most optimal environment, we developed five fundamental principles that guide the evolution of a space safety framework. The safety framework should exhibit the following characteristics:

1. **Adaptive and evolutionary.** Technologies and safety aspects change through continuous innovation. As such, a framework should be able to evolve and adapt to various transportation and launch methods. It should also be adaptive to the various maturities of individual operators and companies.

2. **Innovation permissible.** A safety framework should encourage innovation and be open to new approaches to accomplish safety goals.

3. **Comprehensive.** A framework should consider all system risks and not ignore risks absent of regulatory authorities; hazards exist along all phases of flight. However, it should be flexible enough to address the range of risk factors appropriately.

4. **Quantifiable and technically informed.** Identified hazards and associated risks should be assessed in a quantifiable manner, which calls for consistent data collection and analyses. Similarly, best practices, voluntary consensus standards, and regulations need to be technically informed and based on quantifiable data.

5. **Collaborative and transparent.** Safety is a shared interest of all stakeholders. Approaches and solutions to safety issues should be shared as broadly as possible.

These five fundamental principles can guide the development of a safety framework that enables the envisioned future of a safety framework. Each regulatory activity should be assessed against these five principles.

3. Case Studies

3.1 Introduction

This section summarizes our findings from case studies across various transportation and leisure sectors. Details of the case studies are described in Appendix D. The case studies may help guide the future of cHSF safety in a positive direction, drawing from their success stories and seeing how they address safety challenges and risks that also apply to cHSF. We identified various commonalities and major differences, concluding that unique transportation sectors likely need different safety framework solutions.

Table 2. An Overview of the Case Studies in Comparison to Space Tourism/cHSF

	Operations	Reason	Danger to Uninvolved 3rd parties	Reporting System	Level of Regulation	International Coordination	Unique Vehicles or Mass Produced
Commercial Human Spaceflight	Controlled by operator	Adventure, leisure, research	During launch and reentry	N/A	N/A, emerging market	No	Unique
Cars	Self-operated	Transportation	Continuous	FARS; states	Highly regulated; state level	Yes	Mass produced
Autonomous Vehicles	AI controlled	Transportation	Continuous	Voluntary self-reporting	N/A, emerging market	Not yet	Mass produced
Cruise Ships	Controlled by operator	Leisure	In harbor	IMO, DOT, and more	Highly regulated	Yes	Unique to operator, but with standards
Commercial Aviation	Controlled by operator	Transportation	During takeoff and landing	ASRS, ASIAS, ASAP	Highly regulated	Yes	Mass produced
Commercial Submarines	Controlled by operator	Research/ Leisure	Continuous	SUBSAFE/US Navy	Small market, but regulated	For search and rescue	Unique

Our case study research included cars, autonomous vehicles, cruise ships, commercial aviation, and commercial submarines. Cruise ships and commercial aviation have long-established safety traditions and correspondingly lower risks. While autonomous vehicles represent a new market entrant, similar to cHSF, they can serve as a useful model for sectors with a strong safety culture. Table 2 provides an overview of the differences and similarities with commercial human spaceflight.

The findings include a separation of key elements for each transportation model, such as method of operations, production, reason for undertaking the activity, risk and reporting, and levels of regulation and coordination. Comparisons are made for each case study with the current model for space tourism. While no case study is identical to cHSF, they all highlight different aspects that are comparable. They all share unique insights that can be applied to cHSF. The most important takeaway from the analysis of these case studies is that all have some common factors including (1) people, (2) safety culture, and (3) data and analytics[1].

Additionally, we examined government spaceflight missions to provide space-specific models for comparison, investigating the National Aeronautics and Space Administration (NASA) Challenger and Columbia accidents, and surveying current NASA crew and suborbital crew safety standards.

[1] Details of our findings for each case study are described in Appendix D.

4. Safety Framework

4.1 Introduction

Based on our analysis of other transportation sectors and their approaches to safety, we identified several key building blocks that contribute to a safety framework. Considering the unique aspects of each sector, we determined which building blocks of the safety framework stood out, which ones might be applicable to a cHSF safety framework in the near term or far term, and which ones might not be as applicable. We conducted several interviews with industry stakeholders and subsequently concluded that people, a positive safety culture, and data/analytics are key factors spanning across all sectors.

The following sections describe each building block for a cHSF safety framework in detail, including a roadmap with recommendations at the end.

4.2 Building Blocks for Spaceflight Safety

As various transportation sectors have evolved, each of them being distinct and unique, all experienced catastrophic accidents and failures that led to the deaths of many people. Starting out in a nonregulatory environment, those accidents were often the reason for oversight, regulations, and even treaties to protect the lives of passengers and the uninvolved general public. All safety frameworks have evolved, none are static. Looking at the history and evolution of each safety framework, we identified several building blocks. Some of them unique, some of them common across all sectors.

There is one key takeaway from our analysis: *There is no single silver bullet to accomplish safety*. There are many components that contribute to safety. Not all of them are necessary, none are mutually exclusive. Some might be premature, some could be seen as overdue. Some components include a top-down, regulatory aspect, some leave more decisions to the entities that perform the activity. However, all of them contribute and strengthen a safety framework.

In addition, our findings show that accomplishing safety is an evolutionary and iterative process. None were born and perfect from the beginning. However, throughout the evolution and development, regardless of the sector, all safety frameworks have a critical common denominator: (1) **people**. People are the ones who make mistakes, not machines. Equipment failures are not just caused by, for example, materials fatigue, but by people who selected those materials and designed the equipment. Nobody is infallible and people will always make mistakes. That is an unavoidable fact. However, it is up the organizations with an appropriate safety framework to catch those mistakes and prevent the accumulation of mistakes from leading to disaster.

People can recognize hazards and mistakes, and need to feel empowered to speak up. That is where a positive (2) **safety culture** comes into play. A positive safety culture allows for people to make mistakes and learn from them. It is vital to recognize that safety is a key concern and requires cooperation and communication across various stakeholders, especially between regulators and commercial operators.

We identified a third major component across all transportation sectors: (3) **data and analytics**. Without collecting data on hazards, risks, materials, and processes, and analysis, any reaction to mishaps or accidents will be retroactive. However, it might be too late at that point as the paradigm of “failing early and often” does not apply when human lives are at risk. To be proactive and even predictive, data needs to be collected and analyzed in a systematic way.

The following is a comprehensive list of safety components that we were able to identify across all case studies. The list is also loosely ranked by our perceived importance and value for addressing and building

cHSF. In particular, safety culture appears in all transportation sectors and is often described as the key factor for safety.

Building blocks for a safety framework (see Figure 1):

- Positive safety culture
- Safety management systems
- Audits, inspections, and verifications
- Accident investigations
- Safety case approach
- Best practices and standards
- Data collection systems
- Regulatory incentives
- Flight training and health
- Third-party incentives
- Certifications and licensing
- International agreements and treaties

Figure 1. A framework with several components strengthens the safety environment.

Out of all the transportation sectors we analyzed, we identified safety culture as a common element. Often, companies rely on using a safety management system (SMS) to establish a positive and just safety culture as a way and means of promoting safety culture. Some SMS implementations are required by regulators (e.g., commercial aviation), other sectors recognized the value of an SMS implementation internally and use SMSes fully voluntarily (e.g., autonomous vehicles). We will discuss the details of an SMS in a following subsection.

Additional common safety framework components are listed in Table 3 below.

Table 3. Common Safety Framework Components

	International Agreements or Treaties	SMS	Data Collection	Inspections, Audits	Accident Investigations	Safety Case	Certificates and Licenses
Commercial Aviation	ICAO	Yes	ASAP, ASRS, ASIAS	Yes	NTSB	No	Yes
Cruise Ships	SOLIS	Yes	Noncentralized	Yes	Coast Guard	No	Yes
Autonomous Vehicles	Mostly state controlled	Yes	Voluntary Self-Reporting	No	DOT	Yes, voluntary	Pilot licensing programs in some countries

4.3 Promoting a Positive Safety Culture

As discussed above, safety should be addressed as a cultural topic and, as such, promoted as a core value. Recognizing that people are the common denominator across all transportation sectors, two important aspects need to be taken into consideration: (1) people will always make mistakes, and (2) no single regulation can guarantee safety. This leads to the conclusion that safety culture remains one of the core aspects of any safety framework and a key component to any holistic and comprehensive approach.

Our interviews across several transportation sectors confirmed that conclusion. Stakeholders emphasized that a strong safety culture is not only a responsibility, but also a necessity. It empowers employees to speak up and motivates them to make safety part of everything they do. In addition, promoting a positive safety culture is also forward looking and provides the **opportunity to catch mistakes and failure modes before they occur and lead to a disaster(s).**

Regulators are part of the culture equation and can promote a positive safety culture, create industry buy-in, and implement nonpunitive measures. For example, FAA Compliance Philosophy, Order 8000-373, created such fertile ground for industry buy-in. In particular, the commercial aviation sector attributed the change in mindset at the FAA in the late 1990s and early 2000s to the tremendous safety track record in the commercial aviation sector in the United States.

Culture is an integral part of an SMS and is used in other industries as well. It has been very successful in commercial aviation and is currently being expanded to airport management, rotorcraft, and others. The commercial aviation sector is not alone. In addition, the Automated Vehicle Safety Consortium promotes SMS to support organizational safety in a systematic and integrated way and Underwriters Laboratories details the importance of safety culture across industries in their messages as well. It is also used for cruise ship safety operations.

4.3.1 What is Safety Culture?

Safety culture is a set of boundaries for acceptable behavior provided for decision making. It is generated from the top down and rarely developed out of a grassroots initiative. In general, safety culture is a fusion of the following desirable behaviors within an organization:

1. **Informed culture.** People are knowledgeable about human, technical, organizational, and environmental factors.

2. **Flexible culture.** People can adapt flatter organizational processes when facing imminent danger and risk.

3. **Reporting culture.** People are prepared to report their errors and experiences.

4. **Learning culture.** People have willingness to learn and implement reforms.

5. **Just culture.** People are encouraged and rewarded for providing essential safety-related information and decisions are made fairly.

Part of promoting a strong safety culture from a regulatory perspective should also include regular assessments, such as the Safety Culture Maturity Model® [1]. It can be used to evaluate maturity level and plans of reaching the next level of safety culture within particular organizations. Figure 2 illustrates the interconnected components of safety culture, which include ownership, recognition, leadership, rules and procedures, values, communication, and self-verification.

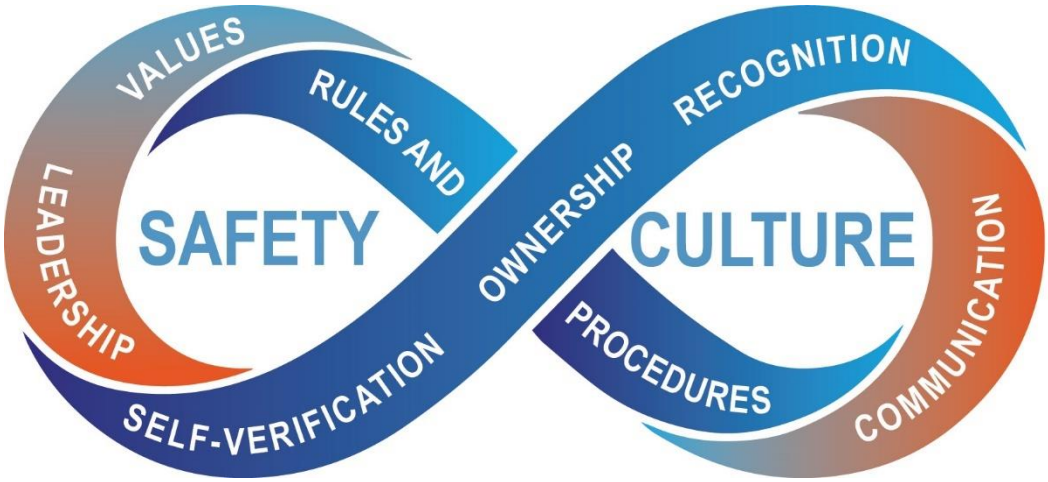

Figure 2. Interconnected components of a safety culture.

Aspects of a positive and strong safety culture include strong top-down, leadership support for all safety aspects over other motivating factors. Senior leadership must set the stage, both verbally and documented in written form, and provide the resources, actions, and management to address safety concerns. Senior management thereby establishes safety as a core value and acknowledges the high-risk and high-consequence nature of their activities. Organizations maintain a healthy sense of vulnerability that way.

Once senior leadership establishes the general tone of a positive safety culture, it must show that trust can permeate throughout the organization as an essential ingredient in a positive safety culture. In addition, hazards and safety risks are proactively sought out and there is not a sense of negativity and repercussions for calling a stop of work and review. Everyone in the organization must be vigilant, predisposed, and trained to recognize and respond to hazards, as safety is a shared responsibility. Furthermore, organizations need to establish high standards and expectations of safety performance.

While a positive safety culture must be implemented internally, based on the organizational structure of each company, it can also be promoted externally and encouraged by the regulators. For example, to establish a *collaborative* safety culture, it is critically important for the regulator to shift the mindset toward a nonpunitive approach, similar to as it occurred for commercial aviation oversight. For example, SMS is, by its very nature, built upon nonpunitive measures (such as retraining rather than threatening to pull a license) and collaboration between regulators and operators. More details are provided in the following subsections and Appendix E.

The most effective safety cultures do not view safety as a competition for success, but rather see it as a key component like all other systems in spaceflight. **Regulators have not only the authority, but the responsibility to promote a positive safety culture as there is an inextricable tie between strong safety culture and accident prevention.** There are several recommendations and examples of how regulators can promote a strong safety culture in commercial human spaceflight safety, even before the learning period ends. These examples and initiatives stem from other modes of transportation and include the following:

- Implementing a safety management system requirement on commercial spaceflight companies. Our research suggests that domestic spaceflight companies working with NASA may already have SMS implement in some form per NASA requirement [2].

- Sponsoring safety information exchanges that could be modeled after InfoShare, which is a successful venue for commercial aviation to share safety information in a noncompeting and nonthreatening environment.

- Holding safety-related workshops with industry to educate, communicate, and collaborate across all stakeholders.

- Developing common understanding between regulators and operators and implement a memorandum of understanding (MOU) between the FAA and each commercial spaceflight operator to promote sharing while providing a level of protection from enforcement, disclosures, and Freedom of Information Act requests.

- Issuing human spaceflight safety awards and recognition for a positive safety culture.

- Assessing the maturity level of corporate safety culture on a regular basis.

A subset of these initiatives could be pursued even before the regulatory learning period ends, perhaps setting the stage for how the regulators will approach human spaceflight safety in a collaborative way. We also believe that the regulator could develop a requirement for companies to implement an effective safety management system. Pending a thorough legal review, an SMS implementation requirement would not directly regulate the safety of spaceflight participants themselves, but rather direct companies to implement SMSes suitable to their organizational structures and missions. How an SMS is implemented could be left to the company's discretion. Because the Secretary of Transportation may issue regulations governing the design or operation of a launch vehicle to protect the health and safety of crew, government astronaut, and spaceflight participants (51 U.S. Code 50905), an argument could be made that implementing an SMS recommendation or requirement falls within the Secretary's authority even before the learning period ends. The learning period pertains to "restricting or prohibiting design features or operating practices" that have resulted in serious or fatal injury. Requiring a safety management system, with the specifics at the discretion of the commercial operator, would benefit crew, government astronauts, and spaceflight participants alike, without specifically regulating their safety. A definitive legal review would likely provide additional details.

4.4 Safety Management Systems

A safety management system (SMS) is an organization-wide, comprehensive, and preventative approach to managing safety. An SMS includes a safety policy, formal methods for identifying hazards and mitigating risk, and promotion of a positive safety culture. Most importantly, an SMS is intended to be designed and developed by the employees of each company and should be integrated into existing operations and business decision-making processes.

Successful SMS implementation is not limited only to commercial aviation, but also includes various other industries. such as autonomous vehicles, cruise ships, chemical, oil, construction, occupational health, food, highway, electrical, and fire protection, among others. It is also used internationally, adopted and promoted by the International Civil Aviation Organization (ICAO) through the SMS standards as published in ICAO Annex 19 for operations covered under Annex 6 Part I. Another example includes the safety of ships at sea through the International Safety Management (ISM) Code that is similarly based on SMS.

To highlight a domestic example that is not aviation related, we studied the autonomous vehicle industry; in particular, Aurora Technologies (Aurora), which acquired the Uber self-driving unit, implemented a voluntary SMS with the goal to "operate with integrity and uphold values by committing to safety culture." According to Aurora, their SMS implementation gives teams the tools to speak up about safety concerns; the resources to support understanding and mitigating them; and to collectively make the best and most informed decisions on how to manage risks. Aurora has implemented policies such as:

- **Universal Grounding Policy.** Any Aurora employee, from vehicle operators to software engineers to the business development team, can request halting operations of autonomous vehicles in the fleet for safety concerns.

- **Safety Concern Reporting.** The team is encouraged to submit safety concerns through a fast-response management system, which elevates potential issues to relevant teams and executives to ensure that they are quickly addressed, and the learnings are documented.

- **Safety Case Framework.** Teams across Aurora, from People Operations to Hardware, are tasked with helping complete a safety case—providing evidence that proves their self-driving vehicles are acceptably safe to operate on public roads.

Safety management systems evolved from the combination of system safety concepts that themselves evolved from the 1960s, combined with concepts of management systems, first in the form of quality management systems and then into occupation health and safety management systems, environmental management systems, and others. Current SMS concepts stress a process approach similar to those in ISO-9000 [3].

In the past, aviation safety improvement was characterized by a fly-crash-fix-fly approach. Airplanes would fly, have an occasional unfortunate crash, and authorities would investigate the cause of the accident, often attributed to pilot error. The solution was to regulate such that operators would not make the same mistake again. This was a very reactionary approach at the expense of people's lives.

Today, we realize that it is much more successful to engineer systems, to the extent possible, to remove failure modes. There are many components to this engineering effort, including hazard identification, risk management, systems theory, human factors engineering, organizational culture, quality engineering and management, quantitative methods, and decision theory.

The FAA began looking at system safety in the late 1990s. For system safety to truly work, it must be practiced by the system/process owner and operator. This led the FAA, in 2003, to further look into SMS, publishing its first air operator SMS guidance in June 2006, AC 120-92, "Introduction to Safety Management Systems for Air Operators." The FAA published the final SMS rule for air carriers in January 2015.

Today, regulatory authorities (not just the FAA), safety experts, and industry leaders believe that SMSes represent the future of safety management in most sectors [4]. SMSes provide organizations with a powerful framework for safety philosophy, tools, and methodologies that improves their ability to understand, construct, and manage proactive safety systems.

Any SMS has four main pillars, listed below, all of which must coexist and be executed concurrently to ensure effectiveness.

1. **Safety policy.** Implement policies and procedures to explicitly describe responsibility, authority, accountability, and expectations. Safety must be a core value for the organization with top management involvement.

2. **Safety risk management (SRM).** Implement a formal system of risk identification and management to control the risk to an acceptable level; then methodically identify hazards, assess risk, and exercise control to mitigate that risk.

3. **Safety assurance (SA).** Once policies, processes, measurements, assessments, and controls are in place, the organization needs to incorporate continuous monitoring, measurement, and data acquisition to assure the system can adapt. Audits, investigations of safety-related events, monitoring of key process indicators, and employee reporting systems can inform regular safety reviews and provide continuous improvements.

4. **Safety promotion.** The organization must continuously promote safety as a core value with practices that support a sound safety culture, including training, communication, and awareness.

An SMS does not need to be large, complex, or expensive to add value. It must be adaptable and flexible to grow. If companies have active involvement of the operational leaders, maintain open lines of communication up and down the organization and among peers, stay vigilant in looking for new issues, and ensure that employees know that safety is an essential part of their job performance, companies will have an effective SMS that helps them make better safety management decisions [See FAA AC 120-92B]. Additional details are provided in 0.

This report recommends using a foundation based on FAA AC 120-92B, which requires air carriers to implement an SMS, combined with the available building blocks of SMSes within AC 450.103-1, "System Safety Program," to implement a comprehensive SMS requirement while leaving the design specifics at the discretion of the companies.

Regulators have the opportunity and responsibility to promote, collaborate, and support the industry through SMS implementations. This could be accomplished through examples such as:

- Creating an FAA Office of Commercial Space Transportation (AST) pilot project for SMS
- Implementing an SMS team at AST
- Organizing workshops to guide SMS implementation
- Performing SMS reviews with recommendations

These activities will not require a change in regulatory authority and could potentially be initiated before the learning period expires. They can be implemented proactively and are poised to shape the approach to safety in the commercial spaceflight industry for years. They are also independent of the mode of transportation (horizontal, vertical, or balloon launch), destination (low Earth orbit, or LEO; geosynchronous Earth orbit, or GEO; cislunar; or interplanetary), and spaceflight participants, crew, or government astronauts.

4.5 Reactive, Proactive, and Predictive Safety

An effective safety framework consists of several components, each of them addressing accidents, mishaps, and failures in a different way. Some components are *reactive* to accidents (such as accident investigations), some are *proactive* and try to capture potential failures before they happen. One step

further is safety implementation that is based on technical data analysis, modeling, data mining, and probabilistic assessments to predict future safety issues.

Reactive safety is a common methodology and used in all transportation sectors. Accidents will happen, they can be studied, analyzed, and learned from. Sometimes they will lead to best practices, standards, regulation, and even treaties (e.g., Titanic accident), but not always. They can also be disregarded as a black-swan event that will likely never happen again; however, public pressure will often require something to provide assurance of the safe operations. While relatively easy to implement, reactive safety, such as event analysis or accident investigations, is retroactive, meaning that people may have already been hurt or even perished. Reactive safety includes the descriptive inferential analysis after the accident, deducing the reasoning based on details and data from past events, and determining contributing factors and risk findings.

Proactive safety, on the other hand, is about inferring future issues, mishaps, and accidents based on information analysis by attempting to infer the future from present observations. Proactive safety requires a different skillset, including statistical tools for analysis and scientific inquiry. It relies heavily on data through voluntary or mandatory reporting systems, safety audits, and surveys. In the commercial aviation sector, the Aviation Safety Action Program (ASAP) is described as one of the most successful voluntary programs in commercial aviation in the United States.

Examples of proactive airline safety programs include the following.

- Aviation Safety Action Program (ASAP)
- Advanced Qualification Program (AQP)
- Air Transportation Oversight System (ATOS)
- Flight Operational Quality Assurance (FOQA)
- Internal Evaluation Program (IEP)
- Line Operations Safety Assessment (LOSA)
- Voluntary Disclosure Reporting Program (VDRP)

Predictive safety goes even further. Predictive safety relies even more on comprehensive and accurate data collection with *quantitative* monitoring. It involves higher levels of analysis using increasingly sophisticated tools and methods such as modeling, probabilistic risk assessment and data mining. While reactive and proactive safety approaches often rely on qualitative measures, predictive safety requires quantitative data, offering great advancements and opportunity. However, because predictive safety is not achievable without quantitative data, it is often limited to specific subsystems and components with characteristics that are measurable.

The use of qualitative and quantitative hazard and risks analysis ranges across systems and operators. Examples of *qualitative* human spaceflight safety include:

- NASA Space Shuttle Program
- Space Station Freedom Program
- International Space Station (ISS) Program
- Commercial Crew Program

Examples of *quantitative* human spaceflight safety studies include:

- Quantitative human rating methodology for NASA Chief Engineer

- Japan Aerospace Exploration Agency (JAXA) study on analytical approach for human spaceflight safety

Examples of safety components on a reactive, proactive, and predictive scale, ranging from qualitative to quantitative methods, are shown in Figure 3.

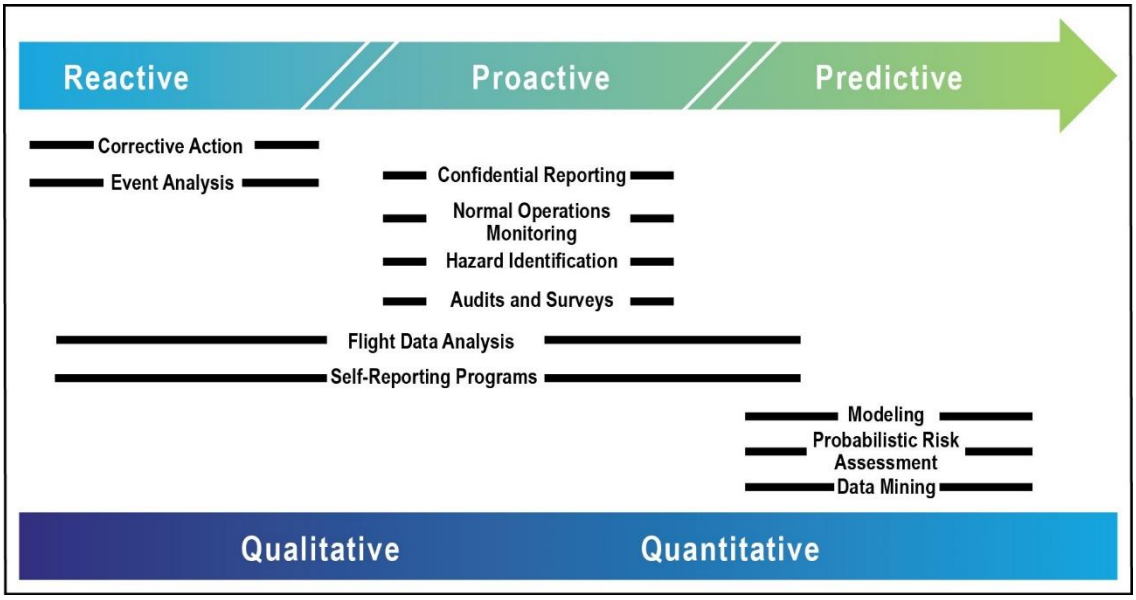

Figure 3. Illustration of the progression from reactive to predictive safety. (adopted from [3])

In summary, our analysis showed that data is needed for both quantitative and qualitative safety studies for human spaceflight, but quantitative analysis cannot be done without data. There are few existing commercial spaceflight vendors who record necessary test and operational data to support a truly quantitative analysis.

To facilitate a long-term and future implementation of risk analysis, we recommend developing a roadmap to identify areas ready for transition from qualitative analyses to more quantitative methods from commercial operators. This would require taking into consideration the impact of new requirements on the industry, technical feasibility, cost, and a timeline driven by industry-wide flight experience.

4.6 Data Collection Systems

4.6.1 Introduction

Data collection plays a key role in understanding safety systems. Collecting data proactively, instead of post-accident during mishap investigation, may help identify hazards and appropriate mitigation measures before an accident occurs. Predictive modeling can also help identify issues that must be mitigated with standard implementation or regulations. As shown in Figure 4, the accumulation of mishap data can help determine when standards implementation or regulation is triggered. The threshold at which standards or regulation implementation occurs depends upon the severity of the mishap incident and its frequency over a period of time. As time moves forward, if standards alone do not limit the frequency or severity of mishap incidents, regulations may become necessary.

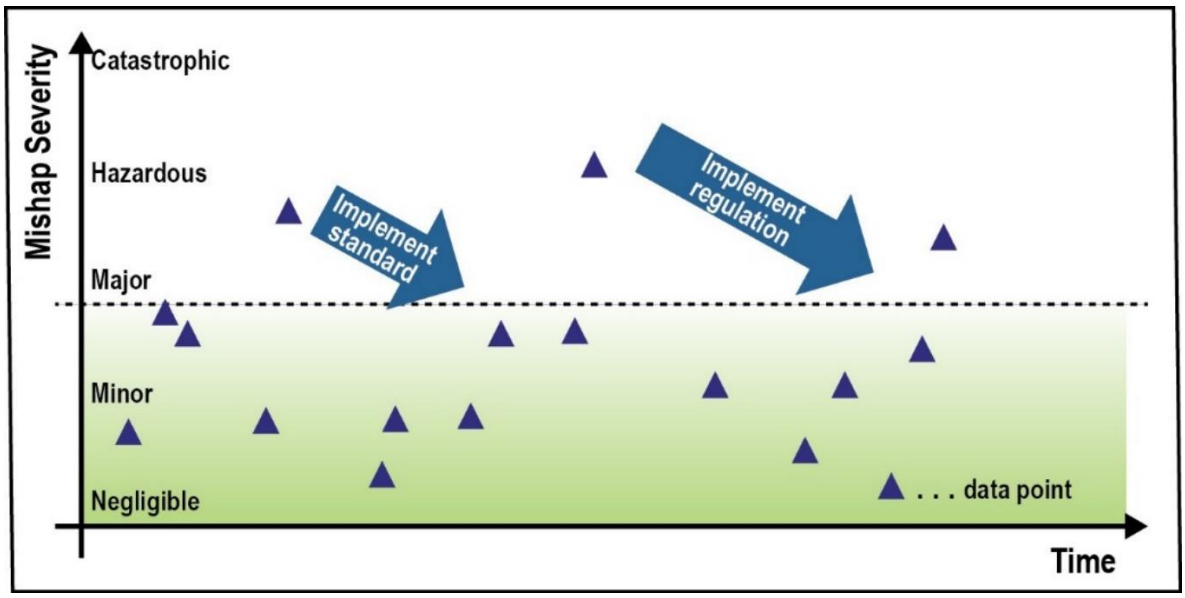

Figure 4. Thresholds for Regulation and Standards Implementations.

The following section analyzes the key components of a data collection system and how data collection reporting mechanisms enable an effective safety culture. This section also examines aviation reporting systems as a model for data collection efforts in human spaceflight safety. Tracking data is a key part of ensuring safety over time and learning from past mishaps.

4.6.2 Components of a Data Collection System

Based on analyses of data collected across various case studies (discussed in Appendix D), the most successful data collection systems include the following components:

1. **Data Sharing.** Data collection includes reporting systems that allow relevant stakeholders to notify each other and share information. Information sharing can be done through a variety of platforms, such as databases, alerts, conferences, newsletters, or reports. Information sharing can be responsive, which includes issuing alerts to relevant parties to prevent mishaps from occurring. It can also be investigative in nature and help determine root causes after incidents have already occurred. For example, the former can include alerts to pilots about weather prior to takeoff and the latter can include accident investigation reports.

2. **Repositories of Data.** Over time, data collection systems accumulate data from past mishaps and issues, as well as synthesize data across multiple sources. This helps to better analyze what the issues are and mishap patterns, and helps identify where corrections are needed. Part of the repository function is the ability to store all the data, and offer analytics and modeling capabilities to enable better insights and solutions.

3. **Building Trust.** Data collection systems may not always be accessible to the public; however, they must foster trust amongst relevant stakeholders and the public. This may be done through a variety of means. Some data reporting systems may make data available to the public and be managed by independent parties, such as data collected by the National Transportation Safety Board (NTSB). Transparency is useful when the mishap has broken trust with the public, the activity is so frequent or highly public, or the information is nonproprietary. At other times, building trust may require discretion between the government and relevant stakeholders, which may be the case when the information is highly proprietary or the primary stakeholders feel more comfortable sharing information in a safe, closed environment (e.g., InfoShare).

4. **Nonpunitive.** Part of fostering a safe environment for data collection and sharing may include a provision for a voluntary or anonymous process. For example, many aviation reporting systems allow for pilots and operators to report issues without fearing penalty, fostering open dialogue to solve issues.

These four key components of a data collection system promote a just and collaborative safety culture where stakeholders—operators and government officials—can have nonantagonistic dialogue to improve safety conditions. The goal is to build a constructive relationship based on transparency and collaboration to support the identification of safety hazards and system deficiencies in a timely manner, thus improving operator safety management systems and overall trends in safety.

4.6.3 Aviation Safety—A Data Collection Success Story

As described in the commercial aviation case study in Appendix D, passenger aviation has some of the lowest rates of mishap incidents of all transportation activities, in large part due to its comprehensive safety reporting systems. Aviation safety data systems have been held as the model industry standard by other sectors and include three main data collections programs [5]:

- Aviation Safety Reporting System (ASRS)
- Aviation Safety Action Program (ASAP)
- Aviation Safety Information Analysis and Sharing (ASIAS)

These interconnected systems work in concert with each other. For example, ASAP data gets rolled into the ASIAS system in which the data are then analyzed by an independent party (e.g., MITRE) and other data analysts to identify safety issues and trends. For more information on these three systems, see Table 4. The table shows which stakeholders use each of the systems and their purposes, as well as who has access to the data and how reporting is enforced. The table also shows how the key components of a data collections system, such as repository and data sharing functions, are integrated in these aviation safety systems.

Table 4. Three Aviation-Based Data Collection Systems

	ASRS	ASAP	ASIAS
Use	• NASA • Anonymous submission • Issue alerts on hazards/deficiencies	• MOU between FAA and operator • Investigate root cause • Augments operator SMS	• FAA • Safety repository for operators • IDs safety trends
Access	• Publicly available	Only program participants; prevents FOIA release	Program participants; some public access
Enforcement	• Report cannot be used against submitter • May receive violation	• Voluntary submission • Nonpunitive unless criminal or reckless	• Submissions are protected • Nonpunitive unless criminal or negligent

4.6.4 ASAP Enables Broad Data Sharing

Of the three programs, the Aviation Safety Action Program (ASAP) is described as, by far, the most successful *voluntary* data sharing program. At first, industry was greatly concerned that such reporting systems would lead to punitive actions and disclosure of proprietary information. However, today ASAP is a widely accepted program and embraced by flight crews, dispatchers, maintenance technicians, and flight attendants.

ASAP was originally pioneered by American Airlines in 1994. It is based on a voluntary MOU between airline operators and the FAA. It encourages airline employees to report possible violations, safety issues, and events to an ASAP review committee with representatives from each party. To encourage reporting, the FAA limits enforcement actions against employees covered by ASAP (within a certain time limit specified by MOU). The MOU covers genuine mistakes and inadvertent violations. The intentional disregard for safety that involves criminal activity or reckless behavior may still result in enforcement action.

To further foster data sharing, the FAA MOU also protects proprietary information from disclosure. In addition to the MOU, 14 CFR Part 193, "Protection of Voluntarily Submitted Information," addresses the initial industry concerns of information disclosure and fear of punitive action.

Finally, for many major airline operators, the ASAP system has been fully integrated into company safety processes; for example, through internal monthly company meetings, which include a holistic and systematic approach for reviewing ASAP data. The airline community also presents results of studies and shares mishaps and other errors at an annual InfoShare conference. These conferences provide a nonthreatening and closed environment that offers a learning opportunity to the aviation community at large (operators, manufacturers, government, pilots, and other aviation personnel) without access from the general public or press.

4.6.5 Conclusion on Data Collection

While aviation is a long-standing sector with decades of mishap data and mature data collection systems in place, it is a critical model for emerging transportation sectors. Sufficient mishap data to build comprehensive assessments might come later in the process, but building the cornerstones of data sharing, collaboration, and constructive learning from mistakes will enable better relationships between stakeholders and ultimately better safety culture. Positive safety systems can exist while addressing industry reservations about mishap repercussions and information disclosure.

4.7 Safety Case Method

4.7.1 Introduction to the Safety Case Method

A safety case is a structured, iterative process that was developed to provide a flexible safety review approach for hazardous systems, culminating in a safety case report. It was initially developed from lessons learned in the review of the United Kingdom 1988 North Sea offshore oil and gas design and operations of the Piper Alpha oil platform disaster. Recognizing the benefits that a safety case provides, the safety case method is used today in several other sectors domestically and internationally, including autonomous vehicles (Aurora and Uber), medical equipment, geological disposal of radioactive waste, offshore drilling, pipelines, and many others. The term "safety case" is also used in a variety of existing autonomous vehicle industry standards, such as ISO 26262 and UL 4600 [6].

The safety case process is designed to demonstrate a valid argument, with evidence, that a high-risk system (including operations, facilities, and personnel) is appropriately safe for a given use. The process uses the "as low as reasonably practicable" (ALARP) methodology that requires developers to reduce

hazard risks to an acceptable or tolerable level. Reasonably practicable involves weighing a risk against the effort, time, and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled.

The ALARP terminology does not have a quantifiable definition, nor is the level of hazard acceptance identical across all industries or applications. However, a broad understanding of ALARP can be developed based on the "reasonably practicable" phrase. This phrase is based on the case-by-case interpretation of a cost-benefit assessment for what is reasonably possible (in terms of degree of risk change) to bring the system to an acceptable risk level when compared to the money, time, and effort needed to accomplish that change.

The application of the safety case methodology has several major advantages, listed below, when compared to other safety compliance assessment methodologies.

1. Allows each developer organization to apply their development and documentation products, while minimizing the creation of new ones, to address any regulatory safety assessments. This provides an allowable use of different evidence examples based on their corporate history, corporate risk philosophy, and personal preference.

2. Allows each developer organization to use its unique safety philosophy, to be incorporated to the maximum extent possible, in the safety case framework and evidence. This may highlight the possible existence of a unique interpretation in what each developer organization may consider an appropriate risk. However, identification of any such issue can lead to clarification, resolution, and agreement between the developer and reviewer organizations.

3. Provides a clear, regular communication structure between the reviewer and developer organizations.

The safety case process also has flexibility in "use" cases or options of how it is implemented. Optimally, it starts during the concept stage in a system's development and continues during all subsequent phases, including design, manufacturing, testing, and operations. However, alternative use cases are also possible. One alternative example is to provide a safety case report at the end of every interim phase [7]. This entails formally issuing at least three versions of the (software) safety case:

1. Preliminary Safety Case—after definition and review of the system requirements specification

2. Interim Safety Case—after initial system design and preliminary validation activities

3. Operational Safety Case—just prior to in-service use, including complete evidence of having satisfied the system requirements

In all use cases, however, the safety case methodology is intended to be used as a design tool to improve the safe operation of the system by influencing changes and verifying the design and operation. It documents the risk reduction from system updates and provides supporting evidence with a safety case report at the end of each phase. For an interim safety case report, the safety case report demonstrates satisfactory progression of the work and the safety requirements for that phase have been or are clearly planned to be met.

Whatever use case is chosen, the safety case report remains a valuable tool to document the major safety risks and confirm all controls have been documented and confirmed to be in place and functional. In all use cases, the safety case report is a "living" set of documentation that is continually updated to reflect the system's current safety state of the art. This safety case review schedule and output must be stated in the developer's appropriate safety products.

4.7.2 Safety Case Format

A fundamental basis for successful use of the safety case methodology is clear, concise, and continuous communication between the developer and the reviewer organizations. The communication begins with the reviewer providing the outline of the expected attributes of the safety case report (based on their regulatory requirements); continues via an initial interactive discussion of the corporate philosophies, practices, and internal corporate products; and finishes with an initial agreement on the safety report content and schedule. Following this initial agreement, there will be regularly scheduled meetings to address and resolve any content or review issues that have been developed.

The format for a safety case report is tailorable for both the industry and the developer's organization; however, a baseline format for a safety case report can be defined by the reviewing organization. An example safety case format is shown below.

Example Safety Case Format:

1. Executive Summary

   A summary of the methodology used, a status showing the safety case is progressing satisfactorily and is appropriately proceeding to the next stage, and evidence that the overall safety of the system in review is acceptable at this stage.

2. Summary of System Description

   A brief description of the hardware, software, personnel, and facilities of the system, with a more detailed description documented in the body of the safety case report. It also specifically addresses the system boundaries (i.e., what is outside and inside the system being discussed) and the interfaces of the system to other systems of systems.

3. Assumptions

   The developer's understanding of the foundational assumptions used in developing the safety case. It may include any defined or known quantified levels of safety, any external resource providers, and any operating environment requirements or limitations.

4. Progress of the System

   The current status of the system, including both hardware and software, describing the advancements that have been made since the last safety case assessment.

5. Meeting Safety Requirements

   A description of the regulatory safety requirements, if any, levied on the system and an assessment and evidence that the safety report documents how they have been or will be met.

6. Emergency/Contingency Arrangements

   A description and documentation of the emergency/contingency procedures and systems that have been or will be put in place. Included in this is a discussion and schedule of any incomplete procedures and systems that have not yet reached an appropriate level of maturity.

7. Operational Information

A description of the overall operating envelope and limitations of the system being reviewed. This includes any significant risks and insights on the how the controls for those risks have been integrated into the operating procedures and systems.

8. Independent Safety Auditor Report

   An independent safety auditor is not always necessary for each safety case report. However, if there are additional factors that require them (e.g., legislative, regulatory, technical standards or complexity, and technical skills beyond the standard reviewer's organizational abilities), the independent safety auditor's report should be included.

9. Conclusions and Recommendations

   A summary description of the overall assessment results of the system's safety and any recommendations to further reduce the system's risk. It also provides a discussion of any issues that have yet to be resolved.

10. References

    A list of document references used in the development of the safety case report. It provides additional evidence supporting the conclusions and recommendations of the report.

The resulting safety case report summarizes the major attributes of the safety case, clearly and concisely states the safety of the system, and provides the supporting evidence for the statement. Special attention must be paid to adequately summarize the safety case and the supporting evidence. A full, unabridged set of lower-level technical data could quickly render the safety case report too large and, therefore, cumbersome and unusable. The iterative discussion process with the reviewer organization can aid significantly in defining the appropriate level of detail.

4.7.3 Safety Case Example: Aurora Self-Driving Safety Case

Each safety case, even in the same industry, is a unique example, so no two are identical. In addition, a safety case for an aerospace system may have the same general attributes, but is not identical to a safety case for other systems or products, such as medical equipment or transportation systems. Each safety case is tailored based on the reviewer organization's regulatory requirements, the developer's internal corporate products, and, just as importantly, the internal corporate safety philosophy. An example of these can be seen in the Aurora's safety case framework for their autonomous driving cargo trucks and passenger cars on public roads [8]. Aurora has selected the safety case methodology as a framework to best describe and document that their autonomous vehicles meet their top-level claim (objective) that they are "acceptably safe to operate on public roads."

The Aurora safety case framework integrates guidance from government organizations, voluntary industry standards, academic research, best practices from safety-critical industries, and lessons learned from their own testing to date. The framework thus directly reflects the corporate philosophy on safety as applied to developing and operating autonomous vehicles on public roads. Figure 5 illustrates the Aurora safety case framework.

In addition, Aurora is applying this safety case framework through the entire development lifecycle as they expand testing operations with and without human backup drivers, on a variety of driving platforms and with expanding operating environments. Aurora will eventually use their safety case as the acceptance rationale for the certification of their equipment to operate on public roads when any local, state, and federal operating regulations are put in place.

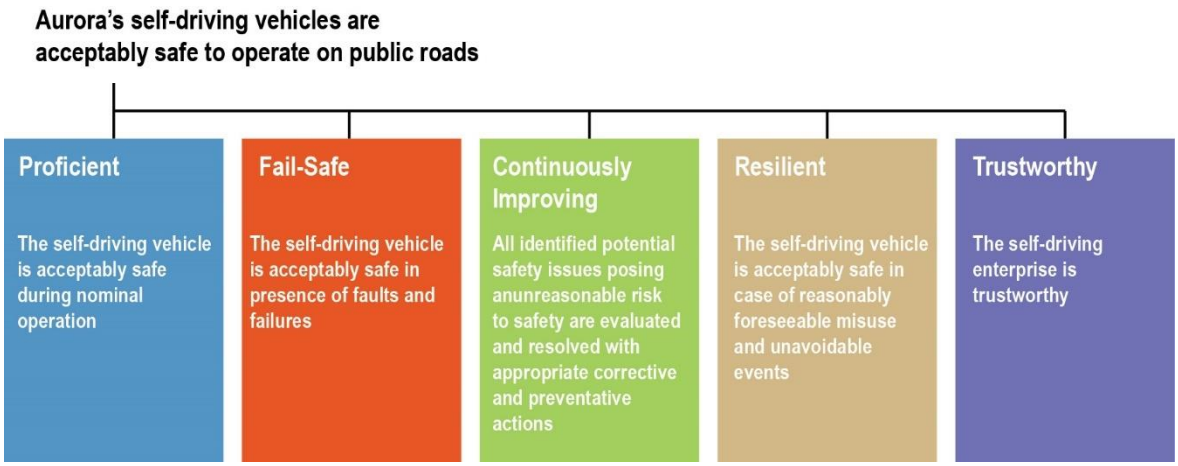

Figure 5. Aurora Safety Case Framework. (adopted from [47])

4.8 Compliance Monitoring and Enforcement

4.8.1 Introduction

The objective of compliance monitoring is to identify safety concerns and deviations from safety standards as set forth in regulations, international agreements, or organizational policies. At the FAA Office of Commercial Space Transportation (AST), compliance works in concert with licensing functions to ensure a licensee complies with the conditions identified in their launch license. However, compliance is not only a one-time verification that systems are safe, but also a process of continuous monitoring with tools such as inspections, audits, and corrective actions.

Historically, compliance has been seen as an enforcement tool that regulators use to apply monetary penalties or legal action against noncompliant entities. However, it is an important process used by many stakeholders to promote safety in a collaborative manner as well. This includes the regulatory body, third-party technical experts or insurance, industry, and the public.

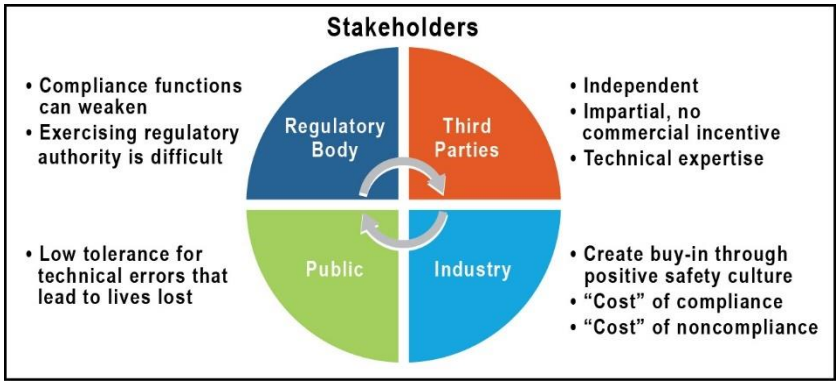

Figure 6. Stakeholders in Compliance Monitoring.

Figure 6 shows that each stakeholder must work collaboratively to promote safety compliance. Industry must weigh the cost of compliance versus the cost of noncompliance, which includes costs of mishap failures, and may be incentivized to integrate internal inspections and audits to maintain their own safety protocols. This process can work in conjunction with regulatory bodies who oversee compliance with safety regulations and law. However, exercising such regulatory authority is costly, requires technical expertise, and can weaken over time if not maintained. Third parties can aid regulators and industry to

maintain compliance by offering inspection services and technical expertise. Finally, public outcry due to mishap failures or fatalities may trigger the use of enforcement. While enforcement can often lead to antagonism between various stakeholders, it is important to strike a balance that allows for a collaborative compliance process and a role for impartiality in inspections and enforcement.

The following subsection examines the key considerations of a multistakeholder compliance process, as well as how the FAA has recently addressed compliance issues in their regulatory oversight. The FAA, particularly in commercial aviation, has largely transitioned from an enforcement-based system to one that recognizes a more collaborative problem-solving approach.

4.8.2 Key Considerations of a Compliance Monitoring Program

Compliance monitoring is tightly integrated with other safety building blocks as a process that works best as a complement to other regulatory functions. For example, inspections may be used for license and certification, compliance tools help enforce regulations, and, most importantly, inspections can help promote a safety culture using self-monitoring and collaborative problem solving.

Compliance tools include inspections, audits, reviews of procedures/operations/design, safety testing and rating systems[2], evaluations of preparedness, mitigation measures or corrective actions, and enforcement actions, such as monetary and civil penalties.

To build a robust compliance system, some key considerations include:

- **Impartiality and independence.** Using third-party organizations with no commercial incentives for inspections and audits, and keeping compliance functions separate from other regulatory functions, such as licensing or commercial advocacy.

- **Using internal and external controls.** Third-party inspectors provide an external control on a company's compliance with safety standards, but inspectors also can be evaluated or certified, which adds an additional level of control[3]. Companies may also conduct internal audits for anomalies, risks, and safety compliance to limit costs of noncompliance.

- **Time dependent**. Inspections or audits may be completed at specific times, such as prior to use (e.g., to check for flightworthiness). They may be continuous in that they take place annually or quarterly to detect anomalies and other deviations. Comprehensive technical inspections may take days to conduct (e.g., ship inspections can take 5–7 days).

- **Consequences for noncompliance.** Mitigation measures depend upon the level of a safety risk and can go all the way up to grounding a vehicle that might have an immediate safety risk. Depending on the severity of a violation, consequences can include enforcement actions, such as civil and other legal penalties (e.g., criminal activity or reckless behavior).

These considerations help determine which tools are most appropriate in any given circumstance.

[2] For example, the National Highway Transportation Safety Administration uses vehicle safety ratings to determine how safe a vehicle is after putting it through various safety tests (e.g., crash tests).
[3] For example, the U.S. Coast Guard evaluates their examination teams for how well they did their jobs completing ship inspections.

4.8.3 FAA Compliance Philosophy

49 USC Chapter 701, "Commercial Space Launch Activities," as well as 14 CFR Part 405 and Part 406, enumerate several compliance-based functions and tools for commercial space launch activities, including commercial human spaceflight. These include (1) FAA licensees must allow FAA compliance officers to monitor licensed facilities and activities, (2) FAA has the authority to modify, suspend, or revoke licenses, and (3) FAA can issue emergency orders to suspend activities if they are discovered to be detrimental to public health and safety, the safety of property, or any other national security or foreign policy interest (14 CFR Part 405.5). In addition, the FAA can enforce civil penalties if a person is found to be in violation of a requirement of the Commercial Space Launch Activities Act, FAA regulations, or a condition of their license or permit.

However, regulatory functions take considerable resources and are not always easy to enforce. A collaborative compliance system can help address some of these issues. Considering the strengths and weaknesses of each stakeholder, facilitating a collaborative compliance system is becoming ever more important across several transportation sectors. The FAA offers an example of how a more collaborative approach might work in the compliance process.

Historically, the FAA relied on enforcement actions to facilitate adherence to safety conditions. In 2015, the FAA took steps towards changing the culture of compliance by issuing its "Compliance Philosophy." This philosophy focuses on transparency and collaboration and emphasizes taking nonenforcement actions ("corrective") instead of violations. Compliance is the standard, and enforcement action is only taken when inappropriate risk taking occurs.

A key part of FAA compliance, now called the "Compliance Program" feeds into their Corrective Action Plan. The FAA recognizes the distinction between a compliance action and enforcement as the following:

> A Compliance Action is not a finding of a violation. Rather, it is an open and transparent exchange of safety information between you and the FAA. Its only purpose is to restore compliance and correct the underlying causes that led to the deviation. In other words, if you've made an honest mistake, a temporary lapse of judgment, or have let your skills become rusty, you may be able to 'fix' the problem without facing a violation.
>
> However, an airman who indicates that he or she is unwilling or unable to comply, or shows evidence of intentional deviation, reckless or criminal behavior, or other significant safety risk, would be ineligible for a Compliance Action. [9]

Whereas an enforcement action is reserved for the latter type of behavior (criminal, reckless, or unwilling to comply), a compliance action allows for the use of positive reinforcement as a tool, especially when it is an honest mistake, a temporary lapse of judgment, or a need for enhanced training.

The FAA Compliance Philosophy constitutes a major cultural change with respect to how the agency goes about ensuring regulatory compliance, shifting from a culture that is restrictive or reactive to more collaborative. It is an important step toward fostering an open and transparent exchange of safety information and obtaining a higher level of safety and compliance with regulatory standards.

4.8.4 Conclusion on Compliance Monitoring and Enforcement

The FAA Compliance Philosophy is a relatively new culture shift. The FAA believes it is improving aviation safety and the culture of safety across its programs. The commercial space transportation sector could benefit similarly from such a compliance philosophy [10].

The Government Accountability Office (GAO) conducted an analysis of the FAA enforcement policy and its impacts on safety standards [11]. The report examines the three years prior to the implementation of FAA's Compliance Philosophy in 2015 and the three years after. As shown in Figure 7, the number of enforcement actions decreased after the implementation of the Compliance Philosophy, while the number of compliance actions increased. The GAO report looks at these actions across the whole of the FAA portfolio, including commercial space launch and human space flight activities.

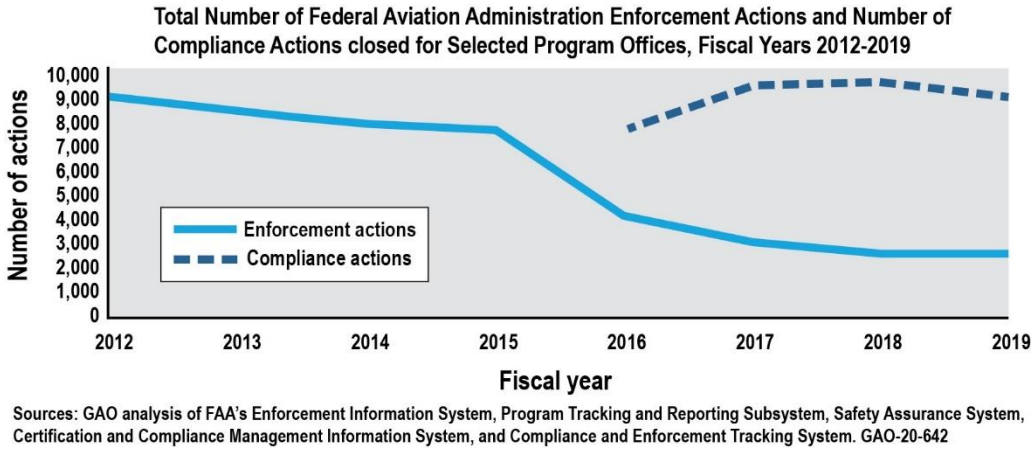

Figure 7. Impact of the Compliance Action Program on FAA Enforcement Actions.

The GAO's report suggests that more can be done to evaluate the impact of the FAA Compliance Philosophy across each of its programs. This includes identifying lingering safety concerns and determining whether noncompliance violations are repeated. In the GAO's testimony before the House of Representatives' Subcommittee on Aviation, the GAO suggested that a growing number and diversification of launch and reentry operations and locations warrants a review of AST's approach to overseeing compliance and enforcement.

As commercial human spaceflight continues to grow, FAA will be required to determine how to best apply their recently developed compliance philosophy to this activity to improve collaboration between industry and regulators on safety concerns. However, this must be a strategy that is part of a larger approach to determine how to best utilize the portfolio of compliance tools at their disposal.

4.9 Accident Investigations

An important component of developing a cHSF safety regulatory framework is the investigations of accidents and mishaps. As a cornerstone of the framework, it is one of the most useful mechanisms of ensuring problems in spacecraft design and manufacture of commercial systems are discovered and resolved. Accident investigations also serve as a pillar of confidence and transparency, which are important considerations for public trust and, therefore, successful development of this sector. The history of accident investigations in different modes of transportation offers an example when low public trust in the safety of the technology can lead to a stifling of industry growth and investment.

This section examines the current scope of accident and mishap investigation of commercial launches, potential gaps, and analysis on how it fits into a future cHSF safety regulatory framework.

4.9.1 Current Scope of HSF Investigations

There are three main mechanisms for investigating human spaceflight accidents, mishaps, and other incidents: FAA's mishap investigations, the NTSB, and Presidential commissions. The FAA and NTSB focus on commercial transportation activities, and the Presidential commission primarily focuses on

government missions. However, NTSB has been involved in government-related transportation investigations. While the FAA and NTSB were originally housed under the Department of Transportation (DOT), NTSB eventually separated to serve as a fully independent investigative board. This separation allowed FAA to focus on the regulation and promotion of commercial activities. As a result, both have different scopes and approaches to accident investigations.

4.9.2 FAA Mishap Investigations

Codified under 14 CFR 450.173, the FAA oversees investigations and corrective actions of commercial space activities following a mishap event [12]. The FAA defines these to include serious injury or fatality or a high risk of it, malfunction of a safety-critical system, failure of safety operations, substantial damage to property, permanent loss of vehicle, impact of hazardous debris, or launch or reentry failure.[4]

Launch providers operating under an FAA license to launch must report any mishaps, implement a mishap plan, mitigate risks, conserve mishap data, and work with the FAA to conduct investigations. The process primarily relies on a mishap plan the operators submit prior to FAA approval of a launch license. The FAA may elect to investigate an event, or it may authorize the operator to perform the investigation in accordance with its approved mishap plan. The FAA oversees an operator-performed mishap investigation to ensure public safety. Once the FAA has been notified of a mishap, an operator's launch license will be suspended and they cannot launch again until the FAA finds that corrective action has been taken to mitigate the mishap.[5]

A current hurdle for cHSF at the FAA is not a new one—its potentially conflicting dual mandate: (1) to oversee, authorize, and regulate launch and reentry of vehicles to ensure public health and safety, safety of property, national security, and foreign policy interests of the U.S., and (2) to promote commercial space launches in the private sector, including those that include spaceflight participants. As seen in the past in aviation investigations prior to an independent NTSB, the dual mandate arguably limits the independence of the agency conducting the investigation. However, the FAA has only exercised its investigation authority with Virgin Galactic's SpaceShipTwo accident, and there is scope for further exercising this authority.

4.9.3 National Transportation Safety Board (NTSB)

The NTSB is "an independent investigatory agency charged with determining the facts, circumstances, and causes of transportation accidents and incidents." However, transportation accident investigations have not always been independent. Accident investigation evolved over the 20th century. Congress created the NTSB to investigate transportation accidents, including aviation, in 1967 and placed it under the DOT. The Independent Safety Board Act of 1974 reestablished NTSB as independent because"...[n]o federal agency can properly perform such (investigatory) functions unless it is totally separate and independent from any other ... agency of the United States." Importantly, NTSB has no regulatory authority, whereas FAA does [13]."

[4] Accident, incident, and mishap are defined separately within 14 CFR Part 450 and determine whether FAA or NTSB has oversight over the investigation, further established in the MOUs between NTSB and FAA.
[5] "An operator must identify and implement preventive measures for avoiding recurrence of the mishap prior to the next flight, unless otherwise approved by the Administrator." 14 CFR Part 450.173, https://www.ecfr.gov/current/title-14/chapter-III/subchapter-C/part-450/subpart-C/section-450.173.

49 U.S.C. 1131(a)(1)(F) grants NTSB investigatory authority of commercial space launch accidents[6]. In addition to having the authority to investigate and determine probable causes, it can also issue recommendations to the FAA. The FAA has discretion to adopt those recommendations.

Regarding the investigation process, NTSB uses a party system. The NTSB appoints an investigator in charge (IIC) to lead the entire investigation. NTSB's specialists, including operations specialists, participate. Additionally, NTSB appoints the parties, including the oversight agency (i.e., FAA), experts from the organization involved in the accident, and other outside experts. Each party provides a party coordinator and participates in the fact finding. The investigation results in NTSB producing a factual report with its analysis. All parties are allowed to give comments on the investigation and report; however, NTSB has discretion to include those comments and analyses. This final report is entered into the public docket system[7]. Making the documents public provides transparency and the appearance of independence in the system, one of the main rationales for reestablishing NTSB as independent.

Finally, NTSB was involved in the investigation for the SpaceShipTwo and the Columbia investigation: "[s]ix NTSB investigators also helped NASA engineers reassemble the shuttle at Cape Canaveral. Overall, more than 50 NTSB employees supported this investigation [14]."

4.9.4 Memoranda of Understanding (MOUs) and Other Interagency Agreements

Interagency MOUs have long been part of the accident investigation process. In 1975, an agreement between FAA and NTSB established the "relationships, notification procedures, coordination requirements, and reporting responsibilities of both agencies." Called the Reimbursable Memorandum of Agreement (MOA), it also "identifies and describes the conditions and agreements that exist regarding the exchange of data, availability of resources, conduct of studies and other services, and reimbursement for services rendered [15]." Although several previous MOUs established this relationship, in 2004, a new MOU established a relationship among NTSB, FAA, and USAF during space launch accidents [16]. It provides a guide to the exchange of information and participation in accident investigations.

The Agreement and MOU specify when NTSB initiates an investigation into a commercial space mishap. However, according to the NTSB, the 2004 MOU is limited in scope, suggesting that because this MOU and Agreement were developed before cHSF, or reusable launch vehicles, it was realistically foreseen to only address cargo operations. Therefore, it has recently been suggested that there is a need to update and bolster these agreements to account for growing space transportation activities [69].

On September 9, 2022, the NTSB and FAA signed an MOA on Commercial Space Mishap Investigations. It "replaces Appendix H to the 1975 Reimbursable Agreement between the NTSB and FAA as well as all prior MOAs, Memoranda of Understanding (MOUs) and agreements between the NTSB and FAA for commercial space mishap investigations." [68]

Pursuant to the new MOA, Section 3:

a. The NTSB will be the lead investigative agency for FAA permitted, licensed, or otherwise FAA approved, commercial space launch or reentry mishaps resulting in—

[6] 49 U.S.C. 1131(a)(1)(F) provides in pertinent part that the NTSB "shall investigate and establish the facts, circumstances, and probable cause of any other accident related to the transportation of any other individuals or property when the Board decides the accident is catastrophic, the accident involves problems of a recurring character, or investigating the accident would carry out the NTSB's statutory mandate." See NTSB NPRM, supra.
[7] NTSB reports are public, though redacted, but cannot be used in litigation as evidence of fault or liability.

i. A fatality or serious injury (as defined in 49 C.F.R § 830.2) to any person, regardless of whether the person was on board the commercial space launch or reentry vehicle; or

ii. Damage to property from debris (intact vehicle, vehicle fragments, payload, or any planned jettison bodies or substance) that could reasonably be expected to cause death or serious injury, and the property is not associated with commercial space launch or reentry activities or the launch site.

Further, the "FAA will be the lead investigative agency for all other commercial space mishaps as defined in 14 C.F.R § 401.7, as in effect on the date of the signing of this MOA." [68]

Finally, these agreements and MOUs are also supported by a "quad-chair" forum for NASA, USAF, FAA, and NTSB to work together and meet to discuss and resolve ongoing issues.

4.9.5 Presidential Commissions

Under certain circumstances pursuant to statute 51 U.S.C. 70702, the president will establish an investigation commission called a Presidential Commission. Within seven days of an accident that fits the conditions, the president:

> … shall establish an independent, nonpartisan Commission within the executive branch to investigate any incident that results in the loss of (1) a space shuttle; (2) the International Space Station or its operational viability; (3) any other United States space vehicle carrying humans that is owned by the Federal Government or that is being used pursuant to a contract with the Federal Government; or (4) a crew member or passenger of any space vehicle described in this subsection. [50]

The Presidential Commission's duties are to investigate, determine cause and contributing factors, make recommendations, and submit a report. The Act also specifies that no employee of the federal government shall serve as a member of the commission nor can a member have, or have pending, a contractual relationship with NASA. Given these membership limitations, it may be difficult to establish a knowledgeable and adequately experienced commission. Indeed, the Aerospace Safety Advisory Panel (ASAP) noted in its 2018 Annual Report that the Presidential Commission Requirement may have outlived its time and should be reviewed and revised especially in light of commercial human spaceflight [17].

There are also questions whether this statute applies to NASA's commercial crew. Since 2015, ASAP has recommended NASA decide whether it will recommend any changes to the statute's authority. In 2021, according to the ASAP report, NASA was reaching out to the FAA and the NTSB to "jointly develop viable options to revise the Authorization language with today's systems in mind [18]."

To date, a president has never established a commission under this statute. In 1986, prior to statute enactment, the president established a committee for the Challenger accident. As for the Columbia accident, NASA established the Columbia Accident Investigation Board (CAIB).

Regarding applicability to strictly commercial launches, it seems unlikely a Presidential Commission would apply.

4.9.6 The Pending NTSB Notice of Proposed Rulemaking

In the recent Notice of Proposed Rulemaking (NPRM), the NTSB proposes the addition of Subpart F for Commercial Space Investigations. It states that 49 U.S.C. 1131(a)(1)(F) provides NTSB the authority to:

> … investigate and establish the facts, circumstances, and probable cause of any other accident related to the transportation of any other individuals or property when the Board decides the accident is catastrophic, the accident involves problems of a recurring character, or investigating the accident would carry out the NTSB's statutory mandate.[71]

Importantly, the existing MOUs would stay in place. While this would leave the existing MOUs in place, industry, Congress, and the FAA, for the most part, opposed this proposed rule. The general consensus is that the MOUs should be updated instead of creating new regulation. Specifically, public comments, including from the FAA, pointed out FAA's current authority over mishap investigations [18]. It is argued that the new rule would introduce regulatory uncertainty and dual regulation. FAA suggests taking the three current MOUs between NTSB and FAA on commercial space investigations and combining them into one overarching and stronger MOU. However, some public comments support addition of Subpart F, claiming that it would strengthen current coordination policies in place between DOT/FAA, USAF, and NTSB.[71]

Some members of Congress also responded, requesting NTSB rescind the proposed rule. Representatives Eddie Johnson and Frank Lucas sent letters stating that the NPRM contravenes current agreements and statutory authorities [19]. They believe it is strictly within Congressional authority to update any frameworks for accident investigations.

Indeed, there is no consensus on how to move forward. Apparent in the NPRM responses, there are debates in industry and government as to whether FAA has the authority to (and should) investigate space-related accidents and whether NTSB is overreaching in its NPRM. Some argue the new proposed regulation is too broad and gives NTSB too much access. Additionally, intellectual property and International Traffic in Arms Regulations/Export Administration Regulations (ITAR/EAR) information becomes an issue in commercial space if reports are publicly released. However, given the independence of NTSB, its involvement in commercial space accident investigations is important.

4.9.7 Conclusion of Accident Investigations

There are many considerations regarding accident investigations when developing a cHSF safety framework. Two main items are at the forefront based on history and current debate: (1) the statutory authority and regulation must be clear to avoid regulatory uncertainty, and (2) regulation must balance industry concerns with public safety and trust. As mentioned at the beginning of this section, accident investigation and assurance that safety problems are discovered and remedied are cornerstones of the safety regulatory framework. The independence and transparency of this process will be very important in developing a successful cHSF industry that holds the public's trust.

4.10 The Range of Safety Incentives

Incentives for improving safety in any sector can include a multitude of activities and stakeholders. There is, of course, the usual direct market driver for incentivizing safety. It is a valid argument to make that accidents in spaceflight would be detrimental to the industry itself and hence, the industry will work diligently at assuring spaceflights are conducted without any safety incidents. Otherwise, public perception that spaceflights are unsafe will drive the market. In addition to market incentives for safety, there are other incentives that promote safety. They range from using best practices and standards to

offering regulatory incentives as well. The current approach would be to ask the industry to develop consensus standards that could subsequently be used in stricter regulatory requirements as needed.

Several activities are currently underway to develop such industry best practices and standards including ASTM International F47 Committee and ISO Subcommittee 14. In addition, the FAA issued recommendation for best practices for human spaceflight occupancy safety.

Conceptually, Figure 8 describes a possible progression from unregulated activities to industry consensus standards, and FAA recommended practices. These can be implemented during the learning period. After the learning period expires, stricter requirements through regulations may be issued as needed. The open question is what triggers a decision point to move a particular activity into the next phase.

Taking into account the number of human spaceflight companies, the methods of transportation (vertical, horizontal, and balloon rides) and the overall readiness of the industry, it may take a considerable time to identify the sublevel safety issues that require regulation.

We recommend focusing, in the near future, on incentivizing activities that benefit the safety record of the industry in the future (not just the near term) without the specific transportation mechanism and without appearing to regulate a single company. Those activities are related to promoting a positive safety culture, activities centered around people, and activities that promote data collection, analysis, and sharing.

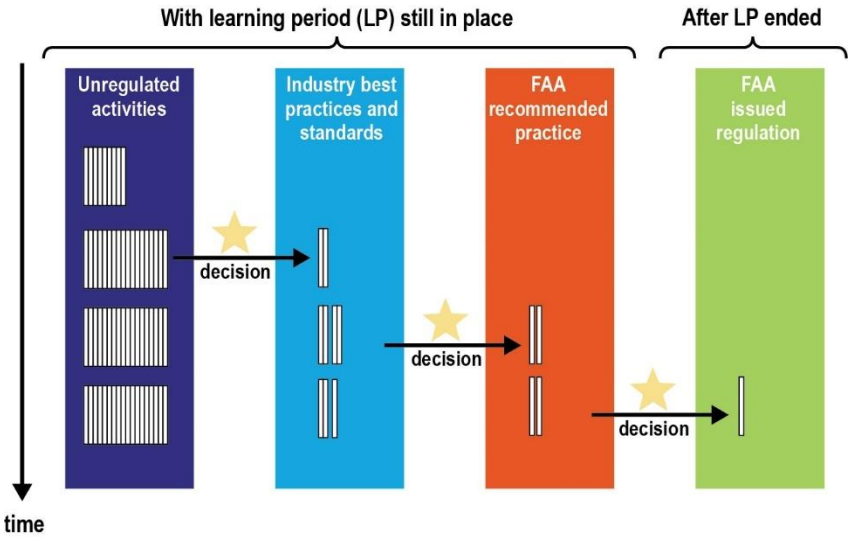

Figure 8. Progression from unregulated through end of learning period.

Over time and as the industry matures, best practices and standards will likely move to officially recommended practices to a regulatory action driven by trigger events or decision points. The status of voluntary consensus standards is described in Appendix F.

4.11 Licensing and Certifications

The fundamental aim of licensing and certification is to determine if an activity is safe enough to be permitted. This is based on whether it meets certain standards and regulations. Currently, the FAA's Office of Commercial Space Transportation uses a licensing process for launch and reentry of commercial human spaceflight vehicles. This is part of their broader mandate to license launch and reentry of all commercial space transportation vehicles, including for suborbital and orbital missions. The FAA licensing regime is a "light touch" approach to allow for the nascent cHSF sector to further develop and grow.

A certification regime usually certifies the vehicle, airline, or pilot, whereas the FAA Office of Commercial Space Transportation licenses the launch operation [20]. Commercial suborbital space vehicles are still relatively new and it is unclear what designs will be commercially successful. Through the use of performance-based requirements, FAA licensing allows technology innovation to give industry the flexibility to meet safety objectives without specifying how safety must be achieved.

In contrast, the European Union (EU) explored the possibility of using a certification process for suborbital flights in 2008, managed by the European Aviation Safety Agency. This is in part because Europe has long-established expertise with air law and safety standards, and less expertise with space law and cHSF safety standards [21]. The EU put the process on pause in 2011 and has more recently launched a Higher Airspace Operations (HAO) Task Force and European Concept for Higher Airspace Operations (ECHO) project to determine how to regulate higher airspace [22]. While this process might be useful in the short term, space law might be more appropriate for when suborbital and orbital missions enter outer space.

In summary, we recognize the maturity of the industry has not yet grown to a level where space vehicles are "mass produced." Hence, certification of vehicles similar to cars, cruise ships, and airline jets, that can be resold to other companies and operators, may be premature at this point. Using a collaborative approach to safety with individual companies focusing on a safety case approach, positive safety culture, and collecting/sharing relevant safety data might be more appropriate at this time.

4.11.1 Types of Licenses and Certifications

Vehicles are not the only aspect of a transportation activity that is subject to the licensing or certification process. There are many types of certifications and licenses that ultimately incorporate or impact safety. These include vehicle design and operations (e.g., airworthiness), personnel training and competency (e.g., driver's license or pilot's license), registration and classification (e.g., registration of ships to a particular national jurisdiction), and direct safety requirements (e.g., safety and rescue equipment, safety management system certificates, radio requirements).

Some of these processes require a more mature commercial market, such as "airworthiness," while others are easier to implement on an as-needed basis, such as personnel training, competency licenses, and safety and rescue certifications.

4.11.2 "Spaceworthiness" as a Benchmark for Commercial HSF Vehicles

"Spaceworthiness" borrows from aviation's concept of "airworthiness," which is the required level of safety an aircraft needs to be able to fly [23]. Standards are initially set at the international level by ICAO. At the federal level, the FAA issues certifications, using their Aircraft Certification Service and, more recently, aid from third-party certification services called Organization Delegation Authorities. The process is based on expertise from more than 1,000 engineers, scientists, pilots, inspectors, etc. and it can take from five to nine years to certify, and three to five years for amendments.

Commercial aviation vehicles are mass produced and the processes are well-established, making a certification process easier to implement. Certification includes: (1) reviews of designs, methods, and construction of vehicles; (2) passing required tests and inspections; (3) a variety of "expert" stakeholders; and (4) standards of maintenance with established timelines for validation and expiration. The evaluation standards are usually set by overarching third parties with no commercial stakes. While these processes are mature, they do account for the testing of new and novel features through the Flight Standardization Board.

Because cHSF is an emerging industry, there is little in terms of standardized design and construction principles and even less mishap data to use for safety certification processes. Therefore, a

"spaceworthiness" concept must consider the lack of data and the unique and complex production of cHSF vehicles for any type of certification process. What might be more useful is a long-term plan with a hybrid approach that determines when and where licensing or certification is most appropriate.

4.11.3 Conclusion of Licensing and Certifications

Licensing may be appropriate for now in the commercial space launch and reentry industry, as it has been well-established in the United States. The cost to comply with certification might outweigh current revenue generation prospects for cHSF. However, it is an evolving process. FAA's certification process for aviation was ultimately implemented after a long period of commercial development when there were regularly scheduled commercial flights. Commercial human spaceflight is a long way from that, but as the frequency and number of spaceflight participants increases, there will be a need for additional requirements to incorporate lessons learned and to mitigate any further risks [24].

4.12 Flight Training and Health

Unlike the human spaceflight programs of NASA and other space agencies, cHSF does not enjoy the well-established training regimes through which all government astronauts are exposed. Space medicine has evolved to include the conditions in orbit and their effects on the human body to ensure the overall health and well-being of professional astronauts. Through testing and evaluating many potential countermeasures for bone loss, muscle atrophy, vestibular issues, radiation exposure, and other deleterious effects caused by living in a microgravity and higher radiation environment, many of the problems resulting from spaceflight can now be mitigated. The lessons learned through over 60 years of human spaceflight may certainly be applied as civilian astronauts and spaceflight participants (SFPs) engage in longer stays in the space environment [25].

4.12.1 Spaceflight Participant Medical Challenges

There are currently no established medical standards in place for SFPs; there are only guidelines. Participants in cHSF activities will represent a very different demographic than that of professional astronauts, who are selected in part based on their physical health and capabilities in accordance with a highly prescriptive set of requirements that they must meet. The most likely cHSF customer demographics, in the near term, are expected to include individuals ranging in age from 25 to 75 years with approximately 80% of them being male and 20% female. Their medical status will likely range from very healthy to debilitated with unknown physiological status.

The health conditions of high-net-worth individuals aged mid-fifties to mid-seventies, which is the most likely demographic to have the means to participate in cHSF, could include one or several of the following, as well as medical conditions that may have not yet been diagnosed.

- Coronary bypass surgery
- Hypertension
- Use of multiple medications
- Diabetes
- Asthma
- Chronic obstructive pulmonary disease

The launch environment for both suborbital and orbital spaceflight includes exposure to higher gravity (G) levels than most individuals experience. There are several conditions that should be considered from a medical status point of view, including the considerations listed below:

- Acceleration levels:
  - Launch: approximately +4 Gx (chest to back) and +4 Gz (head to toes)
  - Reentry: up to +6 Gx
- Flying into space without pressure suits can lead to hypoxia, dysbarism, and hyperventilation.
- Onboard medical capability will likely not be available.
- Very little centrifuge data on this population.

Physiological responses to the G-level transitions (going from the higher G levels during launch to the microgravity environment) might include the following [26]:

- Space motion sickness:
  - Can result in an uncontrolled release of biohazardous material.
  - Typically occurs within minutes after insertion into microgravity.
- Cardiovascular and respiratory system issues (e.g., low arterial oxygen levels)
- Endocrine, hematological, and immune system issues (orbital flights)

4.12.2 Medical Requirements and Guidelines

NASA and other space agencies conducting human spaceflight programs have developed strict medical guidelines and requirements, which are imposed on all professional astronauts. As mentioned in the previous subsection, no medical requirements have been established for cHSF programs. Each company providing flight services has their own guidelines for their customers, though these guidelines may not be rigidly enforced. The medical and health philosophies are different for government programs as opposed to cHSF.

Government programs flying professional astronauts have the following constraints:

- **Exclusion** – There are many disqualifying conditions that can prevent an individual from being selected to serve as a professional astronaut; also called a *select-out* philosophy.
- There must be **no** mission impact as a result of a medical condition.
- The risk of a medical event during a mission must be extremely low.
- This philosophy is imposed in efforts to maintain crew safety.
- Professional astronauts are granted longer-term medical clearances to fly in space.

Commercial orbital HSF programs, on the other hand, embrace a more inclusive philosophy. Characteristics of cHSF programs include the following:

- **Inclusion** – The goal is to maximize the number of passengers, hence increase profitability; also called a *select-in* philosophy.
- A limited mission impact is accepted.
- Acceptance of some risk of a medical event occurring during the mission.

- Maintaining safety is emphasized.

- In general, SFPs will be one-time flyers.

For suborbital commercial flights, the following medical requirements are imposed:

- Crewmembers, those who play safety-critical roles, must possess and carry FAA second-class (Class II) airman medical certificates.

- For SFPs, no medical certificate is required. Passengers are encouraged to discuss their participation with their personal physicians.

- SFPs are required to sign an informed consent and waiver of claims against the U.S. Government.

- SFPs must have training for emergency situations (i.e., smoke, fire, depressurization, and other situations).

- SFPs must meet minimal security requirements to fly (e.g., they are not allowed carry explosives, weapons, or any item or material that could lead to a hazardous outcome).

4.12.3 Training for Spaceflight Participants

Training requirements for SFPs have not been formally established. Similar to the various medical guidelines implemented by each flight service provider, training recommendations vary in terms of length of time and the elements of the training. Most of the training involves familiarization with safety equipment and procedures for a particular spacecraft.

The FAA has mandated that all passengers read and sign an informed consent and are trained on how to respond to emergency situations involving smoke or fire as well as cabin depressurization. There are some recommended physiological and spaceflight system trainings for individuals participating in suborbital or orbital spaceflight as listed below:

- Recommended physiological training includes:

  - Centrifuge training to experience expected G loads associated with a typical flight profile.

  - Parabolic flight for first exposure to zero G. The first reaction to becoming weightless is to make swimming and kicking motions, which can be problematic for fellow passengers. It is better to experience this in a large aircraft cabin before entering microgravity in a much smaller crew capsule or vehicle.

  - Altitude chamber training to experience a decompression event. Individuals manifest various responses to decompression, including nosebleed, which would obviously be quite undesirable in a confined space.

- Recommended spaceflight system training includes:
  - Life support system familiarization.
  - Use of the emergency oxygen equipment.
  - Communications.
  - Donning and doffing and the use of pressure suits (if applicable).

- Recommended training for emergency scenarios:
  - Training should be provided for situations such as onboard emergencies, emergency egress, and preparation for an off-nominal landing.
  - Training in behavioral health and responses to the stresses involved in spaceflight are highly recommended, not only for the enjoyment of the flight, but also for protection of other crewmates.

The training suggested by spaceflight providers varies from the absolute minimum to full-up astronaut-like training experiences. As this sector of the space enterprise continues to grow, refinements to both medical and training recommendations or requirements will evolve.

4.13 International Treaties and Agreements

4.13.1 International Treaties

A long-term consideration for the cHSF safety regulatory framework is the development and application of international law, treaties, and agreements. Treaties and resolutions obligate the U.S. and other treaty parties to conduct space activities based on enumerated conditions and principles. As the cHSF sector grows, coordination across multiple entities and countries might become necessary. However, as discussed below, international agreements are typically more difficult to achieve and can take many years to draft. In the interim, the United Nations Office for Outer Space Affairs (UNOOSA) members have been meeting to discuss and draft reports and resolutions relating to human space flight.[8]

Currently, there are no international treaties that are clear on cHSF. However, the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS) reports, resolutions, and other international agreements relating to safety are valuable resources when developing an effective safety framework that can withstand the rapid development of technology. For example, the *International Space Station Agreement* [27] offers a model of successful and longstanding international cooperation dealing with human spaceflight. Likewise, the UN resolution *Principles Relevant to the Use of Nuclear Power Sources In Outer Space* offers a model framework for operational safety in space [28].

Importantly, the distinction between air law and space law will need to be defined and harmonized with the regulations of other nations. This uniformity will become essential when point-to-point suborbital flights across national boundaries are possible and orbital flights with international stakeholders begin.

This section briefly addresses international considerations, current relevant treaties and agreements, obligations, and how they may be used to assist in developing a cHSF safety regulatory framework.

4.13.2 Brief History of International Treaties Related to Space and Space Safety

Although the first international space treaty, the *Outer Space Treaty* (OST) [29], was signed over 50 years ago, only a few additional space-related treaties have been signed by a significant number of countries.[9] The last space-exploration-related treaty was the *Moon Agreement* in 1984; however, only several countries signed and the U.S. did not. [51] Despite the lack of treaty updates, the international community (i.e., United Nations—UNOOSA and UNCOPUOS[10]) continue to work on cooperation and safety in

[8] For example, The Human Space Technology Initiative, UNOOSA, https://www.unoosa.org/oosa/en/ourwork/psa/hsti/index.html

[9] See Appendix H: List of International Treaties and Agreements.

[10] Committee on the Peaceful Uses of Outer Space, "The Committee has two subsidiary bodies: the Scientific and Technical Subcommittee, and the Legal Subcommittee, both established in 1961. The Committee reports to the Fourth Committee of the

space. Several resolutions have been endorsed by COPUOS and adopted by the UN General Assembly (UNGA), including *Principles Relevant to the Use of Nuclear Power Sources in Outer Space* (PRUNPSOS).

4.13.2.1 OST and the Astronaut Rescue Agreement

All space activities, including commercial human spaceflight, are authorized and supervised by each nation—mandatory for parties to the OST, Registration Convention [30], and Liability Convention [31]. No international outer space agreement covers the safety dimensions of private citizens in space, and even the *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space* (Rescue Agreement)[11] has a limited scope. Under the Rescue Agreement, parties are obligated to assist astronauts in distress and return them to "representatives of the launching authority" if the astronauts have an accident, need help, or make an emergency landing in a party's country, or in the high seas. However, it is unclear whether "astronaut" or "personnel of a spacecraft" under the Rescue Agreement applies to private citizens in space.

4.13.2.2 Application of International Treaties and Agreements

Current cHSF is dominated by suborbital flights that launch and land in the same country of origin, primarily in the United States, where the FAA licenses and regulates their launches and landings. However, cHSF activities will eventually extend beyond suborbital into the realm of orbital and point-to-point or from one country to another. This will expand the level of coordination and enforcement required at the international level.

A thriving cHSF market with commercial entrants from various countries will necessitate the coordination of traffic management systems, point-to-point transportation, and clarification of liabilities. responsibilities, and rescue agreements. While launch countries are ultimately liable for any damages under the Liability Convention and the OST, the level of commercial activity might eventually necessitate a different system, where in-orbit liabilities and risk might be shared across multiple stakeholders.[12]

Aviation and air law might offer a starting point, but the particularities of cHSF may require expansion of space law itself. For example, the Rescue Agreement might be clarified to include all spaceflight participants, including tourists.[13]

As more countries enter the market with differing expectations and capabilities, an international agreement or treaty can facilitate uniform global technical and other safety standards. Finally, while individual countries might have their own laws, international agreements help facilitate enforcement for international norms of behavior, especially in space where cooperation is critical for the safety of all.

4.13.2.3 International Agreement Considerations

A successful international agreement requires building consensus among all the relevant parties on the norms of behavior for cHSF. This can be done through various negotiating platforms, including

---

General Assembly, which adopts an annual resolution on international cooperation in the peaceful uses of outer space." See https://www.unoosa.org/oosa/en/ourwork/copuos/index.html.

[11] Entered into force on December 3, 1968.

[12] More space-faring states are requiring insurance and proof of financial responsibility to go toward the potential state liability in the event of damage.

[13] Space tourism vehicles might need safety standards for their "design, construction, and operation." There also needs to exist an internationally agreed-upon responsibility and liability scheme, also implemented at a national level, for the safety, adequate risk avoidance, and certainty of process in the case of injury or loss to a space tourist. Space tourists cannot claim compensation under the Liability Convention.

international working groups, bilateral and multilateral meetings, and more. Depending on the number of parties involved in the activity, some of the questions open for discussion include:

1. Should these activities be housed under space or air law or some hybrid combination?

    a. Who will implement and monitor agreement adherence? This may include establishing an organization like the International Maritime Organization (IMO) [31] or the International Civil Aviation Organization (ICAO) [32]. In this case, it might include establishing an UNOOSA office or expanding the ICAO.

2. What should be the breadth or depth of the agreement?

    a. Will such agreements be particular to cHSF, or is a more comprehensive agreement on safety in space that covers all manner of space activities appropriate?

    b. How will point-to-point transportation occur across international boundaries to facilitate launch and reentry?

We can examine other relevant or similar international agreements for guidance on developing a safety framework. For example, the *Safety Framework for Nuclear Power Source Applications in Outer Space*[14] can offer a model structure of how a cHSF framework may look.

4.13.3 Conclusion of International Treaties and Agreements

The OST, Registration Convention, Liability Convention, and the Rescue Agreement obligate the U.S. to conduct its space activities in certain ways; therefore, a safety framework needs to ensure compliance.

A new international treaty on commercial spaceflight safety is unlikely to be drafted soon, though it may be a piece of the framework in the future. Another issue with international treaties, for the purposes of a developing a safety framework now, is the lack of enforcement mechanisms. Currently, if a dispute arises under one of the space treaties, the International Court of Justice hears the case.

Furthermore, many agreements have compliance mechanisms that depend on whether the agreement is legally binding or politically binding. Legally binding treaties might not include all norms of behavior related to cHSF, but offer legal tools of enforcement where necessary, whereas politically binding agreements might not trigger the full force of the law, but a political response if broken. Different safety standards might require different types of response and compliance. For example, in the case of space tourists, liability should be clear and developed internationally with a harmonization of domestic regulation.

Additionally, given how long treaties can take, bilateral or multilateral agreements are more likely in cases requiring cross-border cooperation and coordination. Regardless of mechanism, an international safety framework will need international buy-in through agreements and norms.

As cHSF develops, countries will inevitably develop regulations. Complying with international obligations, establishing norms of behavior, and international cooperation will be vital for the safety of SFPs.

[14] Endorsed by the Committee on the Peaceful Uses of Outer Space at its 52nd session and contained in A/AC.105/934.

We recommend starting discussions soon to develop international agreements to cover international and multinational aspects of spaceflight safety. Those include in-space astronaut rescue, point-to-point travel between nations, and commercial space habitats with international SFPs.

4.14 Roadmap and Recommendations

Taking into account case studies, commonalities among the different transportation sectors, readiness of the industry, and the principles of a safety framework described earlier, we recommend a series of activities. Some can be implemented in the (1) near future, before the learning period expires; (2) midterm, after the learning period expires; and (3) far future as the industry matures as indicated in the list below and in Figure 9.

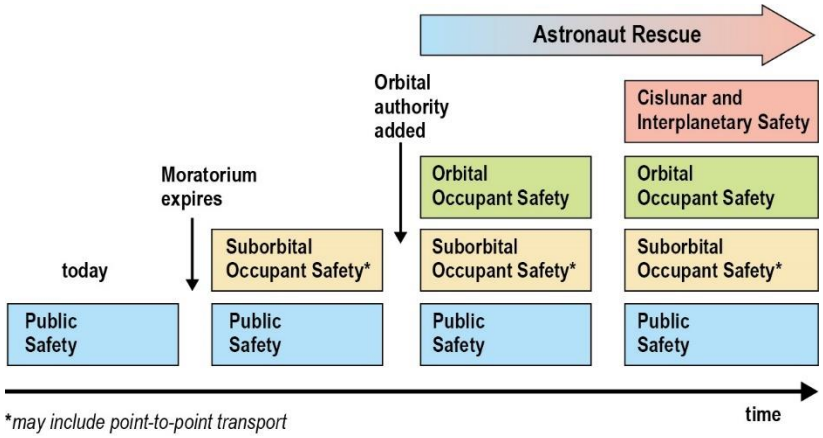

Figure 9. A roadmap based on ongoing and anticipated activities.

Near term (feasible even before the learning period ends):

- Establish activities that promote positive and just safety culture.
- Affirm FAA Compliance Philosophy, Order 8000.373, to include space more prominently.
- Implement a scalable SMS recommendation/requirement building on the existing System Safety Program, AC 450.103-1.
- Develop an MOU with individual spaceflight providers on data sharing.
- Develop a system to collect safety-related data to enable technical analyses on hazards and risks.
- Establish a whole-of-government government strategy for astronaut rescue.

Midterm (after the learning period ends):

- Obtain a “selective” authority, specific to commercial human spaceflight safety, that extends beyond launch and reentry.
- Implement industry consensus standards together with audit and enforcement mechanisms.
- Establish a Safety Case Approach with an independent review function.

Long term (as the industry matures):

- Engage in discussions and conversations internationally to promote international standards on commercial spaceflight safety supporting point-to-point transportation, in-space flight participant rescue, and multinational activities.

5. Human Spaceflight Hazards and Risks

5.1 Introduction

The keystone for safety in human spaceflight has been hazard identification, risk evaluation, trade, and mitigation. This process should begin early in the design phase, allowing for design mitigations or changes. This results in lower cost, and prevents costly redesign later or acceptance of unnecessarily high risks. The hazard analysis is intended to provide a comprehensive understanding of the hazards associated with an item of hardware, a subsystem, and/or the interaction of several systems together (integrated hazard). Design mitigations and elimination, redundancy, and procedural safeguards tracked and verified in the hazard reports can reduce the risks of such hazards and allow for reaching an acceptable risk threshold.

5.2 NASA Approach to Hazard Analysis

For decades, NASA has used the hazard analysis approach for assessing risk.

Following the Challenger accident, NASA implemented a process for the space shuttle. It began a complete reanalysis of the documented hazards for the entire program as part of the return-to-flight effort. Personnel and contractors considered this implementation a "fresh look." Hazards were categorized into "catastrophic" (i.e., loss of vehicle or crew) and "critical" (i.e., all others), and identified by compartment (i.e., aft, midbody, etc.). Subsequently, the process included a thorough hazard analysis tree (e.g., over-pressurization due to a ruptured pressurant bottle) or fire/explosion (e.g., due to ruptured propellant line).

At the same time, NASA began a similar complete and independent reanalysis of the failure modes and effects analysis (FMEA) and the Critical Items List (CIL) identification of all components. All items that could cause loss of vehicle or loss of crew were deemed "Criticality 1." Items causing only loss of mission were deemed "Criticality 2." All other failure modes were deemed "Criticality 3." CIL elements were Criticality 1 or 2 FMEAs, and were called that to differentiate them from the very large number of total FMEAs, and given special attention.

New reviews based on years of actual ground refurbishment and flight operations experience identified numerous new hazards and FMEA/CIL elements. The process revisited existing hazards and mitigations, compared the changes, experience, and flight operations, and adjusted accordingly.

NASA quickly recognized the result of these two independent efforts as a "top down" (hazards) review and a "bottoms up" (FMEA/CIL) review. When integrated, they became a "cross check" on the accuracy and completeness of both. Specifically, all Criticality 1 CIL elements were required to be linked directly with a catastrophic hazard, and all hazards were required to document all the applicable FMEAs and CILs. The result was extremely successful and led to numerous new crew procedures, flight rule changes, refurbishment (turnaround) procedure changes, and hardware redesigns. The complete effort took approximately 2.5 years.

Subsequently, NASA implemented a process to revisit those analyses when changes were made to the system; when anomalies and failures were reported, either in ground test or flight; or when environments or conditions changed. Because FMEA/CILs were tied to hazard reports and vice versa, changes in one would be carried to the other and verifications were ensured to be repeated as necessary for each flight (a verification matrix was devised and checked as part of flight preparations). This documentation was also available to mission control personnel so that in-flight issues could be assessed against the hazard analyses and CILs to determine appropriate steps or remediations in real time.

The ISS hazard analyses benefited from the experience gained from the space shuttle return-to-flight hazard analysis. The ISS predecessor, space station Freedom, was a significantly different design so very few hazards could be modified and applied to the ISS. The NASA ISS Office of Safety and Mission Assurance (OSMA) was declared as the overall safety integration organization for this multinational effort, allowing cross coverage not only for individual components and segments to the ISS, but also as part of the integrated whole. This required insight into all aspects of the U.S.-based assets, as well as the international partner's design details, material selection, manufacturing processes, test procedures, anomaly resolution, operations concept, etc. NASA's ISS OSMA was also given the responsibility to ensure payload safety so that no catastrophic experiment would be brought onboard. Similar to the shuttle effort, NASA developed a hazard analysis tree to capture the applicable hazards for each module or segment of the ISS with each module then evaluated against it. Similarly, the FMEA/CIL analysis was done for all components and integrated with the hazards analysis.

However, NASA quickly realized "integrated hazards" existed because of the distributed nature of the vehicle (e.g., Russian radio frequency high-power transmissions during a U.S.-based extravehicular activity, or EVA). These integrated system hazards were analyzed, mitigated (and controlled) by a joint agreement between the program participants.

The hazard analysis efforts resulted in a plethora of new crew procedures, flight rules, design modifications (e.g., Space Station Remote Manipulator System (SSRMS) "ALL STOP" button and software), software changes, material selection, test guidelines, and preflight test procedures.

NASA put into place a similar process to revisit those analyses when changes were made to the system, when anomalies and failures were reported in ground test or flight, and when environments or conditions changed. This documentation was also available to mission control personnel so that in flight issues could be assessed against the hazard analyses and CILs to determine appropriate steps or remediations in real time.

5.3 Identifying Hazards and Mitigation Efforts

Identifying hazards is the first and most crucial step in the process. Every foreseeable adverse consequence in the operation of a design, from the obvious fire/explosion hazards inherent to rocket design to potential energy release (e.g., springs, batteries, pyrotechnics), leaks of toxic materials, structural failure, premature activation of a function, failure of a function to perform when required, etc. must be identified. Once the hazards are identified, causes that can result in the hazard should be identified individually, allowing mitigation and verification for each cause. Historically, the worst-case result of a hazard determines the severity of risk associated with the hazard.

For example, a fire/explosion hazard may be caused by leakage in the rocket itself or an improper mixing ratio, but could also be caused by the systems that feed the rocket engine (tanks), ground systems supporting the rocket prior to launch, or other causes. By identifying the causes that can result in a catastrophic hazard, the design and procedural mitigations can manage the likelihood of worst-case consequences.

The most effective mitigation measures are by design improvements, including material selection, design margins against failure (e.g., structural margins), system design, adding redundancy, seals, or other actions. Therefore, it is important to begin the hazard identification process early in the design. Design mitigation is usually less expensive in the beginning, whereas it may become prohibitively expensive or even impossible later.

Once designs are optimized, other mitigations (in order of effectiveness) include: (1) safety devices/features like physical barriers, check valves, fire suppression systems, or software devices that shut down a process at certain indications; (2) monitoring and warning devices to allow for correction;

and (3) procedural methods to prevent and respond to hazardous results. Mitigations and safety devices are the most effective, but the most expensive and challenging to implement late in the design process, whereas warning and procedural mitigations are the easiest to implement, but are the least effective.

In the final evaluation, hazards, particularly those with the greatest severity, will likely require multiple mitigations in multiple categories to reduce risk to an acceptable level (see Section 5.4 for more on risk assessment). Operators can perform a preliminary risk assessment with identified mitigations to ensure there are sufficient controls in place to have an acceptable risk posture before moving forward with the design. Verification of intended implementation is typically the next step. Next, data collection and implementation of those mitigations are required to ensure the intended impact. Qualification testing, materials analyses, and analyses of systems and system interactions ensure a design functions as intended and includes the safety mitigations.

To be effective, the process must continue iteratively. A hazards analysis is a living document and requires an iterative approach as the system matures. Test and operational anomalies, as well as failures, are incorporated and addressed with corrective actions that may become part of the mitigations. Diligence is required to ensure that materials and designs originally qualified continue to be provided at the same level as originally specified and remain adequate for operational conditions, and that reused hardware still meets the qualifications originally imposed. Verifications can therefore be based on the original design or may require revisiting as new hardware is built or old hardware is used over multiple missions. Flight data with unexpected results, even if not catastrophic, but showing less margin or more extreme environments than predicted, may force revisiting the original mitigations and margins to address hazards.

Complacency is dangerous. Ensuring hazard reports and risk assessments remain valid and up to date is essential to ensuring a reasonable level of risk. In some cases, use of an independent organization to monitor and evaluate risk is effective and multiple government organizations do this. This allows for a perspective uninfluenced by schedule or economic pressure. However, no safety program is successful without the active involvement and commitment of the design personnel, operations personnel, and system level experts. Safety and risk reduction are collaborative efforts and most successful when all involved are committed to ensuring a system is as safe as reasonably possible. A strong safety culture is imperative.

The advantages to this type of risk mitigation system include the allowance of evaluations and maintenance of risk, and design changes. Additionally, operators can adapt it to address new hardware or reused hardware. It accommodates changes in an environment and provides a mechanism to allow anomalies and corrective actions to be incorporated into the existing risk landscape. Moreover, it is not limited to any particular system type or design. Variations can address software systems, hardware systems of significantly different designs, integrated systems, and specific safety equipment. The hazard format and usage can be different and still serve the same function: identification of hazards, mitigations, and verification of those mitigations, as well as an assessment of the resultant risk.

However, it is essential to understand that the risk assessment and mitigation system is most effective when adopted early in the design process. Additionally, it can only be effective if safety is considered a key element (i.e., that design changes to mitigate risk are given sufficient weight to be included in the process instead of relegated to incorporation after the design is mature and implementation is either risky itself or economically infeasible). Diligence is also required to ensure that the mitigations called out remain effective throughout the life of the system; are not negated by changes in hardware, processing, vendor, or reuse; that anomalies and disturbing observations from test and flight are addressed; and any changes are captured in the hazard and resultant risk assessment.

Identifying hazards and mitigating risks work best in an iterative and collaborative environment.

5.4 Assessing Risk

While the values and thresholds for acceptable risk vary from program to program, the basics of risk assessment remain essentially the same. Risk (or R) is generally defined as

$$R = \text{Severity} \times \text{Likelihood}.$$

Likelihood is often quantifiable and allows for objective comparison of risk and evaluation of what risks require further mitigation, whereas hazard analysis allows for identification of hazards and classification of the severity of problems, as well as determining if a hazard can be designed out and eliminated. Risk assessment deals with the management of those hazards that could not be eliminated by assessing the effectiveness of controls on reducing the likelihood of the hazard manifesting, or manifesting in the worst-case condition. As risk is determined by a combination of severity and likelihood, the best way to reduce the risk for a catastrophic or other high consequence hazard that cannot be eliminated is to reduce the likelihood.

Operators can use design choices, safety devices, warning/monitoring, and procedural mitigations to reduce the likelihood of the worst-case repercussions. Like hazard analysis, the risk assessment process is best started early in the design process as different mitigations can be assessed and pursued based on effectiveness and then continued through the entire design process. Additionally, as designs often require choices and trade-offs, focus can be on the highest risks and allow for implementing those mitigations when they are least expensive to implement and when any repercussions to other systems are most easily accommodated. An example is redundancy. Redundancy adds complexity, cost, and weight to a design. By being able to assess the risk of various components or subsystems within a system, it becomes easier to determine what components/subsystems merit redundancy and which ones can be built without it, perhaps by making a more robust design or improving a characteristic.

While companies or regulators can define what is reasonably acceptable and practicable, it is important that the risks, especially within a program, are subject to similar thresholds and standards to allow for comparison of risk and for ensuring most critical risks are addressed properly. Levels can be qualitative or quantitative, but there are advantages to moving to a quantitative level as systems mature. It is the most easily verifiable, so therefore more robust if changes or future anomalies appear, and can be assessed and compared to the original levels.

The risk matrix in Table 5 is modeled after AC 120-92B. Variations exist, but the concept tends to remain the same across industries. Note that the risk matrix is by nature backward looking.

Table 5. Probability Definitions

Value	PROBABILITY	ICAO SMM	FAA ARP Internal Order 5200.11A	Commercial HSF (suggested)
1	Extremely Improbable	Almost inconceivable that the event will occur	Expected to occur < every 100 years	Potential hazard is essentially eliminated
2	Improbable/ Extremely Remote	Very unlikely to occur (not known to have occurred)	Expected to occur once every 10–100 years or 25 million departures, whichever occurs sooner	So unlikely it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission
3	Remote	Unlikely to occur, but possible (has occurred rarely)	Expected to occur about once every year or 2.5 million departures, whichever occurs sooner	Unlikely, but possible to occur in the life of an item, with a likelihood of occurrence less than 10^{-5} but greater than 10^{-6} in any one mission
4	Occasional	Likely to occur sometimes (has occurred infrequently)	Expected to occur about once every month or 250,000 departures, whichever occurs sooner	Likely to occur sometime in the life of an item, with a likelihood of occurrence less than 10^{-3} but greater than 10^{-5} in any one mission
5	Frequent	Likely to occur many times (has occurred frequently)	Expected to occur more than once per week or every 2,500 departures, whichever occurs sooner	Likely to occur often in the life of an item, with a likelihood of occurrence greater than 10^{-3} in any one mission

SMM = Safety Management Manual ARP = Office of Airports

5.5 Risk matrix examples

Likelihood probability values are one way to further refine a risk matrix. Industry or the FAA can define the values. Probability values shown in Table 6 are based on AC 450.103-1. An operator might use a qualitative probability early in the design process and move to a quantitative one as the design matures. However, for effective risk assessment, it is best if the final risk characterization remains consistent within a system or as a standard.

Table 6. Severity Definitions

Value	Severity	ICAO SMM	FAA ARP Internal Order 5200.11	Commercial HSF (suggested)
A	Catastrophic	• Equipment destroyed • Multiple deaths	• Complete loss of aircraft and/or facilities or fatal injury in passenger(s)/ worker(s); or • Complete unplanned airport closure and destruction of critical facilities; or • Airport facilities and equipment destroyed	• Complete loss of spacecraft, facilities, or equipment • Fatal injuries in spaceflight participants, crew, government astronauts, and/or workers
B	Hazardous	• A large reduction in safety margins, physical distress, or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely • Serious injury • Major equipment damage	• Severe damage to aircraft and/or serious injury to passenger(s)/ worker(s); or • Complete unplanned airport closure, or • Major unplanned operations limitations (e.g., runway closure); or • Major airport damage to equipment and facilities	• Severe damage to spacecraft, facilities, or equipment • serious injury to spaceflight participants, crew, government astronauts and/or workers
C	Major	• A significant reduction in safety margins, reduced ability of the operators to cope with adverse operating conditions as a result of an increase in workload or of conditions impairing their efficiency • Serious incident • Injury to persons	• Major damage to aircraft and/or minor injury to passenger(s)/worker(s); or • Major unplanned disruption to airport operations; or • Serious incident; or • Reduction of the airport's ability to deal with adverse conditions	• Major damage to spacecraft, facilities, or equipment • Major injury to spaceflight participants, crew, government astronauts and/or workers

Value	Severity	ICAO SMM	FAA ARP Internal Order 5200.11	Commercial HSF (suggested)
D	Minor	• Nuisance • Operating limitations • Use of emergency procedures • Minor incident	• Minimal damage to aircraft; or • Minor injury to passengers; or • Minimal unplanned airport operations limitations (e.g., taxiway closure); or • Minor incident involving the use of airport emergency procedures	• Minor damage to spacecraft, facilities, or equipment • Minor injury to spaceflight participants, crew, government astronauts and/or workers
E	Negligible	• Few consequences	• No damage to aircraft, but minimal injury or discomfort of little risk to passenger(s) or workers	• No damage to spacecraft, facilities, or equipment • Minimal injury or discomfort to spaceflight participants, crew, government astronauts and/or workers.

SMM = Safety Management Manual ARP = Office of Airports

Each NASA program may have a slightly different risk score card implementation based on the complexity and risk associated with a particular program. However, all have the same fundamental properties. Typically, the more complex and human-based a program is, the more complex the risk score card.

5.6 Other Safety Program Options

Another useful tool for safety programs is evaluating lessons learned from testing and early design efforts. This helps ensure optimized designs and documentation of failures so that different personnel or future programs are informed. Evaluation of lessons learned from human spaceflight are available publicly and provide insight into catastrophic failures and potentially catastrophic failures. Understanding successful systems and controls in adverse conditions is as important as understanding the fatal failures.

6. Role of the FAA in Safety Frameworks for cHSF

6.1 Public and Private Sector Alignment

The emerging commercial space transportation industry has been convened through the Commercial Space Transportation Advisory Committee (COMSTAC) advisory group operating under the Federal Advisory Committee Act (FACA). COMSTAC issued a Safety Working Group report, in draft, that concluded "...Once the moratorium on new human spaceflight regulations, currently in force until 2023, expires (or if it should be terminated for any reason), an evolved safety framework must provide the basis for systems and operations that instill public confidence." The report goes onto to state "...FAA has a critical role in ensuring the safety of human spaceflight while establishing a safety framework that enables flexibility for industry to continue with innovation."[33] While COMSTAC is the recognized FACA advisory committee, other industry groups have been either convened or formed to develop industry-driven solutions to commercial space transportation during the "learning period" established by Congress under the Commercial Space Launch Competitiveness Act (CSLCA).[34] The combined initiatives and reports of the industry groups provide a foundation on which to build a human spaceflight safety framework that provides both innovation flexibility and FAA engagement to build confidence in the fledgling industry.

The industry-driven initiatives to create consensus on human spaceflight include multicompany membership organizations for standards setting [35], safety guidelines policy papers [36], and international. global data exchange agreements endorsed by the U.S. Space Command.[37] The FAA has convened meetings or working groups to discuss shared concepts and invest in collaborative research and development for technology-based solutions, including safety measures and data generation [38]. The NIST has convened events to harmonize emerging standards.[39] The combined approach of industry-driven initiatives with government support and investment was designed to maximize both innovation and build industry consensus as the learning period draws to a close. The outcome of the collective industry initiatives is a mix of progress toward a consensus-driven safety framework, offset by a lack of a single industry voice to reconcile existing differences in scope, concepts of mission operations, technology standards, and risk mitigation.

The FAA leadership role should be to build on industry progress by aligning stakeholders around a safety framework that evolves based on cocreated, data-based evidence. The future capability of the commercial spaceflight industry requires the FAA to build on the industry progress by aligning all the stakeholders to create a shared Human Spaceflight Safety Framework that evolves based on innovation supported by cocreated, data-based evidence. This approach maximizes building on the private sector leadership and safety agreements built during the learning period while recognizing the distinct role of the FAA to provide a leadership role similar to that in aviation that created alignments such as the Safe Skies Initiative.[40] The core elements of the FAA leadership include:

- **Convening**. The convening of stakeholders that collectively define and implement human safety within an industry.

- **Facilitating**. Providing objective facilitation among the stakeholders to create agreement on key concepts, principles, practices, and ongoing implementation.

- **Creating.** Generating the studies and data necessary to support a fact-based, objective debate necessary to establish guidelines that can be applied in multiple venues, including standards.

- **Maintaining**. Building and maintaining ongoing research, development, testing, and evaluation capabilities necessary for continuous improvement of the safety framework and content.

- **Extending.** Extending the safety framework through international agreements and organizations to maximize collective global safety for space operations (e.g., space debris, including human spaceflight safety).

These elements are reflected in the best practice for collaborative, public/private partnership processes to meet public benefits through private sector actions.[41]

6.2 Understanding System Risk and Mitigation

The COMSTAC Safety Working Group draft report recognized the "FAA has a critical role in ensuring the safety of human spaceflight. ... In the absence of clear and sufficient regulation, safety risk might negatively impact growth of the industry."[41] This critical role reflects the macroscale responsibility of the FAA to address these safety needs:

- **Understand Systemic Risks.** The economic-technological-social complexity of commercial space transportation will require the ability to identify systemic risks from possible human spaceflight failures, such as public reaction resulting in policy pressure to limit flight capacity or financial sector reaction that reduces availability of long-term and working capital.

- **Convene All Stakeholders.** The range of stakeholders in human spaceflight safety will require convening commercial space transportation companies and economic sectors that are industry inputs. This includes, for example, the aerospace parts and materials companies currently serving aviation, financial and risk management organizations at risk with the startup industry, and educational institutions developing the expertise necessary to maintain and grow the sector.

- **Facilitate Collaborative Agreement.** The different safety definitions and approaches will require facilitating the companies, industry groups, investors, and others currently working on distinct elements of the safety framework. This will also require ongoing facilitation to maintain and evolve the safety framework with content, including standards, best practices, or data exchange arrangements.

- **Invest in Continuing Innovation, Monitoring, and Maintenance.** The need for ongoing innovation and data-based insights will require investment in facilities, personnel, and experts that can provide independent research, development, testing, and evaluation, similar to the FAA's Technical Center for Aviation. The monitoring capabilities would be scoped to be macroprudential to supplement, rather than duplicate, the internal safety and risk management systems of the private commercial space transportation companies.

6.3 Precedents for this Role and Approach: Safer Skies Initiative, NextGen Transformation

The FAA has multiple successful aviation precedents of a collaborative leadership and implementation role in advancing safety concurrent with industry innovation. This is reflected in the FAA Integrated Oversight Philosophy, which balances regulation with encouragement of voluntary standards and nonpunitive, advisory, and learning approaches to implement a collaborative consciousness to create culture for safety.

The aviation precedents that reflect and build to support this approach include:

- **Safer Skies Initiative.** The Safer Skies Initiative was a FAA-led nationwide collaboration that encompassed the public, private, and academic sectors to identify and create solutions to the root causes of commercial and general aviation accidents. The GAO report reviewing the results stated that the "... FAA is coordinating the Safer Skies Initiative with other safety activities conducted throughout the agency, in partnership with the aviation industry, and by other federal agencies." [40]

- **NextGen Transition-Joint Planning and Development Office-Industry Collaboration Teams.** The FAA undertook the transformation of the nation's airspace traffic and management system from a controller-direct, radar-monitor-based approach to a shared traffic decision system using tracking by GPS, supported by a real-time, digital communications network. This transformation was called Next Generation Air Transportation System (NGATS) and the FAA led the formation of a multidepartmental group called the Joint Planning and Development Office (JPDO) that undertook the planning, including safety, in concurrence with multiple aviation industry working groups.[43]

- **AIR AGATE-Link to FAA Certification Requirements-AGATE Alliance.** The FAA formed a certification guidance work team within a broader, multiparty, research and development alliance for the general aviation industry that was initiated by NASA. The work team, known as the Aircraft Certification Service (AIR) Advanced General Aviation Transportation Experiments (AGATE), "... met collectively with industry technical counterparts within the AGATE Alliance to review the type and quality of information necessary to establish standards that could support possible certification guidelines." The creation of a national group provided for an increased level of consistency when applying such standards and certification guidelines by the FAA. The ability of industry specialists to collectively discuss technical standards with the FAA permitted private corporations to effectively plan product innovations for future review according to FAA expectations. This, in turn, resulted in lower certification costs and better conformance to FAA certification guidelines.[44]

7. Definitions

Modeled after FAA definitions

Accident. An unexpected event that causes damage, injury, or harm.

ALARP. The risk is mitigated to the extent that is "as low as reasonably practicable." Note it is "practicable," not "possible."

Hazard. Any existing or potential condition that can lead to injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. *Note: environmental issues are not usually within the scope of an SMS.*

Incident. Any unexpected event that does not result in serious losses or injury.

Risk. The composite of predicted severity (how bad) and likelihood (how probable) of the potential effect of a hazard in its worst credible (reasonable or believable) system state. Risk assessment is subjective, typically based on qualitative rather than quantitative criteria.

Risk Control. A means to reduce or eliminate the effects of hazards.

Safety. Freedom from risk.

Safety Assurance (SA). Processes within the SMS that function systematically to ensure the performance and effectiveness of safety risk controls and that the organization meets or exceeds its safety objectives through the collection, analysis, and assessment of information.

Safety Management System (SMS). The formal, top-down, organization-wide approach to managing safety risk and ensuring the effectiveness of safety risk controls. It includes systematic procedures, practices, and policies for the management of safety risk.

Safety Objective. A measurable goal or desirable outcome related to safety.

Safety Performance. Realized or actual safety accomplishment relative to the organization's safety objectives.

Safety Policy. The certificate holder's documented commitment to safety, which defines its safety objectives and the accountabilities and responsibilities of its employees regarding safety.

Safety Promotion. A combination of training and communication of safety information to support the implementation and operation of an SMS in an organization.

Safety Risk Management (SRM). A process within the SMS composed of describing the system, identifying the hazards, and analyzing, assessing, and controlling risk.

8. References

[1] Fleming, M., *Safety Culture Maturity Model,* Offshore Technology Report Series, HSE Books, January 14, 2001.

[2] "40 Years of Safer Aviation through Reporting," NASA, September 29, 2016, https://phys.org/news/2016-09-years-safer-aviation.html.

[3] Stolzer, A. J.; C. D. Halford; and J. J. Goglia, *Safety Management Systems in Aviation,* p. 62, Ashgate Publishing, 2008.

[4] Air Line Pilots Association. Interview, April 13, 2022.

[5] "ASAP vs. ASIAS vs. ASRS: Safety Reporting Programs Uncovered," ARC Safety Management, https://arcsky.com/arc_blog/asap-vs-asias-vs-asrs/.

[6] "Presenting the Standard for Safety for the Evaluation of Autonomous Vehicles and Other Products," Underwriters Laboratories Standards and Engagement, https://ulse.org/UL4600.

[7] UK Ministry of Defense (MoD), *Requirements for Safety Related Software in Defense Equipment*, Defense Standard 00-55, August 1997.

[8] *Habli, I.; M. Sujan; S. Gerasimou; E. Schoitsch; and F. Bitsch, Computer Safety, Reliability, and Security. SAFECOMP 2021 Workshops: DECSoS, MAPSOD, DepDevOps, USDAI, and WAISE, York, UK, September 7, 2021, Proceedings*, Lecture Notes in Computer Science Series, Volume 12853, Switzerland: Springer Cham, Springer Nature Switzerland, Springer International Publishing, 2021.

[9] FAA Safety Briefing, *Compliance Philosophy*, General Aviation Joint Steering Committee Safety Enhancement Topic AFS-850 16_10, FAA Aviation Safety, Federal Aviation Administration, 2016, https://www.faa.gov/news/safety_briefing/2016/media/SE_Topic_16-10.pdf.

[10] "Aviation Safety: Actions Needed to Evaluate Changes to FAA's Enforcement Policy on Safety Standards," GAO-20-642, Government Accountability Office, August 18, 2020, https://www.gao.gov/products/gao-20-642.

[11] U.S. Government Accountability Office, *Commercial Space Transportation: FAA Continues to Update Regulations and Faces Challenges to Overseeing an Evolving Industry, Statement of Heather Krause*, GAO-21-105268, Testimony Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives June 16, 2021, https://www.gao.gov/assets/720/715062.pdf.

[12] "Compliance, Enforcement, and Mishap," Federal Aviation Administration, last modified September 23, 2021, https://www.faa.gov/space/compliance_enforcement_mishap.

[13] "Commercial Space Investigations," National Transportation Safety Board Notice of Proposed Rulemaking, Document Citation 86 FR 63324, CFR 49 CFR 831, Docket No. NTSB-2021-0008, RIN 3147-AA19, Document No. 2021-24766, November 16, 2021, https://www.federalregister.gov/documents/2021/11/16/2021-24766/commercial-space-investigations.

[14] National Transportation Safety Board, *Aerospace Accident Report: In-Flight Breakup During Test Flight, Scaled Composites SpaceShipTwo, N339SS, Near Koehn Dry Lake, California, October 31, 2014*, NTSB/AAR-15/02, PB2015-105454, Washington, D.C., July 28, 2015, https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1502.pdf.

[15] "1975 Reimbursable Memorandum of Understanding Between Department of Transportation and National Transportation Safety Board," Pipeline and Hazardous Materials Safety Administration, March 5, 1975, https://www.phmsa.dot.gov/about-phmsa/1975-reimbursable-memorandum-understanding-between-dot-and-ntsb.

[16] "Memorandum of Understanding Between the National Transportation Safety Board, Department of the Air Force and Federal Aviation Administration Regarding Space Launch Accidents," Federal Aviation Administration, September 2004, https://www.faa.gov/space/legislation_regulation_guidance/media/mou_space_launch_accidents.pdf.

[17] "Aerospace Safety Advisory Panel Annual Report for 2018," NASA Aerospace Safety Advisory Panel, National Aeronautics and Space Administration, NP-2018-12-2655-HQ, pp. 3 and 38, January 1, 2019, https://oiir.hq.nasa.gov/asap/documents/2018_ASAP_Report-TAGGED.pdf.

[18] "Commercial Space Investigations," Document ID NTSB-2021-0008-0001, Docket No. NTSB-2021-0008, National Transportation Safety Board, November 15, 2021, https://www.regulations.gov/document/NTSB-2021-0008-0001/comment.

[19] Johnson, E. B., and F. Lucas, "Congress of the United States, House of Representatives, Committee on Science, Space, and Technology Letter," Washington, D.C., April 6, 2022, https://republicans-science.house.gov/_cache/files/6/2/623a9a53-1e94-4364-bfc5-b26831ab7db8/3D1A03297C1D292E540655A82F6E2D5B.2022-04-06-ebj-fdl---biden-ntsb.pdf.

[20] Nield, G.; M. Toure; J. Sloan; and D. Gerlach, "Certification versus Licensing for Human Space Flight in Commercial Space Transportation," *63rd International Astronautical Congress*, IAC-12-D6.1.3, Naples, Italy, 2012. https://www.faa.gov/space/additional_information/international_affairs/media/Certification_vs_Licensing_Nield_FAA-IAC-Naples-Oct-2-2012.pdf.

[21] Masson-Zwaan, T.; R. Moro-Aguilar; and A. Lentsch, "The Future Regulation of Suborbital Flight in Europe," *Space Policy*, Volume 30, Issue 2, pp. 75-82, 2014, https://www.sciencedirect.com/science/article/abs/pii/S0265964614000101.

[22] "Regulatory Perspectives on Emerging Higher Airspace Users," Di Antonio, G., EUROCONTROL, October 20, 2021, https://www.eurocontrol.int/article/regulatory-perspectives-emerging-higher-airspace-users.

[23] "Airworthiness Certification," Federal Aviation Administration, last modified June 29, 2022, https://www.faa.gov/aircraft/air_cert/airworthiness_certification/.

[24] Masson-Zwaan, T., and M. Hofmann, "Chapter 6: Human Space Flight," *Introduction to Space Law, Fourth Edition*. Alphen aan den Rijn, the Netherlands: Kluwer Law International, January 11, 2019.

[25] Clément, G. R., *Fundamentals of Space Medicine, Second Edition*, Microcosm Press and Springer Science+Business Media, LLC, El Segundo, California, 2011.

[26] Clément, G. R., and M. F. Reschke, *Neuroscience in Space*, Springer Science+Business Media, LLC, New York, New York, 2008.

[27] "Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of the United States of America Concerning Cooperation on the Civil International Space Station," The Aerospace Corporation, January 29, 1998, https://aerospace.org/sites/default/files/policy_archives/Space%20Station%20Intergovernmental%20Agreement%20Jan98.pdf.

[28] "United Nations: General Assembly Resolution Principles Relevant to the Use of Nuclear Power Sources In Outer Space, Resolution 47/68, 32 I.L.M. 917 (1993)+, The Aerospace Corporation, December 14, 1992, https://csps.aerospace.org/sites/default/files/2021-08/Principles%20on%20Nuclear%20Power%20Sources%20in%20Space.pdf.

[29] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," United Nations General Assembly Resolution 2222 (XXI), United Nations Office for Outer Space Affairs, October 10, 1967, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

[30] "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies," United Nations General Assembly Resolution 34/68, United Nations Office for Outer Space Affairs, July 11, 1984, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html.

[31] International Maritime Organization, https://www.imo.org/.

[32] International Civil Aviation Organization, https://www.icao.int/Pages/default.aspx.

[33] U.S. Department of Transportation, Safety Working Group, Commercial Space Transportation Advisory Committee (COMSTAC), *Safety Working Group Report*, Federal Aviation Administration, Washington, D.C., September 2020, p. 1, accessed on June 9, 2022, https://www.faa.gov/sites/faa.gov/files/space/additional_information/comstac/presentations/COMSTAC_Safety_WG_white_paper_14_Sept_2020.pdf.

[34] "Section 111: Consensus Standards and Extension of Certain Safety Regulation Requirements," *Public Law 114-90, U.S. Commercial Space Launch Competitiveness Act*, p. 129 STAT. 709, Washington, D.C., November 25, 2015, https://www.congress.gov/114/plaws/publ90/PLAW-114publ90.pdf.

[35] ASTM International (formerly American Society of Testing and Materials), *Committee F47 Commercial Spaceflight*, Washington, D.C., accessed on June 10, 2022, https://share.ansi.org/Shared%20Documents/Standards%20Activities/Commercial%20Space%20Industry/December%207%2C%202020%20ANSI%20Informational%20Meeting%20-%20Standardization%20and%20the%20Commercial%20Space%20Industry/Final%20F47%20Pamphlet.pdf.

[36] Space Safety Coalition, *Best Practices for the Sustainability of Space Operations*, September 16, 2019, accessed on June 14, 2022, https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/Endorsement-of-Best-Practices-for-Sustainability_v42.pdf.

[37] "U.S. Space Command signs data-sharing agreement with Libre Space Foundation," Erwin, S., SpaceNews, July 3, 2021, accessed June 2, 2022, https://spacenews.com/u-s-space-command-signs-data-sharing-agreement-with-libre-space-foundation/.

[38] Hubbard, S., *Federal Aviation Administration Center of Excellence for Commercial Space Transportation Commercial Space Transportation Research Roadmap*, Washington, D.C., December 2015, http://coe-cst.org/wp-content/uploads/2020/04/2015-12-15-Updated-Research-Roadmap-Report.pdf.

[39] American National Standards Institute (ANSI), *Standardization and the Commercial Space Industry - Space Situational and Domain Awareness, Space Traffic Coordination and Management, and Orbital Debris Mitigation Meeting Report*, Washington, D.C., December 7, 2020.

[40] U.S. General Accounting Office, *Aviation Safety: Safer Skies Initiative Has Taken Initial Steps to Reduce Accident Rates by 2007*, Report to the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives, GAO/RCED-00-111, Washington, D.C., June 2000, https://www.gao.gov/assets/rced-00-111.pdf.

[41] Norment, R., and P. Masson, *Best Practices for Innovation Public-Private Partnerships (I-PPP), Decision and Formation Process*, National Council of Public/Private Partnerships, Report, p. 5, October 6, 2000.

[42] Federal Aviation Administration Commercial Space Transportation Advisory Committee, *Safety Working Group Report, Draft*, Washington, D.C., September 14, 2020, https://www.faa.gov/space/additional_information/comstac/media/COMSTAC_Safety_WG_white_paper_14_Sept_2020.pdf.

[43] U.S. Department of Transportation, Federal Aviation Administration, *Partners in the Next Generation Air Transportation System*, Briefing to Joint Planning and Development Office (JPDO) Executive Team, Diana Takata, Acting JPDO Chief Architect, Washington, D.C., April 28, 2010.

[44] Masson, P., "Link to FAA Certification Requirements," *An Assessment of the Effectiveness of the AGATE Program Management Model*, NASA Contractor Report NASA/CR-2005-213275, p. 27, Hampton, Virginia, July 2005, https://core.ac.uk/download/pdf/42756278.pdf.

[45] "Human-Rating Requirements for Space Systems (w/change 4 dated 8/21/2012)," NPR 8705.2B, National Aeronautics and Space Administration, May 6, 2008, https://nodis3.gsfc.nasa.gov/displayCA.cfm?Internal_ID=N_PR_8705_002B_&page_name=Chapter1.

[46] "Deaths by Transportation Mode, Passenger Death Rates, United States, 2007-2020," NSC Injury Facts, https://injuryfacts.nsc.org/home-and-community/safety-topics/deaths-by-transportation-mode/#:~:text=Additional%20data%20on%20the%20number,available%20by%20selecting%20Data%20Table.&text=The%20death%20rate%20per%20100,22%25%20to%200.56%20in%202020.

[47] "Aurora's Safety Case Framework," Aurora, https://safetycaseframework.aurora.tech/gsn.

[48] Federal Aviation Administration, *AC 120-92B - Safety Management Systems for Aviation Service Providers*, Washington, D.C., January 8, 2015,

https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/1026670.

[49] Stolzer, A. J., and J. J. Goglia, *Safety Management Systems in Aviation, 2nd Edition*, Routledge, August 10, 2015.

[50] "Title 51 – National and Commercial Space Programs, Subtitle VII - Access to Space, Chapter 707 – Human Space Flight Independent Investigation Commission, Sec. 70702 - Establishment of Commission," Pub. L. 111-314, §3, Dec. 18, 2010, 124 Stat. 3432, *United States Code, 2012 Edition*, https://www.govinfo.gov/app/details/USCODE-2012-title51/USCODE-2012-title51-subtitleVII-chap707-sec70702.

[51] "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies," RES 34/68, United Nations Office for Outer Space Affairs, December 5, 1979, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html.

[52] "Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation," National Conference of State Legislators, February 18, 2020, https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

[53] "Navigating Toward Safer Deployments," Automated Vehicle Safety Consortium, 2022, https://avsc.sae-itc.org/#roadmap.

[54] "Autonomous Vehicles Readiness Index," KPMG, July 2020, https://home.kpmg/xx/en/home/insights/2020/06/autonomous-vehicles-readiness-index.html.

[55] "Memorandum of Understanding Between the Federal Aviation Administration (FAA) and the National Aeronautics and Space Administration (NASA) for Achievement of Mutual Goals in Human Space Transportation," National Aeronautics and Space Administration, Washington, D.C., January 4, 2012, https://www.nasa.gov/sites/default/files/files/NASA-FAAMOU_signed.pdf.

[56] "Memorandum of Understanding Between the National Aeronautics and Space Administration and the Federal Aviation Administration Regarding Achievement of Mutual Goals in Commercial Space Activities," Federal Aviation Administration, Washington, D.C., January 4, 2021, https://www.faa.gov/space/legislation_regulation_guidance/media/FAA_MOU_signed_by_NASA_and_FAA.pdf.

[57] "Statement of Rear Admiral Paul E. Sullivan, U.S. Navy Deputy Commander for Ship Design, Integration and Engineering, Naval Sea Systems Command, Before the House Science Committee on the SUBSAFE Program," Thresher Base: United States Submarine Veterans Incorporated, Washington, D.C., October 29, 2003, https://www.thresherbase.org/assets/subsfafe-radm-paul-e.-sullivan.pdf.

[58] "Report of Columbia Accident Investigation Board, Volume I," National Aeronautics and Space Administration, August 26, 2003, https://www.nasa.gov/columbia/home/CAIB_Vol1.html.

[59] "Cyclops 1: 5-Person Submersible | 500 Meters," OceanGate, 2015-2022, http://www.oceangate.com/pdf/oceangate-cyclops-2.pdf.

[60] Naval Sea Systems Command, *Naval Sea Systems Command, System and Certification Procedures Criteria Manual for Deep Submergence Systems, SS800-AG-MAN-010/P-9290, Rev. A*, Washington Navy Yard, D.C., November 3, 1998.

[61] Webb, D. W.; G. S. Williams; A. Q. Tu; R. W. Seibold; C. E. Baker; and R. M. Young, "Market Demand Methodology for U.S. Suborbital Reusable Launch Vehicle Industry," AIAA paper 2014-4201, American Institute of Aeronautics and Astronautics, *Space 2014 Conference and Exposition*, San Diego, CA, August 4–7, 2014.

[62] UK Civil Aviation Authority, *Global Fatal Accident Review, 2002 to 2011*, CAP 1036, London, UK, June 2013. https://publicapps.caa.co.uk/docs/33/CAP%201036%20Global%20Fatal%20Accident%20Review%202002%20to%202011.pdf.

[63] U.S. Food and Drug Administration, *Appropriate Use of Voluntary Consensus Standards in Premarket Submissions for Medical Devices – Guidance for Industry and Food and Drug Administration Staff*, September 14, 2018, https://www.fda.gov/media/71983/download.

[64] American Society of Safety Professionals, *Position Statement of the Role of Consensus Standards and Governmental Regulations in Occupational Safety and Health*, Approved by the ASSP Board of Directors August 25, 1995, Reaffirmed June 2018, https://www.assp.org/docs/default-source/standards-documents/assp-position-statement-on-consensus-standards.pdf?sfvrsn=8dcdb147_2.

[65] FAA Office of Commercial Space Transportation, *Interim Report on Voluntary Industry Consensus Standards Development, Report to Congress – January 2022*, January 14, 2022, https://www.faa.gov/sites/faa.gov/files/2022-01/PL_114-90_Sec_111_5_Voluntary_Industry_Consensus_Standards.pdf.

[66] Nield, G. C.; J. Sloan,; and D. Gerlach, "Recommended Practices for Commercial Human Space Flight," IAC-14-D6.1.2, *65th International Astronautical Congress*, Toronto, Canada, October 2014, https://www.faa.gov/space/additional_information/international_affairs/media/recommended_practices_human_space_flight_iac_toronto_nield_october_2014_508.pdf.

[67] FAA Office of Commercial Space Transportation, *Recommended Practices for Human Space Flight Occupant Safety, Version 1.0*, Washington, D.C., August 27, 2014, https://www.faa.gov/about/office_org/headquarters_offices/ast/media/Recommended_Practices_for_HSF_Occupant_Safety-Version_1-TC14-0037.pdf.

[68] National Transportation Safety Board and Federal Aviation Administration, *Memorandum of Agreement Between National Transportation Safety Board and Federal Aviation Administration Concerning Commercial Space Mishap Investigations*, Washington, D.C., September 9, 2022, https://www.ntsb.gov/legal/gc/Documents/NTSB-FAA-Commercial-Space-MOU.pdf.

[69] Dickson, Steve. Federal Aviation Administration comment letter to National Transportation Safety Board Notice of Proposed Rulemaking, January 14, 2022, https://www.regulations.gov/comment/NTSB-2021-0008-0017.

[70] Federal Aviation Administration, *Report to Congress: Interim Report on Voluntary Industry Consensus Standards Development–January 2022*, Washington, D.C., January 14, 2022, https://www.faa.gov/sites/faa.gov/files/2022-01/PL_114-90_Sec_111_5_Voluntary_Industry_Consensus_Standards.pdf.

[71] Office of the Federal Register of the National Archives and Records Administration, “National Transportation Safety Board, 49 CFR Part 831, Docket No. NTSB-2021-0008, RIN 3147-AA19, Commercial Space Investigations, Notice of Proposed Rulemaking,” *Federal Register, Vol. 86, No. 218*, Washington, D.C., November16, 2020, https://www.govinfo.gov/content/pkg/FR-2021-11-16/pdf/2021-24766.pdf.

Appendix A. The Team

Dr. Josef Koller

- Space policy systems director with focus on regulatory and commercial topics
- Cofounder of the Aerospace Space Safety Institute

Samira Patel

- Space policy analyst with focus on Earth observation and commercial space issues
- Supported the National Oceanic and Atmospheric Administration's Commercial Remote Sensing Regulatory Affairs office, including developing updated regulations for the licensing of private remote sensing systems and managing the Advisory Committee on Commercial Remote Sensing

Dr. Angie Bukley

- Aerospace engineer with NASA experience in various human spaceflight systems, including the ISS
- Extensive experience in parabolic flight studies of human neurophysiology [European Space Agency, Centre National D'études Spatiales (CNES), and Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center, or DLR)]

Stephanie Barr

- Human spaceflight expertise (33 years) with 17 years specific to safety, including expertise in micrometeroid/orbital debris, space shuttle main engine, extravehicular activity (EVA), and overall system safety—published multiple International Association for the Advancement of Space Safety (IAASS) papers on these topics
- Participated in 2008 study, "Analysis of Human Space Flight Safety—Report to Congress"

Lee Graham

- Recently retired from NASA-Johnson Space Center (JSC)—20 years relevant experience, former ISS Program Safety and Mission Assurance Manager
- Key leader of NASA Commercial Crew Program (CCP) and Suborbital Crew (SubC) office

Bob Seibold

- Managed approximately 50 tasks for FAA's Office of Commercial Space Transportation (AST)
- Led 2008 study, "Analysis of Human Space Flight Safety—Report to Congress"
- Background research on human spaceflight safety for NASA Flight Opportunities program—summarized in 2019 IAASS paper

Catrina A. Melograna, J.D., LL.M.

- Project engineer – Civil Space Programs
- Air and Space Law LL.M.

Consultants

- Dr. George Nield
- Paul Masson

Appendix B. Task Description

Objectives

The objective of the Commercial Human Space Flight Safety Framework report is to provide the FAA with an updated human spaceflight safety report in preparation for a report submitted to Congress.

The CSLCA, Section 50905(c)(7), requires the U.S. Department of Transportation (DOT) to provide a report that identifies the activities most appropriate for a new safety framework that may include regulatory action, if any, and a proposed transition plan for such a safety framework. The report shall be drafted with inputs from COMSTAC.

Tasks and Deliverables

In support of AST, The Aerospace Corporation will:

1. Provide an assessment and recommendations for the human spaceflight regulatory framework.

2. Provide an assessment of the risks associated with commercial human spaceflight.

3. Support AST development of a draft report for AST Associate Administrator approval that assesses regulation and licensing processes that may be applicable to addressing commercial human spaceflight activities.

The deliverables are outlined in Table B-1.

Table B-1. Deliverables

Task	Deliverable/Milestone	Anticipated Due Date
1	Kickoff Meeting	10 days after task release
2	Draft Report	April 15, 2022
3	Final Report	July 15, 2022
4	Monthly project status and financial reports	Through End of Work Plan term

Period of Performance: January 10 – October 30, 2022

Appendix C. List of Interviews

- George Nield (Commercial Space Technologies)—March 6, 2022
- Darrell Pennington, Randy Kenagy, and Ed Hahn (Air Line Pilots Association, or ALPA)—April 1, 2022
- Bill Tuccio (Southern California Safety Institute)—April 1, 2022
- CDR Jason Kling (Cruise Ship National Center of Expertise, Coast Guard)—April 4, 2022
- Robert Geske (Aircraft Owners and Pilots Association, or AOPA)—April 8, 2022
- Jean-François Clervoy and Thierry Gharib (Novespace, FR)—April 12, 2022
- Keith Phillips, Fran Pizzonia, Randy Kenagy, Darrell Pennington, and Elisabeth Zurek (ALPA)—April 13, 2022
- Chris Cooper (AOPA)—April 15, 2022
- Phil McAlister (NASA)—April 21, 2022
- Mark Hitt (Space Perspective)—May 5, 2022
- Andrew Humphreys (Zero-G Corp.)—May 17, 2022
- Tim Alatorre and Eric Ward (Orbital Assembly Corporation)—May 31, 2022

Appendix D. Case Studies

Case Study 1: Cruise Ship Tourism

> When anyone asks me how I can best describe my experiences of nearly forty years at sea, I merely say uneventful. Of course, there have been Winter gales and storms and fog and the like, but in all my experience I have never been in an accident of any sort worth speaking about. I have seen but one vessel in distress in all my years at sea, a brig, the crew of which was taken off in a small boat in charge of my third officer. I never saw a wreck and have never been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort.
> I will say that **I cannot imagine any condition which could cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel**. Modern shipbuilding has gone beyond that."
>
> – E.J. Smith, Captain of the Titanic, 1912
> [1503 Titanic passengers died on April 14-15, 1912]

Titanic Captain E.J Smith did not imagine that an incident like the sinking of the Titanic could happen, and yet it became the most well-known and fatal cruise ship accident in history. It eventually led to the development of the International Convention for Safety of Life at Sea, which, among other things, implemented lifeboat protection for all passengers—a lesson learned from the disaster of Titanic.

In addition to providing lifeboat protection, safe cruise ship passage now sets standards for everything from reasonable search and rescue of passengers to international crime and biosecurity incidents, such as disease control, piracy, illegal trafficking of goods and persons, and environmental damages. All of these building blocks to safety now contribute to keeping incidents like the Titanic from happening again and build consumer confidence and trust.

Building Blocks of Safety in the Cruise Industry

There are many building blocks of safety within the cruise industry. At the international level, standards of safety are primarily promulgated within the International Convention for Safety of Life at Sea (SOLAS). SOLAS has 164 signatories, which covers 99% of merchant ships, including cruises. It addresses design safety standards, fire safety, life-saving devices, search and rescue, navigation safety and more.

SOLAS is administered by the International Maritime Organization (IMO), which also manages many other programs, conventions, and guidelines that help improve safety within the industry. This includes other safety treaties that deal with load lines and collision prevention, search and rescue, and training programs, such as the Standards of Training, Certification and Watchkeeping for Seafarers (STCW Convention) program.

Cruise ships require a high level of international coordination, especially as ships go from the port of one country to another. Cruise lines operate across the world, but because their primary activity is at sea in international waters, they are subject to international treaties that govern operations at sea.

Simultaneously, cruise ships are also subject to the individual jurisdictions of the countries within which they are registered (flag states) and permitted (port states). For example, ships subject to United States law are subject to inspections and strong search and rescue laws administered by the U.S. Coast Guard.

Third-Party Technical Expertise: Classification Societies

Cruise lines, subject to many of the same standards as shipping, have a long history of using third-party technical expertise. This is in part due to the amount of coordination required and stakeholders involved, including manufacturers, ship operators, ship personnel, passengers, insurers, multicountry government personnel, and more. In shipping, and by extension cruise ships, this is highlighted by the role of *classification societies*, which are third parties that conduct inspections on behalf of port cities and flag states. They are involved in many aspects of the construction and operation of ships, establishing technical rules and guidelines for those ships, as well as issuing certifications to meet those standards. In fact, insurance companies require these certifications before providing insurance.

This stems out of a long history of coordination efforts, particularly in the late 17th century, when London merchants, shipowners, and captains often gathered at Edward Lloyd's coffee house to discuss shipping issues. It eventually led to the development of Lloyd's Register, the first register to classify the condition of ship hulls and equipment. Prior to this development, two separate registers were used by shipowners and underwriters (insurance and other financial institutions), and eventually merged into one: Lloyd's Register.

There continues to be a symbiotic relationship between insurers and classification societies, whereby insurance companies may require a ship to be classed by one of the main classification societies. This example also shows the history of coordination between four power groups: shipowners, captains, merchants, and underwriters. The effect of having multiple stakeholders and third-party involvement is to distribute risk and interests, which makes the overall system safer. It also counterbalances other interests, such as profits, shareholders, and competition, and provides macroeconomic system stability.

While classification societies are the most integral to ship operations, other third-party organizations, such as trade associations like the Cruise Lines International Association (CLIA), also promote issues of safety. CLIA primarily does this by issuing annual safety reports and promoting voluntary reporting of incidents.

Comparison to Commercial Human Spaceflight

The cruise sector is a very mature market as cruise ships have been operating for at least 200 years, with P&O Cruises (UK) the first to offer passenger cruising services in between the 1820s and 1840s. As a result, they have focused on the most critical aspects of passenger safety at sea. In contrast, cHSF is an emerging market and does not have the benefits of lessons learned stemming from the mistakes and disastrous incidents in cruising, such as the sinking of the Titanic.

Much like cHSF, cruises operate in "remote" commons (sea and space) and the passengers are not operators. This increases operators' liability, and as seen in cruise ships, there are strong requirements for performing reasonable search and rescue in the event that something happens to a passenger. Table D-1 compares cruise ship tourism to space tourism.

Table D-1. Comparison of Cruise Ship Tourism and Space Tourism

	Operations	Reason	Danger to Uninvolved 3rd Parties	Reporting System	Level of Regulation	International Coordination	Unique Vehicles or Mass Produced
Space Tourism	Controlled by operator	Adventure and research	During launch and reentry	N/A	N/A, emerging market	No	Unique
Cruise Ships	Controlled by operator; manufacturer separate from operator	Leisure	In harbor, but low risk	Yes	Highly regulated	Yes	Unique to operator, but standards in place

While cHSF currently does not require the same level of coordination as shipping activities, the role of classification societies provides a useful model for the role of third parties. These are also platforms where experts, inspectors, and owner/operators can meet (currently on a monthly basis) to discuss new innovations in design and technology that might impact safety. How the cHSF market will handle the intersection between technological design and innovation and safety will be critical to its future.

Case Study 2: Autonomous Vehicles

> Delivering self-driving cars at scale isn't just about winning the tech race, it's about winning the tech race and the trust race.
>
> – Mo Elshenawy, VP at GM Cruise

According to the U.S. National Safety Council, automobile accidents killed 42,060 people and seriously injured 4.8 million more in 2020. For many in the autonomous vehicle (AV) industry, the goal is to eliminate these fatalities and accidents, making improving general automobile safety a core mission. While there are currently no fully autonomous vehicles available for purchase, many cars have increasingly built-in driver assistance technologies for the very purpose of saving lives and preventing injuries (i.e., collision avoidance systems). Road and traffic safety is key to the mission and an end goal for many AV companies.

Therefore, when incidents do occur, such as the fatality in Arizona in 2018, it hugely impacts the emerging sector. This was also the first accident with an autonomous vehicle. The operator (Uber) removed all autonomous vehicle testing from Arizona as a result. The National Transportation Safety Board sharply criticized Uber, but ultimately, Uber was not found criminally responsible. Instead, the driver was charged with negligent homicide.

Building Blocks of Safety for Autonomous Vehicles

AV is unique from the other examples in that the "driver" is also a passenger. It is also unique in that much of its coordination and regulation is done at the state and local levels. Since 2018, a total of 15 states have enacted 18 AV-related bills and many more state governors have issued Executive Orders. [52] However, no autonomous vehicle may operate without a driver, who is still ultimately liable,

present to override any issues,. In the future, the car itself, with AI-enabled technology, would operate on its own.

At the national level, in the U.S., the DOT has ultimate authority over any nationwide standards and regulations. Within DOT, the National Highway Traffic Safety Administration (NHTSA) provides a federal AV policy (currently on Version 4.0), which includes vehicle performance guidance, a model state policy, and various regulatory tools and authorities. Primarily, this includes a Voluntary Safety Self-Assessment (VSSA), a self-reporting tool used by AV companies including Uber, Lyft, Aurora Technologies, and General Motors, whose reports are published on the NHTSA website.

The VSSA highlights 12 elements for achieving a set of listed safety goals: (1) system safety, (2) operational design domain, (3) object and event detection and response, (4) minimal risk condition, (5) validation methods, (6) human-machine interference, (7) cybersecurity, (8) crashworthiness, (9) post-crash automated behavior, (10) data recording, (11) consumer education and training, and (12) federal, state, and local laws.

Primarily, such data collection, reporting, and safety testing is industry led, and even internationally, we see governments working quite closely with companies to ensure that all necessary safety elements are in place.

Industry-Led Safety Example

The primary example of the AV sector's industry-led safety initiative is the Automated Vehicle Safety Consortium, which includes many of the same companies that are at the forefront of AV development. The members are actively involved in testing and on-road pilots of AVs and work together to develop the standards and best practices for automated vehicles. The consortium was formulated under SAE International, formerly the Society of Automotive Engineers, who provides automotive and engineering expertise, automotive safety benchmarks, and guidance on safety management systems. All best practice and safety materials are published on their website. [53]

One such member company, Aurora Technologies/Uber Advanced Technologies Group**,** has developed the first-of-its-kind *Safety Case Framework* for AVs. This framework promotes positive and progressive safety culture through five major goals: (1) proficient, (2) fail-safe, (3) continuously improving, (4) resilient, and (5) trustworthy. [47] Aurora uses this tool as a way of assessing the entire development lifecycle of their AVs, using it as a building block to assess against internal standards, and shares progress externally against set benchmarks.

Comparison to Commercial Human Spaceflight

Much like cHSF, AVs are an emerging market, but a subsector of a long-standing automotive industry with growing automated capabilities over time. From 1950 to 2000, the automotive industry continued to introduce safety convenience features, such as cruise control and antilock brakes, and now most cars have partially automated features. According to the NHTSA, they hope to see fully automated safety features by 2025 and beyond.

This is an industry that is also intimately intertwined with the ridesharing industry, for which the operator/driver is different from the passenger purchasing the ride. Presumably, the eventual goal is for passengers to purchase rides on AVs, cutting out a vehicle operator completely. This is quite different from cHSF, where the operator or "pilot" will likely continue to play a key role in the operations of the vehicle and require intensive technical training, much like in the aviation industry.

Finally, whereas many U.S. companies are leading the way on cHSF, the AV sector is a budding area of focus for many countries even though its governance is quite localized. Up to 25 other countries are

preparing for autonomous vehicles, including the Netherlands, Singapore, Norway, Germany, China, and more. KPMG has produced an annual report with details on its global development, called the *Autonomous Vehicles Readiness Index*. [54]

Approaches to AVs vary from country to country. For example, the Netherlands are attempting to test and award AVs driver's licenses (unsuccessful so far). Some countries have begun to introduce new rules for AV safety, with most countries in the pilot test phase. Some safety policy highlights include:

- South Korea: Autonomous Vehicles Act
- Canada: multilevel regulation at federal, provincial, and municipal levels
- China: Innovative Development Strategy of Intelligent Vehicles (includes safety standards)
- Netherlands: serving as testing ground for broader EU legislation
- UN: published a framework for AVs in 2019

A comparison of autonomous vehicles to space tourism can be found in Table D-2.

Table D-2. Comparison of Autonomous Vehicles for Space Tourism

	Operations	Reason	Danger to Uninvolved 3rd Parties	Reporting System	Level of Regulation	International Coordination	Unique Vehicles Or Mass Produced
Space Tourism	Controlled by operator	Adventure and research	During launch and reentry	N/A	N/A, emerging market	No	Unique
Autonomous Vehicles	AI Controlled (manufacturer designs the systems)	Transportation	Continuous	Voluntary self-reporting	N/A, emerging market	No	Mass produced

Case Study 3: Commercial Aviation

The history of commercial aviation in many ways provides the most relatable and useful example of a roadmap for commercial human spaceflight. Aviation has greatly evolved in the last century, since its inception, from a primarily government-owned and military-based enterprise to a thriving commercial market with high levels of safety. Transportation risk statistics consistently show air flight as one of the safest modes of transportation.

While there are other uses for air flight—including military, cargo carriers, private, and sport—this example focuses on commercial passenger air flight. Passenger aircraft have been in use for about 108 years, but the size and scale of the sector took off in the 1980s with a transition from personally owned to government-owned airlines, to what is now a largely commercially owned and operated market.

While some would consider civil aviation a "highly regulated" industry, it is one that shows a success of working closely with industry to promote a positive safety culture at all levels. The FAA has effectively and successfully worked with the many stakeholders within this industry, including airline operators, manufacturers, pilots, and other third parties. Rather than over-penalizing, the sector allows for honest mistakes and promotes safe spaces for reporting and problem solving, while ensuring compliance where necessary.

Building Blocks to Safety

A series of accidents in the "barnstorming" era, which was the performance of plane tricks by pilots and the first form of nonmilitary airplane activity, led to the creation of the first U.S. legislation, the Air Commerce Act of 1926. The Air Commerce Act gave way to the Federal Aviation Act, which formed the FAA. Part of the impetus for the FAA was the Grand Canyon Collision of 1956, the deadliest collision of its time with 128 fatalities. Due to its remote location, it was a difficult collision to investigate and there were no clear reporting mechanisms. To decrease risk of accidents and conduct proper investigations, the FAA improved air traffic control and collision avoidance systems.

This became especially important as many factors go into making passenger aviation safe, including manufacturing issues and system failures, inclement weather, airline communications and crew errors, fire safety, onboard injuries, runway safety, and other flying objects, such as birds, drones, and balloons in the air.

Due to the sheer number of safety considerations, the building blocks to aviation safety are complex, technically advanced, and exist at many levels.

The Convention on International Civil Aviation (Convention) establishes the international standards for civil aviation, with 193 UN member parties. The Convention also established the International Civil Aviation Organization (ICAO), which ensures adherence to rules of the air, aircraft licensing, safety standards, certification programs for competency, accident investigation, and inspections. The ICAO also manages the State Safety Programme, which sets safety risk management, standardization, implementation guidance, and reporting and monitoring procedures for all member countries.

At the U.S. national level, the FAA oversees federal aviation regulations and safety oversight, and the Aviation Safety office oversees certifications of "airworthiness," inspections, and standards development. Perhaps the most successful of its programs is its reporting systems, which include the: Aviation Safety Action Program (ASAP), Aviation Safety Information Analysis and Sharing (ASIAS), and Aviation Safety Reporting System (ASRS).

In addition, the civil aviation sector, much like cruise lines, includes a great number of stakeholders, and many third-party organizations help promote a positive safety culture. Some of these organizations include the Flight Safety Foundation (nonprofit that provides safety guidance) and many more professional safety training and advocacy programs, and pilot unions like ALPA.

Comparison to Commercial Human Spaceflight

While civil aviation requires international coordination of airspace, in many countries like the U.S., aviation is highly regulated at the federal level. There is less of a need, at least currently, for international coordination of commercial human spaceflight, but the regulatory mechanisms at the federal level, like the FAA, are highly comparable for cHSF.

However, the one unique feature of civil aviation is its reliance on the manufacturing ecosystem, whereby Boeing (U.S.) and Airbus (Europe) are the major manufacturers of passenger airplanes. Airline operators are separate entities and lead many of the safety efforts within the industry. However, due to recent, high-visibility accidents of Boeing planes, there is an effort underway to better incorporate manufacturers with reporting and other safety structures.[15]

Currently, cHSF operators also manufacture their vehicles. Table D-3 provides a comparison of civil aviation to space tourism.

[15] Recent 2020 legislation enhances FAA oversight over manufacturers and requires their disclosure of critical safety information. https://www.popularmechanics.com/flight/g73/12-airplane-crashes-that-changed-aviation/

Table D-3. Comparison of Civil Aviation to Space Tourism

	Operations	Reason	Danger To Uninvolved 3rd Parties	Reporting System	Level Of Regulation	International Coordination	Unique Vehicles Or Mass Produced
Space Tourism	Controlled by operator	Adventure and research	During launch and reentry	N/A	N/A, emerging market	No	Unique
Aviation	Controlled by operator	Transportation	During takeoff and landing	ASRS, ASIAS, ASAP	Highly regulated	Yes	Mass produced

Case Study 4: Government Spaceflight

Challenger Accident and Safety Attitude

On January 28, 1986, Challenger (STS-51L) was launched on the 25th flight in NASA's space shuttle program. Less than two minutes into the flight, the spacecraft exploded, killing all seven astronauts on board. The cause was failure of an O-ring seal of a solid rocket motor (SRM) joint. The O-rings were designed to prevent the release of hot gases produced during combustion. The O-ring failed because low temperatures at the launch site stiffened the rubber.

A Presidential Commission found that NASA's drive to achieve a launch schedule of 24 flights/year created pressure throughout the agency that directly contributed to unsafe launch operations, jeopardizing the promotion of a "safety first" attitude throughout the shuttle program. The Commission stated that the underlying problem was poor technical decision-making over a period of several years by top NASA and contractor personnel, who failed to act decisively to solve increasingly serious anomalies in the SRM joints. More specifically:

- The flight readiness review for STS-51L was conducted in accordance with established procedures, while the decision to launch was based on a faulty engineering analysis of the SRM field joint seal.

- Compounding this erroneous analysis were serious ongoing weaknesses in the Shuttle Safety, Reliability, and Quality Assurance Program, which had failed to exercise control over the problem-tracking systems, had not critiqued the engineering analysis advanced as an explanation of the SRM seal problem, and did not provide the independent perspective required by senior NASA managers at flight readiness reviews.

In addition, NASA identified communications and organization failures within the safety program:

- Lack of problem-reporting requirements
- Inadequate trend analysis
- Misrepresentation of criticality
- Lack of involvement in critical discussions

Numerous corrective actions were taken immediately following independent reviews. Despite this, a second space shuttle program accident occurred on February 1, 2003: The space shuttle Columbia (OV-102) disintegrated as it reentered the atmosphere, killing all on board. The cause was a piece of insulating foam that broke loose from the shuttle's external tank and struck the leading edge of the left wing. The principal lesson was that NASA had become too complacent about safety over the years following the Challenger disaster.

The importance of a properly managed systems integration organization was found to be crucial. NASA was the systems integrator for the space shuttle, and Boeing (previously Rockwell) was the systems integration contractor. The importance of integration was not fully appreciated after the initial development phase, and NASA revitalized systems integration twice during the shuttle program's life, once after the Challenger accident and again after the Columbia accident. Each time, a strong leader was put in charge of integration and the integration resources were revitalized. The primary lesson was that adequate resources committed to integration and the strength of integration leadership are very important to the success of a program. Integration should remain the "watchful" eye as a program evolves to an operational status. Full flight data evaluation should continue for the life of the program.

Human Spaceflight Safety at NASA Today

NASA is conducting three initiatives on commercial human spaceflight safety: the Commercial Crew Program (CCP), the Suborbital Crew (SubC) office, and the Commercial LEO Development Program (CLDP). The CCP addresses safety of NASA astronauts aboard commercial rockets en route to and from the International Space Station (ISS). Within the CCP, the SubC office is exploring game-changing methods to "perform a safety assessment to enable NASA astronauts, principal investigators, and 'other NASA personnel' to fly on suborbital missions." Two memoranda of understanding, signed by the FAA and NASA, address these mutual goals [55][56]. The CLDP is in the early stages of funding the design, development, and test of commercial space stations in LEO (to replace the ISS).

The governing document for all three examples is NASA Procedural Requirements (NPR) 8705.2B, *Human-Rating Requirements for Space Systems* (see Figure D-1). This NPR requires applicable space systems to obtain a Human-Rating Certification prior to the first NASA crewed mission and maintain the rating throughout the system life cycle. It applies to the development and operation of crewed space systems developed by NASA and used to conduct NASA human spaceflight missions. Compliance is mandatory for all NASA employees. As illustrated in Table D-1, this NPR uses the full resources and safety processes of NASA.

Specifically, the CCP, SubC office and CLDP address the flight of NASA and international partner (IP) personnel aboard commercial orbital and suborbital vehicles, respectively, not NASA-developed vehicles. NASA does not provide significant support to the purely commercial flights such as Axiom-1.

CCP holds the vendors, presently SpaceX and Boeing, to full NASA safety and technical standards. The SubC office is performing safety case evaluations of the technical design and operations for the two operational vendors, Blue Origin and Virgin Galactic, and is funding their support. The safety case evaluations are done based on NPR 8715.3D, *NASA General Safety Program Requirements*, which states, "It is NASA policy to formally review and approve NASA participation in hazardous work activities that are outside NASA operational control … This policy applies unconditionally to NASA participation in

commercial human spaceflight where current federal regulations do not necessarily provide for the safety of spaceflight vehicle occupants." The SubC office is not requiring the vendors to meet NASA CCP safety or technical standards, but is assessing the overall safety of the system, including operations.

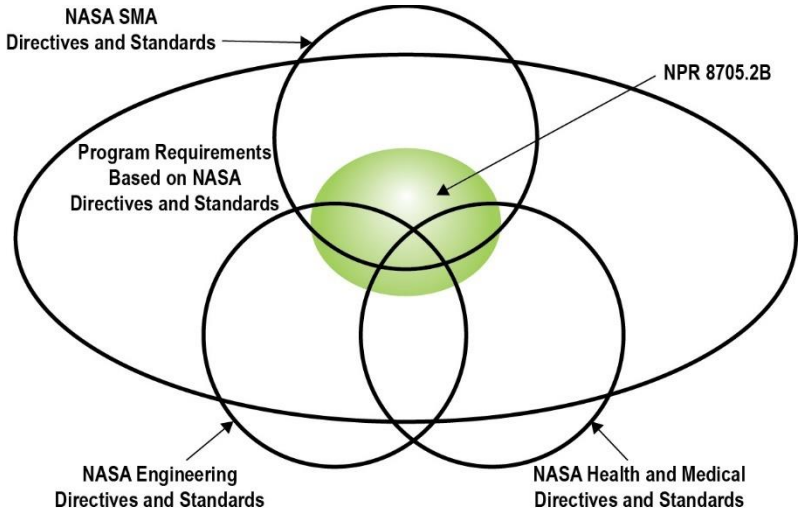

Figure D-1. NASA Commercial Crew, Suborbital Crew, and Commercial LEO Development Program Approach. (adopted from NPR 8705.2B [45])

NASA is also in the early program development cycle for the CLDP. This program is tasked with providing support to commercial providers in their development of commercial space stations in LEO, where NASA, IPs, and general public individuals may fly to and live. The program is attempting to develop a "true" public/private partnership between NASA and the commercial providers, something the CCP attempted to do, but did not entirely succeed. While it is still early in the program development cycle, the program is focusing the processes and approaches (including safety) based on a true "shared assurance" model. This requires NASA and the commercial providers to work cooperatively to establish their respective roles and responsibilities to ensure the overall safety of the NASA, IP, and general public crew members.

Case Study 5: Submarines and Other Deep-Sea Submersibles

Submarines and other deep-sea submersibles operate in a challenging environment for human safety that includes very high external pressures and potential flooding. Successful approaches to addressing these challenges are discussed below.

The Submarine Safety Program (SUBSAFE) is a quality assurance program of the U.S. Navy designed to maintain the safety of its submarine fleet, specifically to provide maximum reasonable assurance that submarine hulls will stay watertight and that they can recover from unanticipated flooding.

SUBSAFE covers all systems exposed to sea pressure or critical to flooding recovery. All work done and all materials used on those systems are tightly controlled to ensure the material used in their assembly, as well as the methods of assembly, maintenance, and testing, are correct. They require certification with traceable quality evidence, which track each item from the point of manufacture—including records of the creation of the product (i.e., source materials as well as smelting and hardening processes for metals)—to the point of installation within a SUBSAFE boundary. Although these measures increase the cost of submarine construction and maintenance, they are necessary to ensure the safety of the humans on board [57].

SUBSAFE certification is carried out in four areas: Design, Material, Fabrication, and Testing. The procedures are documented during the initial design and construction of new submarines, while undergoing routine maintenance in naval depots, and in the fleet maintenance manual for operating submarines. During each step, quality evidence is collected, reviewed, approved, and stored for the life of the submarine. This process is reinforced with external and internal audits.

SUBSAFE addresses only flooding, but mission assurance is also a benefit. Other safety programs and organizations regulate fire safety, weapons systems safety, and nuclear reactor systems safety. From 1915 to 1963, the United States Navy lost 16 submarines to non-combat-related causes. Since SUBSAFE began in 1963, only one submarine, the non-SUBSAFE-certified USS Scorpion (SSN-589), has been lost.

After the loss of the space shuttle Columbia, the Columbia Accident Investigation Board described SUBSAFE as one of the "successful safety programs and practices that could be models for NASA" [58].

Other Deep-Sea Submersibles

Representative active submersibles, each owned by a national government, include:

- U.S.: Alvin (DSV-2) is a crewed deep-ocean research submersible that descends to 4,500 m, is owned by the U.S. Office of Naval Research (ONR), and is operated by the Woods Hole Oceanographic Institution (WHOI). Research conducted by Alvin has been featured in nearly 2,000 scientific papers. It has visited the sunken Titanic.

- Cyclops 2 is a non-government submersible developed by a U.S. commercial company, OceanGate, Inc. It is designed to accommodate five people for descents to 500 m. [59]

- Australia: Deepsea Challenger (DCV 1) carried Titanic director, James Cameron, to the ocean's deepest point, Challenger Deep, at a depth of greater than 10,900 m.

- France: Nautile, operated at depths of up to 6,000 m.

- Japan: Shinkai, operated at depths of up to 6,500 m.

- China: Jiaolong, operated at depths of up to 7,500 m.

Human safety in government submersibles is assured via a detailed systems certification approach. For example, safety of Alvin is controlled by a 350-page Naval Sea Systems Command manual specifying detailed certification procedures for materials and components, design factors, testing parameters, life support systems, airborne contaminants, and much more [60].

Overall Conclusion Case Studies

These case studies highlight some of the building blocks to safety that many across the transportation industries have adopted. These building blocks of safety have been hard fought and the product of many years of experience and lessons learned from a series of failures as shown in Figure D-2.

Failures That Have Revolutionized Safety Frameworks And Culture

- **Cruise Ships**
  - ***Titanic:*** *led to international treaty, Safety of Life at Sea*
- **Passenger Aviation**
  - ***Crash over Grand Canyon (1956):*** *led to creation of FAA, better air traffic control*
  - ***Trans-Australian Crash (1960):*** *use of "black boxes"*
  - ***Tenerife (1977):*** *improved communications*
  - ***Air Canada Crash in Kentucky (1983):*** *implementation of fire safety standards*
  - ***Delta Crash (1985):*** *onboard weather systems to detect inclement weather*
  - ***Cerritos Midair Crash (1986):*** *air traffic collision avoidance systems*
  - ***Boeing 737 Max Lion Air (2018) and Ethiopian Airlines (2019) crashes:*** *expanded safety disclosure requirements*
- **Autonomous Vehicles**
  - ***First person killed in Arizona:*** *liability in case of accident*
- **Passenger Rail**
  - ***Chatsworth Crash (2008):*** *killing 25 and injuring 135 passengers, led to positive train control safety system and the Rail Safety Improvement Act*
- **Motor Sports (Federation Internationale de l'Automobile (FIA)-regulated)**
  - ***Le Mans Disaster (1955):*** *killed 83 and injured 180 spectators, led to motorsports bans in several countries, forced sector to address safety concerns or stay banned*
  - ***Formula 1 (F1) Crash (1994):*** *system failure, led to sweeping changes in F1 safety regulations, added many technical requirements*
- **NASA Challenger and Columbia**

References for Figure D-2:

https://origins.osu.edu/connecting-history/top-ten-origins-aviation-disasters-improved-safety?language_content_entity=en
https://www.wired.com/story/uber-self-driving-car-fatal-crash/
https://www.fia.com
https://www.latimes.com/world-nation/story/2021-01-02/nationwide-positive-train-control-safety-system

Figure D-2. Failures impacting safety frameworks and safety culture.

While it is easy to focus on the failures of each sector as they turn to commercial and civil applications, the larger lesson from these accidents reveals that safety is critical to the success of these industries. Without it, there is a lack of consumer trust and confidence. Building a positive safety culture from the beginning, together with data collection and analytics, will limit frequency, size, and impact of accidents from the start and allow for continuous learning from mishaps before disaster occurs.

Comparison of Fatality Rates across Transportation Sectors

Risks of accidents and fatalities happen across all different types of transportation sectors and leisure activities. Most people are aware of the level of risk they may be taking when using different transportation options. However, overall, fatality rates have decreased over time in each transportation sector. This correlates with improved standards, regulations, more experience, and more advanced technology and automation. While none of these guarantees safety by itself, each is a contributing factor to safety.

Figure D-3 shows recent fatality rates across four different transportation modes: passenger vehicles, buses, passenger rail, and passenger airflight. Rates may vary country by country, based on their own standards of safety for certain modes of transportation. The list also does not account for cruise ships, as many are registered in countries like the Bahamas. These low fatality rates, especially in the case of passenger airflight, show how valuable it would be to see where other long-standing transportation sectors have gotten safety right and lessons learned. In contrast, Table D-4 shows how risk probabilities across transportation modes, leisure and sport activities, space launch and transportation, and military activities compare. It is a useful tool for commercial human space flight, which combines elements of all these categories.

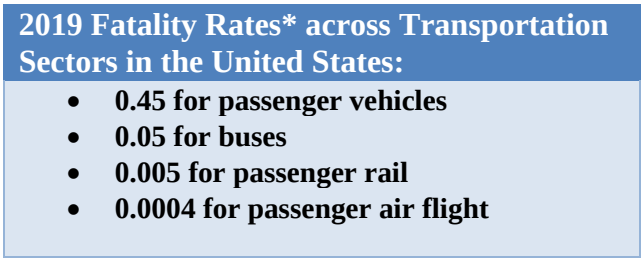

Figure D-3. Fatality statistics across transportation sectors in the United States from the National Safety Council. (*Deaths per 100,000,000 passenger miles [46])

Table D-4 shows the probabilities of catastrophic failure or fatality across various comparable activities, showing the comparison of many activities, such as aviation, skydiving, and racing, with some space-based activities, such as orbital launches, space transportation systems (STSes) like the Space Shuttle Program, and expendable launch vehicles (ELVs). The table also makes some comparisons with military-grade planes from the last century (XB-70, X-15, and the Concorde), flown primarily by Air Force pilots.

Table D-4. Probability of Catastrophic Failure or Fatalities for Flight Vehicles and from Other Activities [61][62]

A: Expected ($Pr > 10^{-1}$)	B: Probable ($10^{-1} \geq Pr > 10^{-2}$)	C: Likely ($10^{-2} \geq Pr > 10^{-3}$)	D: Unlikely ($10^{-3} \geq Pr > 10^{-6}$)	E: Improbable ($Pr \leq 10^{-6}$)
• New ELVs (first 10 launches) • U.S. Civil War (Union) • WWII U-Boat • High-Altitude Mountaineering	• Orbital Launch (all vehicles) • STS • XB-70 • Normandy (D-Day) • Grand Prix Racing • Base Jumping	• X-15 • Hang Gliding • Motorbike Racing	• Concorde • Automobiles • Skydiving • Bungee Jumping • Swimming • Fire	• General Aviation • Skiing • Lightning Strike

Whereas everyday modes of transportation have become commonplace, and their rates of fatality much lower, Table D-4 compares commonplace activities (automobiles, swimming) with unique military activities (fighter planes) and extreme sports (i.e., motorsport racing, base jumping) [31][32]. Human spaceflight might be closer in nature to the more unique activities listed, but with time, proper investment in safety, and experience, such risks can be lowered.

Appendix E. Safety Management Systems

One key component of any safety management system (SMS), permeating throughout and essential to safety performance, is the culture of the organization. "Safety culture" is the term that we apply to those aspects of the organization's culture that relate to how people value safety over other competing interests. The concept of how safety culture relates to safety management is described in detail in FAA AC 120-92B.

1. **Safety Culture.** Cultures are the products of the values and actions of the organization's leadership, as well as the results of organizational learning. Cultures are not really "created" or "implemented," they emerge over time and because of experience. Organizations cannot simply purchase a software program, produce a set of posters filled with buzzwords, require their people to attend an hour of slide presentations, and instantly install an effective SMS. As with the development of any skill, it takes time, practice and repetition, the appropriate attitude, a cohesive approach, and constant coaching from involved mentors.

2. **Interdependence.** Because the culture of an organization includes the deeply ingrained and automatic psychological and behavioral aspect of human performance, there is a strong correlation between safety culture and accident prevention. Therefore, safety culture and SMSes are interdependent. Management's constant attention, commitment, and visible leadership are essential to guiding an organization toward a positive safety performance.

3. **Management Involvement.** Management leadership should demonstrate their visible commitment to and involvement in safe operation while performing their daily work. SMS processes do not have to be expensive or sophisticated; however, active personal involvement of operational leaders is essential. Safety management must be accomplished by those managers who "own" the processes in which risks reside. Safety cultures also cannot be "created" or "implemented" by management decree, no matter how sincere their intentions. Every organization has a safety culture. It is embodied in the way the organization and its members approach safety in their jobs. If positive aspects of culture are to emerge, the organization's management must set up policies and processes that create a working environment that fosters safe behavior. That is the purpose of the SMS processes.

4. **Management Framework.** It is for these reasons that a management framework, one that facilitates decision-making and shapes the environment in which employees work, is crucial to organizational performance in all aspects of the organization's business, including safety. A safety culture matures as safety management skills are learned and practiced and become second nature across the entire organization. The following have been found to be characteristics of organizations that consistently achieve safe results:

    a. *Open Reporting.* Policies and processes that foster open reporting while, at the same time, stress the need for continuous diligence and professionalism. The organization should encourage disclosure of error without fear of reprisal, yet it should also demand accountability on the part of employees and management alike.

    b. *Just Culture*. The organization should engage in identification of systemic errors, implement preventative corrective action, and exhibit intolerance of undesirable behaviors, such as recklessness or willful disregard for established procedures. This is often referred to as a "just culture."

c. *Personnel Involvement.* Involvement of line personnel and all levels of management in functions dealing with aviation safety, including the accountable executive, is critical to effective safety management throughout an organization.

d. *Use of Information*. Effective use of all safety information ensures informed management decision-making.

e. *Commitment to Risk Reduction*. The organization expects direct management involvement in identifying hazards and managing risk.

f. *Vigilance*. Processes that provide vigilance of ongoing operations and the environment to ensure effectiveness of risk controls and awareness of emerging hazards.

g. *Flexibility*. Using information effectively to adjust and change to reduce risk, and a willingness to commit resources to making changes necessary to reduce risk.

h. *Learning*. The organization learns from its own failures and from those of allied and similar businesses. The organization is committed and uses acquired data to feed analysis processes, the results of which yield information that can be acted upon to improve safety.

Again, these concepts have been proven successful in other industries. They are designed and implemented by the organization's management and employees in collaboration.

The Safety Management Decision-Making Process

Design and performance for safety risk management and safety assurance are iterative processes. Following FAA AC 120-92B, and also described by Stolzer and Goglia [49], safety management decision-making processes provide an expanded view of the principal two sets of processes of the SMS: safety risk management (SRM) and safety assurance (SA), as shown in Figure E-1. In the discussion that follows, key terms and concepts related to SMS processes are introduced. Because safety management is a decision-making process, the SRM and SA processes follow a set of processes outlined in Figure E-1.

The processes work as follows: The Description and Context step requires the user of the process to gain an overall understanding and context of the operation that either is being or will be performed. The Specific Information step requires the user of the process to obtain information about aspects of the systems and environments involved that may present risk. Under the Analysis step, the user analyzes or makes sense of that information. The Assessment step requires the user to make decisions regarding the acceptability or risk of system performance. Finally, under the Action: Problem Resolution step, the user takes necessary action.

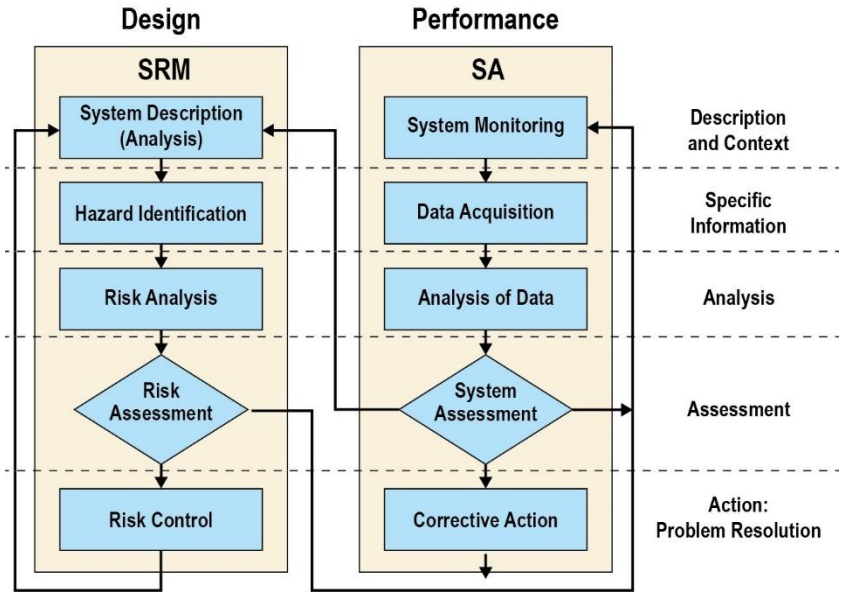

Figure E-1. Safety management and decision-making process. (adopted from FAA AC 120-92B [48])

Safety Risk Management (SRM)

1. In SRM, the first step, System Description (Analysis), is used to understand the aspects of the operation that might cause harm. In most cases, Hazard Identification flows from this system analysis. Hazard identification requires you to ask: What hazards exist in the operational environment? What are the human factors issues of the operation (e.g., workload, distraction, fatigue, or system complexity)? What are the limitations of the hardware, software, procedures, etc.?

2. While the diagram above depicts processes as distinctly defined components, in practice they flow from one to the other. For example, in a careful discussion of how a system currently works [System Description (Analysis)], hazards will often become evident. Thus, the hazard identification step has also been at least partially accomplished.

3. The process then progresses into an analysis of the potential consequences of operation in the presence of the identified hazards (Risk Analysis). This culminates in an assessment of the acceptability of operating with these hazards, Risk Assessment, or if the risk of such operations can be mitigated to an acceptable level, Risk Control. For this reason, operational managers must be the ones who are accountable for these decisions.

4. After a system has been designed or revised using the SRM process, special attention should be given to the new or revised system using the SA process. It should not be surprising to find at this time that there are still things that might not have been considered or that there are changes over time in the operational environment, requiring a return to SRM. Thus, the SRM and SA processes operate in a continuous exchange.

Safety Assurance and Feedback Loop to Safety Risk Analysis

1. In SA, the process continues with measuring and monitoring the performance of the system operation, System Monitoring, with the designed risk controls in place. This involves a variety of data sources (Data Acquisition). As in SRM, the data will need to be analyzed for it to be used in decision-making, Analysis of Data. In the case of SA, the decision-making can result in several paths, System Assessment. If the data and analysis say that the system and its risk controls are

functioning as intended, the result is confirmatory: the management now can have confidence in system safety performance.

2. If this is not the case, the analysis needs to continue to determine if the shortfall is because the controls are not being used as intended (e.g., required training not accomplished, procedures not followed, or improper tools or equipment provided), or if, even though the system is being used as intended, it is not producing the expected results. In the former case, action should be taken to correct the problem, Corrective Action. In the latter case, the system design should be reconsidered using the path back to the SRM process.

3. The path back to SRM is a particularly important part of the SA process, especially for operators who are transitioning into SMS. Their operational systems have likely not been built using an SRM process, so they may lack formal or well-understood risk controls. The SA process covers the day-to-day life of system operations, so, in many cases, the determination to review existing processes for hazard and risk may be the first time that these aspects of operation have been considered.

4. As in SRM, managers who are responsible for operational processes are the ones who are also responsible for assuring that they are performing as intended from a safety, as well as operational, standpoint. Moreover, correct design, performance, and risk control need to be a concern of top management, including the accountable executive.

Appendix F. Status of Voluntary Consensus Standards

Congress enacted the National Technology Transfer and Advancement Act of 1995 (NTTAA), which encourages formal adoption of national consensus standards by American regulatory agencies. Section 12(d) of the Act is primarily limited to "technical standards," but was implemented by OMB Circular A-119 with expanded scope. The circular directs federal agencies to use voluntary consensus standards, both domestic and international, in its regulatory and procurement activities. The circular defines voluntary consensus standards as those having the following attributes: openness, balance of interest, due process, an appeals process, and consensus. Some agencies (e.g., the Food and Drug Administration) have published guidelines on appropriate use of such standards [63]. The American Society of Safety Professionals has listed four advantages of voluntary consensus standards [64]:

1. National consensus standards have fewer procedural burdens.

2. The consensus method provides for a balance between competing interests.

3. The voluntary nature of consensus standards enables users to adapt provisions to meet unusual circumstances.

4. Much lower standards development costs are obtained.

FAA-AST Report to Congress on Voluntary Consensus Standards

In January 2022, FAA-AST submitted to Congress an *Interim Report on Voluntary Industry Consensus Standards Development* [65], as required by Public Law 114-90, *U.S. Commercial Space Launch Competitiveness Act (CSCLA)*, Section 111(5). The report updated the information provided in the initial 2017 report titled *FAA Evaluation of Commercial Human Space Flight Safety Frameworks and Key Industry Indicators*. In the 2022 report, FAA reviewed voluntary industry consensus standards development and acceptance by industry and identified areas that have the potential to become voluntary consensus standards. The report also contained an assessment of the general progress of the industry in adopting voluntary industry consensus standards, and provided COMSTAC's recommendations, findings, and observations related to voluntary industry standards consensus development and promotion of best practices.

The report mentioned several organizations that are engaged in working on industry consensus standards, including: ASTM International, the American Institute of Aeronautics and Astronautics (AIAA), the International Organization for Standardization (ISO), SAE International, the National Fire Protection Association (NFPA), and the Commercial Spaceflight Federation (CSF). An appendix to the report listed nine standards under development or published by ASTM International, three under revision or in development by the AIAA [one in affiliation with the American National Standards Institute (ANSI)], ten published or under revision by ISO, one under development by the SAE Commercial Space Committee, and one under development by the NFPA. A final appendix in the report summarizes industry and government readiness indicators and progress in developing a safety framework.

Key International Committees Developing Consensus Standards

Two key international committees developing consensus standards addressing human spaceflight safety are (1) ISO Technical Committee 20, Aircraft and Space Vehicles, and (2) ASTM International Committee F47 on Commercial Spaceflight.

ISO Technical Committee 20, Aircraft and Space Vehicles

ISO Technical Committee 20 (TC20), Aircraft and Space Vehicles, was founded in 1947 and is devoted to the standardization of materials, components, and equipment for construction and operation of aircraft and space vehicles, as well as equipment used in the servicing and maintenance of these vehicles. The AIAA holds the secretariat for ISO TC20 Subcommittee 14 (SC14) for Space Systems and Operations. Founded in 1992, the scope of work by this subcommittee is the standardization for manned and unmanned space vehicles, their design, production, maintenance, operation, and disposal, and the environment in which they operate. Six working groups provide an international forum for addressing the standardization needs and concerns of organizations and personnel involved with the development and operation of space systems. Approximately 40 standards are currently in progress, and over 180 have been published; these completed standards are available for purchase from ISO and continue to be updated.

ASTM International Committee F47 on Commercial Spaceflight

ASTM International's Committee F47 on Commercial Spaceflight, formed in 2016, is developing and maintaining voluntary consensus standards and recommended practices for the commercial spaceflight industry. The voluntary consensus standards are being developed by groups of subject matter experts through a formal drafting and review process. Technical subcommittees, discussed below, develop and maintain these standards and recommended practices. Specific areas addressed include design, manufacturing, and operational use of vehicles used for spaceflight, as well as human spaceflight safety. Stakeholders represented include vehicle operators and parts manufacturers, the CSF, regulators including the FAA Office of Commercial Space Transportation, U.S. Government users including NASA centers and headquarters, National Air Space users, spaceport operators, medical professionals, the AIAA, academia, and other interested stakeholders. Completed ASTM standards are available for purchase for nominal fees from ASTM and continue to be updated.

The following five ASTM subcommittees have embarked on development of numerous additional standards:

- Subcommittee F47.01, Occupant Safety of Suborbital Vehicles
- Subcommittee F47.02, Occupant Safety of Orbital Vehicles
- Subcommittee F47.03, Unoccupied Launch and Reentry Vehicles
- Subcommittee F47.04, Spaceports
- Subcommittee F47.05, Cross-Cutting

Two other F47 subcommittees are (1) F47.92, Standards Road Mapping, and (2) F47.93, Liaison.

Other standards under consideration include:

- Approach to development of emergency response plan
- Flight operations
- Update to data exchange guidance with FAA and ATM
- Fire safety for launch and space vehicles
- Interface standards for payload and launch/reentry vehicles

- Ground rules and assumptions, inputs, and data used to produce an aircraft hazard area (AHA) analysis
- Autonomy
- Payload-to-launch vehicle attachment
- Post-flight requirements
- Orbital debris/end-of-life decommissioning standards activity
- Guide to industry regulations for a voluntary space safety reporting system
- Reusable launch vehicle (RLV) maintenance
- Documentation of intended/expected envelope requirements for critical subsystems
- Depressurization safety for launch and space vehicles
- Launch and orbital rules of the road
- Flight safety system certification
- Pressure suits
- Occupant/passenger restraints
- Micrometeorite impact
- Breathable atmosphere, medical certifications (health monitoring)

Other Organizations Developing Voluntary Consensus Standards

As discussed above, other organizations developing voluntary consensus standards include the AIAA, SAE International, the NFPA, and the CSF.

Status of Commercial Space Industry Consensus

The considerable advantages of voluntary consensus standards were discussed in the introduction to this section. Some perceived disadvantages are decreased competitiveness, lack of opportunity to validate the standards before they are implemented, and the substantial time required to develop the standards. For example, the time from project initialization to publishing an ISO standard has ranged from one to four years. Although ASTM International estimates that 18 months is a typical timeframe for development of a new standard, experience has shown that, in some cases, balloting cycles can extend to multiple years for a given standard.

That said, we expect that most commercial spaceflight companies will welcome the opportunity to implement voluntary consensus standards that are applicable. That perception is in part because companies developing and flying commercial spaceflight vehicles are participating directly in development of relevant ISO and ASTM standards, including those addressing human spaceflight safety. Example participating companies include SpaceX, Blue Origin, Virgin Galactic, United Launch Alliance (ULA), Boeing, Honeywell, and Worldview (a high-altitude balloon flight provider). Moreover, the CSF's Safety Committee supports standards development by the above committees to ensure the

safety of spaceflight participants and, as stated by the committee, to provide the FAA with means of compliance that can be used in the future to assist in creating regulations.

The aforementioned standards are in a constant state of development, so a list of current standards and revisions here would quickly become obsolete. A list of standards and their status as of January 2022 is available from the FAA in Appendix A of Reference [70].

Appendix G. Recommended Practices for HSF Occupant Safety and Training

FAA-AST developed, and published in 2014, recommended practices for human space flight occupant safety and training, to serve as guidelines for developers during the statutory-mandated learning period. This document, "Recommended Practices for Human Space Flight Occupant Safety" [66][67], is intended to be translated into a regulatory safety certification regime after the learning period expires. To develop this document, FAA-AST worked closely with NASA, industry, and other key stakeholders. The document was the culmination of a three-year effort, which involved researching existing human space flight standards, conducting a series of public teleconferences to gather recommendations, and soliciting feedback from the Commercial Space Transportation Advisory Committee (COMSTAC). FAA chose to primarily use NASA's requirements and guidance for the Commercial Crew Program (1100 Series) as a guide. The purpose was not to copy NASA's requirements but to use them to capture relevant safety concepts.

The FAA document addresses occupant safety only. Public safety and mission assurance are not directly addressed. Both orbital and suborbital flights are covered. Orbital vehicles are defined as those that stay on orbit for two weeks maximum and can return to Earth in under 24 hours if necessary. Orbital rendezvous and docking, long-duration flights, extravehicular activity, and flights beyond Earth orbit are not explicitly covered. The period of coverage is from when occupants are first exposed to vehicle hazards prior to flight through when they are no longer exposed to vehicle hazards after landing.

The document covers recommended practices in three categories: (1) design (human needs and accommodations, human protection, flightworthiness, human/vehicle integration, system safety, and design documentation), (2) manufacturing, and (3) operations (management, system safety, planning, procedures and rules, medical considerations, and training). No specific level of safety (risk) is defined due to the wide variety of systems and flight profiles. Two levels of care are articulated: (1) occupants should not experience an environment during flight that would cause death or severe injury, and (2) the level of care for the flight crew when performing safety-critical operations is increased to a level necessary to perform those operations. In an emergency, the same level of care is not expected to be maintained—only a reasonable chance of survival is mandated. Key assumptions were: (1) each flight crew member is safety critical, (2) SFPs may be called upon to perform limited safety-critical tasks, and (3) clean sheet philosophy—no other regulations act to protect occupants from harm.

There are notable omissions: (1) although medical consultation is recommended, SFPs are free to assess their individual risk, (2) long-term health issues from ionizing radiation are not addressed, and (3) integration of occupant and public safety was stated to be an area for future FAA-AST work. FAA-AST is presently updating these recommended practices.

Appendix H. List of International Treaties and Agreements

Document	Year	Total Ratification, Acceptance, Approval Accession or Succession	Total Signature-Only States	U.S.
Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies	1967	112	23	Yes
Agreement on the Rescue of Astronauts, the Return of Astronauts, and Return of Objects Launched into Outer Space (ARRA)	1968	99	23	Yes
Convention on International Liability for Damage Caused by Space Objects	1972	98	19	Yes
Convention on Registration of Objects Launched into Outer Space	1974	72	3	Yes
Agreement Governing the Activities of States on the Moon and Other Celestial Bodies	1984	18	4	No
UNGA Resolution 41/65, Principles Relating to Remote Sensing of the Earth from Outer Space	1986	--	--	--
UNGA Resolution 47/68, Principles Relevant to the Use of Nuclear Power Sources in Outer Space	1992	--	--	--
UNGA Resolution 37/92, The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting	1982	--	--	--
UNGA Resolution 51/122, Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries	1996	--	--	--
UNGA Resolution 68/74, Recommendations on National Legislation Relevant to the Peaceful Exploration and Use of Outer Space	2013	--	--	--
ST/Space/49, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space	2010	--	--	--
A/AC.105/934, Safety Framework for Nuclear Power Source Applications in Outer Space	2009	--	--	--
The Artemis Accords	2020	--	21 (including U.S.)	Yes

External Distribution

REPORT TITLE

Commercial Human Spaceflight Safety Regulatory Framework

REPORT NO.	PUBLICATION DATE	SECURITY CLASSIFICATION
ATR-2022-02101	September 30, 2022	UNCLASSIFIED

Stephen Earle
FAA
stephen.earle@faa.gov

Stephanie.McKnight-Bailey
FAA
stephanie.mcknight-bailey@faa.gov

Paul A. Masson
StarNet, LLC
paul_masson@starnetllc.net

Release to Public	Control Export
Yes ☑ No ☐	Yes ☐ No ☑

APPROVED BY (AF OFFICE)_____ DATE_____

AEROSPACE REPORT NO.
ATR-2022-02101

Commercial Human Spaceflight Safety Regulatory Framework

Cognizant Program Manager Approval:

Patrick M. Bauer, SYSTEMS DIRECTOR
HOMELAND SECURITY & LAW ENFORCEMENT PROG
CIVIL SYSTEMS OPERATIONS
CIVIL SYSTEMS GROUP

Aerospace Corporate Officer Approval:

James M. Myers, SENIOR VP CIVIL SYSTEMS GROUP
OFFICE OF EVP

Content Concurrence Provided Electronically by:

Josef S. Koller, SYSTEMS DIRECTOR
NATIONAL SPACE SYSTEMS ENGINEERING
DEFENSE SYSTEMS OPERATIONS
DEFENSE SYSTEMS GROUP

Office of General Counsel Approval Granted Electronically by:

Kien T. Le, ASSISTANT GENERAL COUNSEL
OFFICE OF THE GENERAL COUNSEL
OFFICE OF GENERAL COUNSEL & SECRETARY

SQ0493

AEROSPACE REPORT NO.
ATR-2022-02101

Commercial Human Spaceflight Safety Regulatory Framework

Export Control Office Approval Granted Electronically by:

Angela M. Farmer, SECURITY SUPERVISOR
GOVERNMENT SECURITY
SECURITY OPERATIONS
OFFICE OF THE CHIEF INFORMATION OFFICER

SQ0493