National Aeronautics and Space Administration

CCTS Certification Requirements	Document No: ESMD-CCTSCR-12.10	
	Revision: Basic	Effective Date: December 8, 2010

Commercial Crew Transportation System Certification Requirements for NASA Low Earth Orbit Missions

ESMD-CCTSCR-12.10
Revision-Basic

Douglas R. Cooke

12/9/10
Date

Douglas R. Cooke
Associate Administrator
Exploration Systems Mission Directorate

Record of Revision/Changes

Revision	Description	Date
Draft	Draft for NASA Request for Information	05/21/2010
Basic	Extensive revision and de-scoping	12/08/2010

Table of Contents

List of Tables

1.0 Introduction

The Commercial Crew Transportation System (CCTS) Certification Requirements Document is a consolidated set of technical requirements, standards, and processes built upon the National Aeronautics and Space Administration's (NASA's) vast human spaceflight knowledge and experience. The intent of this document is to define the requirements, standards, and certification package contents that will be used to certify a CCTS to carry NASA crewmembers on Low Earth Orbit (LEO) Missions.

NASA plans to purchase commercial crew space transportation services to LEO and the International Space Station (ISS) as part of NASA's exploration plans and policies. Certification of a commercial space transportation system during development/demonstration and procurement of services, rather than the space system itself, represents a significant departure from the way NASA has approached human spaceflight in the past. Agency policy does not currently mandate human rating for anything but NASA developments. However, as outlined in NASA Procedural Requirement (NPR) 8715.3C, NASA General Safety Program Requirements, paragraph 1.14, Agency policy does require NASA to analyze the risk and decide on necessary steps for safety when putting NASA personnel in harm's way using designs or operations that NASA does not control. Per this policy, NASA's approach for commercial crew transport is to base CCTS certification on NPR 8705.2, Human Rating Requirements for Space Systems. This certification will apply to NASA missions only (i.e. those carrying NASA or NASA sponsored crew members). The term 'human rating' is intentionally not used when referring to the certification of commercial systems because it implies a broader context of certification to fly any humans. NASA will not be involved in the certification of commercial systems when they are used for other purposes.

1.1 Philosophy

Protecting the health and safety of humans is of paramount importance for those involved in or exposed to space activities. For NASA, safety is a core value, and NASA recognizes that there can be no successful missions without first ensuring the safety of all personnel including the public, crew, passengers, and ground personnel. A crew transport capability that meets the safety requirements in this document will be approximately an order of magnitude safer than the Space Shuttle for ascent plus entry. The overall mission risk requirement will depend on the specific Design Reference Mission (DRM).

1.2 Purpose

This document defines the requirements, standards and certification package contents that will be used to certify a CCTS for LEO Missions. It will be the responsibility of the NASA Program Manager and Technical Authorities to determine the applicability of individual requirements and standards based on the DRM being certified and apply the Agency risk posture (for the DRM) to arrive at the final set of requirements and standards for certification. The Program Manager will then request Certification from NASA HQ per Agency policy.

1.3 Verb Application

Statements containing "shall" are used for binding requirements that must be verified and have an accompanying method of verification; "will" is used as a statement of fact, declaration of purpose, or expected occurrence; and "should" denotes a statement of best practice.

2.0 Reference Documents

Document Number	*Title*: Description
NPR 8705.2	NASA Human-Rating Requirements for Space Systems

3.0 Approach

3.1 Certification Philosophy

Certification of a spaceflight system to transport NASA or NASA sponsored personnel to/from the ISS or to other low earth orbit destinations consists of four separate functions: 1) validation of the technical and performance requirements/standards; 2) verification of compliance with those requirements/standards; 3) consideration of relevant operational experience; and 4) acceptance of residual technical risk due to hazards, waivers, non-compliances, etc. The NASA Program Manager is responsible for ensuring that the operational and design certification requirements and standards are met through the appropriate instrument (agreement milestone, statement of work, contract requirements, engineering and operations plans etc). The NASA Program Manager is also responsible for ensuring that a CCTS Certification Package (based on the Human Rating Certification Package in NPR 8705.2) is compiled. At each of the major program milestones, the Certification package contents are endorsed by the Program Manager and Technical Authorities (TAs) and the JSC Center Director (for crew risk acceptance). The Program Manager is also responsible for coordination with the Mission Directorate AAs at each milestone, in accordance with the NASA governance model. Thus, the Program Manager will be able to ensure satisfactory progress toward certification. Prior the first crewed flight for the reference mission, the Certification Package is submitted for approval to the NASA Associate Administrator as chair of the Agency PMC.

In the event that existing commercial systems (or elements of a system) are proposed for transport of NASA crewmembers, NASA will take into account the flight history along with existing design, flight data, and test results to determine compliance and/or equivalence in meeting the intent of applicable CCTS Certification Requirements. At the discretion of NASA, modifications to existing space systems may be required along with the appropriate milestone reviews. The CCTS Certification process will still be followed, but may be accelerated and milestones may be combined based on flight history and heritage.

As with earlier requirements and design reviews during the development, NASA will participate in the CCTS Flight Readiness Review for NASA missions. NASA will collectively evaluate CCTS design changes, manufacturing (or refurbishment) process changes, and testing changes to verify the mission falls within the bounds of the CCTS certification and that anomalies from previous missions have been addressed. NASA will decide, based on the flight readiness certification and residual risk posture, whether to authorize the NASA mission. During the operations/services phase, NASA will monitor the safety performance by evaluating the risk based on the significance of observed anomalies, and by updating its independent assessments of safety performance. This will ensure that safety requirements continue to be met and there is an established process for continuous improvement towards achievement of the safety goal.

3.2 Certification Applicability

Based on the mission phases, the required systems for the LEO mission are:

- Spacecraft (includes any Launch Abort or Launch Escape system)
- Launch Vehicle

- Ground Systems
- Mission Systems

Certification will apply to the integrated spacecraft, launch vehicle, ground systems, and mission systems in combinations specific to the NASA DRM.

3.3 Configuration Management

ESMD will maintain configuration management and control of the CCTS Certification Requirements for NASA LEO Missions. The NASA Program Manager for the CCTS development/services will maintain configuration management and control of their specific certification requirements documents for each DRM.

3.4 Certification Change Authority

After the NASA Associate Administrator has granted CCTS design Certification, all changes that affect the Certification will be evaluated and approved by the NASA Program Manager and cognizant TAs as part of the flight readiness review process. Any changes that affect the risk to the crew also require endorsement from the JSC Center Director. If determined that a recertification is required, the Program Manager will submit a revised certification package to the NASA Associate Administrator as Chair of the Agency PMC, per the process defined in NPR 8705.2.

4.0 CCTS Certification Package

For a CCTS development, the NASA Program Manager will use an appropriate instrument (agreement milestone, statement of work, contract requirements, etc) to ensure that the delivery of a CCTS Certification package is as described in the subsequent paragraphs.

The form of the CCTS Certification Package is a compilation of pertinent plans and documents, plus presentation material to help guide reviewers through the package. The package collectively illustrates with supporting evidence that the system has met the technical requirements and is safe to carry NASA crewmembers. The CCTS Certification Package shall be maintained under configuration management (especially to referenced/linked material) to clearly track changes made between milestones.

The material provided prior to and during each milestone review will be considered draft and for review/comment. An update will be provided after all changes resulting from the review have been incorporated. The post review CCTS Certification Package will be maintained in a location and in a manner that supports review by the NASA Program and TAs.

The CCTS Certification Package Content is summarized in the Table 4-1 below. The milestones listed are based on a NASA development and may be adapted to the CCTS Program's development plan. The NASA Program Manager will use the detailed description in Chapter 2 of NPR 8705.2 to provide additional guidance (through the applicable instrument). At each of the major program milestones, the Certification package contents are endorsed by the Program Manager and TAs and the JSC Center Director (for crew risk acceptance). The Program Manager is also responsible for coordination with the Mission Directorate AAs at each milestone, in accordance with the NASA governance model. Thus, the Program Manager will be able to ensure satisfactory progress toward certification. Prior the first crewed flight for the reference mission, the Certification Package is submitted for approval to the NASA Associate Administrator as chair of the Agency PMC.

X - One time item
I - Initial release of item
U - Update of item

Table 4-1 CCTS Certification Package Content

CCTS Certification Package Content	SRR	SDR	PDR	CDR	ORR
A description of the systems for which CCTS Certification will be requested.	X				
A description of each reference mission for which CCTS Certification is being pursued.	X				
A link to the Safety and Mission Assurance Plan and the documented safety analysis processes.	I	U	U	U	
A description of the program's philosophy as it relates to utilization of the crew's capabilities to execute the mission, prevent aborts, and prevent catastrophic events.	X				

CCTS Certification Package Content	SRR	SDR	PDR	CDR	ORR
An explanation of how the program plans to implement the CCTS Certification technical requirements or the trade studies/analysis to determine implementation; and a matrix that traces the capability described in chapter 5 to the program requirements (highest level where the capability is implemented).	I	U	U	U	
A description of the Human-Systems Integration Team and their authority within the program.	X				
A list of approved alternate standards documents (in place of those in section 6)	X				
An assessment of the risk of loss of crew and associated level of uncertainty substantiated by evidence.		I	U	U	
A ranking of the safety risks to which the crew is subject.		I	U	U	
A list of all requested waivers and exceptions to CCTS requirements, with justification and disposition, and access to the waivers and exceptions.	I	U	U	U	U
A summary of how safety analysis related to prevention of catastrophic events influenced the system architecture, system design, and the crew survival approach.		I	U	U	
A description of the approach to crew survival for each mission phase of each reference mission being taken by the program; the system capabilities or the trade studies/analysis to determine implementation; and a matrix that traces the capabilities to the program requirements (highest level where the capability is implemented).		I	U	U	
A summary of the level of failure tolerance implemented in the system to include a discussion of the use of dissimilar redundancy and backup systems/subsystems to prevent catastrophic events with special rationale for dynamic flight phases.		I	U	U	U
An explanation of how crew workload will be evaluated for the reference missions.		I	U	U	
The preliminary plan for the flight test program with the number and type of flights.		X			
A summary of the usability and human-system performance testing performed to date and the influence on the system design with links to the detailed test results.			I	U	
A summary of the human error analysis performed to date and the influence on the system design with links to the detailed analysis results.			I	U	U

CCTS Certification Package Content	SRR	SDR	PDR	CDR	ORR
An updated Flight Test Program with flight objectives linked to program development/validation needs. The breadth and depth of the flight test program will depend on a number of factors including system maturity and depth of insight into the design and verification. The flight test program, which may include a combination of suborbital, orbital, landing, and abort system tests, must be robust enough to prove confidence in the system design. The following flight test objectives shall be addressed before NASA will certify the vehicle: • Validate the nominal performance of the system. • Validate the dynamic response characteristics of the system. • Validate the structural integrity of the system. • Demonstrate the critical separation systems performance. • Demonstrate the entry, landing, and recovery systems. • Validate the critical system environments. • Demonstrate the abort system performance during critical phases of flight. • Demonstrate the critical ground and mission support systems. • Demonstrate the reliability of a common launch vehicle and spacecraft configuration.			I	U	
A plan, with rationale, for verification and validation of the following: • Implementation of capabilities identified for crew survivability. • Implementation of CCTS Operational and Design Technical Requirements. • Critical (sub)system performance • Integrated performance of critical (sub)systems. • Critical software performance, security, and safety. • Implementation of the standards cited in NPR 8705.2 paragraph 2.2.5 Human System Standards	I	U	U	U	U
The configuration control and maintenance plan for the system	I (CCP)			U (CCP)	X (MP)

CCTS Certification Package Content	SRR	SDR	PDR	CDR	ORR
A summary of the verification and validation results for the following (with links to the detailed results): • Implementation of capabilities identified for crew survivability. • Implementation of CCTS Operational and Design Technical Requirements. • Critical (sub)system performance. • Integrated performance of critical (sub)system performance. • Critical software performance, security, and safety. • Integrated human-system performance. • Implementation of the standards cited in NPR 8705.2 paragraph 2.2.5 Human System Standards					X
A summary of the flight test results for each test objective with links to the detailed test reports.					X
A description of how the crew workload for the reference mission was validated and determined to be acceptable.					X
A summary of how the safety analysis related to loss of crew and loss of mission was updated based on the results of validation/verification and used to support validation/verification of the design in circumstances where testing was not accomplished.					X

5.0 CCTS Operational and Design Certification Technical Requirements

5.1 Overview

The technical requirements in this chapter identify capabilities in three primary categories:

a. System Safety
b. Crew/Human Control of the System
c. Crew Survival/Aborts

These requirements are not intended to be all inclusive or an absolute prescription for certification. Compliance with these requirements does not assure a safe system for human missions to LEO. These technical requirements are intended to provide the foundation of capabilities upon which the Program Manager will build by identifying and incorporating additional unique capabilities for each reference mission. Furthermore, some of these requirements were intentionally written to force the design team to bound the problem. The design team should evaluate the intent of these technical requirements and use their talents to deliver the safest practical system that will accomplish the mission within the constraints. Technical requirements, along with history's lessons, legacy solutions, expert opinions, and best practices, are only as good as the implementer's understanding of their origins and assumptions.

The term 'crewed CCTS' refers to the applicable in-space elements (i.e. launch vehicle and spacecraft). Requirements that specify crewed CCTS must be met by the in-space elements without utilizing the capabilities of the ground or mission systems.

5.2 System Safety Requirements

5.2.1 The CCTS shall provide the capability to sustain a safe, habitable environment for the crew.

Rationale: Protection from the hazardous environment of space is fundamental to crew survival. Also, the space system should be inherently safe and designed to minimize risk (e.g., no exposed sharp edges, no exposed high temperature surfaces). This requirement includes protection from known environments such as space radiation hazards. Providing a habitable environment is also fundamental to the integration of the human into the space system. In order for the crew to contribute to the safe conduct of the mission, their basic habitability needs to be met.

5.2.2 The CCTS shall safely execute the Loss of Crew (LOC) requirements specific to the NASA Design Reference Mission (DRM). The Programs shall determine and document the LOC risk when DRMs are specified. The following are current:

a. The LOC probability distribution for the ascent phase of a 210 day ISS mission shall have a mean value no greater than 1 in 1000
b. The LOC probability distribution for the entry phase of a 210 day ISS mission shall have a mean value no greater than 1 in 1000

c. The LOC probability distribution for a 210 day ISS mission shall have a mean value no greater than 1 in 270

5.2.3 The CCTS shall limit the Loss of Mission (LOM) risk for the specified NASA DRMs. The Programs shall determine and document the LOM risk when DRMs are specified. The following are current:

a. The LOM probability distribution for a 210 day ISS mission shall have a mean value no greater than 1 in 55
b. A spacecraft failure that requires the vehicle to enter earlier than the pre-launch planned end of mission timeframe shall be considered a loss of mission

Rationale: These LOC and LOM requirements are flown down from the NASA ESMD Exploration Architecture Requirements Document (EARD) and are consistent with NASA's defined goals and thresholds for crewed vehicles. The LOC values are part of the overall certification process for the commercial launch vehicle and spacecraft and establish a basis for decision-making relative to safety enhancing features in the design including failure tolerance.

5.2.4 The CCTS shall provide failure tolerance to catastrophic events, with the specific level of failure tolerance (one, two, or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis.

a. Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process approved by the NASA Program and in which standards and margins are implemented that account for the absence of failure tolerance.
b. All potentially catastrophic hazards that cannot be controlled using failure tolerance may be excepted from the failure tolerance requirement with specific approval from the NASA Program provided the hazards are controlled through a defined process in which standards and margins are implemented that account for the absence of failure tolerance.

Rationale: The overall objective is to provide the safest design that can accomplish the mission given the constraints imposed on the program. Since a CCTS development will always have mass, volume, schedule, and cost constraints, choosing where and how to apply failure tolerance requires integrated analyses at the system level to assess safety and mission risks. First and foremost, the failure tolerance is applied at the overall system level to include all capabilities of the system. While failure tolerance is a term frequently used to describe minimum acceptable redundancy, it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures, or additional features that completely mitigate the effects of failures. Even when assessing failure tolerance at the integrated system level, the increased complexity and the additional utilization of system resources (e.g. mass, power) required by a failure tolerant design may negatively impact overall system safety as the level of failure tolerance is increased.

Ultimately, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the

responsibility of the engineering and safety teams to determine the safest practical system design given the mission requirements and constraints. Additionally, the overall system reliability is a significant element of the integrated safety and design analysis used in the determination of the level of redundancy. Redundancy alone without sufficient reliability does not meet the intent of this requirement. Catastrophic events, as defined in this document and consistent with NPR 8715.3, NASA General Safety Program Requirements, include crew fatality and the unplanned loss/destruction of a major element of the crewed space system during the mission that could potentially lead to death or permanent disability of the crew or passengers.

Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to: (1) recognize the importance of the hazards being controlled; (2) ensure robustness of the design; and (3) ensure adequate attention/focus is being applied to the design, manufacture, test, analysis, and inspection of the items. The NASA Program will approve any system or component that does not meet this failure tolerance requirement.

5.2.5 The CCTS shall provide the appropriate failure tolerance capability defined in 5.2.4 without the use of emergency equipment and systems.

a. Appropriate credit may be taken for emergency equipment and systems for the LOC assessments (defined in Section 5.2.2 of this document.)

Rationale: Emergency systems and equipment, such as fire suppression systems, fire extinguishers, emergency breathing masks, launch/entry pressure suits, ballistic unguided entry capability, and launch aborts, are not to be considered part of the failure tolerance capability. Emergency systems are there 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 may be used for LOC assessments even though some of these capabilities such as launch aborts or ballistic entry may return the crew to Earth someplace other than the nominal or backup landing locations and place the crew in a survival situation.

5.2.6 For an ISS DRM, the CCTS shall comply with requirements for failure tolerance during ISS proximity operations and the ISS docked phase as defined in SSP 50808 Section 3.3.11.1.

Rationale: The ISS Program has specific additional failure tolerance requirements documented in SSP 50808 Section 3.3.11.1. For the ISS, catastrophic hazards are controlled so that no combination of two failures, or two operator errors, or one of each can result in a catastrophic hazardous event. These ISS requirements take precedence for the applicable mission phases and the ISS Program will approve any variance request to these requirements. Even though these additional ISS requirements exist, the CCTS is still required to perform the integrated safety and design analysis to determine the level of failure tolerance.

5.2.7 The CCTS shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as identified by a human error analysis, without causing a catastrophic event.

Rationale: An operator is defined as any human that commands or interfaces with the space system during the mission, including humans in the control centers. The appropriate level of protection (i.e., one, two, or more inadvertent actions) is determined by an integrated human error and hazard analysis.

5.2.8 The CCTS shall tolerate inadvertent operator action in the presence of any single system failure.

Rationale: The intent of this requirement is to provide a robust human-system interface design that cannot be defeated by a system failure. Where the system is designed to protect for more than one inadvertent action, the level of protection after a single system failure may be reduced - but still protects from a single inadvertent operator action.

5.2.9 The CCTS shall provide the capability to mitigate the hazardous behavior of critical software where the hazardous behavior would result in a catastrophic event.

Rationale: According to current software standards, the software system will be designed, developed, and tested to:
1) Prevent hazardous software behavior.
2) Reduce the likelihood of hazardous software behavior.
3) Mitigate the negative effects of hazardous software behavior.
However, for complex software systems, it is very difficult to definitively prove the absence of hazardous behavior. Therefore, the crewed system has the capability to mitigate this hazardous behavior if it occurs. The mitigation strategy will depend on the phase of flight and the "time to effect" of the potential hazard. Hazardous behavior includes erroneous software outputs or performance.

5.2.10 The CCTS shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, and/or crew health.

Rationale: A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware or software item's intended function. The definition of the term "fault" envelopes the word "failure," since faults include other undesired events such as software anomalies and operational anomalies. It is necessary to alert the crew to faults (not just failures) that affect critical functions.

5.2.11 The CCTS shall provide the capability to isolate and/or recover from faults identified during system development that would result in a catastrophic event.

Rationale: This capability is not intended to imply a failure tolerance capability or expand upon the failure tolerance capability. The intent is to provide isolation and recovery from faults where the system design (e.g., redundant strings or system isolation) enables the implementation of this capability. Also, any faults identified during system development should be protected by isolation and/or recovery.

However, it is acknowledged that not all faults that would cause catastrophic events can be detected or isolated in time to avoid the event. Similarly, system design cannot ensure that once the fault is detected and isolated that a recovery is always possible. However, in these cases, isolation of the fault should prevent the catastrophic event.

5.2.12 The CCTS shall provide the capability to utilize health and status data (including system performance data) of critical systems and subsystems to facilitate anomaly resolution during and after the mission.

Rationale: Access to health and status data is a key element of anomaly resolution during the mission, which could prevent the crew from executing an abort or prevent the situation from developing into a catastrophic event. Resolving anomalies between missions is just as important. This requirement intentionally does not specify a crash survivable data recorder. That determination is left for the program. The program also determines what data should be available to facilitate anomaly resolution.

5.2.13 The CCTS shall provide the capability for autonomous operation of system and subsystem functions, which, if lost, would result in a catastrophic event.

Rationale: This capability means that the crewed system does not depend on communication with Earth (e.g., mission control) to perform functions that are required to keep the crew alive.

5.2.14 The CCTS shall provide the capability for the crew to readily access equipment involved in the response to emergency situations and the capability to gain access to equipment needed for follow-up/recovery operations.

Rationale: Fire extinguishers are one example of the type of equipment needed for immediate response to a fire emergency. "Ready access" means that the crew is able to access the equipment in the time required without the use of tools. The ready access time will depend on the phase of flight and the time to effect of the hazard. Ready access also accounts for suited crewmembers if the equipment could be needed during a mission phase or operation where the crew is suited. A contamination clean-up kit is an example of equipment needed for follow up/recovery operations.

5.3 System Control Requirements – General

5.3.1 The crewed CCTS shall provide the capability for the crew to monitor, operate, and control the crewed space system and subsystems, where:

a. The capability is necessary to execute the mission; or
b. The capability would prevent a catastrophic event; or
c. The capability would prevent an abort.

Rationale: Within the context of this requirement, monitoring is the ability to determine where the vehicle is, its condition, and what it is doing. Monitoring helps to create situational awareness that

improves the performance of the human operator and enhances the mission. Determining the level of operation over individual functions is a decision made separately for specific space systems. Specifically, if a valve or relay can be controlled by a computer, then that same control could be offered to the crew to perform that function. However, a crewmember probably could not operate individual valves that meter the flow of propellant to the engines, but the function could be replaced by a throttle that incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust). Meeting any of the three stated conditions invokes the requirement. The first condition recognizes that the crew performs functions to meet mission objectives and, in those cases, the crew is provided the designated capabilities. The second and third conditions recognize that, in many scenarios, the crew improves the performance and safety of the system and that the designated capabilities support that performance and safety improvement.

5.3.2 The crewed CCTS shall provide the capability for the crew to manually override higher level software control/automation (such as automated abort initiation, configuration change, and mode change) when the transition to manual control of the system will not cause a catastrophic event.

Rationale: This is a specific capability necessary for the crew to control the crewed space system. While this capability should be derived by the program per paragraph 5.3.1, the critical nature of software control and automation at the highest system level dictates specific mention in these requirements. The program and Technical Authorities will determine the appropriate implementation of this requirement.

5.3.3 The CCTS shall provide the capability for humans to remotely monitor, operate, and control the crewed system elements and subsystems, where:

a. The remote capability is necessary to execute the mission; or
b. The remote capability would prevent a catastrophic event; or
c. The remote capability would prevent an abort.

Rationale: This capability will likely be implemented using a mission control on Earth. Logically, there will be times when the crew is unavailable to monitor, operate, and control the system. If the crew vacates the CCTS as part of the reference mission (for example, after docking to ISS), there must be a capability for humans to monitor the unoccupied elements. In some of these cases, the crew may be able to perform this function from their new location. In other cases, mission control may perform this function. This requirement is not intended to force 100 percent of communication coverage for all elements of the system.

5.4 System Control Requirements – Spacecraft

5.4.1 The crewed CCTS shall provide the capability for the crew to manually control the flight path and attitude of their spacecraft, with the following exception: during the atmospheric portion of Earth ascent when structural and thermal margins have been determined to negate the benefits of manual control.

Rationale: The capability for the crew to control the spacecraft's flight path is a fundamental element of crew survival. Manual control means that the crew can bypass the automated guidance of the vehicle to

interface directly with the flight control system to affect any flight path within the capability of the flight control system. Limiting the crew to choices presented by the automated guidance function is not a valid implementation of manual control. Manual control does not mean the capability to bypass the flight control system. Also, for phases of flight where there is no active control of the spacecraft, such as when under passive parachutes, then manual control cannot be provided and this requirement would not apply. During the atmospheric portion of Earth ascent (approximately the first 100,000 feet), where the trajectory and attitude are tightly constrained to maintain positive structural and thermal margins, the trajectory and attitude constraints are not typically available independent of guidance. In this case, if the only option is for the crew to follow guidance then nothing is gained by manual control over automated control.

5.4.2 The crewed CCTS shall exhibit Level 1 handling qualities (Handling Qualities Rating (HQR) 1, 2 and 3), as defined by the Cooper-Harper Rating Scale, during manual control of the spacecraft's flight path and attitude.

Rationale: Level 1 handling qualities are the accepted standard for manual control of flight path and attitude in military aircraft. Level 1 handling qualities will allow the crew to effectively control the spacecraft when necessary for mission completion or to prevent a catastrophic event. Selected manual control scenarios that must meet Level 1 handling qualities will be defined via review of potential manual control scenarios scoped with NASA agreement. Reference NASA TND-5153 for the Cooper-Harper Rating Scale.

5.5 System Control requirements – Proximity Operations

5.5.1 The CCTS shall provide the capability for the crew to monitor, operate, and control an uncrewed spacecraft during proximity operations, where:

a. The capability is necessary to execute the mission; or
b. The capability would prevent a catastrophic event; or
c. The capability would prevent an abort.

Rationale: Proximity operations cover several scenarios, but this term is specifically defined as two (or more) systems operating in space) within the prescribed safe zone for either system.
When an un-crewed space system is the active spacecraft performing proximity operations with a crewed spacecraft, this requirement includes the capability for the crew to monitor the trajectory of the un-crewed system. At a minimum, the crewed system will have the capability to send basic trajectory commands to hold/stop, continue, and breakout to the un-crewed spacecraft. Active means the spacecraft is changing the flight path/trajectory/orbital parameters to affect the desired result during proximity operations.

5.5.2 The crewed CCTS shall provide the capability for direct voice communication between crewed spacecraft (2 or more) during proximity operations.

Rationale: Direct voice communication means that the signal is not routed through mission control or another communication relay satellite.

5.6 Crew Survival/Abort Requirements

5.6.1 Ascent

5.6.1.1 The CCTS shall provide the capability for unassisted crew emergency egress to a safe haven during prelaunch activities.

Rationale: For contingency situations, where the ground crew is not immediately available, the crew will need the capability for unassisted egress from the vehicle for safety reasons.

5.6.1.2 The CCTS shall provide abort capability from the launch pad until orbit insertion to protect for the following ascent failure scenarios (minimum list):

a. Complete loss of ascent thrust/propulsion.
b. Loss of attitude or flight path control.
c. Catastrophic event on pad or in flight

Rationale: Flying a spacecraft through the atmosphere to orbit entails inherent risk. Three crewed launch vehicles have suffered catastrophic failures during ascent or on the launch pad (one Space Shuttle and two Soyuz spacecraft). Both Soyuz crews survived the catastrophic failure due to a robust ascent abort system. Analysis, studies, and past experience all provide data supporting ascent abort as the best option for the crew to survive a catastrophic failure of the launch vehicle. Although not specifically stated, the ascent abort capability incorporates some type of vehicle monitoring to detect failures and, in some cases, impending failures.

5.6.1.3 The crewed CCTS shall monitor the ascent launch vehicle performance and automatically initiate an abort when an impending catastrophic failure is detected.

Rationale: Launch vehicle performance monitoring may include specific system or subsystem performance. The program will determine the appropriate parameters to monitor in the launch vehicle. Not all potentially catastrophic failures can be detected prior to manifestation. Similarly, system design and analysis cannot guarantee the crew will survive all catastrophic failures of the launch system, but the abort system should provide the best possible chance for the crew to survive. When an impending catastrophic failure of the launch vehicle is detected, the time to effect requires the abort system to be initiated automatically. Also, if the catastrophic failure itself is detected by a monitoring system, the abort is initiated automatically. This is not intended to require independent implementation by the crewed space system of capabilities inherent to the launch vehicle (the launch vehicle is part of the crewed space system).

5.6.1.4 Ascent Abort

5.6.1.4.1 The CCTS shall provide the capability for the crew to initiate the ascent abort sequence.

5.6.1.4.2 The CCTS shall provide the capability for the ground control to initiate the ascent abort sequence.

Rationale: The crew and ground control will likely have access to more data than an automated abort system. Therefore, both the crew and ground control have the capability to initiate the abort when necessary for crew survival.

5.6.1.5 If a range safety destruct system is incorporated into the design, the CCTS shall automatically initiate the ascent abort sequence when range safety destruct commands are received onboard, with an adequate time delay prior to destruction of the launch vehicle to allow a successful abort.

Rationale: Prior to destruction of the launch vehicle by means of a range safety destruct (flight termination) system, the abort system is initiated. An automated initiation of the abort sequence provides the best chance for crew survival while protecting the public from a range safety violation. It is left to the program to determine which range safety command (arm or fire) will result in the initiation of the abort sequence.

5.6.2 Orbit

5.6.2.1 The crewed CCTS shall provide the capability to autonomously abort the mission from orbit by targeting and performing de-orbits to a safe landing.

5.6.3 Reentry Systems

5.6.3.1 The crewed CCTS shall provide the capability for unassisted crew emergency egress after landing.

Rationale: This requirement assumes the crew is able to function in a 1-g environment. Unassisted means without help from ground or rescue personnel or equipment.

5.6.3.2 The crewed CCTS shall provide a safe haven capability for the crew inside the spacecraft after landing until the arrival of the landing recovery team or rescue forces.

Rationale: If the crew is physically unable to egress the spacecraft or does not choose to egress the spacecraft due to a hazardous environment outside, then the spacecraft provides a safe haven until the arrival of recovery forces. This requirement is not intended to establish the boundaries of the hazardous environment (for example, the maximum sea state) or the duration of the safe haven. The program, with concurrence from the Technical Authorities, specifies these conditions in their requirements documents. The nominal return to Earth will have well-established timelines and expectations for the habitation conditions inside the spacecraft. Conversely, after an ascent abort or emergency return to Earth, the timeline may be less certain and the expectations of comfort will be different from the nominal mission return.

5.6.3.3 The CCTS shall provide recovery forces with the location of the spacecraft after return to Earth.

Rationale: In the event of a contingency, the spacecraft may not return to the nominal preplanned location. Experience has shown that the system needs to provide a means for recovery forces to be provided with the spacecraft location. The ISS Expedition 6 crew returned to Earth in a Soyuz spacecraft. A system failure caused the Soyuz to downmode to a ballistic entry. When this happened, the Soyuz landed 'short' of the targeted landing zone. The system could not provide the recovery forces with an accurate location and the crew was placed in a survival situation while waiting for recovery. Subsequently, the Soyuz system was modified with a location system for recovery forces. This system was successfully utilized on Expedition 15, when another ballistic entry occurred.

6.0 Technical Authority Mandatory Standards and Requirements

This section lists the documents that contain requirements applicable to CCTS development and operational activities per NASA Federal Acquisition Regulation (FAR) Supplement 1852.223-70 and Safety and Health, paragraphs 1.1.2, 1.4.2.a, 1.4.3.a, and 1.4.4.a of NPR 8705.2B. These requirements have been designated by the NASA Technical Authorities as the superset of requirements for NASA human spaceflight missions to LEO.

The NASA Program Manager and the TAs are responsible for determining the application of these standards and requirements to the specific DRM. The applicable revision of documents listed shall be the current revision in effect on the date of the agreement or contract. When the normative references cited within documents do not have an applicable revision specified, the applicable revision shall also be the current revision in effect on the date of the agreement or contract. The below listed requirements are in addition to all federal/state/local/tribal laws whose applicability takes precedence over NASA requirements unless otherwise stated therein.

The mandatory NASA TA documents are separated into 3 types:

Type 1 documents are those that contain requirements the CCTS Program must meet as written. Any Applicable Document listed within a Type 1 document is considered to be Type 2 document unless specifically noted.

Type 2 documents are those that contain requirements the CCTS Program can either choose to adopt, or propose an alternate. The Program will be allowed to propose alternate requirements and documents that they consider to meet or exceed the intent of the Type 2 document. The cognizant NASA TAs will evaluate the equivalency of the requirements and documents proposed by the CCTS Program. It will be the responsibility of the CCTS Program to demonstrate that a proposed alternate requirement or document fully meets the intent and the requirements of the document(s) listed herein, and obtain formal NASA approval.

Type 3 documents are those that contain requirements where the CCTS Program does not need to either formally adopt the document or recommend an alternate. Rather, these documents represent the 'best practices' observed by or normally used by NASA over the substantial development history of both human and non-human space flight missions. As such, they will form an integral reference in the development of Program requirements.

NASA Policy Documents NPD) and NPR documents can be found at: http://nodis3.gsfc.nasa.gov/.
NASA Standards can be found at: http://standards.nasa.gov/documents/nasa.

6.1 Mandatory Health and Medical TA Requirements and Documents

Mandatory Health and Medical TA requirements and documents are fully applicable except as noted in Tables 6-1, 6-2, and 6-3. While these documents are under the control of the Health and Medical TA, documents marked with a "#" are also documents which are required by the Safety and Mission Assurance TA.

Table 6-1: Type 1 Health and Medical TA Documents

Document Number	Document Name	Applicability
NASA-Standard-3001 Volume 1[1#]	NASA Space Flight Human System Standard Volume 1: Crew Health	Fully Applicable.
NASA-Standard-3001 Volume 2[1#]	NASA Space Flight Human System Standard Volume 2: Human Factors, Habitability, and Environmental Health	Fully Applicable. Volume 2 is in the approval process and with Volume 1, will supersede NASA-STD 3000 Volume I and II.
FAA HFDS[1#]	Human Factors Design Standard	This Standard is only invoked while NASA-STD 3001 Volume 2 is in the approval cycle. Once approved, FAA HFDS will be superseded by NASA-STD 3001 Volume 1 and 2.
MIL-STD-1472[1#]	Human Engineering, Design Criteria for Military Systems, Equipment, and Facilities	This Standard is applicable for ground processing only.
NASA-Standard-3000 Volume I – II[1#]	Man-Systems Integration Standards.	This Standard is only invoked while NASA-STD 3001 Volume 2 is in the approval cycle. Once approved, NASA-STD 3000 will be superseded by NASA-STD 3001 Volume 1 and 2.

[1]The Type 1 Health and Medical TA mandatory documents listed above are tailored for use by CCTS Program for an ISS crew transport mission in the following documents. For LEO missions other than ISS crew transport missions, the HMTA mandatory standards must be applied.

- CCT-1002 Commercial Human Systems Integration Requirements [#]
- CCT-XXXX Commercial Medical Operations Requirements Document [#]
- CCT-XXXX Commercial Human Systems Integration Process Document

[#]This Health and Medical TA document is also required by SMA TA.

Table 6-2: Type 2 Health and Medical Documents

Document Number	Document Name	Applicability
	None	

Table 6-3: Type 3 Health and Medical Documents

Document Number	Document Name	Applicability
NASA/SP-2010-3407[1]	Human Integration Design Handbook	

[1]The Human Integration Design Handbook establishes the currently recognized data and guidelines for space facilities and related equipment that directly interface with crewmembers during space flight. The Human Integration Design Handbook was developed to serve as a companion document to NASA-STD-3001, Volume 2 and provides the necessary guidance to comply with the Standard.

6.2 Mandatory Engineering TA Requirements and Documents

Mandatory Engineering TA requirements and documents are fully applicable except as noted in Tables 6-4, 6-5, and 6-6. While these documents are under the control of the Engineering TA, documents marked with a "#" are also documents which are required by the Safety and Mission Assurance TA.

Table 6-4: Type 1 Engineering TA Documents

Document Number	Document Name	Applicability
	None	

Table 6-5: Type 2 Engineering TA Documents

Document Number	Document name	Applicability
NASA-STD-0005	NASA Configuration Management (CM) Standard	Fully applicable.
NASA-STD-4003	Electrical Bonding For NASA Launch Vehicles, Spacecraft, Payloads, And Flight Equipment	Fully applicable.
NASA-STD-4005	Low Earth Orbit Spacecraft Charging Design Standard	Fully applicable.

Document Number	Document name	Applicability
NASA-STD-5005	Standard for the Design and Fabrication of Ground Support Equipment	Applicable sections are: 4.2.3.2 a & d; 4.2.4.6; 4.3.1 4.6.2.1 a & b; 5.1.2 a & b; 5.1.2.1; 5.2.3; 5.2.8; 5.2.9a; 5.2.13 a & b; 5.2.13.2; 5.4.21; 5.11.3.1.3.1a; 5.11.3.1.3.2a; 5.11.3.1.3.2.1a; 5.11.4.1; 5.11.4.8 a
NASA-STD-5017	Design and Development Requirements for Mechanisms	Sections 4.7 and 4.8.9 are not applicable.
NASA-STD-5019	Fracture Control Requirements For Spaceflight Hardware	Fully applicable.
NASA-STD-6016	Standard Manned Spacecraft Requirements for Materials and Processes	Fully applicable.
NPR 2810.1	Security of Information Technology	Fully applicable.
NPR 7120.5	NASA Space Flight Program and Project Management Requirements	Fully applicable.
NPR 7123.1	NASA Systems Engineering Processes and Requirements	Fully applicable.
NPR 7150.2#	NASA Software Engineering Requirements	Fully applicable.
JSC 65828	Structural Design Requirements and Factors of Safety for Spaceflight Hardware	Revised version of CxP 70135 to remove CxP references and document number, make more generic for commercial crew development.
JSC 65829	Loads and Structural Dynamics Requirements for Spaceflight Hardware	Revised version of CxP 70137 to remove CxP references and document number, requires extensive tailoring to make suitable for commercial crew development.
JSC 62809#	Human Rated Spacecraft Pyrotechnic Specification	Revised version of CxP 70199 to make suitable for commercial crew development.
JSC 65827	Thermal Protection System Design Standard for Spacecraft	Revised version of CxP 72095 to remove CxP references and document number, make more generic for commercial crew development.

Document Number	Document name	Applicability
JSC 20793#	Crewed Space Vehicle Battery Safety Requirements	Fully applicable.
JSC 62550	Strength Design and Verification Criteria for Glass, Ceramics, and Windows in Human Spaceflight Applications	Currently in work to become NASA-STD-5018. Sections 3.1.5.3/4.1.5.3, 3.1.6.14/4.1.6.14, and 3.4.2/4.4.2 are not applicable.
JSC 65830	Interim Requirements and Standard Practices for Mechanical Joints with Threaded Fasteners in Spaceflight Hardware	Fully applicable.
JSC 65985	Deployable Aerodynamic Decelerator Requirements for Human Spaceflight	Fully applicable.
MIL-STD-461	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment	Fully applicable.
MIL-STD-464	Electromagnetic Environmental Effects Requirements for Systems	Fully applicable.
MIL-STD-981#	Design, Manufacturing and Quality Standards for Custom Electromagnetic Devices for Space Applications	Fully applicable.
MIL-STD-1540E/ Aerospace Report No. TR-2004 (8583) -1 Rev. A	Test Requirements for Launch, Upper-Stage, and Space Vehicles	Fully applicable.
AIAA S-111-2005	Qualification and Quality Requirements for Space Solar Cells	Fully applicable – if part of architecture
AIAA-S-112-2005	Qualification and Quality Requirements for Space Solar Panels	Fully applicable – if part of architecture
ANSI/ESD S20.20-1999#	ESD Association Standard for the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies	Fully applicable.
IPC-2221	Generic Standard on Printed Board Design	Fully applicable.
IPC-2222	Sectional Design Standard for Rigid Organic Printed Boards	Fully applicable.
IPC-6011 1996	Generic Performance Specification for Rigid Printed Boards	Fully applicable.
IPC-6012	Qualification and Performance Specification for Rigid Printed Boards	Fully applicable.

Document Number	Document name	Applicability
IPC-CM-770E	Component Mounting Guidelines for Printed Boards	Fully applicable.
SAE ARP 5412A	Aircraft Lightning Environment and Related Test Waveforms	Fully applicable.
SAE ARP 5413	Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning	Fully applicable.
SAE ARP 5414A	Aircraft Lightning Zoning	Fully applicable.
SAE ARP 5577	Aircraft Lightning Direct Effects Certification	Fully applicable.

Table 6-6: Type 3 Engineering TA Documents

Document Number	Document Name	Applicability Comments
GSFC-STD-1000	Goddard Space Flight Center Rules for the Design, Development, Verification, and Operation of Flight Systems	
JPR 8080.5	JSC Design and Procedural Standards	
KSC-DE-512	Facility, System, and Equipment General Design Requirements	
KSC-NE-9439	KSC Design Engineering Handbook for Design and Development of Ground Systems	
NESC-RP-06-108/05-173-E	Design, Development Test and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems	
RTCA DO-160E	Environmental Conditions and Test Procedures for Airborne Equipment	
SAE ARP 5416	Aircraft Lightning Test Methods	

6.3 Mandatory SMA TA Requirements and Documents

The SMA TA does not have any documents that are "Type 1" documents as previously defined. Requirements of special interest to NASA are noted on the table with a "*" that come from regulations placed on NASA (i.e.; Federal Law), affect national policy (i.e.; orbital debris), or are of special interest to the NASA Administrator (i.e.; safety).

Mandatory SMA TA requirements and documents are fully applicable except as noted in Tables 6-7, 6-8, and 6-9.

Table 6-7: Type 1 SMA TA Documents

Document Number	Document Name	Applicability

	None	

Table 6-8: Type 2 SMA TA Documents

Document Number	Document Name	Applicability
NPD 8700.1	NASA Policy for Safety and Mission Success	5.f, 5.g, 5.j, & 5.k
NPD 8710.5*	Policy for Pressure Vessels and Pressurized Systems	Fully applicable when operating on a NASA Facility, and when NASA personnel or critical NASA hardware are exposed to the PV/S. For flight hardware paragraphs 5.b.2-3
NPD 8730.1	Metrology and Calibration	Paragraphs 1.a & 1.b.
NPD 8730.2	NASA Parts Policy	Chapter 1*, Attachment A
NPR 8000.4	Risk Management Procedures and Guidelines	Fully applicable.
NPR 8621.1	NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping	***See Note #1***
NPR 8705.5	Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects	If PRAs are delivered to NASA, the format and content in this document is fully applicable.
NPR 8705.6	Safety and Mission Assurance Audits, Reviews, and Assessments	Only 4.2.6
NPR 8715.3	NASA General Safety Program Requirements	Only paragraphs 1.3.1.a*, 1.3.1.b, 1.5.2, 1.5.3*, 1.7, 2.5, 2.6 (with 2.6.1.b*) 2.7, 2.8, 3.2.3*, 3.5.1*, 3.8.2*, 3.11.2*, 3.12.2*, and 3.18.6*, and Chapter 6* (for any quantity of radioactive material in the launch system or spacecraft)
NPR 8715.5	Range Safety Program	Fully applicable when using NASA launch facilities/ranges
NPR 8715.6	NASA Procedural Requirements for Limiting Orbital Debris	1.3.10, 1.3.13, 2.1, & Chapters 2 & 3

Document Number	Document Name	Applicability
NPR 8735.1	Procedures for Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program (GIDEP) and NASA Advisories	Guidance in addition to NASA FAR Supplement for paragraphs 1.2.4, 4.1, 4.3, and 4.4.
NPR 8735.2	Management of Government Quality Assurance Functions for NASA Contracts	Fully applicable *
NASA-STD 8709.20	Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements	Fully applicable
NASA-STD 8719.12*	Safety Standard for Explosives, Propellants, and Pyrotechnics	Fully applicable to spacecraft and launch site. Personnel protection must be provided to all NASA personnel per document when NASA personnel are operating at CCT company or facility/location.
NASA-STD 8719.13	NASA Software Safety Standard	Fully applicable
NASA-STD 8719.14*	Process for Limiting Orbital Debris	***See Note #2.***
NASA-STD 8719.17*	NASA Requirements for Ground-Based Pressure Vessels and Pressurized Systems (PV/S)	Fully applicable when operating on a NASA Facility, when NASA personnel or critical NASA hardware are exposed to the PV/S and for flight hardware
NASA-STD 8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies	Fully applicable.
NASA-STD 8739.4	Crimping, Interconnecting Cables, Harnesses, and Wiring	Fully applicable.
NASA-STD 8739.5	Fiber Optic Terminations, Cable Assemblies, and Installation	Fully applicable.
NASA-STD 8739.8	Software Assurance Standard	Only Sections 6.0, 7.1, 7.2.4, 7.3, & 7.4.

Document Number	Document Name	Applicability
ANSI Z117.1	Safety Requirements for Confined Spaces	Fully applicable.
ANSI Z136.2	Safe Use of Optical Fiber Communication Systems Utilizing Laser Diode and LED Sources	Fully applicable when fiber optics are used.
ANSI/AIAA S-080	Space Systems-Metallic Pressure Vessels, Pressurized Structures, and Pressure Components	Fully applicable.
ANSI/AIAA S-081	Space Systems – Composite Overwrapped Pressure Vessels (COPV)	Fully applicable.
ANSI/ESD S20.20	Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	Fully applicable.
ANSI/NCSL Z540.3-2006	Requirements for the Calibration of Measuring and Test Equipment	Fully applicable.
ASTM Manual 36	Safe Use of Oxygen and Oxygen Systems: Guidelines for Oxygen System Design, Materials Selection, Operations, Storage, and Transportation	Fully applicable.
GEIA-STD-005-1	Performance Standard for Aerospace and High Performance Electronic Systems Containing Lead-Free Solder	Fully applicable.
IEEE 730-2002	IEEE Standard for Software Quality Assurance Plans	Fully applicable.
IPC J-STD-001D	J-STD 001D, Requirements for Soldered Electrical and Electronic Assemblies	Fully applicable with IPC J-STD-001DS Amendment 1.
IPC J-STD-001DS Amendment 1	Space Applications Electronic Hardware Addendum to J-STD 001D, Requirements for Soldered Electrical and Electronic Assemblies	Fully applicable.
SAE/AS5553*	Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition	Fully applicable.
SAE/AS9100	Quality Management Systems – Aerospace-Requirements	Fully applicable.

Note #1: NPR 8621.1 Applicability:
NASA-STD 8621.1 is fully applicable to NASA spaceflight programs in addition to the mishap response requirements in NASA FAR Supplement 1852.223-70 paragraph d/e.

Note #2: NASA-STD 8719.14 Applicability:
NASA-STD 8719.14 is fully applicable to NASA spaceflight programs.

The CCTS Program shall provide a full Orbital Debris Assessment Report (ODAR) per Appendix A prior to the first flight of each configuration as a part of HR Cert. For follow-on flights of a configuration, a memorandum delineating changes from the delivered ODAR will be provided.

Table 6-9: Type 3 SMA TA Documents

Document Number	Document Name	Applicability Comments
NPR 8621.1	NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping	Reference in addition to requirements noted in Table 6-1
NPD 8700.3	SMA Policy for NASA Spacecraft, Instruments, and Launch Services	Reference
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy	Reference
NPR 8715.3	NASA General Safety Program Requirements	Paragraphs not addressed in Tables 6-1 or 6-2
ANSI/ISO/IEC 17025-2000	General Requirements for Competence of Testing and Calibration Laboratories	Reference
ANSI/NCSL Z540.1-1994 (R2002)	General Requirements for Calibration Laboratories and Measuring and Test Equipment	Reference
AS 9003	Inspection and Test Quality System	Reference
NASA-STD 2202-93	Software Formal Inspections Standard	Reference
GIDEP S0300-BT-PRO-010	GIDEP Operations Manual	Reference
GIDEP S0300-BU-GYD-010	Government-Industry Data Exchange (GIDEP) Requirements Guide	Reference
GSFC-STD-1000	Goddard Space Flight Center Rules for the Design, Development, Verification, and Operation of Flight Systems	Reference

Appendix A: Acronyms

Acronyms	Phrase
AIAA	American Institute of Aeronautics and Astronautic
ANSI	American National Standards Institute
ARP	Aerospace Recommended Practice
CCTS	Commercial Crew Transportation System
CDR	Critical Design Review
CHRP	Commercial Human-Rating Plan
COPV	Composite Overwrapped Pressure Vessels
CxP	Constellation Program
DDT&E	Design, Development, Test, & Evaluation
DRM	Design Reference Mission
EEE	Electrical, Electronic, and Electromechanical
ESD	Electrostatic Discharge
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FCOD	Flight Crew Operations Directorate
GEIA	Government Electronics and Information Technology Association
GFE	Government Furnished Equipment
GIDEP	Government Industry Data Exchange Program
GSFC	Goddard Spaceflight Center
HFDS	Human Factors Design Standard
HRCP	Human-Rating Certification Package
IEEE	Institute of Electrical and Electronics Engineers
IPC	IPC – Association Connecting Electronics Industries
ISS	International Space Station
JPL	Jet Propulsion Laboratory
JPR	JSC Procedural Requirement
JSC	Johnson Space Center
KSC	Kennedy Space Center
LEO	Low Earth Orbit
MIL	Military
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NPD	NASA Policy Document
NPR	NASA Procedural Requirement
ODAR	Orbital Debris Assessment Report
ORR	Operational Readiness Review
PDR	Preliminary Design Review

Acronyms	Phrase
PMC	Program Management Council
PRA	Probabilistic Risk Assessment
RTCA	Radio Technical Committee for Aeronautics
R&M	Reliability and Maintainability
SAE	SAE International
SDR	System Definition Review
SMA	Safety and Mission Assurance
SRR	System Requirements Review
SSP	Space Station Program
STD	Standard
TA	Technical Authority

Appendix B: Definitions

Term	Definition
Abort	The forced early return of the crew to a nominal or contingency landing site when failures or the existence of uncontrolled catastrophic hazards prevent continuation of the mission profile and a return is required for crew survival. The crew is safely returned to a landing site in the space system nominally used for entry and landing/touchdown. Same as Mission Abort.
Analysis	A verification method utilizing techniques and tools such as math models, prior test data, simulations, analytical assessments, etc. Analysis may be used in lieu of, or in addition to, other methods to ensure compliance to specification requirements. The selected techniques may include, but not be limited to, engineering analysis, statistics and qualitative analysis, computer and hardware simulations, and analog modeling. Analysis may be used when it can be determined that rigorous and accurate analysis is possible, test is not cost effective, and verification by inspection is not adequate.
Ascent	The period of time from initial motion away from the launch pad until physical separation from the launch vehicle during nominal flight or during an abort.
Ascent Abort	An abort performed during ascent, where the crewed spacecraft is separated from the launch vehicle without the capability to achieve a safe stable orbit. The crew is safely returned to a landing site in a portion of the spacecraft nominally used for entry and landing/touchdown.
Automated	Automatic (as opposed to human) control of a system or operation.
Autonomous	Ability of a space system to perform operations independent from any ground-based systems. This includes no communication with, or real-time support from, mission control or other ground systems.
Catastrophic Event	An event resulting in the death or permanent disability of a crewmember or an event resulting in the unplanned loss/destruction of a major element of the CCTS during the mission that could potentially result in the death or permanent disability of a crewmember.
Catastrophic Hazard	A condition that could result in the death or permanent disability of a crewmember or in the unplanned loss/destruction of a major element of the CCTS during the mission that could potentially result in the death or permanent disability of a crewmember.
Crew	Any human onboard the spacecraft after the hatch is closed for flight or onboard the spacecraft during flight.

Term	Definition
Commercial Crew Transportation System (CCTS)	The collection of all space-based and ground-based systems (encompassing hardware and software) used to conduct space missions or support activity in space, including, but not limited to, the integrated space vehicle, space-based communication and navigation systems, launch systems, and mission/launch control. (This definition is the same as the definition of Space System found in NPR 8705.2).
CCTS Certification	CCTS Certification is the documented authorization granted by the NASA Associate Administrator that allows the use of the CCTS within its prescribed parameters for its defined reference missions. CCTS Certification is obtained prior to the first crewed flight (for flight vehicles) or operational use (for other systems).
Critical Software	Any software component whose behavior or performance could lead to a catastrophic event or abort. This includes the flight software as well as ground-control software.
Demonstration	A method of verification that consists of a qualitative determination of the properties of a test article. This qualitative determination is made through observation, with or without special test equipment or instrumentation, which verifies characteristics such as human engineering features, services, access features, and transportability. Demonstration requirements are normally implemented within a test plan, operations plan, or test procedure.
Emergency	Either an ISS emergency or medical emergency unless specifically stated.
Emergency Egress	Capability for a crew to exit the vehicle and leave the hazardous situation or catastrophic event within the specified time. Flight crew emergency egress can be unassisted or assisted by ground personnel.
Emergency Equipment and Systems	Systems (Ground or Flight) that exist solely to prevent loss of life in the presence of imminent catastrophic conditions. Examples include fire suppression systems and extinguishers, emergency breathing devices, and crew escape systems. Emergency systems are not considered a leg of failure tolerance for the nominal, operational equipment and systems, and do not serve as a design control to prevent the occurrence of a catastrophic condition. Emergency equipment and systems are not required to be designed and tested to the full range of functional, performance and certification requirements defined for the nominal, operational equipment and systems
Failure Tolerance	The ability to sustain a certain number of failures and still retain a specific capability (e.g. capability to control hazards, capability to continue the mission, etc.). A component, subsystem, or system that cannot sustain at least one failure is not considered to be failure tolerant.
Habitable	The environment that is necessary to sustain the life of the crew and to allow the crew to perform their functions in an efficient manner. These environments are described in NASA-STD-3000.

Term	Definition
Hazard	A state or a set of conditions, internal or external to a system, that has the potential to cause harm (Source - NPR 8715.3).
Hazard Analysis	The process of identifying hazards and their potential causal factors.
Health & Status Data	Data including Emergency, Caution, and Warning data that can be analyzed or monitored describing the ability of the system or system components to meet their performance requirements.
Human Error	Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence.
Human-System Integration	The process of integrating human operations into the system design through analysis, testing, and modeling of human performance, interface controls/displays, and human-automation interaction to improve safety, efficiency, and mission success.
Loss of Crew	Death or permanently debilitating injury to one or more crewmembers.
Loss of Mission	Loss of or the inability to complete the primary mission objectives defined in DRM
Manual Control	The crew's ability to bypass automation in order to exert direct control over a space system or operation. For control of a spacecraft's flight path, manual control is the ability for the crew to affect any flight path within the capability of the flight control system. Similarly, for control of a spacecraft's attitude, manual control is the ability for the crew to affect any attitude within the capability of the flight/attitude control system.
Mission	The mission begins with entry of the crew into the spacecraft, includes delivery of the crew to/from ISS, and ends with successful delivery of the crew to NASA after landing.
NASA Crew	The NASA crewmembers or the NASA sponsored crewmembers. These include international partner crewmembers.
Passenger	Any human on board the space system while in flight that has no responsibility to perform any mission task for that system. Often referred to as "Space Flight Participant."
Proximity Operations	Two or more vehicles operating in space near enough to each other so as to have the potential to affect each other. This includes rendezvous and docking (including hatch opening), undocking, and separation (including hatch closing).
Reliability	The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions.

Term	Definition
Rescue	The process of locating the crew, proceeding to their position, providing assistance, and transporting them to a location free from danger.
Risk	The combination of (1) the probability (qualitative or quantitative) including associated uncertainty that the space system will experience an undesired event (or sequences of events) such as internal system or component failure or an external event and (2) the magnitude of the consequences (personnel, public, and mission impacts) and associated uncertainties given that the undesired event(s) occur(s).
Risk Assessment	An evaluation of a risk item that determines (1) what can go wrong, (2) how likely is it to occur, and (3) what the consequences are.
Safe Haven	A functional association of capabilities and environments that is initiated and activated in the event of a potentially life-threatening anomaly and allows human survival until rescue, the event ends, or repair can be affected.
Safety	The absence from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
Software	Computer instructions or data, stored electronically. Systems software includes the operating system and all the utilities that enable the computer to function. Applications software includes programs that do real work for users, such as word processors, spreadsheets, data management systems, and analysis tools. Software can be Commercial Off-The-Shelf (COTS), Contractor developed, Government Furnished, or combinations thereof.
Technical Authority	The NASA individual who specifically maintains technical responsibility for establishment of, changes to, and waivers of requirements in a designated area. There are three Technical Authorities: Engineering, Safety and Mission Assurance, Health and Medical.
Test	A method of verification in which technical means, such as the use of special equipment, instrumentation, simulation techniques, and the application of established principles and procedures are used for the evaluation of components, subsystems, and systems to determine compliance with requirements. Test will be selected as the primary method when analytical techniques do not produce adequate results; failure modes exist which could compromise personnel safety, adversely affect flight systems or payload operation, or result in a loss of mission objectives; or for any components directly associated with Space Station and orbiter interfaces. The analysis of data derived from tests is an integral part of the test program, and should not be confused with analysis as defined above. Tests will be used to determine quantitative compliance to requirements and produce quantitative results.
Validation	Proof that the product accomplishes the intended purpose. May be determined by a combination of test, analysis, and demonstration.

Term	Definition
Verification	Proof of compliance with a requirement or specifications based on a combination of test, analysis, demonstration, and inspection.
Verification Plan	A formal document listing the specific technical process to be used to show compliance with each requirement.
Waiver	A written authorization allowing relief from a requirement.