DOI: 10.13009/EUCASS2023-893
Aerospace Europe Conference 2023 – 10TH EUCASS – 9TH CEAS

Space System Certification for Human Spaceflight-Historical Practices and New Approaches for Safety

Tim A. Bulk, Bill Clark, Chris Jones
SAS International
3005 30th St, Boulder CO USA
Tim.Bulk@sas-intl.com – Bill.Clark@sas-intl.com – Chris.Jones@sas-intl.com
†

Abstract

With the growth of new space systems for human exploration, including those international partners developing systems for future NASA and commercial missions, many international companies are challenged by the process of space system certification for Human Spaceflight. The process that is currently implemented has worked well from a safety perspective for the last 40 years, but at times is not compatible to commercial development timelines or budgets. The time and costs associated with organizations meeting the regimented and prescriptive safety requirements for an international government funded human exploration program, may be cost prohibitive for a commercial company to participate.

1. Introduction

With the growth in privately funded commercial LEO Destinations, future private cis-lunar missions, and eventual private lunar missions; utilizing lessons learned from historical approaches coupled with best practice commercial systems engineering can be an effective means to develop safe and reliable commercial human space systems and spacecraft.

This approach has been successfully utilized in the United States by commercially funded companies in the sub-orbital regime and is now being applied for orbital systems including the new Commercial LEO destinations program, and future crew landing systems for lunar missions. This process though is based on over 60 years of human space system knowledge, experience and lessons learned. The process has been tailored in some respects that allows for commercial developers to demonstrate good coupled systems engineering and system safety reviews, with proper independent review to meet necessary "human certification" requirements. Although never a guarantee of 100% mission success, the process has been successfully or currently being utilized on such systems as the Orion/Artemis System, Dragon, Cygnus, New Shephard, and CST-100 Starliner spacecraft.

2. Historical Perspective

Since 1961, there have 372 human spaceflight launches[1], of course which will be quickly expanded with more scheduled human spaceflight launches on the Dragon, Starliner, New Shephard, Virgin Galactic, Orion and Shenzhou spacecraft. The critical aspects of successful human spaceflight is not only the complexity of launch and orbital operations, but the necessary systems to maintain human sustainability in the vehicle from minutes to days or weeks. This complex 'systems of systems' is not forgiving of poor engineering or a lack of physical understanding of the physics, flight environments or interaction of dissimilar systems. Since 1961, there have been 19 fatalities of

[1] As of July 1st, 2023 encompassing suborbital launches including the June 29th , 2023 launch of Virgin Galactic 01

DOI: 10.13009/EUCASS2023-893

astronauts on a mission, –11 during training accidents, and over 188 fatalities in incidents regarding spaceflight (testing personnel, launch pad technicians, and ground personnel). In addition, there have been 38 near misses or non-fatal incidents not including the non-fatal mishaps on Extravehicular Activity (EVA's). NASA Johnson Space Center, Safety Mission Assurance Office keeps a detailed database of all mishaps for spaceflight activities (Reference Figure 1.)

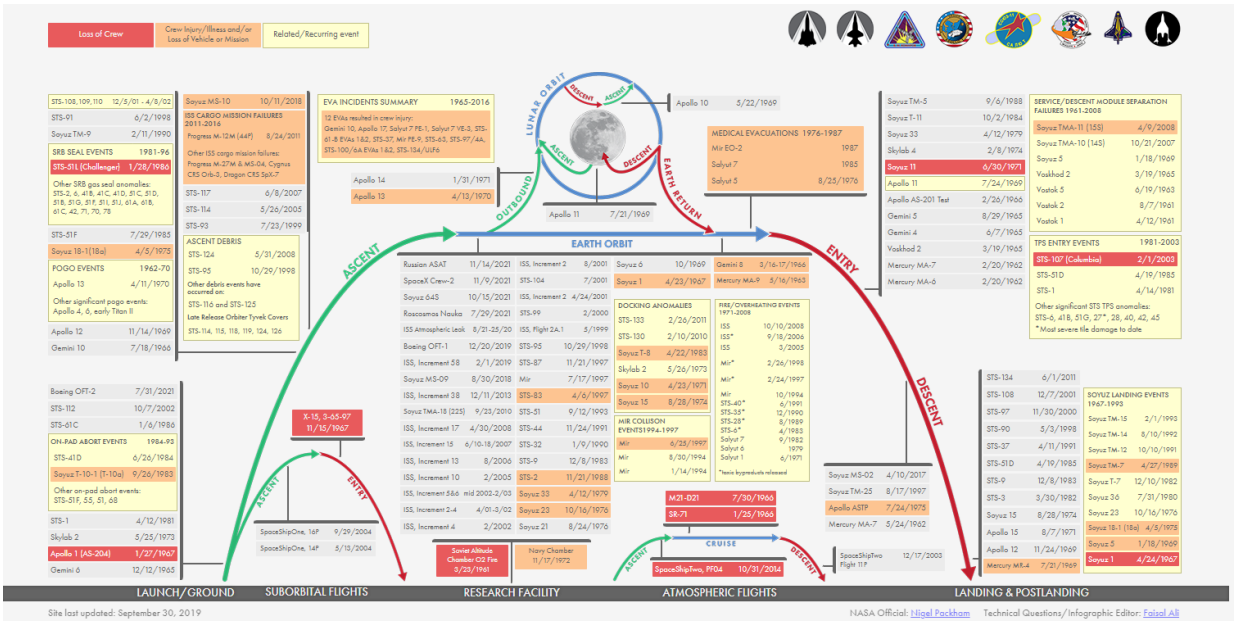

Figure 1. Significant Incidents and Close Calls in Human Spaceflight *Courtesy of the NASA JSC SMA Flight Safety Office*

Table 1: Summary of Spaceflight Accidents (Fatal and Non-Fatal)

	Fatal Spaceflight Accidents/Fatalities/	**Non-Astronaut Fatalities**	**Mishaps Non-Fatal**
Observation	19	188	38
In Training Accidents	11	NA	NA

[a]Data as of July1, 2023 only for reference

In the early days of rocketry, spaceflight and human spaceflight, the learning experience of working with toxic chemicals, cryogenics, new solid propellants, and complex operations attributed to a steep learning curve and at times learning through deadly failures. Currently, even with proper safety protocols, chances of injury or death during testing operations, component manufacturing, test stand operations, or launch pad processing are higher for technicians than astronauts in boost phase of flight.

2.1 Failures and Impacts to Programs

DOI: 10.13009/EUCASS2023-893

Failures are expected in high-risk development programs, and hence the necessity to manage development risk through regimented processes. Historically, a major subsystem failure during a development program impacts the development schedule between 2 and 12 months. A failure of an inaugural flight (rocket or spacecraft), typically impacts the program from 6 months to 24 months. Human Spaceflight operational systems with a major failure (fatality) is impacted between 2.5 and 3.5 years (Reference the U.S. Space Shuttle Return to Flight Missions).

Under NASA's new Commercial Crew Program (Space X and Boeing) the impacts to subsystem failures have been between 6 months and 18 months based on the significance of the failure. There have been no fatalities with these systems to date.

In all cases, impacts to the Programs budgets and schedules have been seen and in some cases with non-human launch systems (expendable launch vehicles), those companies have not survived the failures. Going forward, public and private investment into high-risk space systems will be extremely dependent on mission success, reliability and safety.

2.2 Traditional Approach to Safety in Human Spaceflight Programs

Safety in human spaceflight programs has traditionally followed a process similar to the NASA safety process which assesses not only the safety of spaceflight vehicle occupants, but safety of the public as well. This has involved not only complying with prescribed safety requirements and design and construction standards defined for the system or program, but also performing the necessary system safety analyses and conducting phased system safety reviews to assess all safety and risk related documentation. For example, NASA developed *NPR 8705.2, Human-Rating Requirements for Space Systems* which identifies the processes, design standards, and requirements needed to ensure a system safe for humans in a space environment. For visiting vehicles to the International Space Station (ISS), these have been incorporated through the use of NASA visiting vehicle requirements (*SSP 50808 International Space Station (ISS) to Commercial Orbital Transportation Services (COTS) Interface Requirements Document (IRD)*), including the Safety and Mission Assurance (S&MA) requirements and design and construction standards (additional documents) which are covered in a variety of NASA documents, and amounts to thousands of requirements. Successful verification of these requirements typically involves many discussions with key stakeholders (from both the visiting vehicle/company as well as from NASA) to ensure requirement owners are satisfied with the implementation of these requirements and standards, which can take up large amounts of resources. Compliance with these requirements can take weeks and months as data is compiled, submitted, reviewed, discussed, updated, and re-submitted. In some cases, waivers or tailoring of these requirements and design and construction standards may be required and can also take months of effort.

System safety analyses are also performed by providers and reviewed by independent NASA safety review panels to ensure all hazards and hazard causes are identified and adequately controlled and that safety requirements are met, as well as ensure all risks are adequately characterized and the risk is As Safe As Reasonably Practicable (ASARP). These analyses may include preliminary hazard lists (PHL), functional hazard analyses (FHA), fault tree analyses (FTA), subsystem hazard analysis (SSHA), and integrated hazard analysis (IHA). Phased safety reviews are typically conducted during conceptual design, preliminary design, detailed design, and design certification milestones. Each review can take weeks and months to successfully complete based on the level of detail and depth of the reviews. Similarly, these reviews can absorb large amounts of resources that can be very burdensome for commercial providers.

3. System Certification Approaches for Human Spaceflight

3.1 Commercial NASA Approach and Expectations

Certification for commercial human spaceflight systems typically starts with strong systems engineering processes and principles, which begin at the conceptual phase and continue throughout the life cycle of the program. Figure 2 below is taken from NPR 7123.1C, *NASA Systems Engineering Processes and Requirements*, and shows the typical systems engineering engine for a simple single-pass waterfall-type life cycle.

DOI: 10.13009/EUCASS2023-893

At each stage in the Systems Engineering process, System Safety functions must be evaluated at the appropriate level of system maturity. This includes the Key Human Rating requirements and flow downs, Hazard Analysis, Failure Mode Effects Analysis, Parts list review, Design verifications, Hardware and Software reviews and releases, appropriate standards analysis and acceptance, Operational Testing, and Verifications. In all cases, ultimately Risk Criteria must be developed and accepted/dispositioned.

For visiting vehicles to the ISS, these safety evaluations occur through the NASA safety review process. As mentioned previously, these safety reviews are typically conducted during conceptual design (Phase 0, if required), preliminary design (Phase I), detailed design (Phase II), and design certification milestones (Phase III). At each phased safety review, the design, along with all system safety products are reviewed and approved by a NASA Safety Review Panel (SRP). The products are reviewed to ensure they are at the appropriate level of maturity, and associated risks are acceptable. All review material is usually submitted weeks in advance of the actual review, and the reviews themselves can take weeks and months to complete, depending on the complexity of the system and the amount of material to be reviewed.

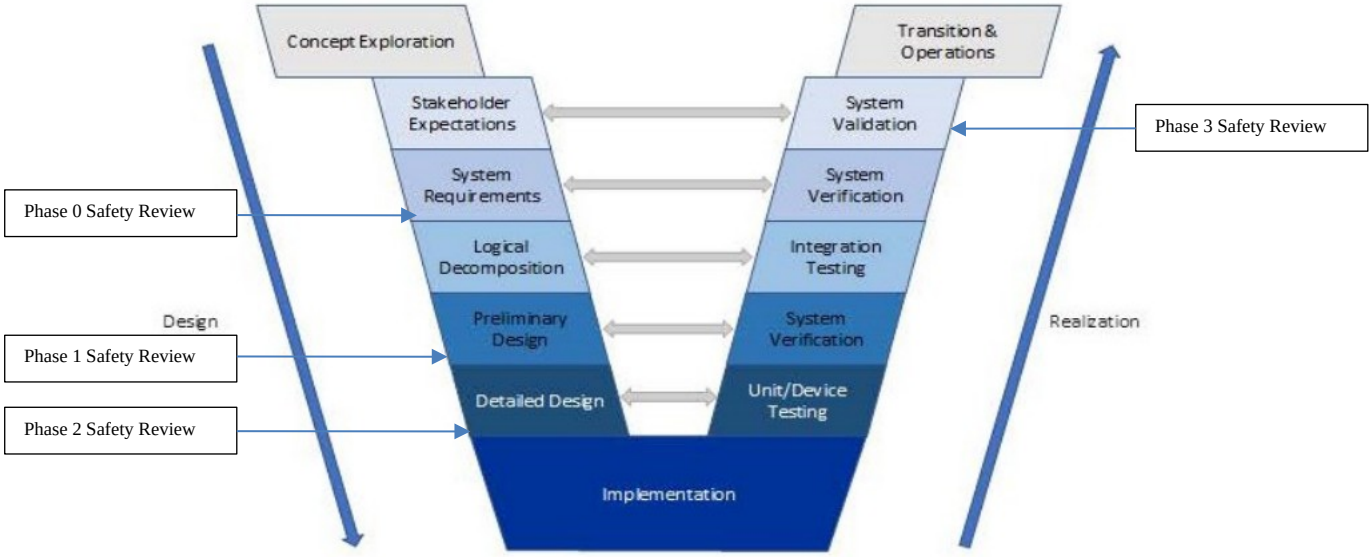

Figure 2. SE Engine Implemented for a Simple Single-Pass Waterfall-Type Life-Cycle Including Locations of Phased Safety Reviews

The life cycle for NASA programs are also divided into various phases and can be found in NASA SP-2016-6105 Rev 2, *NASA Systems Engineering Handbook*. The System Safety Process is integrated into each Phase.

These phases are briefly summarized below:

- Pre-Phase A: Concept Studies

  During this phase, mission concepts and system level requirements are developed, the Concept of Operations is developed and baselined, and some program plans such as the program Systems Engineering Management Plan (SEMP) are also established, including a preliminary verification and validation approach. Risk classifications and any initial technical risks are identified.

- Phase A: Concept and Technology Development

  During Phase A, final mission concepts and system-level requirements are developed, as well as program/project technical management plans. A human rating plan is established, and initial evaluations are performed. Program milestones such as System Definition Review (SDR) and/or Systems Requirements Review (SRR) are held during this phase. Risks are identified and analysed. Preliminary safety products

DOI: 10.13009/EUCASS2023-893

may also be reviewed during this phase, such as Preliminary Hazard Lists (PHL) and/or Functional Hazard Analyses (FHA). Other system safety activities within the systems engineering process for this phase include setting initial constraints (applicable safety requirements and risk tolerances), compliance with tailored requirements, standards and best practices, conducting Risk Informed Decision Making (RIDM), allocating requirements using performance commitments, conducting Continuous Risk Management (CRM), and selecting a design solution for implementation.

- Phase B: Preliminary Design and Technology Completion

  In Phase B, the project is further defined to establish an initial baseline. The preliminary design of the system is developed. Risks are further identified and existing risks are updated. Safety analyses and safety data packages and are developed to the appropriate level of maturity. The Preliminary Design Review (PDR) is held during this phase, as well as Phase I Safety Reviews, where the hazard analyses are reviewed to ensure all hazards, hazard causes, and preliminary control strategies are identified. Other system safety activities within the systems engineering process for this phase include setting initial constraints (applicable safety requirements and risk tolerances), compliance with tailored requirements, standards and best practices, conducting Risk Informed Decision Making (RIDM), allocating requirements using performance commitments, conducting Continuous Risk Management (CRM), and selecting a design solution for implementation.

- Phase C: Final Design and Fabrication

  During Phase C, the detailed design of the system is completed, hardware is fabricated, and software is coded. Previously baselined documentation is reviewed and updated appropriately. Verification and validation plans are also developed and/or further defined. Program risks are again identified and updated. The Critical Design Review (CDR) is held during this phase, as are Phase II safety reviews where the hazard analyses are reviewed. During Phase II safety reviews, detailed safety controls are identified, as well as detailed safety control verification type and details. Other system safety activities include conducting CRM activities (e.g. maintaining safety analyses and controlling individual risks) as well as program control and commitments (e.g. proactively seeking safety improvements, implementing lessons learned, and verification and validation that safety requirements are being met)

- Phase D: System Assembly, Integration and Test, Launch

  During this phase, the system is assembled, integrated, verified, validated, and launched. All documents previously baselined are updated as needed. Verification and Validation (V&V) activities are performed according to the V&V plans and procedures. Several milestone reviews also occur during this phase as well, including Test Readiness Reviews (TRR), System Acceptance Review (SAR) or pre-Ship Review, Flight Readiness Review (FRR) as well as Phase III safety reviews where updates to the hazard analyses are reviewed, and safety control verifications are reviewed for proper implementation and closure. Other system safety activities include conducting CRM activities (e.g. maintaining safety analyses and controlling individual risks) as well as program control and commitments (e.g. proactively seeking safety improvements, implementing risk informed maintenance, auditing, and inspections).

- Phase E: Operations and Sustainment

  During Phase E, the prime mission is executed. Data is collected during the mission, and that data is reviewed for anomalies and abnormal system behavior. Any lessons learned are captured and post-flight reviews are conducted such as Post-Launch Assessment Review (PLAR), Post-Flight Assessment Review (PFAR), as well as safety reviews. Other system safety activities include conducting CRM activities (e.g. maintaining safety analyses and controlling individual risks) as well as program control and commitments (e.g. proactively seeking safety improvements, implementing risk informed maintenance, auditing, and inspections).

- Phase F: Closeout

  Phase F essentially implements the system's decommissioning/disposal plan developed in previous phases. All data is archived, final reports are completed, and lessons learned are further captured.

DOI: 10.13009/EUCASS2023-893

During all of these phases, systems engineering, and the system safety organizations work hand-in-hand to ensure safe design, manufacture, and operation of the system. System safety activities are an integral part of each phase of the systems engineering process as described above. For programs on the scale of typical NASA human spaceflight programs, the overall design and certification activities prior to first flight can take years to complete. Most programs average between 5 and 7 years for completing certification, which can be financially arduous for commercial companies. A tailored, more efficient approach should be considered to ensure a more cost-effective solution.

3.2 Tailored Approach to System Certification

Because the NASA human certification process can be costly and burdensome for commercial companies, a tailored approach should be considered. As previously discussed, the typical NASA certification process includes showing compliance to many NASA standards and thousands of requirements, as well as going through multiple system safety reviews which can take years. However, the goal should not be a comparison of a commercial companies processes and standards to those of NASA, nor should it be for the certifying entity to manage the design of the system. The goal should be an independent assessment of the engineering and manufacturing processes and quality based on historical experience and provide an objective assessment regarding the systems performance and safety capabilities. The results of such an assessment should be an overall evaluation of the safety of the vehicle and its operation, along with identified and evaluated risks. After this evaluation is complete, discussions can begin as to whether or not the system is safe enough.

3.3 Safety Case Experimental Approach for Suborbital Systems

Strict compliance to NASA and/or Industry standards, processes, and requirements is not the best path forward. The most efficient approach would be a performance-based or goal-setting approach that focuses on desired, measurable outcomes, rather than on required system features or prescriptive processes, techniques, or procedures. A similar approach is already discussed in existing NASA handbooks, specifically in “NASA System Safety Handbook, Volume 1, System Safety Framework and Concepts for Implementation” (NASA SP-2010-580) and in “NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples” (SP-2014-612).

This approach can be tailored slightly to provide a more cost-effective solution to certification of commercial human spaceflight systems. It should be left up to the commercial companies to create the justification for the safety of their systems, using structured arguments showing their designs and processes meet pre-established safety goals and objectives. The safety case approach has been successfully utilized in other industries and has also been used as an experimental approach for suborbital systems. In the case of commercial human spaceflight systems, safety goals and objectives would be pre-established. The commercial provider would provide the “safety case” including the evidence and justification showing how they meet the safety goals and objectives, as well as focus on the risks and safety concerns of the system. The safety cases are then reviewed by the certifying entity, and system risks are identified and characterized.

3.4 Critical Lessons Learned

1. Safety reviews or designed-in safety cannot occur after the design is completed.

   Safety must be considered in the earliest phases of the program and continue throughout the life cycle of the program. If not, it could be too costly to make critical design changes to improve the safety and reliability of the system.

2. Commercial Off-The-Shelf (COTS) components are not necessarily designed for critical space systems.

   Special care must be taken when choosing and utilizing COTS items in space systems. They may not be designed or built to the level of rigor of typical space system and may not withstand the harsh environments of space. If COTS items are used in critical systems, the consequences of failure could be catastrophic.

3. Safety review of “integrated software systems” can be one of the longest aspects of the safety review process.

DOI: 10.13009/EUCASS2023-893

The integration of hardware and software systems can be very complex, and ensuring the integrated system is safe for human spaceflight can be a time-consuming process. The software development process, as well software safety and software assurance can be very challenging due to system complexities and typically are the most difficult parts of the safety review process.

4. Ground processing and pre-launch operations shall not be overlooked during the integrated system safety/systems engineering development process.

   So much focus is placed on safety of the flight systems and safety during the mission, it can be easy to overlook the safety aspects prior to flight. Ground processing and operations, launch operations, as well as the design of ground support equipment (GSE) are also extremely important aspects to safely execute the mission. Failure to consider safety prior to flight could lead to costly and potentially catastrophic consequences.

5. Reentry Systems

   Complexities related to thermal control systems, deceleration systems, and parachutes have been a point of extreme schedule delays, costs, and impacts to commercial spaceflight development. All aspects of the fault tolerance, single point failures, systems analysis and system safety process should not be overlooked and proper risk management is critical in this area.

6. Understand of visiting vehicle requirements (for commercial vehicles docking with ISS or new commercially developed space stations) is critical for not delaying the development of commercial transportation systems.

   It is important for commercial companies developing visiting vehicles to understand the requirements and processes which will be required during the design and certification. Failure to do so could result in wasted time and resources performing re-work activities or performing additional analyses not initially expected.

4. Recommendations for Commercial Safety Certification for Human Spaceflight

A safety case approach, or a similar tailored approach, provides an opportunity to assess the safety of human spaceflight systems more efficiently. It is believed this method is a sound approach to meeting program safety goals and objectives without completing detailed compliance assessments. As part of the safety case justifications, companies would need to show they have specifications, processes and procedures that are in family with aerospace standards, that they follow and verify their design to those standards, processes, and procedures as well as document exceptions and assess the final risk. They would need to show they have a safety program that identifies, controls and then verifies hazards and risks. They would need to show a configuration control strategy and implementation that maintains their certification in the presence of design changes and upgrades, in addition to providing a trigger for recertification when required and would also need to demonstrate they have implemented an independent review process, that provides outside surveillance for their certification.

It is recommended this approach be implemented for commercial human spaceflight companies. Safety case justifications and associated evidence could be reviewed in a similar fashion to AS9100 audits, confirming the commercial company has the necessary processes defined, and that they are compliant with those processes, without performing a full compliance review. Rather than validating a technical design, Deep Dives/Audits would be used to demonstrate the commercial companies followed their internal processes with primary focus on significant contributors to risk and safety issues. Deep Dives would require justification based on Lessons Learned, near misses, and flight experience, and would be focused on how each informed the safety case justification.

DOI: 10.13009/EUCASS2023-893

References

[1] Bulk, Tim A. Human Rating ELVs-Past Challenges and New Opportunities, AIAA 2009-6731, *AIAA Space 2009 Conference & Exposition, Pasadena, California*

[2] Bulk, Timothy A. *How to Keep the Dream Alive*, AIAA 2002-4314, 38th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, Indianapolis, Indiana

[3] Kutter, Bernard F; Zegler, Frank; Barr, Jon; Bulk, Tim A; Pitchford, Brian;, *Robust Lunar Exploration Using an Efficient Lunar Lander Derived from Existing Upper Stages*, AIAA 2009-6566, AIAA Space 2009 Conference & Exposition, Pasadena, California

[4] https://en.wikipedia.org/wiki/List_of_spaceflight-related_accidents_and_incidents#Non fatal_incidents_during_spaceflight.

[5] *International Space Station (ISS) to Commercial Orbital Transportation Services (COTS) Interface Requirements Document (IRD)*), SSP 50808

[6] *NASA Systems Engineering Processes and Requirements*, NPR 7123.1C

[7] Alexander, Michael, et al. ; *NASA Systems Engineering Handbook*, NASA SP-2016-6105 Rev 2

[8] Dezfuli, Dr. Homayoon, et al. ; *NASA System Safety Handbook, Volume 1, System Safety Framework and Concepts for Implementation*, NASA SP-2010-580

[9] Dezfuli, Dr. Homayoon, et al. ; *NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples*, SP-2014-612