Federal Aviation Administration

# Draft

# Established Practices for Human Space Flight Occupant Safety

7/31/2013

# With Rationale

Added 9/23/2013

# TABLE OF CONTENTS

# A. INTRODUCTION

## 1 Purpose

The issuance of this document continues a conversation – a conversation between the Federal Aviation Administration's Office of Commercial Space Transportation (AST), the commercial space transportation industry, and other stakeholders on commercial human space flight occupant safety. AST has developed this document to share our thoughts about established practices for human space flight occupant safety. Ultimately, our goal is to gain the consensus of government, industry, and academia on established practices as part of our mandate to encourage, facilitate, and promote the continuous improvement of the safety of launch and reentry vehicles designed to carry humans. The outcome of this effort may also serve as a starting point for a future rulemaking project, although AST has no plans to start a rulemaking project in the near term.

## 2 Scope

The scope of this document includes suborbital and orbital launch and reentry vehicles. The document assumes that any orbital vehicle will stay on orbit for a maximum of 2 weeks, and can return to earth in under 24 hours if necessary. Orbital rendezvous and docking, long duration flights, extravehicular activity, and any flights beyond earth orbit are not explicitly covered in this document. Future versions of this document may cover such additional human space flight operations.

The established practices in this document cover occupant safety only; public safety and mission assurance are not covered. This document also takes a clean sheet approach to occupant safety, that is, it assumes no other regulations act to protect occupants from harm. This includes AST's existing regulations in 14 CFR Chapter III.

Lastly, the established practices in this document cover occupants from when they are exposed to vehicle hazards prior to flight through when they are no longer exposed to vehicle hazards after landing.

## 3 Development Process

Fifty years of human space flight by governments has provided AST with a wealth of information to use in developing this document. AST reviewed a number of existing government and private sector requirements and standards including those from the National Aeronautics and Space Administration (NASA), the European Space Agency, and the International Association for the Advancement of Space Safety. AST chose to primarily use

NASA's requirements and guidance for its Commercial Crew Program[1] to guide the development of this document. The purpose was not to copy NASA's requirements, but to use them as a means to capture areas of concern for human space flight.

We also worked closely with three organizations. We held 8 teleconferences with the Commercial Space Transportation Advisory Committee (COMSTAC) from the summer of 2012 to the spring of 2013 on various topics reflected in this document. We also worked closely with the FAA's Civil Aerospace Medical Institute on medical issues. Lastly, studies related to human space flight safety were conducted by the FAA's Center of Excellence for Commercial Space Transportation, particularly the University of Colorado and the University of Texas Medical Branch.

# 4 Level of Safety and Level of Care

## 4.1 Level of Safety

The established practices in this document are not meant to achieve a single level of safety for the industry as a whole. The wide variety of commercial human space flight activities likely to take place in the near future makes a single level of safety impractical and inappropriate. What this document does aim to achieve is to provide occupant safety measures that have historically proven to be worth the cost for most human space flight system concepts.

## 4.2 Level of Care

Two levels of care are articulated in this document. First, the occupants of commercial human spacecraft should not experience an environment during flight that would cause death or serious injury. This is a low bar, below the level of comfort that most space flight participants would want to experience.

Second, the level of care for flight crew when performing safety critical operations is increased to the level necessary to perform those operations. For example, if planned translational forces will not result in serious injuries, but the flight crew needs lower forces in order to move their arms to perform a safety critical operation, then an increased level of care is reflected in this document.

Note that we have assumed for purposes of this document that each member of the flight crew is safety critical. Also note that we have assumed that space flight participants may be called upon to perform limited safety critical tasks, such as emergency egress and restraining themselves in their seats.

[1] Specifically, CCT-PLN-1120, CCT-REQ-1130, and CCT-STD-1150.

### 4.3 Early Return and Emergencies

The assumption in this document is that if a failure occurs that leaves the system in a state where another failure may lead to a catastrophic situation, the operator will terminate the flight, providing the occupants the same level of care through the end of flight. However, in an emergency the same level of care is not expected to be maintained. The expectation in emergencies is only a reasonable chance of survival.

## 5 Structure and Nature of the Established Practices

### 5.1 Categories and Subjects

The established practices are divided into three categories: design, manufacturing, and operations. The design and operations categories are further broken down into subcategories as shown in Figure 1. Established practices that are applicable in more than one category, such as configuration management, are written only once and then referred to in subsequent categories.

### 5.2 Performance and Process Based

The established practices in this document are primarily performance based, stating a safety objective to be achieved, leaving the design or operational solution up to the designer or operator. A few process based practices are included in the document, system safety being the most prominent. The performance based practices address hazards that are present regardless of system design and operation, while the system safety process systematically addresses design and operations-unique hazards.

### 5.3 Depth and Breadth

The established practices in this document are broadly written, not going deeply into any particular practice. AST would prefer to gain consensus with industry and other stakeholders on these established practices before addressing any topic in detail.

Note also that we do not discuss how a designer or operator would verify that they meet each safety measure in this document. We recognize that this is extremely important, and is an area that we plan to work on in the future.

### 5.4 Notable Omissions

Some notable omissions from the established practices include the following:

#### *5.4.1 Pressure Suits*

Government human space flight experience has demonstrated that the ascent and reentry timeframes are the highest risk period for catastrophic failures. Given the hazard time to effect, having occupants wear pressure suits during ascent and reentry is beneficial to protect

the occupants from a potential low pressure cabin environment. However, integrating pressure suits into a spacecraft design is not trivial, nor inexpensive. Because it may not be an ideal design trade in all cases, AST has not included pressure suits as an established practice. The conduct of an occupant survivability analysis is included in the document in order to identify measures, such as pressure suits, that may increase the occupants' chance of survival in an emergency.

#### *5.4.2 Launch Escape Systems*

Government human space flight experience has also demonstrated that for some orbital systems, having the capability to separate the occupants from the launch vehicle during ascent provides a significant enhancement to occupant safety. However, escape systems are not practical for all vehicle designs, so AST has not included escape systems as an established practice. As noted above, the conduct of an occupant survivability analysis is included in the document in order to identify measures, such as a launch escape system, that may increase the occupants' chance of survival in a launch emergency.

#### *5.4.3 Health Status of Space Flight Participant*

This document does not include any medical criteria that would limit who should fly in space due to medical conditions. There is little clear statistical evidence on the actual impact of space flight on the health of an occupant with pre-existing conditions. Medical screening of space flight participants is included as a practice to inform them of risks and to ensure they will not be a danger to other occupants.

#### *5.4.4 Integration of Occupant and Public Safety*

This document does not attempt to address the integration of occupant and public safety. Actions that may be appropriate for occupant safety may have public safety implications and vice versa. This is an area of future work for AST.

# 6 This Document's Relation to …

## 6.1 Industry Standards

Given that any AST regulation of occupant safety is years away, we have collected established practices to assist in the continuous improvement of the safety of launch and reentry vehicles designed to carry humans by identifying subject areas that could benefit from industry consensus standards. There are a number of industry and government standards that address the topics covered in this document; NASA relies on many of them in its requirements for its commercial crew program. The development of industry consensus standards for these and other subject areas could have significant benefits for the safety of future commercial operations.

### 6.2 NASA Requirements

Any space transportation system that complies with NASA commercial crew requirements would likely be consistent with the established practices in this document. NASA commercial crew requirements are much more exhaustive because NASA is buying a service - for astronaut transportation services to and from the International Space Station with a 180 day duration – and needs to address mission assurance and other mission needs in addition to safety. NASA also addresses verification and incorporates a number of government and industry standards that AST has yet to address.

## 7 Technical Note

The title for each established practice in this document includes an AST-XXXX number in a parenthetical. This is for AST internal use.

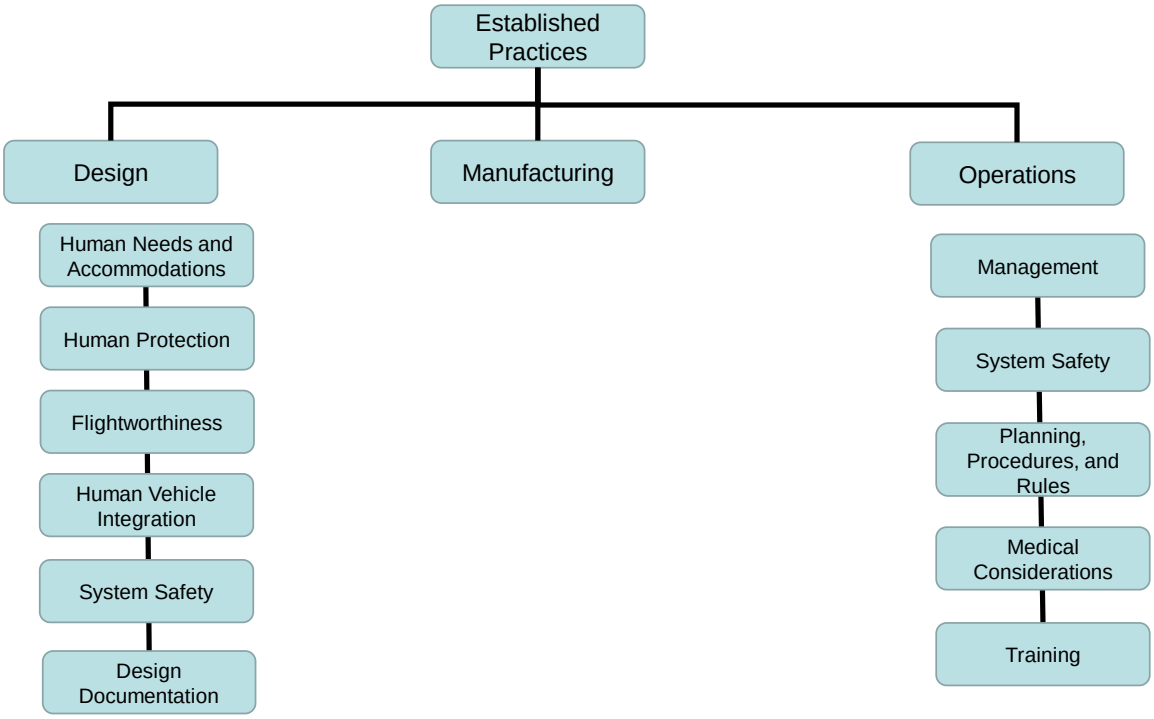


**Figure 1 - Established Practices Framework**

# B. ESTABLISHED PRACTICES

## 1 DESIGN

### 1.1 Human Needs and Accommodations

#### *1.1.1 Atmospheric Conditions (AST-1669)*

The vehicle should provide atmospheric conditions adequate to protect all occupants from serious injury and allow safety critical operations to be performed for all inhabited areas within a vehicle or a pressurized suit (if applicable). The flight crew or ground crew should be able to monitor and control the following atmospheric conditions in the inhabited areas:

a. Composition of the atmosphere, which includes oxygen and carbon dioxide, and any revitalization;
b. Pressure, temperature and humidity;
c. Contaminants that include particulates, and any harmful or hazardous concentrations of gases, vapors, and combustion byproducts; and
d. Ventilation and circulation.

Direct monitoring and control may not be necessary if analysis and testing demonstrates that they are not needed to protect the occupants from serious injury or to allow safety critical operations to be performed.

*Rationale: Occupants, including safety critical flight crew, may become sick or incapacitated if the habitable environment is either contaminated or otherwise degraded. In addition, a sick or incapacitated occupant may divert the flight crew's attention from the performance of safety critical tasks, thus endangering occupant safety. For example, very low oxygen partial pressure constitutes a severe hazard, resulting in impaired judgment and ability to concentrate, shortness of breath, nausea, and fatigue, thus affecting crew performance and potentially resulting in occupant casualty. Likewise, hazardous concentrations of gases or vapors that build up during the course of a space flight due to metabolic or other processes occurring in the cabin, or contaminants for which a source is present in the cabin (and could be further exacerbated by a lack of ventilation and circulation), can have the same result. In addition, high humidity is a factor in the formation of condensation, which is detrimental to avionics and mechanisms, and could lead to the growth and proliferation of harmful bacteria and fungi. Therefore, the capability to monitor and control these atmospheric conditions is necessary to protect occupants from harm. However, direct monitoring and control may not be necessary in all vehicle concepts, such as suborbital flights of limited duration.*

#### *1.1.2 Body Waste and Emesis Management (AST-1690)*

The system should manage body waste and emesis to protect all occupants from serious injury. For orbital missions, this should include supplies, containment, isolation, stowage, odor control, and labeling for waste containers.

*Rationale: Occupants may become sick or incapacitated if the habitable environment is either contaminated or otherwise degraded by occupant body waste and emesis. In addition, sick or incapacitated flight crew may not be able to perform their safety critical tasks. Errant body waste and emesis may also divert the flight crew's attention from the performance of safety critical tasks, thus endangering occupant safety. Because orbital flights are longer than suborbital flights, containment, isolation, stowage, odor control, and other considerations are necessary to help ensure the safety of occupants.*

### 1.1.3 Food and Water (AST-1691)

Any food and water provided to the occupants for consumption should be handled, stored, and dispensed to protect against sickness or harm.

*Rationale: Occupants may become sick or incapacitated if food and water are contaminated. In addition, sick or incapacitated flight crew may not be able to perform their safety critical tasks. A sick or incapacitated occupant may also divert the flight crew's attention from the performance of safety critical tasks, thus endangering occupant safety.*

### 1.1.4 Survival Kit (AST-1605)

The vehicle should include a survival kit that provides a reasonable chance of survival of all occupants for post-landing emergencies. The operator should consider, consistent with the design reference mission, items from each of the following categories:

a. First aid;
b. Water, water collection, and water purification;
c. Fire starter;
d. Shelter;
e. Floatation device;
f. Food;
g. Signals;
h. Navigation;
i. Communication; and
j. Survival tools.

*Rationale: A survival kit provides for occupant safety and improves an occupant's chance of survival in post-landing emergency situations. The survival kit should provide readily-accessible survival rations and equipment to support occupant needs while awaiting rescue. Since emergency landing locations and conditions are often unpredictable, the operator should use the design reference mission as a basis for determining which items should be included in the survival kit.*

## 1.2 Human Protection

### *1.2.1 Acceleration Protection (AST-1636)*

The vehicle should be designed to limit occupant exposure to transient and sustained linear and angular acceleration such that occupants are protected from serious injuries and safety critical operations can be performed successfully.

*Rationale: High rates of acceleration and extended periods of acceleration can significantly increase the risk of long term incapacitation, serious injury, or death of occupants. Excessive acceleration can also significantly increase the risk of momentary incapacitation of flight crew, such that critical tasks may be affected and, as a result, threaten occupant safety.*

### *1.2.2 Vibration Protection (AST-1641)*

The vehicle should be designed to limit occupant exposure to vibration such that occupants are protected from serious injuries, and safety critical operations can be performed successfully.

*Rationale: Excessive vibration can significantly increase the risk of long term incapacitation, serious injury, or death of occupants. Excessive vibration can also significantly increase the risk of momentary incapacitation of flight crew, such that critical tasks may be affected and, as a result, threaten occupant safety.*

### *1.2.3 Radiation Protection (AST-1661)*

The vehicle should be designed to limit occupant exposure to the following types of radiation such that occupants are protected from serious injuries, and safety critical operations can be performed successfully:

a. Radiofrequency non-ionizing radiation; and
b. Near infrared, visible, and ultraviolet radiation.

*Rationale: Exposure to excessive radiation can significantly increase the risk of long term incapacitation, serious injury, or death of occupants. Excessive radiation can also significantly increase the risk of momentary incapacitation of flight crew, such that critical tasks may be affected and, as a result, threaten occupant safety.*

### *1.2.4 Noise Exposure Protection (AST-1653)*

The vehicle should be designed to limit occupant exposure to noise such that occupants are protected from serious injuries, and safety critical operations can be performed successfully.

*Rationale: Excessive sound pressure (noise) can cause permanent injury to occupants. Excessive sound pressure can also lead to lack of concentration and distort communications, such that critical tasks may be affected and, as a result, threaten occupant safety.*

### *1.2.5 Response to Contaminated Atmosphere (AST-1562)*

In order to respond to a contaminated atmosphere, the vehicle should provide equipment and provisions to limit occupant exposure to the contaminated atmosphere such that occupants are protected from serious injuries, and safety critical operations can be performed successfully. The vehicle should:

a. Provide breathable air and eye protection for each occupant;
b. Provide voice communication between the flight crew and the ground crew; and
c. Provide voice communication from the flight crew to the space flight participants.

*Rationale: Fire, toxic out gassing, and chemical leaks can degrade a spacecraft's atmosphere such that occupants become casualties due to asphyxiation, chemical burns, or eye injury. In addition, such emergencies are difficult to manage by the flight crew due to the hazard of inhalation or eye injuries. The use of a self-contained breathing apparatus, for example, can protect occupants from the hazard, and allow the flight crew to manage the emergency. The ability to communicate orally with the ground and within the spacecraft while wearing emergency gear is important to respond to the event.*

### *1.2.6 Medical Kit (AST-2205)*

The vehicle should provide first aid and medical equipment for treatment of injuries or medical emergencies that might occur during flight, consistent with the design reference mission and the number of occupants.

*Rationale: Injuries to astronauts have been common during space flight, including musculoskeletal injuries, abrasions, contusions, lacerations, a foreign body in the eye, burns, and common illnesses. As such, it is expected that medical injuries may be sustained during space flight. Having first aid and medical equipment on board, consistent with the design reference mission and the number of occupants, should help mitigate illness and credible injuries sustained in flight.*

## 1.3 Flightworthiness

### *1.3.1 Failure Tolerance to Catastrophic Events (AST-1551)*

a. The system should control hazards that can lead to catastrophic events with no less than single failure tolerance, except when redundancy adds complexity that results in a decrease in overall system safety, or when fault tolerance is not practicable as a system safety solution.
b. When failure tolerance is not practical, such as for primary structure, pressure vessels, and thermal protection systems, an equivalent level of safety should be achieved through other means such as factors of safety, high reliability, and other design margin techniques.

*Rationale: Failure tolerance can mitigate critical hazards leading to catastrophic events and improve the overall system safety. In cases where the risk remains high after applying single failure tolerance, additional redundancy may be appropriate. Additionally, the overall system reliability is a significant*

*element used in the determination of the level of redundancy. Redundancy alone without sufficient reliability does not improve the overall system safety.*

*Where failure tolerance is not the appropriate approach to control hazards, specific measures should be employed to achieve an equivalent level of safety. Measures that may achieve an equivalent level of safety include demonstrated reliability, design margin, and other techniques that account for the absence of failure tolerance.*

### *1.3.2 Limitations on Failure Tolerance (AST-1552)*

The system should provide failure tolerance capability without:

a. Using extravehicular activity;
b. Using emergency equipment;
c. Using abort systems, such as a launch escape system;
d. Using emergency operations; or
e. Relying upon in-flight maintenance.

*Rationale: Effective failure tolerance should not rely on time consuming and potentially dangerous crew intervention. Where redundancy is required to satisfy failure tolerance requirements, the redundancy should be built into the system and not rely on in-flight maintenance or extravehicular activities to replace a failed component or avionics unit. An additional component that is onboard the spacecraft but not designed to be a functional operating part of the system without in-flight maintenance would not be considered to meet this established practice.*

*Emergency operations, equipment, and abort systems should be reserved only for emergency situations to mitigate the effects of a hazard, when the first line of defense, in the form of failure tolerance, cannot prevent the occurrence of the hazardous situation. Emergency systems and equipment, such as fire suppression systems, fire extinguishers, emergency breathing masks, launch and entry pressure suits, ballistic unguided entry capability, and ascent aborts, are not considered part of the failure tolerance capability.*

### *1.3.3 Separation of Redundant Systems (AST-1553)*

The vehicle should separate or protect redundant safety critical systems and subsystems such that an unexpected event which damages one is not likely to prevent the other from performing its function.

*Rationale: Redundancy alone does not meet the full intent of failure tolerance. Separation of redundant systems reduces the likelihood that an unexpected event which damages one system will prevent the other from performing its function. Occupant safety can be improved with a design that provides the maximum protection possible from a common cause event that would lead to failure of redundant systems.*

### *1.3.4 Isolation and Recovery from Faults (AST-1554)*

The system should detect and isolate faults that could lead to loss of a safety critical function, and recover the lost function.

*Rationale: Safety critical functions should continue in the presence of a fault. Detecting and isolating a fault prevents further propagation of the hazard. The system should recover functionality by activating the associated redundant system in time to prevent a catastrophic event. The isolation of faults should not interfere with the implementation of failure tolerance.*

### 1.3.5 Structural Design (AST-1772)

The vehicle's structural design should have sufficient strength to withstand operational loads and the thermal environment throughout the design reference mission without experiencing yield or detrimental deformation. The vehicle structure should be designed with appropriate margin to account for the uncertainty of the maximum expected operational environment, design tolerances, and manufacturing variations.

*Rationale: Maintaining structural integrity is a fundamental safety aspect of human space flight. The vehicle should be designed with sufficient margin such that operational loads and the thermal environment expected during the design reference mission do not exceed the upper load limits of the structure. Accounting for the uncertainties in the maximum expected operating environment, design tolerances, and manufacturing variations in the structural margin assures structural integrity.*

### 1.3.6 Probability of No Penetration by Micrometeoroids or Orbital Debris (AST-2210)

For orbital flight, the vehicle should provide micrometeoroid or orbital debris shielding sufficient to be equal or better than the probability of 0.99995 of experiencing no safety critical penetration over the period of the mission.[2] The operator may use a combination of design and operations (e.g. attitude) to satisfy this practice.

*Rationale: For micrometeoroids and orbital debris (MM/OD) that cannot be detected or avoided, shielding mitigates damage to safety critical systems that could result in the loss of a vehicle or endanger the occupants. Allowing for no critical penetrations is not achievable; therefore, using a probabilistic model reasonably protects the occupants while allowing for a technically feasible design.*

*The minimum acceptable probability derives from International Space Station (ISS) experience as documented in NASA's SSP 50808 interface requirements document for the ISS. The minimum allowable probability of no penetration (PNP) is a function of the vehicle MM/OD critical surface area and its total exposure time to the environment: PNP >= (0.99998) ^ (Area* Time) where Area is the surface area of the vehicle containing MMOD critical hardware (in square meters) and Time is in years of exposure to the environment. Given the assumption of a two week flight (0.038356 years), conservatively assuming the entire vehicle surface area is critical and has an area of 46.43 $m^2$ (representative of many operational and proposed vehicles), and then reducing it slightly to allow for even an more achievable design yields a PNP of 0.99995.*

*In addition to shielding and reduction of the critical surface area, operational attitudes may be used to satisfy this practice by reducing exposure of the critical surface area to the MM/OD environment.*

[2] The use of a specific number is not typical in this document. We are interested in COMSTAC's view of a different way to state this established practice.

### *1.3.7 Materials and Processes (AST-1737)*

The vehicle should be designed to ensure that materials are compatible and do not result in a hazardous condition. For habitable volumes, the materials must be compatible such that they do not result in a toxic atmosphere, act as an ignition source, or generate particulates that could lead to serious injury.

*Rationale: Poor material choices may lead to a hazardous condition that unnecessarily puts occupants at risk. This practice significantly mitigates hazards that can be avoided with proper selection or testing of materials during design. More stringent material selection is necessary in the habitable volume because the occupants are susceptible to additional hazards such as a toxic atmosphere or particulates.*

### *1.3.8 Natural and Induced Environments (AST-1560)*

The system should be designed to operate in all expected natural and induced environments.

*Rationale: The environment (natural and induced) impacts the design and operation of a system and, if not accounted for properly, can have detrimental effects on safety. An understanding of the environment is necessary to identify the design and operational limitations of the system. For example, certain natural environments (e.g. temperature, humidity, and lightning) and induced environments (e.g. propulsive thermal loads, acoustic shock, and vibration) should be taken into account to avoid exceeding any system capability.*

### *1.3.9 Electrical Systems (AST-1754)*

The vehicle's electrical circuitry and electrical power distribution, including mating and demating of electrical connectors, should be designed to:

a. Prevent any electrical shock hazard to occupants;
b. Fail safe;
c. Prevent the generation of molten material; and
d. Prevent electrical wires from overheating.

*Rationale: Improperly designed electrical systems could lead to a fire, injury, or damage to safety critical systems such that the occupants are unnecessarily put at risk.*

### *1.3.10 Vehicle Stability (AST-1548)*

A vehicle whose safe flight requires a certain attitude during one or more phases of flight, should be either inherently statically and dynamically stable in that orientation during that phase or phases, or controllable to a safe attitude.

*Rationale: Maintaining a safe attitude is a fundamental safety aspect of human space flight. When a vehicle requires maintenance of a specific attitude, maintenance of that attitude may be accomplished with either an inherently stable design (statically and dynamically) or using control systems such as thrusters and aero surfaces. Either method should account for normal flight, dispersed conditions, and certain failure conditions. For vehicles utilizing control systems to maintain a safe attitude, they should*

*have sufficient control power available to initiate or counter a translation or rotation in the presence of disturbances.*

*Not all phases of flight may require a specific attitude to be safe. For example, the Vostok spacecraft was designed to reenter in any attitude, having a spherical design with thermal protection on all sides. Some control of the capsule orientation was possible by repositioning heavy equipment to offset the vehicle's center of gravity, which was done to maximize the cosmonauts' chance of surviving the g-forces.*

### *1.3.11 Smoke Detection and Fire Suppression (AST-1565)*

The vehicle should have the ability to detect smoke within the habitable volume and alert the flight crew. The vehicle or an occupant should have the ability to extinguish a fire in the habitable volume.

*Rationale: In enclosed spaces, fire significantly threatens occupant safety and alerting the flight crew to the presence of smoke allows for quick action to mitigate the hazardous effects. Firefighting capability may be accomplished using a fire suppression system integrated with the vehicle, portable fire extinguishers, or both.*

### *1.3.12 Occupant Location Post-Landing (AST-1568)*

The vehicle should have an independent, portable, and automatic means to provide occupant location to rescue personnel. The vehicle should also be equipped with visual aids to assist rescue personnel. This practice does not apply to local suborbital flights.

*Rationale: In unforeseen or emergency situations, the vehicle may not land at its preplanned location. Experience has shown that providing rescue teams with information as to the vehicle's location increases their probability of being found; thereby increasing their chance of survival. A portable locating method, which is independent of the vehicle, allows the locator to remain with the occupants if they must depart from the vehicle area. Automatic activation of the locator increases the occupant's chance of survival in the event they become incapacitated or unable to manually activate the device. Visual aids such as flashing lights, sea dye smoke, or high contrast portions of the vehicle assist rescue forces in locating the vehicle. The limited range of local suborbital flights significantly constrains the search area leading to a high probability of locating the occupants quickly even without these provisions; therefore, the established practice does not apply.*

### *1.3.13 Vehicle Communication With Rescue Personnel (AST-1599)*

Post-landing, the vehicle should be capable of communicating with rescue personnel on an International Air Distress (IAD) frequency.

*Rationale: In unforeseen or emergency situations, communicating with rescue personnel improves the occupant's probability of being rescued thereby increasing their chance of survival. Communicating on an International Air Distress (IAD) frequency follows search and rescue standards and allows for worldwide coverage. Human space flight history provides numerous examples of vehicles failing to land at their preplanned landing location, and of forces searching to find them. Both vehicle design and operations work cooperatively to successfully communicate with rescue personnel.*

### *1.3.14 Qualification (AST-1865)*

The design of the vehicle's safety critical systems should be tested beyond the maximum expected operating environment, to demonstrate adequate design margin. The level beyond the maximum expected operating environment should be selected to encompass the uncertainty of the environment, design tolerances, and manufacturing variances.

*Rationale: Qualification of safety critical systems demonstrates that they function properly in the maximum expected operating environment. Qualification beyond the maximum expected operating environment ensures margin for potential uncertainties in the design, manufacturing, operations, or environment.*

### *1.3.15 Flight Demonstration (AST-1866)*

Prior to any flight with a space flight participant, the integrated performance of a vehicle's hardware, any software, and operational procedures should be demonstrated by successfully executing a flight of the vehicle's design reference mission. Further flight demonstration should be conducted for any subsequent modifications that cannot be tested at the integrated system level on the ground.

*Rationale: Completion of a flight demonstration assures the system has been exposed to its expected operating environment, and verifies its flightworthiness. This demonstration does not test the entire operating envelope but sufficiently exercises the system capabilities, software, operations, and procedures necessary to safely execute a flight carrying space flight participants.*

*Any subsequent modification potentially invalidates the original demonstration and should be addressed through testing at the integrated system level or by another demonstration test before subjecting space flight participants to risk of the change.*

## 1.4 Human Vehicle Integration

### *1.4.1 Anthropometric Considerations (AST-1684)*

The vehicle should be designed such that any safety critical operation requiring human interaction with the vehicle can be physically performed by an occupant. At a minimum, the following factors should be taken into account:

a. The flight configuration of the occupants, vehicle, and equipment;
b. Acceleration limits;
c. Vibration limits;
d. Noise limits;
e. Vision limits;
f. Tactile limits;
g. Temperature (environmental and touch);
h. Sharp edges; and

i. Ergonomics.

*<u>Rationale</u>: Ignoring human-to-vehicle interface issues can have adverse and unpredictable effects on an occupant's ability to perform safety critical tasks. History with space flight systems has demonstrated a large variability in the occupants that execute flight operations. Without accommodation of these variables, i.e. measurements and proportions of the human body and other factors, safety critical operations may become hindered causing serious injury to the occupant.*

a. *Flight crew's ability to successfully actuate controls in their intended flight configuration and environment (e.g. vertical launch configuration, space suited crew, and loaded crew compartment) is extremely important during dynamic phases of flight. Considerations include hand controls, seat dimensions, hatch or entry opening size, the distance from the seat to controls, and handle dimensions.*
b. *Control interfaces (e.g. control stick pivot axis) should be designed to be operable, appropriately, by the flight crew during vehicle acceleration and deceleration.*
c. *Proper occupant restraints are critical while operating controls in vehicle vibration scenarios. During flight phases where high vibration is expected, relevant displays may also need to be designed with legibility in mind (e.g. analog versus digital displays, and larger graphics and text).*
d. *Loud noises for extended durations in the habitable volume can distract occupants resulting in mistakes during safety critical operations.*
e. *Improper font size, viewing angle, parallax, and legibility can result in mistakes during safety critical operations.*
f. *If pressurized suits are worn by occupants, the ability to use the sense of touch is diminished as a gloved hand may not have the dexterity to operate certain safety critical vehicle interfaces.*
g. *An occupant's ability to perform safety critical tasks could be hampered by the temperature of the interface (e.g. touchscreen that is too hot to touch). Extreme touch temperatures, both hot and cold, can cause an occupant pain and distract from the performance of safety critical tasks.*
h. *An occupant's ability to perform safety critical tasks could be hampered by surfaces with sharp edges. Sharp edges can cause an occupant pain and distract from the performance of safety critical tasks.*
i. *Ergonomics is important for the timely and accurate processing of information by the occupant. Discomfort, due to poor ergonomics, could distract an occupant from a safety critical task.*

### *1.4.2 System Health, Status, and Data (AST-1557)*

For safety critical functions allocated to the ground crew or flight crew, the system should provide the health, status, and engineering data necessary to perform the function. At a minimum, the ground crew or flight crew should be able to determine if a level of failure tolerance is lost in a safety critical system.

*<u>Rationale</u>: To make informed decisions and perform anomaly resolution during a flight, the flight crew or ground crew requires accurate vehicle health, status, and engineering data. Conducting safety critical operations without necessary data could result in catastrophic consequences. A safe operation depends on accurate information.*

### 1.4.3 Manual Override of Automatic Functions (AST-1570)

The system should allow the flight crew or ground crew to manually override any automatic safety critical function when the override of the function will not directly cause a catastrophic event.

*Rationale: During certain unforeseen events, the capability to manually override automatic functions may prevent serious injury to the occupants. Without this functionality, an automatic function could have an undesirable effect and result in injury to the occupants. Engineering judgment and historical events (e.g. engine sensor failure in STS-51-F overridden to prevent shutdown) show that this functionality is important and should not be overlooked during the design of the vehicle. As long as an override of an automatic function is feasible and will not directly cause a catastrophic event, the flight crew or ground crew should have this capability.*

### 1.4.4 Detection and Annunciation of Faults (AST-1556)

The system should detect and annunciate safety critical vehicle system faults to the flight crew.

*Rationale: To make decisions, and perform anomaly resolution during a flight, the flight crew needs to be alerted whenever a safety critical system experiences a fault. Without this detection and annunciation, the flight crew would not be aware of the vehicle state of health and would lack insight on whether the flight crew needs to recover a safety critical system or terminate the flight. A detection and annunciation system decreases the cognitive load on the flight crew and allows the flight crew to concentrate on safety critical tasks.*

### 1.4.5 Orthostatic Protection (AST-1596)

The vehicle should provide orthostatic protection to the extent necessary for occupants to perform safety critical operations.

*Rationale: Orthostatic intolerance is a well-described consequence of space flight, and prevention is needed to protect occupant safety. Symptoms and consequences of orthostatic intolerance include dizziness, confusion, and loss of consciousness, which may result in an inability to operate controls, complete safety critical tasks, and egress from the vehicle without assistance. Thus, without appropriate mitigation, an occupant suffering from the effects of orthostatic intolerance could jeopardize safe and successful reentry, landing, and egress, particularly in the event of an emergency before first responders are available.*

### 1.4.6 Voice Communication Between Flight Crew and Ground Crew (AST-1617)

The system should provide single fault tolerant two-way voice communication between the ground crew and the flight crew from pre-launch through landing. This practice is not meant to imply 100% continuous communication for all phases of flight.

*Rationale: Communication between the ground crew and flight crew enhances the ability to resolve anomalies should they occur. The intent of this practice is to ensure communications availability during critical flight phases.*

*Historically, the ascent and entry phases of human space flight have been the timeframe of greatest risk for occupants. Previous space flights have shown that for powered ascent, there are a multitude of timely systems responses that ground crew can assist with, leading to the need for communications that can be accommodated by ground or space based communication assets. By contrast, for reentry, due to its dynamic conditions and communications dropouts, the need for continuous communication is less than that for ascent. Critical events during reentry (e.g. separations, parachute deployment, and key navigation events) and the final phase of landing where the risk is the highest warrant voice communication between the ground crew and flight crew.*

### *1.4.7 Noise Level for Occupant Communication (AST-1657)*

The vehicle should be designed such that occupants can communicate orally with each other during safety critical operations.

*Rationale: Oral communications is instrumental for effective communications during safety critical operations. Loud environments can become distracting, become a communication barrier, and put occupants at risk. Limiting background noise, intermittent noise, sound pressure levels, or providing volume control or noise canceling on an electronic communication device contributes towards enabling effective voice communication. If an electronic communication device is not used, the habitable volume sound levels would need to be adjusted to allow for an occupant to speak and be heard during safety critical operations.*

### *1.4.8 Views for Flight Crew Tasks (AST-1628)*

For a safety critical operations requiring an external view by the flight crew, the vehicle should provide direct, non-electronic, through-the-hull viewing and the unobstructed field-of-view necessary to perform the operations.

*Rationale: Providing direct, non-electronic, through-the-hull viewing may be essential to safety critical operations, such as landing the vehicle, as well as to maintain flight crew situational awareness and safety. A window is an example of a design that would meet this practice as it can provide a direct, non-electronic, through-the-hull viewpoint. While windows do have some design drawbacks, windows do not have the failure modes associated with cameras and display systems that, if failed, could put the flight crew in an emergency scenario. Other operations that benefit from this practice, aside from landing the vehicle, include on-orbit vehicle piloting tasks, stellar navigation, and vehicle anomaly detection and inspection.*

### *1.4.9 Inadvertent Actions (AST-1630)*

No single inadvertent flight crew or ground crew action should result in an event causing serious injuries to occupants.

*Rationale: In the unforgiving environment of space flight, an inadvertent flight crew or ground crew action could lead to serious injuries to occupants. Inadvertent action could occur due to a number of factors such as recency of crew experience, gloved hands, ambiguous procedures, the flight environment (e.g. vibration), a stressed operational environment, and inadvertent bumping of controls. For example, an inadvertent hatch opening and subsequent cabin depressurization while in the vacuum of space would lead to serious injuries to occupants. Preventing the hatch from opening, in this example, should*

*be part of the vehicle design. From the ground crew perspective, using an "arm-fire" method to initiate events could prevent serious injuries to occupants.*

### *1.4.10 Flight Crew Loads (AST-1687)*

Safety critical vehicle systems (e.g., switches, knobs, handles) should be designed to withstand intentional flight crew input loads without losing safety critical functionality.

*Rationale: Humans may exert high forces when operating controls, such as attempting to open a hatch for emergency egress. The resulting damage to equipment could make it impossible to perform a safety critical task. Therefore, safety critical systems should be designed to withstand foreseeable forces exerted by a flight crewmember without breaking or sustaining damage that would deem the hardware inoperable. This includes hardware that may be inadvertently used as a mobility aid or restraint. This practice is applicable to intentional forces imparted on hardware by a flight crewmember as opposed to unintentional or accidental forces (e.g. kicking).*

### *1.4.11 Instrumentation Displays (AST-1705)*

Instrumentation should display safety-critical information that is readable in the environment of intended use. At a minimum, the following factors should be taken into account: luminance, contrast, ambient illumination, glare, resolution, vehicle vibration, and viewing angle.

*Rationale: Readable displays are necessary in the environment that safety-critical tasks are being performed. Internal and external sources of light can create glare or reflections that can interfere with the flight crew's performance of safety critical operations. The sun, Earth, and any solar arrays, external reflective material, camera lights, and internal volume lighting are just some of the sources that can result in glare or reflections on displays. In addition, these sources of light can also obscure or distort a display image and distract the flight crew from their task. Vehicle vibration and user viewing angle can also affect the readability of the information.*

### *1.4.12 Control of Glare and Reflection (AST-1721)*

Glare and reflection on windows and displays should not interfere with flight crew performance of safety critical operations.

*Rationale: Internal and external sources of light can create glare or reflections that can interfere with the flight crew's performance of safety critical operations.*

*The sun, Earth, and any solar arrays, external reflective material, camera lights, and internal volume lighting are just some of the sources that can result in glare or reflections on windows and displays. In addition, these sources of light can also obscure or distort a display image and distract the flight crew from their task.*

*The design and operation of the vehicle should plan for these vehicle orientations and allow for safe operations by blocking or eliminating glare and reflection. By varying the orientation of a launch or reentry vehicle, instances in which the sun will shine directly on windows or displays creating glare or reflections can be minimized.*

### *1.4.13 Handling Qualities (AST-1627)*

The vehicle should be controllable to the extent necessary to allow the flight crew to perform their safety critical operations.

*Rationale: Proper vehicle handling qualities (e.g. Cooper-Harper Rating Scale) that do not overburden the flight crew are necessary to provide the occupants with a safe flight. Excessive demands on the flight crew due to poor handling qualities could lessen the flight crew's ability to handle off-nominal situations.*

### *1.4.14 Workload Analysis (AST-1646)*

A workload analysis should be conducted to ensure that safety critical operations can be performed under expected flight crew and ground crew workload.

*Rationale: Poorly designed user interfaces tend to increase the probability of certain errors in use, particularly during a heavy workload. An analysis (e.g. Bedford Workload Scale) of the flight crew and ground crew interfaces, tasks, workload, and error rates is important to ensure that crew workload does not result in errors related to safety critical tasks.*

### *1.4.15 Emergency Control Markings (AST-1716)*

The vehicle should provide clearly marked emergency controls that are distinguishable from non-emergency controls.

*Rationale: In emergency situations, quickly identifying emergency controls and not confusing them with non-emergency controls may prevent serious injury to occupants. Coding helps occupants identify appropriate controls or mechanisms allowing faster reaction times in an emergency situation. Coding of controls and mechanisms also helps avoid the accidental accessing of an emergency control.*

### *1.4.16 Emergency Equipment (AST-1561)*

The vehicle should be designed such that the flight crew can access equipment involved in the response to emergency situations, in all flight phases, within the time required to respond to the hazard.

*Rationale: In emergency situations, having timely access to emergency equipment gives the flight crew an opportunity to address the emergency and increases the likelihood of occupant survival. The design should take into account emergency scenarios requiring access to equipment. The location and proximity of emergency equipment to the flight crew impacts accessibility and response time.*

### *1.4.17 Emergency Lighting (AST-1564)*

For orbital flights, and sub-orbital flights at night, the vehicle should provide:

a. Emergency lighting for occupant egress and operational recovery in the event of a general power failure; and
b. A flashlight (or other personal lighting device) for each flight crew member readily available at all times.

*Rationale: In emergency situations, emergency lighting is considered a basic element aiding in a reasonable chance of survival of the occupants. The emergency lighting system could include unpowered illumination sources that provide markers or orientation cues for occupant egress. A flashlight or other personal lighting device is a low cost item that can assist each flight crew member in a lights-out condition to address an unforeseen or emergency situation.*

### *1.4.18 Vehicle Egress (AST-1606)*

The vehicle should:

a. Provide for unassisted egress of the occupants;
b. Be designed to allow all occupants to physically egress in less than 90 seconds[3] to protect the occupants from pre-launch and post-landing hazards;
c. Allow the hatch to be opened from the inside by a single occupant, and from the outside by ground personnel and rescue personnel; and
d. Provide the ability of the occupants to visually determine hazards outside the vehicle on the primary egress path without the use of vehicle electrical power.

*Rationale: Occupants must be able to egress the vehicle to the launch platform or post-landing surface in the event emergencies occur during the pre-launch or the post-landing timeframe. This practice assumes the occupants are able to function in a 1-g environment.*

*In emergency situations:*

*a. Unassisted egress is needed in the event that no one is available to assist occupants to avoid serious injuries.*
*b. Getting the occupants out of the vehicle in adequate time is necessary to avoid serious injuries. The occupants should have an egress path that allows egress of all occupants in enough time to protect from pre-launch and post-landing hazards. The 90 second timeframe is consistent with past space flight programs (e.g. Apollo, Space Shuttle) and current aviation practices (e.g. FAA Part 121).*
*c. Having a hatch that is operable by a single occupant is important in an emergency scenario where the vehicle must be egressed in a timely manner. Allowing the hatch to be opened by ground or rescue personnel would help in an emergency situation where occupants are incapacitated or in a deconditioned state.*
*d. Visual observation of the environment outside the vehicle allows the occupants to determine the conditions or obstructions, such as the presence of fire or debris, and determine if egressing the vehicle is safe. Visually determining hazards outside the vehicle without needing vehicle electrical power, such as through a window, protects occupants from failure scenarios involving the loss of electrical power.*

[3] The use of a specific number is not typical in this document. We are interested in COMSTAC's view of a different way to state this established practice.

## 1.5 System Safety

### *1.5.1 System Safety Management (AST-1855)*

A system safety program plan should be developed and maintained that documents an integrated, systematic, and comprehensive approach for identifying hazards and managing risks to occupants. This plan should:

a. Define the management authority, management functions, and safety responsibilities within the program, and the means by which safety decisions are made throughout the life-cycle of the system;
b. Provide for the communication of risk throughout the program and the approach for acceptance of risk to ensure residual risk is managed;
c. Include methodologies for performing assessments of the likelihood of occurrence and the severity of a mishap should it occur, including definitions for likelihood and severity categories that will be used to ensure a uniform method of assessing hazards;
d. Describe the hazard identification and analysis techniques, including tools, methodologies, and sources from which data is drawn;
e. Provide for closed-loop tracking of hazards, risks, mitigation measures, and verification activities; and
f. Include a process that ensures the accuracy and validity of the hazard analysis throughout the life-cycle of the program, including –
    1. Changes to safety critical designs, procedures, flight rules, flight profiles, and operations, and
    2. Results and corrective actions from anomaly and mishap investigations.

*Rationale: Without a comprehensive and systematic approach to system safety, there exists the potential that the hazards in a system will not be known, understood, and controlled, resulting in an increase in residual risk. Space systems intended to fly people are generally very complex. As the number of subsystems increase, designers and operators are challenged with the identification and mitigation of the risks these space systems introduce. In a very real sense, complexity hides safety concerns in reams of interlocking documentation, all of which appear to demonstrate that the relevant system is safe. A system safety program planning process is a means of synchronizing definitions and methods so that engineers, designers, testers, and users all speak the same language regarding risk and its management. Planning allows an organization to better mitigate the effects of complexity, and a system safety program plan reduces the perceived complexity of hazard analyses by standardizing the definitions and approaches to be used.*

### *1.5.2 System Safety Engineering (AST-1550)*

A hazard analysis process should be implemented at the beginning of the development cycle to identify and characterize each hazard, assess the risk to occupant safety, reduce risks through the use of risk elimination and mitigation measures, and verify that risks have been reduced to an acceptable level as defined in the system safety program plan. Hazard analyses should be

continuously updated throughout the life-cycle of the system. The hazard analysis process should:

a. Identify the causes of each hazard, including those that result from:
    1. Component, subsystem, or system failures or faults;
    2. Software errors and operations;
    3. Environmental conditions;
    4. Human errors;
    5. Design inadequacies;
    6. Procedural deficiencies;
    7. Incompatible materials;
    8. Functional and physical interfaces; and
    9. Component interactions.
b. Characterize the risk for each hazard before risk elimination, mitigation of the causes, or implementation of equipment or capabilities to assist occupant survivability in an emergency.
c. Identify and describe the risk elimination and mitigation measures necessary to ensure that the hazard causes do not manifest themselves. The measures should include one or more of the following:
    1. Designing for minimum risk;
    2. Incorporating safety devices;
    3. Providing warning devices; and
    4. Implementing procedures and training.
d. Demonstrate that the risk elimination or mitigation measures have been successfully implemented by objective verification evidence, in order to ensure that the likelihood of occurrence and consequence of each hazard are mitigated to an acceptable level as defined in the system safety program plan. Verification should include:
    1. Test data;
    2. Inspection results; or
    3. Analysis.
e. Document for each hazard:
    1. The risk elimination or hazard controls for each hazard cause and the associated verification method used to demonstrate that the risk reduction measures have been implemented and are effective in reducing risk prior to each flight; and
    2. A qualitative summary rationale for accepting the risk associated with the hazard.

*<u>Rationale</u>: Complex systems introduce safety concerns, most of which arise from the interactions of subsystems. These complex interactions cannot be thoroughly planned, understood, anticipated, or guarded against and hence increases the potential for unanticipated harm to the occupant. Hazard analysis is a proven engineering discipline that, when applied during system development and throughout the system's life-cycle, identifies and mitigates hazards, and in so doing eliminates or reduces the risk of potential mishaps and accidents. The system safety engineering process outlined in this document is consistent with common industry practice.*

### *1.5.3 Software Safety (AST-1739)*

a. As part of its system safety process, hazards from computing systems and software should be identified and risks to occupants should be assessed.
b. Each safety-critical function associated with computing systems and software should be identified. Safety-critical computing system and software functions should include the following:
    1. Software used to control or monitor safety-critical systems;
    2. Software that transmits safety-critical data, including time-critical data and data about hazardous conditions;
    3. Software used for fault detection in safety-critical computer hardware or software;
    4. Software that responds to the detection of a safety-critical fault;
    5. Software that computes safety-critical data;
    6. Software that accesses safety-critical data;
    7. Software used to model or simulate safety critical parameters or functions; and
    8. Software that shares hardware resources with safety-critical data, or that shares command pathways with safety-critical data.
c. The system safety engineering process should include analysis of software and computing systems.
d. Risk elimination and mitigation measures should be identified for computing system and software risks.
e. The system safety engineering process should include the development and implementation of a computing system and software validation and verification plan.
f. The system safety engineering process should document a software development plan that describes a disciplined approach to software development, verification, and risk analysis.

*Rationale: Software and computing systems have become an integral part in the operations of a space flight system. Software is used to perform complex maneuvers, issue safety critical commands, monitor for and respond to events that could lead to a catastrophic result, and provide critical data used to make safety-critical decisions. Therefore, software can be a source or a control to hazards. Software system safety is an element of the total safety approach, and is implemented in the software development program to achieve an acceptable level of safety for software and computing systems used in safety critical applications. The software safety process outlined in this document is consistent with common industry practice.*

### *1.5.4 Occupant Survivability Analysis (AST-2208)*

An occupant survivability analysis should be conducted to identify what additional equipment or capability might provide the occupants with an increased chance of survival if a catastrophic hazard occurs. The decision whether or not to incorporate any specific result from the analysis should be documented.

*Rationale: Despite best efforts, hazards may occur during space flight. An occupant survivability analysis is intended to determine if there are design changes that may increase the chances of crew survival in emergency situations. Implementation, however, is a function of overall risk the commercial operator is willing to assume verses the cost of implementing a design change or providing additional equipment. The occupant survival strategy is determined by the designer or operator and could include a collective implementation of abort, escape, emergency egress, safe haven, emergency medical, and rescue capabilities throughout a flight.*

## 1.6 Design Documentation

### *1.6.1 Operational Documentation (AST-1844)*

Documentation should be developed and kept current that describes how to operate and maintain the vehicle within the limitations and capabilities of the vehicle. This documentation should include the following items:

a. Vehicle and operations overview;
b. Vehicle systems descriptions, their functions and associated hazards;
c. Normal procedures;
d. Emergency procedures;
e. Performance;
f. Mass properties;
g. Consumable limitations;
h. Any limitations on occupant size, mass, and physical condition;
i. Weather limitations;
j. Landing site limitation; and
k. Maintenance program for continued flightworthiness.

*Rationale: This practice is important to the safe operation of a space system because the operator needs to be provided with a clear understanding of the performance capability, operational procedures, limitations, and hazards of the system so that the vehicle is operated as designed and within its capabilities.*

### *1.6.2 Configuration Management (AST-1847)*

A process should be implemented that provides configuration control over safety critical systems design and operation throughout the system's life.

*Rationale: This practice is important because configuration management is necessary to maintain the established system design throughout the lifecycle of the vehicle. Failure to ensure the system conforms to the established system design can lead to safety critical failures which could cause a loss of vehicle and occupants.*

# 2 MANUFACTURING

## 2.1 Manufacturing

### *2.1.1 Quality Assurance (AST-1851)*

The system should be manufactured and maintained in accordance with a quality process that ensures the system meets design specifications.

*Rationale: The effectiveness of a system safety process is predicated on the fact that the system assessed is the system that was built, maintained, and operated. When hardware or software deviates from the system analyzed, there is a potential that new sources to existing hazards can be generated, that new hazards may be created, or that existing mitigation measures can become ineffective.*

### *2.1.2 Acceptance Testing (AST-2206)*

a. Safety critical vehicle systems should be acceptance tested to their maximum expected operating environment to demonstrate that the vehicle systems are free of defects, integration errors, and are ready for operational use.
b. Safety critical ground systems should be acceptance tested to their maximum expected operating environment to demonstrate that the ground systems are free of defects, integration errors, and are ready for operational use.

*Rationale: Manufactured items are susceptible to a wide range of conditions that could ultimately affect their performance. Safety critical vehicle and ground systems that are manufactured inconsistent with the design may lead to hazards that ultimately affect occupant safety. Acceptance testing is necessary to stress vehicle and ground system hardware in order to precipitate out failures that result from manufacturing workmanship errors, latent defects of parts, and integration. Acceptance testing of safety critical systems demonstrates that they will function properly in the expected operating environment.*

### *2.1.3 Configuration Management (AST-1847)*

Refer to 1.6.2

# 3 OPERATIONS

## 3.1 Management

### *3.1.1 Flight Operations Authority (AST-2119)*

a. An operator should identify lines of communication and approval authority for all occupant safety decisions.
b. An operator should have the following management positions:
    1. An employee, referred to here as the safety official, who is authorized to examine all safety aspects of the operator's flight operations and to monitor independently personnel compliance with the operator's safety policies and procedures. The safety official shall have direct access to decision makers.
    2. An employee, referred to here as the flight director, who has the operator's final approval authority for safety critical flight operations.

*Rationale: Clear lines of communication and approval authority within a program are necessary to avoid confusion and lessen the chance that safety issues will be missed. Having an employee with the ability to independently examine the safety of operations helps ensure that safety concerns are elevated to the appropriate levels. Having one employee on the ground with final approval authority for safety critical flight operations helps ensure that real-time or near real-time safety critical decisions are made in a timely manner.*

### *3.1.2 Flight Crew Decision Authority (AST-1911)*

The operator should designate a member of the flight crew who has ultimate decision authority on the vehicle. This flight crew member is responsible for the safe operation of the vehicle and for the safety of occupants.

*Rationale: The dynamic nature of space flight often requires safety critical decisions to be made in a timely manner. To accomplish this, it is necessary to have a member of the flight crew with decision authority for the safety of the vehicle and occupants. Designating a flight crew member, independent of ground personnel, is necessary due to the flight crew's unique situational awareness.*

### *3.1.3 Quality Assurance (AST-1851)*

Refer to 2.1.1

### *3.1.4 Configuration Management (AST-1847)*

Refer to 1.6.2

### *3.1.5 System Certification (AST-1871)*

Prior to any flight, the operator should document that the system meets design and operational requirements.

*Rationale: Operating a system outside its design and operational requirements can introduce hazards. This can be avoided by the operator adopting a formal process that documents the system's compliance with requirements and readiness for flight.*

### 3.1.6 Anomaly Investigation, Tracking, and Resolution (AST-2138)

An operator should:

a. Document each anomaly that affects a safety-critical function;
b. Assess the effects of safety critical anomalies to ongoing flight operations;
c. Identify all root causes of each anomaly, and implement all corrective actions for each anomaly necessary to avoid recurrence of the anomaly; and
d. Implement each corrective action before the next flight.

*Rationale: Analysis of mishaps often shows that anomalies existed prior to the mishap. Examination and understanding of system and subsystem anomalies throughout the life-cycle can warn an operator of an impending mishap and can provide important information about what corrective actions need to be implemented to mitigate risk. Assessing the effects of safety critical anomalies during flight is important to maintain the system in a safe state, if possible, through short term operational constraints or other corrective actions.*

### 3.1.7 Accident and Incident Investigation (AST-1853)

An operator should investigate and document the cause of any launch or reentry accident or incident, and identify and adopt preventive measures for avoiding recurrence of the event prior to the next flight.

*Rationale: This practice is important because continuing to operate a system that has experienced a launch or reentry accident or incident prior to the completion of an investigation, and the adoption of preventive measures, could jeopardize the safety of occupants.*

## 3.2 System Safety

### 3.2.1 System Safety Management (AST-1855)

Refer to 1.5.1

### 3.2.2 System Safety Engineering (AST-1550)

Refer to 1.5.2

### 3.2.3 Software Safety (AST-1739)

Refer to 1.5.3

### *3.2.4 Payload Safety (AST-2211)*

Prior to each flight, an operator should identify and mitigate payload hazards using the system safety engineering approach defined in this document.

*Rationale: Payloads that are flown either within the pressurized volume or external to a spacecraft could fail or adversely interact with the vehicle and expose the occupants to toxic gasses, explosions, or fire. While the system design and operations are analyzed throughout the lifecycle to mitigate identified hazards, the wide range of potential payloads that may fly introduces the possibility that a payload might be the source of a catastrophic event.*

## 3.3 Planning, Procedures, and Rules

### *3.3.1 Operating Within Constraints (AST-1845)*

The operator should operate the system within the most current documented operating limitations and procedures.

*Rationale: Occupants can be put at risk if operations are conducted outside of documented operating limitations or procedures (e.g. SPARTAN satellite STS-87 had a crew procedural error contributing to a tumbling satellite, Space Shuttle Challenger STS-51-L operated outside its temperature limits contributing to the loss of vehicle and crew).*

### *3.3.2 Operations Products (AST-1941)*

All products necessary to execute safety critical operations, to include plans, procedures, processes, schedules, and supporting information, should be current, and consistent with the operating limits of the vehicle.

*Rationale: The use of outdated procedures can result in confusion amongst flight crew or ground crew personnel resulting in incorrect operations thereby putting occupants at risk. Using current and consistent operations products minimizes confusion and uncertainties, ensures flight safety critical procedures are completed successfully, and allows individuals with safety critical decision authority to make sound decisions.*

### *3.3.3 Procedures (AST-1999)*

An operator should have procedures for safety critical operations to operate the vehicle within its operating limits.

*Rationale: Safety critical operations typically require time critical or sequence critical actions and should be properly documented to operate the vehicle within its limits to avoid putting occupants at risk. Proper documentation, in the form of a procedure, should ensure that any safety critical operations are performed in a safe manner. Typically, procedures formalize the steps to execute operations, enabling ground crew and flight crew to ensure successful preparation and operation of the vehicle. Procedures can help ensure operations are performed within the operating limits of the vehicle, and that operations remain consistent with any launch commit criteria and flight rules.*

### *3.3.4 Integrated Operations Coordination (AST-1950)*

An operator should coordinate all plans and procedures for safety critical integrated operations among all affected entities.

*Rationale: Space flight operations often involve multiple entities, such as a launch vehicle operator, spacecraft operator, the launch complex, and landing facility. Coordinating integrated operations is challenging and it is necessary to coordinate all plans and procedures with affected parties to minimize confusion and uncertainties, ensure flight safety critical procedures are completed successfully, and allow individuals with safety critical decision authority to make sound decisions.*

### *3.3.5 Fatigue Management (AST-1667)*

The operator should implement a fatigue risk management system for all flight crew, ground crew, and safety critical ground personnel.

a. All flight crew, ground crew, and safety critical ground personnel should receive fatigue risk awareness training.
b. Flight crew duty limitations should consider:
    1. Adequate rest periods;
    2. Duty-time limitations; and
    3. Flight-time limitations which include -
        i. Flight duty period for unaugmented operation,
        ii. Split duty,
        iii. Augmented flight crew,
        iv. Flight duty period,
        v. Extensions,
        vi. Reserve status,
        vii. Cumulative, and
        viii. Consecutive nighttime operations.
c. Ground crew and safety critical ground personnel limitations should consider the following limitations:
    1. Adequate rest periods;
    2. Duty-time limitations;
    3. Cumulative; and
    4. Consecutive nighttime operations.

*Rationale: Developing rules pertaining to fatigue management are a key component to ensuring the safety of the occupants aboard a vehicle. This is due in large part to the safety critical role the flight and ground crew have during the operation of the vehicle. A fatigued crew can make mistakes that put the occupants at risk.*

*a. Fatigue risk awareness training is important to provide the flight crew, ground crew, and safety critical ground personnel awareness of the many aspects of crew fatigue, and the ability to identify the appropriate rest periods necessary to allow the crew member to return to duty fully capable.*

b. *Necessary flight crew duty limitations vary based on a number of operational factors, identified in b. of the established practice. Questions that should be considered when developing the crew limitation include whether the operation will use multiple shifts to manage a vehicle, whether crew members will be assigned to a reserve capacity, whether the crew will operate the vehicle on consecutive nights, and how to implement make-up rest to accommodate a crew that has exceeded the duty period.*
c. *Operational factors also affect duty limitations for ground crew and safety critical ground personnel, as identified in the established practice.*

### *3.3.6 Maintenance (AST-2217)*

An operator should perform maintenance and preventive maintenance in accordance with the Operational Documentation to ensure readiness for safe flight.

*Rationale: Maintenance and preventive maintenance are important to ensure the system capabilities are retained throughout the vehicle life cycle. The effectiveness of safety systems can often degrade over time and cycles through continued use, exposure to the flight environment, and testing. Failure to maintain those systems that are life limited can lead to system degradation or failure resulting in serious injury or fatality. Failing to perform maintenance and preventive maintenance in accordance with the Operational Documentation may cause the vehicle to be operated outside the limitations and capabilities of the vehicle.*

### *3.3.7 Flight Readiness (AST-1870)*

Prior to launch and reentry operations, the operator should assess and document the system's readiness for safe flight.

*Rationale: The likelihood of having a safe flight is enhanced when an operator evaluates the system's readiness. A detailed evaluation of the system, prior to launch or reentry, allows for a final review of items that include the system hardware and software, procedures, and the readiness of the flight and ground crew. The operator can assess its ability to resolve any open issues before the intended launch or reentry time. Documenting flight readiness also provides a historical reference for lessons learned and, as an additional benefit, can be useful for post-flight analysis.*

### *3.3.8 Launch Commit Criteria and Flight Rules (AST-2072)*

An operator should document operational rules and criteria that identify the system's condition and capability that should exist in order to safely ingress, begin flight, remain in-flight, reenter, and egress:

a. For nominal events; and
b. For off-nominal events.

*Rationale: Certain events during pre-flight, flight, and post-flight do not afford an operator time to develop a real-time plan to avoid the potential of a serious injury to an occupant. Predetermined operational rules and criteria, such as launch commit criteria and fight rules, help maintain a vehicle*

*within its limits. Rules and criteria can be used to provide direction for safety decisions and management of operational risks during a flight.*

### *3.3.9 Communications Protocol (AST-1983)*

All flight crew, ground crew, and ground personnel should adhere to a defined communications protocol when executing safety critical operations.

*Rationale: Executing safety critical operations using a defined communications protocol helps an operator clearly convey critical information which enhances the safety of the occupants. The use of proper protocol decreases miscommunication and increases message comprehension.*

### *3.3.10 Consumables (AST-1864)*

a. For orbital flight, the operator should carry on-board consumable quantities sufficient for the planned flight duration plus 24 hours margin including deorbit and entry, and maintain the margin up to the deorbit burn. The operator should monitor and maintain the required propellant for a nominal deorbit burn.
b. For suborbital flight, the operator should carry on-board consumable quantities sufficient to cover planned flight duration plus margin to account for variables in usage.

*Rationale: Having adequate consumable quantities with sufficient margins to address weather conditions, unplanned events, and other events outside the control of the operator, increase the likelihood for the safe return of the occupants. For orbital flight, having 24 hours of margin is an established practice for United States space flight systems.*

### *3.3.11 Operations Management (AST-2128)*

An operator should develop and execute a plan or plans to manage system emergencies, including launch escape (if applicable) and occupant rescue and recovery. The flight crew decision authority and flight director may deviate from the plan or plans in an emergency to the extent required to meet that emergency.

*Rationale: In emergency situations, an operator will not have time to develop a plan to avoid the potential of a serious injury to an occupant. In general, having a plan to manage system emergencies is necessary to successfully address the situation in the time available. For example, a launch escape plan may be necessary depending on the vehicle complexity, flight configuration, and integrated operations taking place during a launch.*

*There may be certain situations where deviations to a plan need to take place to meet the needs of an emergency. In those situations, the flight crew or flight director needs the authority to deviate from the plan.*

### *3.3.12 Landing Sites (AST-1545)*

The operator should identify a primary and a minimum of one alternate landing site prior to flight and should identify the criteria for determining when a site will be used.

*Rationale: The identification of landing sites is necessary for the safe conduct of a flight. Having an alternate landing site protects for scenarios due to primary landing site issues (e.g. landing site unavailability, and unanticipated wind gusts) or vehicle configuration issues near the time of deorbit. In addition, clear criteria for a landing site's use is necessary because space flight operations are often time critical.*

### 3.3.13 Collision Avoidance (AST-1592)[4]

a. Prior to launch for flights above 150 kilometers, the operator should verify a predicted miss distance greater than ±8 km x ±30 km x ±30 km (defined in uvw coordinates relative to the vehicle as radial x downtrack x crosstrack) exists between the human occupied object and any known man-made orbital object. If the operator can provide a consistently demonstrated covariance, they may launch if the probability of collision does not exceed 1E-6.
b. On-orbit, the operator should perform a collision avoidance maneuver, if the predicted miss distance is less than ±0.5 km x ±4 km x ±4 km (defined in uvw coordinates relative to the vehicle as radial x downtrack x crosstrack) or if the probability of collision (Pc) exceeds 1E-5. The maneuver should be performed at least 6 hours before a predicted conjunction.
c. Before maneuvering to a new orbit, the operator should have the orbit screened to ensure compliance with paragraph b. of this section.

*Rationale: Avoiding known man-made orbital objects (those tracked by U.S. Strategic Command) by delaying a launch or maneuvering on-orbit protects the occupants from the potentially catastrophic consequences of a collision. Screening for potential conjunctions using an exclusion volume allows for simple and conservative assessments when vehicle states are not well known. If a vehicle's state is well known, after sufficient tracking by U.S. Strategic Command or with a consistently demonstrated launch covariance, probabilistic screening can reduce operational impacts.*

*In the pre-launch timeframe, a launch can be delayed to allow clearance from an object that has a high risk of collision with the vehicle. While on-orbit, exposure to the environment cannot be totally avoided as it can with a launch delay, so a higher risk threshold is appropriate. When the risk exceeds the on-orbit threshold, a translational maneuver is necessary. Performing the maneuver at least 6 hours prior to a predicted conjunction provides sufficient margin to execute the maneuver. Also, the latest, and probably last, tracking updates would be incorporated by this time; therefore, waiting longer to maneuver would not minimize the chance of an unnecessary maneuver. When maneuvers are required, screening the new orbit for potential conjunctions avoids putting the occupants on a collision course with another object. The conjunction analysis can be performed by U.S. Strategic Command based on information provided by the operator.*

[4] The use of a specific numbers is not typical in this document. We are interested in COMSTAC's view of a different way to state these established practices.

*The size of the exclusion volumes and collision probabilities match risk levels NASA has accepted for their human missions. The goal is to provide reasonable protection while minimizing operational impacts. The FAA is consulting with U.S. Strategic Command to assess the exclusion volumes and probabilities. For one study, based on a 2013 analysis of cataloged orbiting objects and a representative launch from Cape Canaveral to an orbit of 200 km at an inclination of 28.5 degrees, the exclusion volume for launch would result in about a third of a launch window being unavailable for launch. These violations are typically short in duration (15-30 seconds) and can be addressed by adjusting the preferred launch time. A probabilistic assessment would reduce the launch window closures by about an order of magnitude. On-orbit, predicted conjunctions vary based on the debris density at the altitude of the vehicle. For altitudes of 350-400 km, approximately 3 maneuvers would need to be made annually.*

*Based on an analysis of a catalog of orbiting objects performed by the U.S. Strategic Command for the FAA's Experimental Permit rulemaking, collision avoidance is not needed for flights with a planned maximum altitude greater than 150 kilometers.*

### *3.3.14 Probability of No Penetration by Micrometeoroids or Orbital Debris (AST-2210)*

Refer to 1.3.6

### *3.3.15 Flight Termination (AST-2207)*

Once a safety critical function becomes zero fault tolerant, an operator should terminate the flight as soon as practicable, normally at the next available primary or alternate landing site.

*Rationale: Continuing a flight with zero fault tolerant safety critical functionality may lead to unacceptable risk. Termination of the flight may protect occupants from serious injury or death. If in-flight maintenance fails to recover fault tolerance prior to the next landing opportunity, then the operator should terminate the flight as the practice suggests.*

### *3.3.16 Natural and Induced Environments (AST-1560)*

Refer to 1.3.8

### *3.3.17 Control Glare and Reflection (AST-1721)*

Refer to 1.4.12

### *3.3.18 Atmospheric Conditions (AST-1669)*

Refer to 1.1.1

### *3.3.19 Food and Water (AST-1691)*

Refer to 1.1.3

### *3.3.20 Emergency Response (AST-2214)*

An operator should have an Emergency Response Plan that:

a. Contains procedures that ensure the containment and minimization of the consequences of a mishap;

b. Contains procedures that ensure the preservation of the data and physical evidence; and
c. Contains procedures for contacting emergency responders to aid in preserving life and treating injured.

*Rationale: Certain events do not afford an operator time to develop a response to an emergency to avoid serious injury to an occupant. An Emergency Response Plan can be used by operators and first responders to preserve life and treat the injured, secure the mishap scene, and preserve physical evidence and data to help determine the root cause of the failure so that it can be prevented in the future.*

## 3.4 Medical Considerations

### *3.4.1 Medical Qualifications (AST-1880)*

a. Flight crew for suborbital flights should possess a valid FAA Class II Medical Certificate.
b. Flight crew for orbital flights should possess a valid FAA Class I Medical Certificate.
c. Ground crew should possess a valid FAA Class II Medical Certificate.

Rationale: This practice is important to aid in determining the fitness of the flight crew and ground crew to perform the safety critical tasks necessary for operating the vehicle. Medical screening by an FAA Aerospace Medical Examiner can identify medical conditions that could prevent a flight or ground crew member from performing his or her safety critical tasks.

### *3.4.2 Space Flight Participant Medical Consultation (AST-2216)*

Within six months of their flight, each space flight participant should consult with an Aviation Medical Examiner to ascertain their medical risks of space flight.

*Rationale: Space flight participants should be evaluated close in time to their planned flight to determine if they are medically fit to withstand the stresses of suborbital or orbital flight so that they do not pose a hazard to themselves or to other occupants. Assessing the medical fitness of a space flight participant is done through a medical examination to raise his or her awareness so that he or she can make an informed decision about their own health and implications of space flight.*

### *3.4.3 Medical Emergency Plan (AST-1996)*

The operators conducting multi-day orbital flights should have a medical plan that:

a. Will prevent acute infectious diseases being manifested during flight, such as through preflight quarantine and social isolation of flight crew and space flight participants;
b. Identifies the medical criteria for early termination of an orbital flight due to illnesses or medical emergencies; and
c. Identifies specific types of medical conditions that could result in an early termination of an orbital flight.

*Rationale: This practice is important because illness could prevent a flight crew member from performing safety critical tasks. An infectious disease could also be spread from a space flight participant to a flight crew member preventing the crew member from being able to perform his or her duties. Medical illness of a space flight participant due to an infectious disease could also affect the safety critical flight crew due to the need for medical care.*

*An organization can be better prepared to react appropriately in a timely manner when a plan is developed that addresses the medical criteria for early termination of an orbital flight due to illnesses or medical emergencies, and identifies specific types of medical conditions that could result in an early termination of an orbital flight. There is often no time to organize subject matter experts to make a decision. Preplanning for critical medical situations is vital to aiding the safety of occupants.*

### *3.4.4 Cabin Hygiene (AST-1680)*

Cabin hygiene procedures preflight and during flight should prevent occupant exposure to microbial contamination and foreign object debris which could cause debilitating illness or injury, which could prevent the performance of safety critical operations by the flight crew. Cabin cleanliness procedures may include cleaning, disinfecting and vacuuming the cabin prior to flight as well as filtering cabin air or cleaning surfaces while inflight.

*Rationale: This practice is important because microbial contamination and foreign object debris could cause debilitating illness or injury, which could prevent the performance of safety critical operations by the flight crew. The history of human space flight has shown that careful attention to cabin hygiene preflight is important as it is very difficult to clean a cabin of foreign object debris in microgravity.*

### *3.4.5 Medical Kit (AST-2205)*

Refer to 1.2.6

## 3.5 Training

### *3.5.1 Safety Critical Training (AST-1872)*

The operator should ensure that all flight crew, ground crew, and safety critical ground personnel are trained and certified to perform their safety critical functions. The operator should retain completed safety critical training and certification documentation for five years.

*Rationale: The use of untrained personnel in safety critical positions could lead to unsafe operations. A process that certifies personnel for the operations they may perform will help ensure safety critical tasks will be properly completed. Records will help ensure completeness of training, and will allow traceability and verification.*

### *3.5.2 Instructor Training Documentation (AST-1873)*

The operator should certify that personnel conducting safety critical training are qualified in the subject matter and qualified to teach.

*Rationale: Safe operations of the system are highly dependent upon the knowledge and experience of the personnel executing safety critical tasks. Instructors need to demonstrate knowledge of the system and the skill set to convey the information such that the personnel execute the necessary steps as required. A formal process that certifies instructors will help ensure that training personnel are qualified, safety critical personnel are trained successfully, and that operations are carried out safely.*

### 3.5.3 Safety Critical Training Requirements and Standards (AST-1874)

The operator should establish and maintain training requirements, completion standards, and any currency requirements for flight crew, ground crew, and safety critical ground personnel.

*Rationale: Safety critical personnel can be sources or controls to hazards. Improperly completed safety critical operations could lead to major injury to occupants. A training program lacking in training requirements, completion standards, and currency requirements could lead to unsafe conditions. A process that tracks requirements, completion standards, and currency requirements will help ensure safety critical in-flight tasks are properly completed.*

### 3.5.4 Crew Resource Management and Communication (AST-1894)

Training for flight crew and ground crew should include clear definitions of roles and responsibilities, use of a defined communications protocol, and crew resource management techniques.

*Rationale: Lack of clarity concerning roles and responsibilities of flight crew and ground crew members, as well as poor communication among the flight crew and ground crew can lead to unsafe operations. This is especially true during dynamic, complex, or high stress situations. Crew resource management training helps the flight and ground crew make good informed decisions using all available resources.*

### 3.5.5 Aerospace Physiology Training (AST-1896)

Training for flight crews should include aerospace physiology, comprising the following components:

a. Aerospace environment;
b. Physiology stress factors (environmental, operational, and self-imposed);
c. Aerospace operations;
d. Aerospace medicine; and
e. Aerospace human factors issues.

*Rationale: Space flight may have negative effects on human physiology such that crew members can become incapacitated or hindered in their ability to complete safety critical tasks.*

*Aerospace physiology training provides knowledge required to recognize human limitations in the aerospace environment, the physiological stress factors associated with flying in a zero-gravity environment, and human factor limitations on flight crew and space flight participants. Knowledge of the effects of space flight on the human body is proven to be an effective means of identifying initial conditions that lead to incapacitation or reduced cognitive abilities. Training also provides each*

*individual with basic knowledge of aerospace medicine and operations in order to respond during these conditions.*

### *3.5.6 Medical Training (AST-1908)*

Training for flight crews should include the use and location of on-board medical equipment, and the recognition of when an occupant requires medical attention that exceeds the capability of the flight crew and on-board equipment.

*Rationale: Injuries and illnesses to astronauts have been common occurrences, including musculoskeletal injuries, abrasions, contusions, lacerations, a foreign body in the eye, burns, and commonplace illnesses. As such, it is expected that medical injuries and illnesses may be sustained during space flight. Inability to locate or improper use of medical equipment can lead to further incapacitation or the inability to perform safety critical tasks.*

*Injuries and illnesses may occur that require medical attention that exceeds the capability of the flight crew or on-board equipment. It is important for the flight crew to recognize such injuries or medical conditions in order to take alternative measures to protect occupants, such as early return to Earth.*

### *3.5.7 Survival Equipment Training (AST-1906)*

Training for flight crews should include the use and location of all on-board survival equipment.

*Rationale: Inability to locate or improper use of survival equipment can further degrade an off-nominal situation. Training flight crews on the use and location of on-board survival equipment will allow immediate access to survival equipment that may be required during extreme conditions and when expedience is essential.*

### *3.5.8 Space Flight Participant Training (AST-1931)*

Prior to flight, an operator should instruct each space flight participant on:

a. The identified hazards of human interactions with the vehicle and other occupants in all phases of flight;
b. Aerospace physiology, commensurate with the expected flight and operational environment;
c. How to respond to emergency situations; including -
    1. The use and location of survival equipment, and
    2. The use and location of smoke detection and fire suppression equipment.

*Rationale: The limited internal volume of spacecraft provides limited mobility of occupants and hence a greater opportunity that a space flight participant can become a source of a hazard as well as a resource to respond to off nominal events. Providing pre-flight instruction to space flight participants on identifying hazards that result from human interactions, how their bodies will react to the space environment, and their expected roles in emergency situations, will provide the operational knowledge required to recognize, avoid, and respond to potential on-board hazards.*

## C. DEFINITIONS

**Acceptance Testing** means any test or inspection conducted on flight components, units, assemblies, subsystems, and systems to demonstrate that flight items are free of defects, latent material deficiencies, workmanship and integration errors, and are ready for operational use.

**Accident** means a fatality or serious injury to a space flight participant or flight crew member.

**Alternate Landing Site** means a supported landing site to which the vehicle landing can be diverted in the event there is an issue with the vehicle or primary landing site.

**Analysis** means a detailed systematic examination of a complex system by breaking it into its component parts to evaluate the interrelationships, or understand the cause-effect relationships. It is generally used when a physical prototype or product is not available or not cost effective. Analysis includes the use of both modeling and simulation.

**Anomaly** means a problem that occurs during operation of a system, subsystem, process, facility, or support equipment.

**Augmented Flight Crew** means a flight crew that has more than the minimum number of flight crew members required to operate a launch or reentry vehicle to allow a flight crew member to be replaced by another flight crew member for in-flight rest.

**Automatic** means an event that can occur without the need for human intervention.

**Catastrophic** means the loss of the vehicle, or a serious injury or fatality.

**Cause** means a reason for an action or condition.

**Collision Avoidance Maneuver** means a maneuver conducted by an orbiting object to avoid colliding with another object in orbit.

**Component** means an assembly of parts that constitute a functional article viewed as an entity for purposes of analysis, manufacturing, maintenance, or record keeping; the smallest entity specified for a distributed system.

**Configuration Control** means a process for establishing and maintaining consistency of a system's functional and physical attributes, safety critical procedures, and operations throughout its life.

**Consumable** means an item intended to be consumed during spaceflight operations. Consumable items include, but are not limited to: food, water, propellant for maneuvering or deorbit propulsion, oxygen and other make-up gasses, and stored energy such as electricity. Consumables do not include the necessary fuel, oxidizer, or mono-propellant necessary to propel a vehicle into suborbital or orbital flight.

**Contaminated Atmosphere** means a collection of unwanted airborne solid or liquid particulates and gasses that is otherwise mixed into the habitable volume air mass. Contamination is commonly caused by a by-product of fire or a leak of an enclosed fluid system.

**Critical** means that the system is at a state or condition in which a dangerous condition exists which could cause serious injury or death.

**Cumulative** means an increased quantity or total number for a given period. Cumulative flight hours are the consecutive hours of flight in a given period of hours or days.

**Design** means activities leading to the development of final drawings and specification for a system. Design includes tests to verify or validate requirements, models, reliability, and performance.

**Design Reference Mission** means a time history or profile of events, functions, and environmental conditions that a system is expected to encounter.

**Design Tolerance** means a permissible limit of variation in physical dimensions for manufacturing purposes where performance will not be degraded.

**Duty Period** means that period which begins when an operator requires a flight crew member to report for duty and ends when that flight crew member is free from all duties.

**Emergency** means a serious or dangerous situation requiring immediate action.

**Extensions** means a period of time allowed in addition to the assigned duty period for unforeseen operational circumstances.

**Extravehicular Activity** means activity outside of a vehicle's environmental control system performed by an individual using a pressure suit.

**Fail Safe** means that systems and associated components, considered separately and in relation to other systems, are designed so that the occurrence of any failure condition which would prevent the continued safe flight and landing is extremely improbable, and the occurrence of any other failure condition which would reduce the capability of the system or the ability of the flight crew to cope with adverse operating conditions is improbable.

**Failure** means the inability of a system, subsystem, component, or part to perform its required function within specified limits.

**Failure Tolerance** means the ability to sustain a certain number of failures and still retain capability. A component, subsystem, or system that cannot sustain at least one failure is not considered to be failure tolerant.

**Fatal Injury** means any injury which results in death within 30 days of the accident.

**Fatigue (Human)** means a physiological state of reduced mental or physical performance capability resulting from lack of sleep or increased physical activity that can reduce a flight crew member's alertness and ability to safely operate a launch or reentry vehicle or perform safety-related duties.

**Fatigue Risk Management System (Human)** means a management system for an operator to use to mitigate the effects of fatigue in its particular operations. It is a data-driven process and a systematic method used to continuously monitor and manage safety risks associated with fatigue-related error.

**Fault** means an undesired system state or the immediate cause of failure. The definition of the term "fault" envelopes the word "failure," because faults include other undesired events such as software anomalies and operational anomalies. Faults at a lower level could lead to failures at the higher subsystem or system level.

**Flight** begins at first motion of a launch vehicle or at brake release and ends when the vehicle stops on the Earth's surface.

**Flight Crew** means the personnel within a launch or reentry vehicle identified by the operator and qualified to operate the vehicle during flight.

**Flightworthiness** means a determination of the suitability for safe flight. If a vehicle is flightworthy, it is capable of safely carrying the occupants on its planned flight.

**Ground Crew** means the personnel identified and qualified by the operator to operate the vehicle during flight from the ground.

**Habitable Volume** means the area of space within a vehicle's environmentally controlled pressure vessel where human life is sustained.

**Hazard** means any real or potential condition that can cause injury, illness, or death to an occupant.

**Hazard Cause** means the primary reason for the occurrence of a hazardous condition.

**Hazard Control** means an attribute of the design or operational constraints of the hardware or function under analysis which prevent a hazard or reduces the residual risk to an acceptable level. Design controls include those attributes of the robustness of the design. Operational controls include both operational constraints as well as crew and support personnel training to prevent a hazard, lessen the likelihood or severity of a hazardous occurrence, or to mitigate the effects of a hazard once it has occurred.

**Hazard Severity** means the most severe effects of a hazard.

**Human Needs and Accommodations** means the steps necessary to accommodate specific human needs such as human waste disposition, consumables, etc. that have no relation to specific mission tasks or physical stress (unless not met).

**Human Protection** means managing occupants' maximum physical and psychological stress to safely complete a flight.

**Human Survivability Analysis** means an assessment of existing hazards after the vehicle is designed to identify additional capabilities that could be incorporated into the system to preserve the crew's life in the presence of imminent catastrophic conditions.

**Human Vehicle Integration** means the process of integrating humans with machines.

**Incident** means an unplanned event during pre-flight, flight, and post-flight that poses a high risk of causing a fatality or serious injury to a space flight participant or crew member.

**Induced Environment** means the environment that is created as a result of the operation of the vehicle.

**Launch Escape System** means a system used on launch vehicles used to separate occupants from the launch vehicle in the case of an imminent catastrophic event.

**Life-Cycle** means all phases of a system's life including design, research, development, test and evaluation, manufacturing, operations and support, and disposal.

**Likelihood** means the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively.

**Management** means program controls necessary to ensure proper implementation of safety requirements.

**Maximum Expected Operating Environment** means the maximum environment (pressure, temperature, vibration, shock, radiation, and loads) that a component, subsystem, or system is expected to experience during its service life**.**

**Mitigation** means any action taken to reduce or eliminate the risk to human life from hazards.

**Natural Environment** means the environment that exists before the vehicle arrives and is present during its operation.

**Nominal** means normal operations, that is, all critical systems performing within expected parameters.

**Normal Procedure** means procedures that are used during the standard or usual operation of the vehicle. Normal procedures can be part of a checklist or do-list, aid the flight crew in recalling a process, or provide a sequential framework to meet internal and external operational requirements.

**Occupant** means flight crew and space flight participants.

**Operation** means all core activities involved in executing a mission of a launch or reentry vehicle.

**Operator** means a person or entity that conducts or will conduct the fight of a launch or reentry vehicle carrying humans.

**Orbit** means an object is on a trajectory where it could remain in space for at least one orbit, and has an altitude at perigee above 100 kilometers (62 mi).

**Orthostatic Protection** means protecting a flight crewmember from the effects of orthostasis such as dizziness, lightheadedness, nausea, headache, temporary decrease in hearing, and blurred or diminished vision from an extended period of microgravity.

**Payload** means an object that a person undertakes to place in outer space by means of a launch or reentry vehicle, including components of the vehicle specifically designed or adapted for that object.

**Post-Landing** means the end of flight when occupants are no longer exposed to the hazardous conditions of the vehicle.

**Primary Landing Site** means a supported landing site that is the intended site for landing.

**Qualification** means the functional testing of components, units, subsystems, and systems at levels beyond the maximum expected operating environment to prove there is design

robustness, and to provide objective evidence that the system will survive the maximum expected operating environment to be experienced during its service life.

**Quality Assurance** means a system for ensuring a desired level of quality in the development, production, or delivery of products and services.

**Reserve Status** means a duty period during which an operator requires a flight crew member to be available to receive an assignment for a human space flight duty period.

**Residual Risk** means the risk left over after risk mitigation measures have been implemented.

**Rest Period** means a continuous period determined prospectively during which a flight crew member is free from all restraint by the operator, including freedom from present responsibility for work should the occasion arise.

**Safety Critical** means crucial to the prevention of serious injury or loss of life. A safety critical system, subsystem, component, condition, event, operation, process, or item is one whose proper recognition, control, performance, or tolerance is essential to ensuring occupant safety.

**Safety Critical Ground Personnel** means any personnel that have a safety critical role pre-flight and post-flight. Safety critical ground personnel may include personnel that assist the flight crew in entering the vehicle, closing the hatch, performing leak checks, and working on the integrated space vehicle at the pad during launch operations or landing.

**Safety Critical Penetration** means when a micrometeoroid or orbital debris damages a safety critical system that results in loss-of-vehicle or serious injury or death of an occupant, either on-orbit or during reentry.

**Safety Device** means a device designed to prevent injury or accidents.

**Serious Injury** means any injury which: (1) requires hospitalization for more than 48 hours, commencing within 7 days from the date of the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than 5 percent of the body surface.

**Split Duty** means a flight duty period that has a scheduled break in duty that is less than a required rest period.

**Supported Landing Site** means a fully supported site with the operator's recovery forces on station at the time of landing.

**Subsystem** means a group of interconnected and interactive major parts that performs an important task as a component of a system and has the characteristics of a system, usually consisting of several components.

**Support Equipment** means any non-flight equipment, system, ground system, or device specifically designed and developed for a direct physical or functional interface with flight hardware to support the execution of ground production or processing.

**System** means an integrated composite of personnel, products, sub-systems, elements, and processes that when combined together will safely carry occupants on the planned flight.

**System Safety** means the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of a system's life cycle.

**Test** means a method of verification wherein requirements are verified by measurement during or after the controlled application of functional and environmental stimuli. These measurements may require the use of laboratory equipment, recorded data, procedures, test support items, or services.

**Trained** means when instruction occurs and the individual can demonstrate that he or she can perform or is knowledgeable on the information, skills, or type of behavior that is expected.

**Unaugmented** (flight duty period) means when there is no other available flight crew member to replace the flight crew members during flight.

**Validation** means the assurance that a product, service, or system meets the needs of the customer and other identified stakeholders.

**Verification** means the activity that establishes acceptable confidence of compliance with specifications.