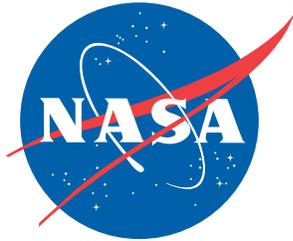


NASA/TM-2011-217089  
NESC-RP-10-00619



# Readiness for First Crewed Flight

*Dawn M. Schaible/NESC  
Langley Research Center, Hampton, Virginia*

## NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

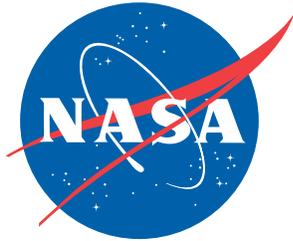
- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at <http://www.sti.nasa.gov>
- E-mail your question via the Internet to [help@sti.nasa.gov](mailto:help@sti.nasa.gov)
- Fax your question to the NASA STI Help Desk at 443-757-5803
- Phone the NASA STI Help Desk at 443-757-5802
- Write to:  
NASA STI Help Desk  
NASA Center for AeroSpace Information  
7115 Standard Drive  
Hanover, MD 21076-1320

NASA/TM-2011-217089  
NESC-RP-10-00619



# Readiness for First Crewed Flight

*Dawn M. Schaible/NESC  
Langley Research Center, Hampton, Virginia*

National Aeronautics and  
Space Administration

Langley Research Center  
Hampton, Virginia 23681-2199

---

April 2011

The use of trademarks or names of manufacturers in the report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

NASA Center for AeroSpace Information  
7115 Standard Drive  
Hanover, MD 21076-1320  
443-757-5802

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>			Page #: 1 of 58

## **Readiness for First Crewed Flight**

**April 12, 2011**

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		2 of 58	

### Approval and Document Revision History

NOTE: This document was approved at the April 12, 2011, NRB. This document was submitted to the NESC Director on April 15, 2011, for configuration control.

Approved:	<i>Original Signature on File</i> <hr style="width: 80%; margin: 0 auto;"/> NESC Director	4/15/11 <hr style="width: 80%; margin: 0 auto;"/> Date
-----------	--	---

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Ms. Dawn Schaible, Manager, NESC Systems Engineering Office	04/12/11

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		<b>3 of 58</b>	

## Table of Contents

<b>1.0</b>	<b>Notification and Authorization .....</b>	<b>5</b>
<b>2.0</b>	<b>Signature Page.....</b>	<b>6</b>
<b>3.0</b>	<b>Team List .....</b>	<b>7</b>
3.1	Acknowledgements.....	7
<b>4.0</b>	<b>Evaluation of Readiness for First Crewed Flight.....</b>	<b>8</b>
4.1	Preface.....	8
4.2	Introduction.....	9
4.3	Need for First Crewed Flight .....	10
4.4	Understanding and Mitigating Residual Risk.....	10
	4.4.1 Focus on Crew Safety .....	10
	4.4.2 System Knowledge and Uncertainty Reduction .....	12
	4.4.3 Proven Means of Return to Earth.....	17
4.5	Confidence .....	17
	4.5.1 Design Maturity and Simplicity.....	18
	4.5.2 Verification and Validation.....	18
	4.5.3 Program Team.....	18
	4.5.4 Program Processes .....	19
	4.5.5 Demonstrated Record of Success.....	20
	4.5.6 Independent Input and Perspective .....	20
4.6	Summary .....	21
<b>5.0</b>	<b>Acronyms List .....</b>	<b>23</b>

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
	Title: <b>Readiness for First Crewed Flight</b>		Page #: 4 of 58

### List of Figures

Figure 4.4-1. Focus on Safety-related Items and Risks .....	11
Figure 4.4-2. Major Contributors to Understanding Residual Risk for First Crewed Flight.....	13
Figure 4.4-3. Understanding Margins and Incremental System Capability Validation.....	15
Figure A.1-1. Progression of Testing to Build Up Evidence for Safe System Operation .....	24
Figure E.1-1. Mercury Redstone and Atlas Critical Path for Return to Earth .....	41
Figure E.1-2. Gemini Critical Path for Return to Earth.....	44
Figure E.1-3. Apollo Critical Path for Return to Earth.....	45
Figure E.1-4. Space Shuttle Critical Path for Return to Earth.....	48
Figure E.1-5. U.S. Human Spaceflight Development.....	52

### Appendices

Appendix A. The Role of Testing.....	24
Appendix B. Techniques for Risk Identification .....	29
Appendix C. Discussion of Risk Contributors.....	33
Appendix D. Evaluation of Risk Analysis Tools.....	35
Appendix E. Historical Perspective on First Crewed Flights .....	39
Appendix F. Benchmarking with U.S. Navy and Air Force Flight Test Center.....	54
Appendix G. Selected References.....	57

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 5 of 58	

## 1.0 Notification and Authorization

On March 11, 2010, the Constellation Program (CxP) Manager, Mr. Jeff Hanley, requested the NASA Engineering and Safety Center (NESC) to “develop a framework for evaluating whether a program has sufficiently complete and balanced plans in place to allow crewmembers to fly safely on newly developed human spaceflight systems for the first time: including technical, risk, and programmatic considerations.” The CxP Manager then asked that the framework be applied to current CxP plans. In addition, the NASA Chief Engineer and Chief Safety and Mission Assurance (S&MA) Officer requested the framework also encompass future human spaceflight systems that may be developed by government and/or commercial providers.

An NESC out-of-board (OOB) activity was approved on March 11, 2010. An OOB summary was presented at the NESC Review Board (NRB) on March 30, 2010. The assessment plan was approved by the NRB on April 29, 2010. A status briefing was presented to the NRB on July 16, 2010.

The key stakeholders for this assessment are CxP, Office of Chief Engineer, Office of S&MA, and Commercial Crew Transportation Planning Office.



	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		<b>Readiness for First Crewed Flight</b>	
		Page #: 7 of 58	

### 3.0 Team List

Name	Discipline	Organization
<b>Core Team and Consultants</b>		
Dawn Schaible	NESC Team Lead	LaRC
Michael Bay	System Engineering	GSFC
Michael Blythe	NESC Deputy Director for Safety	JSC
Patrick Forrester	NESC Chief Astronaut	JSC
David Hamilton	Spacecraft Development/Consultant	JSC - retired
Benjamin Jimenea	NESC Systems Engineer	KSC
T.K. Mattingly	Former Astronaut/Consultant	SPA
Cynthia Null	NASA Technical Fellow for Human Factors	ARC
Victoria Regenie	NESC Systems Engineer	DFRC
Charles Shaw	Missions Operations/Consultant	JSC – retired
J. Phillip Sumrall	Launch Vehicle Development	MSFC
Tricia Johnson	MTSO Program Analyst	LaRC
<b>Project Liaison</b>		
William Arceneaux	CxP Special Assistant for System Integration and Verification	JSC
<b>Administrative Support</b>		
Terri Derby	Project Coordinator	LaRC/ATK
Linda Burgess	Planning and Control Analyst	LaRC/ATK
Carolyn Snare	Technical Writer	LaRC/ATK

### 3.1 Acknowledgements

The NESC team would like to thank Mr. Kenneth Johnson and Dr. William Vesely for their contributions to the development of the appendix on the evaluation of risk analysis tools.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 8 of 58	

## 4.0 Evaluation of Readiness for First Crewed Flight

### 4.1 Preface

The NASA Engineering and Safety Center (NESC) was requested to develop a generic framework for evaluating whether any given program has sufficiently complete and balanced plans in place to allow crewmembers to fly safely on a human spaceflight system for the first time (i.e., first crewed flight). The NESC assembled a small team which included experts with experience developing robotic and human spaceflight and aviation systems through first crewed test flight and into operational capability. The NESC team conducted a historical review of the steps leading up to the first crewed flights of Mercury through the Space Shuttle. Benchmarking was also conducted with the United States (U.S.) Air Force and U.S. Navy.

Historical data shows that there are multiple approaches which have been successful for determining readiness for the first crewed flight. Every approach has to be tailored to the specific system design and situation of that particular system and mission objectives. Because specific approaches may vary significantly between different system designs, the NESC team determined prescriptive instructions or thorough checklists could not be developed to apply to all possible human spacecraft systems. In the course of the team's deliberations, however, it became evident that there are certain guiding principles that should be applied when developing the first crewed flight decision. A general framework for evaluating whether a program has sufficiently complete and balanced plans for the first crewed flight is documented in the narrative that follows. In the appendices that follow, a more in-depth discussion of testing, risk identification, risk contributors, risk analysis tools, and a historical perspective are covered.

The NESC framework presented here includes important factors to consider when developing a new system or evaluating an existing system for the first crewed flight. The NESC team believes that documenting these concepts in one place will help to focus on the critical areas for consideration and additional scrutiny. By applying the following framework to a specific design, test program, and intended mission objectives, decision makers will have better information with which to make the decision for first crewed flight. To focus the NESC team's discussion, only space transportation to and from low Earth orbit was considered, because these stages represent the most relevant and significant risks to a first crewed flight. For considerations beyond low Earth orbit, the framework described in this report can be extended to encompass all mission risks.

The question of when to fly crew for the first time is evaluated at many stages through the development of the human spaceflight system—first during the planning stages and then throughout development and testing and at major milestones. While the NESC team was requested to look at the planning decision, the concepts described in this report are applicable throughout the lifecycle of the program. Determining readiness for a first crewed flight is dependent on the specific system and its mission. In general terms, the system is ready to fly when residual risk has been mitigated to the point where it is outweighed by the need to fly the

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		9 of 58	

first crew. This decision is ultimately the judgment of the program and Agency management in conjunction with the design and operations team.

## 4.2 Introduction

Determining readiness for a human spaceflight system's first crewed flight, especially when the test flight is part of the overall system certification process, has been a challenge for program decision makers. In addition, this question is not limited to human space flight; it is also common in aeronautic and naval applications. Most aircraft and terrestrial systems, however, are designed to have relatively large performance envelopes that allow incremental and reversible envelope expansion techniques during development and testing. In a human spaceflight system, once a ground test program is complete, an incremental test approach is difficult. Many space systems events, especially launch vehicle liftoff, de-orbit, and re-entry, are irreversible events that require using essentially the entire performance envelope to achieve a safe outcome—making this decision process even more difficult.

The decision on first flight is ultimately the judgment of the program and Agency management in conjunction with the design and operations team. There is, however, some general guidance that can be used in making these judgments. Close involvement of the technical and management teams throughout the design and development process is essential. Verification and validation (V&V) of safety-critical systems and survival functions are required. Based on previous experience, historical perspectives, and best practices, this report will illustrate a top-level thought process for making a first flight decision and will help focus the debate and discussion on critical areas for consideration and additional scrutiny.

In the simplest terms, it is time to fly a crew for the first time when it is safe to do so and the benefit of flying a crew is greater than the residual risk (see Section 4.3). This is rarely a straight-forward, clear-cut trade off so experience, sound judgment, and established (and clearly documented) decision-making processes are essential (see Section 4.4). In addition, the underlying level of confidence the manager has in making the decision must be considered (see Section 4.5). The remainder of this report will describe this concept in greater detail.

This report focuses on ways to understand the residual risk<sup>1</sup> and gain confidence in the decision-making processes. Based on the NESC team's deliberations and collective experiences, challenges were identified that are likely to be encountered and examples provided of techniques that have been proven (or may now be available) to manage risk to acceptable levels, as thought provokers (see Appendices).

---

<sup>1</sup> In this report, residual risk is defined as the risk remaining after other known risks have been eliminated, managed, mitigated, or accepted

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		10 of 58	

### 4.3 Need for First Crewed Flight

Given that the human spaceflight system is designed for human spaceflight, it is accepted that the objective is to fly humans when risks to crew safety have been mitigated to the point where the need or benefit is worth the residual risks. The effort then shifts to deciding WHEN it is safe to fly crew, not IF a crew should fly.

Senior leaders and decision makers must evaluate the specific test objectives for the mission to determine the need for a crew. Once this need has been established, the focus then shifts to ensuring that the necessary safety-related crew interface, safety, and survivability requirements are met. A prerequisite for a first crewed flight is confidence gained through understanding of the system design, development, analysis, and testing.

It should be noted that the decision that crew is needed for a particular test or mission is primarily a programmatic decision (program and Agency management). For the technical team, the focus must be on ensuring a safe and technically sound system.

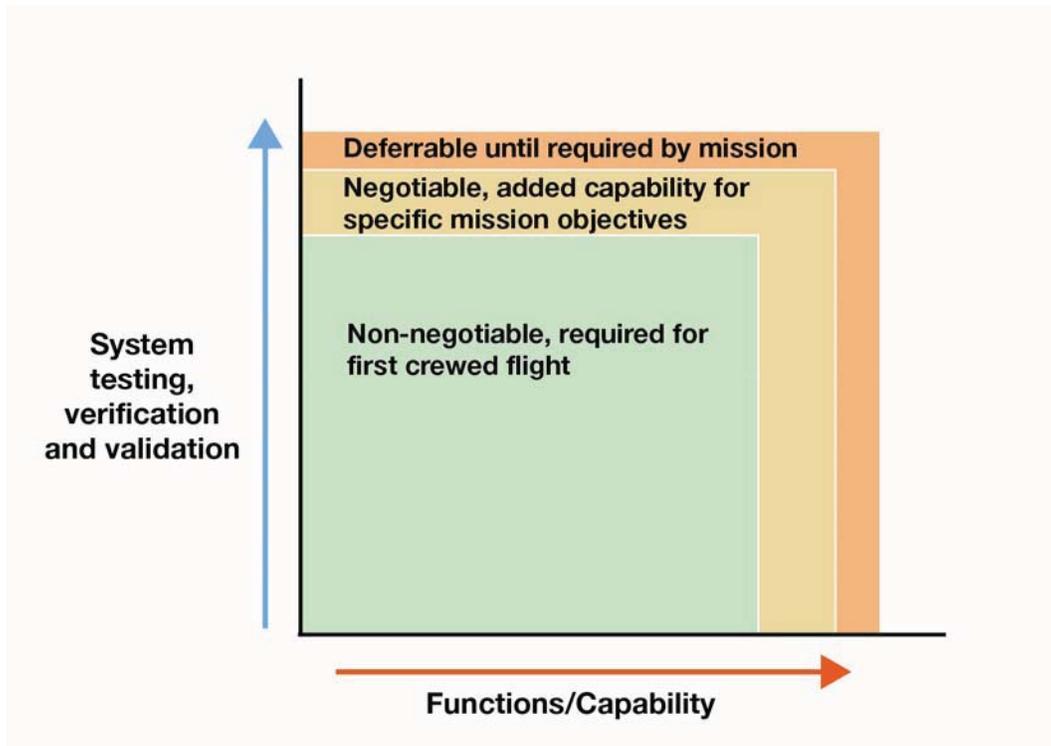
### 4.4 Understanding and Mitigating Residual Risk

#### 4.4.1 Focus on Crew Safety

The process of designing, developing, and testing a new launch system is very complex and involves the spacecraft, launch vehicle, ground systems, mission systems, recovery systems, ground crews, and flight test crews. The program teams have a wide-ranging responsibility to ensure the system is adequately assessed, tested, and deemed safe for human flight. It is recognized that, despite the best efforts of the vehicle team, early flights of new systems will entail some degree of residual risk. Therefore, the focus should be on reducing and managing safety-related risk to the greatest extent practical. Initial crewed missions must be conducted with a minimum of onboard personnel (either active or passive participants). Such flights may warrant unique contingency procedures/capabilities that will preserve a safe return capability (i.e., above and beyond that required for the nominal design mission) utilizing specially trained crews.

In order to focus to those items that are unique to the initial crew participation, it is assumed the system/operations design must preserve a safe return to Earth capability in the presence of any single failure in any critical functional capability to the maximum extent practical. Safety issues, including providing for a safe crew return, should be separated from those needed only to enhance the mission. Mission enhancement functions of the crew are only considered to the extent that they affect safety. Figure 4.4-1 illustrates this concept. Safety and crew survival (such as abort capability) functions are non-negotiable and must be fully tested, verified, and validated prior to the first crewed flight. For each specific test or mission, additional functions will be required to meet objectives that have been defined. Each subsequent test and mission may require additional capabilities.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:			Page #:
<b>Readiness for First Crewed Flight</b>			11 of 58



*Figure 4.4-1. Focus on Safety-related Items and Risks*

Functions that are critical for crew safety and survival must be established early in the design and development process. These crew safety and survival functions should be formed into a set of non-negotiable, first crewed flight requirements that form the basis for required design, development, testing, and V&V. The following criterion is assumed as the basis for determining the minimum requirements that must be satisfied in allowing crew participation:

***System/operations design must preserve a safe return to Earth capability in the presence of any single credible failure in any critical functional path for the intended mission.***

The focus then shifts to determining what these safety-critical functions are and the degree to which they can be validated<sup>2</sup>.

<sup>2</sup> Verification of a product shows proof of compliance with requirements. Validation of a product shows that the product accomplishes the intended purpose—and in the case of models/analysis, that models adequately predict the environment and match actual vehicle performance.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		12 of 58	

#### 4.4.2 System Knowledge and Uncertainty Reduction

Safety must be an inherent part of the design. Programs must establish requirements for each system's specific design that will address safety-related items (e.g., failure tolerance, risk of loss of crew and mission, overall system reliability). A system-level focus on selection of simple and

*Key elements of common aerospace design practices instrumental in the path to first flight include:*

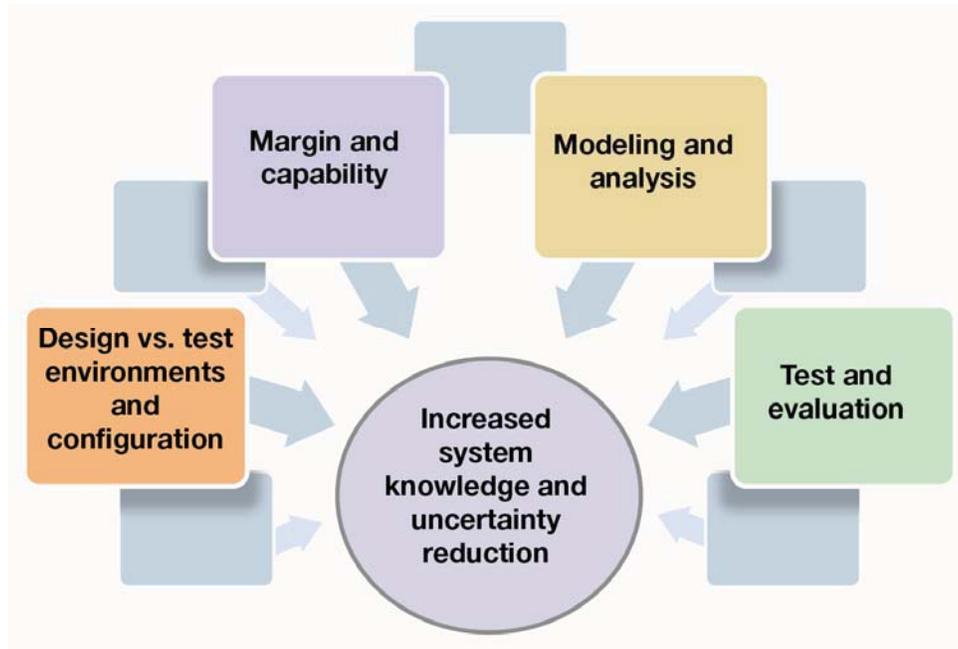
- *Implementation of applicable technical requirements*
- *Utilization of safety analyses in system development*
- *Verification, validation, and testing of critical system performance*
- *Technical authority involvement*
- *Hazard identification and control*
- *Integration of human-in-the-system and human-error management (both ground and flight test crews)*
- *Analyses, tests, demonstrations, and inspections in ground tests and previous flight tests*

safe solutions to meet critical functions necessary to accomplish the mission is required. These safety-critical design requirements must be addressed prior to the first crewed flight. Sound aerospace-engineering practices for design, testing, and analysis must include all disciplines that affect any aspect of a safe design. Examples include: propulsion; environmental control and life support; structures; mechanisms; materials; active/passive thermal; pyrotechnics; aerodynamics; flight mechanics; loads and dynamics; guidance, navigation, and control; electrical systems; avionics; software; thermal protection; crew systems; human factors; communication; space environments; ground operations; and flight operations. In addition, design guidelines and standards associated with each technical and operational discipline must be considered relative to their effect on crew safety (e.g., margins, structural strength, and factors of safety). Including representation from those

organizations that will operate the system (in flight and on the ground) is also important in the design of active systems and user interfaces, as well as during system-level testing.

Gaining understanding of system design, operation, and performance (hence reducing risk) is traditionally accomplished through many factors that have been established as part of sound engineering practices. Figure 4.4-2 highlights areas that warrant particular attention when determining first crewed flight readiness. Specific details and examples are described in Appendices A–D.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:			Page #:
<b>Readiness for First Crewed Flight</b>			13 of 58



*Figure 4.4-2. Major Contributors to Understanding Residual Risk for First Crewed Flight*

Given that the first crewed flight is likely to occur as part of the development process, extra consideration for crew safety must be given to the specific mission plan and vehicle configuration. The flight test environment must be compared to previous test conditions/parameters and analysis assumptions. Understanding the environment in which the system will operate and how it will vary for different phases of the mission allows the system to be tested in relevant conditions and thus reduces uncertainty. Design and analysis should address full flight envelope operation of the spaceflight system’s design capability (including induced and natural environments) and failure/abort conditions. Examples: loads analyses for launch, ascent, orbit, entry, and landing (coupled loads analyses); strength/stress/margin assessments for critical load conditions; entry heating and thermal protection system performance; crew life support; propulsion systems; and trajectories.

The flight hardware/software for test flights may, however, be in a different configuration than for operational flights, or may not be fully qualified. It is imperative that these differences be identified and thoroughly evaluated to fully understand the residual risk. The key areas that require specific attention and scrutiny include:

- Configuration of the vehicle for flight test versus previous tests
- Fidelity, assumptions, and validation of models versus flight configuration

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		14 of 58	

- Analyzed configuration versus flight configuration
- Certification level and fidelity of hardware/software installed for flight test

A review of the specific flight configuration should be conducted, along with the implications of test results and anomaly resolutions from previous testing and analyses. Specific analyses may be performed for the mission, to include any potential contingencies. It is critical, however, to understand the assumptions and fidelity of the models being used, and where the results are valid for that particular flight configuration. Accepting data from models that are not validated within the range of operation can be problematic.

Another area that poses a potential problem for a first crewed flight is the certification level or fidelity of hardware/software installed on the vehicle for that flight (and of the ground systems used to support and operate the vehicle/mission). Due to timing and the requirements for the specific mission, engineering and/or prototype equipment may be used. Additional test instrumentation may also be part of the mission configuration. A decision to use an uncertified or off-nominal configuration requires a thorough review, including an assessment of any possible unintended interactions.

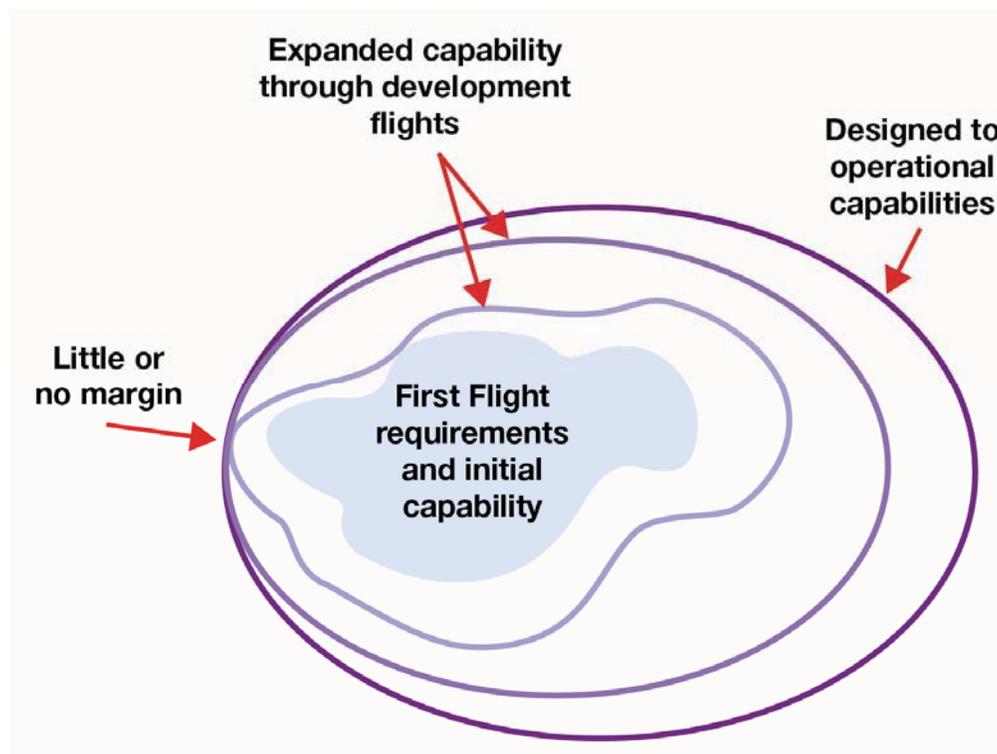
Managing margins is critical to the vehicle design and development. In this case, a margin is the difference between the design requirements (including factors of safety) and the system's actual performance capability in the worst-case environment and operating states. Examples of areas where margins are important include power, mass, delta-velocity, structure, and many others. Decision makers must understand the margins of each system before making a first flight decision. Planned operations are often placarded to stay within system capabilities, especially in the early development flights (in some cases, such as launch, it is difficult to gain margin via placards; propulsion systems may operate near maximum levels on every mission). Through effective testing and proper processing, the actual system capability can be determined. Each development flight test provides increased knowledge and reduces uncertainty within the cleared envelope of operation—allowing for incremental

*“During the second Gemini Launch Vehicle Test (GT-2), the launch vehicle lost hydraulic pressure in its primary control system and had switched over from primary to secondary guidance and control. The system had detected its own hydraulic failure, responded by switching over to its secondary system, and then, because it was still on the ground, commanded its engine to shut off. Subsequent investigation revealed that unexpectedly high pressure in one of the hydraulic lines had burst the aluminum housing of a servovalve. During development, someone had decided that the walls of the housing were twice as thick as they needed to be; a third of a centimeter of aluminum was ample to meet design pressures. No one, however, thought to test the actual pressure the housing would have to withstand, nor was any impulse test, as such, included in system qualification. More likely than not, one or another Titan II had suffered the same sort of hard start, but the stouter housings that remained standard in the missile could survive such a pulse while the lighter structural shell in the Gemini booster could not.”*

*From **On the Shoulders of Titans: A History of Project Gemini** by Barton C. Hacker and James M. Grimwood, NASA Special Publication-4203 in the NASA History Series, 1977.*

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		15 of 58	

envelope expansion as more measurements are obtained and analytical tools are validated. Figure 4.4-3 illustrates this concept. The outer oval represents the operational system capability or “designed to” envelope, as built up/validated over the course of the test program. A robust, reliable, and safe design incorporates the ability to test specific points of the design where lower margins, high risk, etc., occur due to new technology, use of previous technology in an untested environment, or other factors. As in most systems, the amount of margin varies. In some cases the system is quite robust (i.e., large positive margin), in other areas there is little margin (see Figure 4.4-3). Greater margins are required where there is large uncertainty in the design and environments. Understanding the margins, to the maximum extent practical, is vital in determining the safety of first crewed flight.



*Figure 4.4-3. Understanding Margins and Incremental System Capability Validation*

Minimizing risk goes beyond meeting requirements and adhering to established standards. It requires exploring what can go wrong and developing mitigations that either eliminate or reduce the ensuing residual risk to acceptable levels in the as-built system, including where uncertainties might reduce margins to unsafe levels along the flight envelope. Providing sufficient margin is an essential part of mitigating uncertainty and performing a safe mission.

Prior to crewed flight, the system’s performance and operating margin relative to the natural and induced environments must be anchored by validated analysis/modeling and/or testing.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 16 of 58	

Knowledge of the design process improves understanding of the limitations of analysis techniques—as it is these limitations that are critical to understanding the risk and ultimately the safety of the system. The results from analytical tools are dependent on the accuracy of the models and the methods of calculation. While most results can be calculated to multiple significant figures, most models do not have that level of accuracy of the actual system/hardware. Many of the models may be approximations due to limited knowledge of the physics, external environment, systems, or limited resources. These tools have enormous potential for improving the development process once their results are validated by experimentation in each specific application. Furthermore, since these model formulations can be manipulated to match experimental data at a given condition, they cannot be considered accurate until the same formulation is used under multiple plausible conditions. Such validation can, to a large degree, be accomplished through ground testing, but there are several classes of measurements that can only be obtained with accuracy in flight (acoustics, aero-thermal, induced environments, etc.).

A ***critical test list*** is a key tool for determining when a vehicle is ready for flight. This list contains the tests, along with success criteria, that must be completed to reduce the system risk to an acceptable level and would cover the non-negotiable items, as discussed in Section 4.4.1. This list should be created early in the development process. While the overall test requirements will be fluid over the course of the program, changes to this critical test list should be rare and only done after much debate and agreement among the team. Adhering to the list will help guard against the pressures of limited resources (time and budget) that programs often face during development.

The progression from analysis to ground test and then to flight test (uncrewed and then crewed) is also the progression of the fidelity of data that can be generated. Ideally, safety-critical and survival functions would be tested and verified through ground tests. This is not always possible, as flight environments and potential interactions cannot always be anticipated and replicated on the ground. Any safety-critical function that must operate (or must not operate) during a crewed mission must be verified and validated to an accepted confidence level prior to the first crewed flight. Flight and ground tests must have similar instrumentation and be in the same locations, as much as is practical, to compare data and allow the flight test to validate the ground test and the analysis. A single measurement in any of the testing may not be sufficient to validate the system or model. (See Appendix A for a more detailed discussion of testing.)

To understand the uncertainty, and for the flight risk to be accepted, sufficient test measurements are needed to verify the environment, confirm the analysis, and confirm location of flight measurements. Flight tests should include: definition of flight test reference missions, objectives, flight-specific functions, performance, and verification requirements; and assessment of all waivers, deviations, and exceptions. Finally, the program should ensure the resolution of anomalies from previous ground and flight tests and identify deviations from previous tests and baseline design.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		17 of 58	

#### 4.4.3 Proven Means of Return to Earth

A safe return to Earth from any stage of a mission, including launch, must be ensured through contingency capabilities and procedures to the maximum practical extent. Careful thought must be given to the entire mission with the goal of always being able to return the crew safely to Earth. In addition, it must be verified that the intended mission can be controlled, with uncertainties, to remain within the flight envelope validated for that mission.

Launch through the atmosphere inherently poses a tightly constrained flight envelope due to the rapid release of large amounts of energy by the propulsion system, significant aerodynamic loading, and the fact that structural loads may be at their maximum for the launch vehicle and some spacecraft components. Therefore, early human spaceflight designs provided some form of “last resort” escape from the launch vehicle during the period from liftoff through maximum dynamic pressure (max q-bar), transonic transition, stage separation, and the establishment of a functioning upper stage. Because the range of unacceptable conditions is impossible to define with complete confidence, emergency system designs cannot ensure success in every conceivable case, but portions of the envelope can and must be verified and validated to be safe for supporting human flight. If a launch escape capability is available, it should not be factored into reliability considerations but serve as a last resort to preserve the life of the crew.

The Space Shuttle configuration, unlike the small crew capsules used in the early programs, precluded reliance on escape systems while its solid rocket boosters (SRBs) were burning. Because SRB thrust termination designs introduced additional safety risks, the design team elected to invest the resources necessary to provide assurance that the entire launch system could be treated, like primary structure, as having a reliability of 1.0 from ignition through SRB separation. The fact that an unrecognized combination of environments subsequently resulted in a catastrophe does not, by itself, invalidate the selected design approach. Rather, this tragic event reinforced the importance of meticulously monitoring flight and test data relentlessly pursuing, understanding, and resolving every out-of-family (not just out-of-specification) measurement.

Knowledge of the system and understanding of the residual risks are gained as a system evolves. Each step of the design, development, assembly, integration, and test process builds the body of evidence the decision makers can use to determine the acceptability of the residual risks. Therefore, the decision of first flight must be considered, planned, and assessed at each step of the process. An important part of this overall process is maintaining and encouraging the open discussions and debates within the entire program team—and maintaining a healthy tension between the program and technical authorities, operations and design, systems and disciplines, etc.

#### 4.5 Confidence

An important consideration in determining when it is safe to put crews in a human spaceflight system is the overall level of confidence that the decision makers have in the system. For this

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 18 of 58	

report, the NESC team is referring to subjective confidence based on engineering judgment, not statistical projections. Decision makers gain confidence through a combination of several tangible and intangible means. Some examples and descriptions of contributing factors are provided in the following sections.

#### **4.5.1 Design Maturity and Simplicity**

The use of ‘proven’ hardware/software and designs can provide increased confidence, assuming similar environments, conditions, applications, etc. However, the design team should be cautious in using ‘heritage’ and ‘off the shelf’ hardware and software. The use of these proven systems must be analyzed and verified for use in new environments and applications. Designs that have additional safety margins at the component, system, or operations levels (as discussed in Section 4.4.2) may also merit increased confidence.

Systems that employ inherently simpler designs, fewer interfaces, and large margins to meet their needs will likely increase confidence in their ability to perform safely and reliably. For example, the Space Shuttle drops its landing gear by releasing retention hooks and allowing gravity and air loads to deploy the landing gear, avoiding hydraulic or other actuating power devices. Complexity should only be added when there is benefit such as in weight, volume, performance, or operations.

#### **4.5.2 Verification and Validation**

V&V are essential for developing a safe human spaceflight system. When determining if a vehicle is ready for crewed flight, a review of the V&V program should be conducted (as discussed in Section 4.4.2 and Appendix A). A complete and thorough test program will increase confidence in mission success. When a vehicle or system has a significant history of testing prior to the current program and the configuration, operational environment, and performance parameters are similar enough, the applicable historical test data and analyses may be used for verification and can also increase confidence in the system. Analytical design tools, validated with experimental data over a range of conditions, provide the most confidence.

The test program should always include end-to-end testing and integrate humans, hardware, and software to the degree needed to sufficiently understand the dynamics of interaction, control risk, and gain confidence in the integrated system.

#### **4.5.3 Program Team**

The experience and longevity of the program team are significant confidence builders in development of a successful human spaceflight system.

Confidence is enhanced when program management and supporting members of the program team (including safety and mission assurance (S&MA) and medical) are responsible for ensuring an appropriate emphasis on safety during the design, development, and testing of the launch

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		19 of 58	

vehicle, spacecraft, launch-abort system, mission operations, ground operations, manufacturing, and other areas.

Teams consisting of members with significant design/development experience in the fields they currently support and who have already been through major design, development, and testing campaigns provide increased confidence. A strong systems engineering focus is also important in understanding and managing the interfaces and interactions—of both the design and the team.

Confidence increases when decision makers insist on personal accountability (ownership) for the end results; good communication between team members; and operation in an open, positive environment. As stated in Section 4.4.3, maintaining and encouraging open discussions and debates within the entire team—and maintaining a healthy tension between the program and technical authorities, operations and design, systems and disciplines, etc., is an important part of developing confidence. Ideally, the team should be organized so that the decision-making authority is delegated to the hardware/system design level, thereby allowing timely decisions to be made. However, final accountability remains with the program and Agency managers. All decisions must consider safety first and be based on a balance of sound technical and programmatic rationale. It is important to note that organizations should have an alternate reporting path or governance structure that ensures safety and technical concerns are addressed.

*It is important for the entire team to remain focused on building up evidence to prove that the system is safe for first crewed flight. When this focus is lost, the team becomes vulnerable to error, oversights, and poor judgment. For example:*

*“The engineers found themselves in the unusual position of having to prove that the situation was unsafe – a reversal of the usual requirement to prove that a situation is safe.” Columbia Accident Investigation Board Report.*

It should be emphasized that hardware/software and system contractors are an essential part of the program team. The contract should allow open communication and individual responsibility. Since most hardware and software elements are provided by prime and sub-tier contractors, careful attention must be paid to the applicable statements of work, terms, and conditions to make sure that they motivate all parties to ensure safety and reliability. Some contract incentives may drive behavior contrary to what is desired. A simplified example would be if all award fees are based on simply meeting milestones—schedule pressure could take precedence over technical matters.

#### 4.5.4 Program Processes

For any complex program, established, efficient, effective, and documented processes are essential to define how the program functions. Understanding and ensuring proper program processes and outcomes will help determine the level of confidence.

Examples of processes to be analyzed include technical reporting/authority, technical checks and balances, S&MA practices, integration, and documentation. For instance, decision makers may gain confidence when the team has clearly defined and understood roles and responsibilities; a strategy for independent reviews and reporting; well-established risk management practices that

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		20 of 58	

identify and eliminate, reduce, or mitigate risks; readily available and up-to-date documentation; and documented rationale of major decisions.

#### **4.5.5 Demonstrated Record of Success**

Human spaceflight systems typically have well-documented design processes, with thorough engineering standards and processes. Some systems, however, may offer limited access to detailed design information. These systems may have different design and verification approaches, as well as differing processes, documentation, or quality-control plans. From a confidence-building standpoint, these kinds of differences and potential shortcomings may well be offset, in part, by a demonstrated launch performance record. This concept may apply to complete human spaceflight systems, such as the Russian Soyuz, or components or subsystems, such as the RD-180 rocket engine.

An existing system or subsystem may add to the confidence of decision makers if it has established a sound flight record in a similar configuration or operation, or if it has undergone related systems testing. Successful components or systems may function or operate within specific parameters but if those components or systems are introduced into new parameters, their continued success cannot be assumed unless appropriate testing using these new parameters is performed. Decision makers should be cautious if components or systems that were successful in previous programs are now used in environments for which they were not designed or tested. In addition, understanding of all past anomalies is essential.

It is important to note that decision makers must remember that past success does not automatically translate to future success. Previous flight history is only one factor in building confidence—it is not sufficient by itself to determine readiness for a first crewed flight. When using these previously flown systems or components, it is vital that the technical team has a sound basis for confidence in their continued success. Every system will present its own unique set of circumstances that must be thoughtfully considered in a manner consistent with the principles described in this report. In the end, the technical team will be accountable for the final results.

#### **4.5.6 Independent Input and Perspective**

Throughout the process, program and Agency management should seek out and integrate input from competent, current, and independent review teams. It is important that they review the program throughout its life cycle and have relevant insight into and knowledge of the design in order to make sound observations and recommendations. However, care should be taken that the review team retains their independence and maintains a balance between close participation and independence. In addition, independent technical assessments of new technologies, new developments, and expected high-risk areas should be performed throughout the life cycle.

Confidence is not a number or a data point. Decision makers must develop confidence to safely launch humans by working closely with the entire program team throughout the process of designing, building, and testing the vehicle.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 21 of 58	

The factors outlined above, along with others, contribute to building confidence in the human spaceflight system's ability to fly a crew safely. Overall confidence is a combination of many considerations and it is important that the contributing factors chosen encompass the entire system, including the launch vehicle and ground/mission systems. Readiness for crewed flight operations will always be an integrated judgment call based on the decision makers' experience, knowledge, and level of confidence in the system.

#### 4.6 Summary

The key points in this report can be viewed as questions that a decision maker may ask throughout the process of designing, building, and testing a new crewed vehicle. These questions include (but are not limited to):

- Are adequate safety features inherent in the design?
- Does the design preserve a safe return to Earth in the event of a single credible failure?
- Are the design requirements of the entire system understood and implemented?
- Does the team thoroughly understand the design and configuration?
- Has sufficient knowledge been gained through adequate design, analysis, and testing?
- Have models been thoroughly validated with physical data?
- Are hazards adequately identified and controlled, including across systems and interfaces, to the maximum extent practical?
- Have the safety-critical and survival functions been identified, verified, and validated prior to the first crewed flight (including test flights)?
- Have the program management and technical teams worked together and has there been open communication of issues throughout the lifecycle?
- Has the first crewed flight decision been considered at each step of the lifecycle?
- Has confidence been developed throughout the lifecycle and used in making an informed judgment?
- When decisions were made, did the team focus on showing how those decisions affect overall safety and risk?
- Are the program, engineering, S&MA, and operations teams in agreement for system readiness of a first crewed flight?

	<b>NASA Engineering and Safety Center      Technical Assessment Report</b>	Document #: <b>NESC-RP-          10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 22 of 58	

The process of determining readiness for a first crewed flight is dependent on the specific system and mission. In general terms, the vehicle is ready to fly when it has been deemed safe and when any residual risk has been mitigated to the point that it is outweighed by the need for a crew. This decision is ultimately the judgment of the program and Agency management in conjunction with the design and operations team.

	<b>NASA Engineering and Safety Center</b> <b>Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
	Title: <b>Readiness for First Crewed Flight</b>		Page #: 23 of 58

## 5.0 Acronyms List

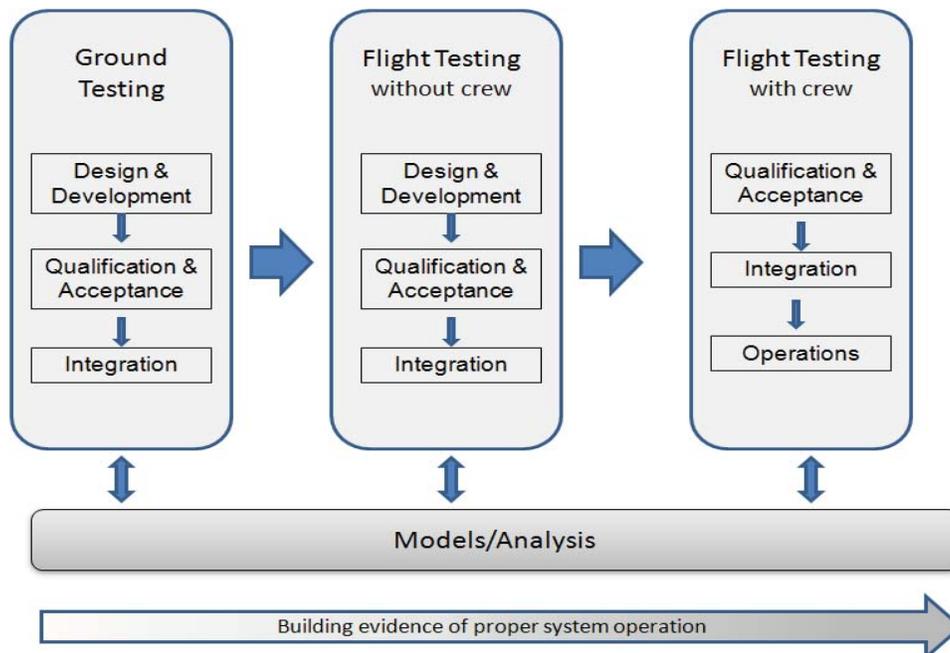
ARC	Ames Research Center
ATK	Alliant Techsystems, Inc.
CAD	Computer-Aided Design
CAM	Computer-Aided Manufacturing
CxP	Constellation Program
DFRC	Dryden Flight Research Center
FEA	Finite Element Analysis
FMEA	Failure Modes and Effects Analysis
FPGA	Field-Programmable Gate Array
GSFC	Goddard Space Flight Center
ISS	International Space Station
JSC	Johnson Space Center
KSC	Kennedy Space Center
LaRC	Langley Research Center
LEO	Low Earth Orbit
MA	Mercury Atlas
MC	Monte Carlo
MCO	Mars Climate Orbiter
MEIT	Multi-Element Integrated Tests
MR	Mercury Redstone
MSFC	Marshall Space Flight Center
MTSO	Management and Technical Support Office
NESC	NASA Engineering and Safety Center
NEST	NESC Engineering Statistics Team
NRB	NESC Review Board
OOB	Out of Board
PRA	Probabilistic Risk Assessment
S&MA	Safety and Mission Assurance
SCA	Shuttle Carrier Aircraft
SEO	Systems Engineering Office
SPA	Systems Planning and Analysis
SRB	Solid Rocket Booster
SRM	Solid Rocket Motor
SSME	Space Shuttle Main Engine
V&V	Verification and Validation
WIRE	Wide Field Infrared Explorer

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		24 of 58	

## Appendix A. The Role of Testing

Testing is often the most reliable and costly method of V&V. Unless there is an extensive and available body of knowledge about the new vehicle operating in its operational environment, testing is often the only way to generate the knowledge needed to buy down risk to an acceptable level. The importance of validating the models and analysis cannot be stressed highly enough. A common thread throughout testing and this discussion is the need to validate the models and analysis, both those used for design and those used for verification. In order to understand the uncertainty and for the risk to be accepted, sufficient test measurements are needed to verify the environment and confirm the analysis. Models, especially complex models, are often not linear and if linear, can include multiple interactions. Therefore attempting to validate a model utilizing a single measurement is not likely to be possible. The number of measurements will depend on the complexity, size of the system envelope, and the model uncertainty.

Testing demonstrates that the system, hardware, software, and interactions operate safely and as expected. Testing builds on each previous test to generate the body of knowledge necessary to determine when it is acceptable to fly a crew for the first time. Testing progresses from ground test to uncrewed flight test and finally to crewed flight tests (see Figure A.1-1).



**Figure A.1-1. Progression of Testing to Build Up Evidence for Safe System Operation**

Determining what tests must be done to ensure that safety-critical items are fully understood is a judgment call. Such a determination is based on model and analysis fidelity and credibility, as well as system complexity, technology maturity, heritage systems, design margins, and previous

	<b>NASA Engineering and Safety Center</b> <b>Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		25 of 58	

experience. Important factors to be taken into account when designing a test program include an understanding of the test environments and their limitations, what system interfaces and interactions are critical to safety, the weak points in the analysis and modeling, and how much data are needed to reasonably verify the system. Repeatability (the ability to demonstrate that the vehicle operates the same way more than once) is another important aspect of a test program. The severe thrust oscillations (often referred to as pogo) during the Apollo Program illustrate how results can be different for the same test. The first Saturn V launch vehicle carrying the uncrewed Apollo 4 spacecraft was thought to have performed nearly flawlessly. The second uncrewed Saturn V unexpectedly experienced pogo greater in amplitude than that tolerated for Mercury or allowed for crew exposure during Gemini.

The definition of the instrumentation and data to be collected from ground and flight testing is critical to reducing the uncertainty of the model. Matching the instrumentation to the models and analysis is essential to validate both model and analysis. While many systems can be mostly validated on the ground, few can be fully validated until flight. Some systems such as propulsion, structures, vibration, and acoustics cannot be fully validated by ground tests, so flight testing is essential. Determining what systems can only be validated through flight testing and concentrating attention and instrumentation on those elements for the test flights are essential.

### **Ground Test**

Ground testing of hardware/systems is necessary before any flight test. Ground tests are the primary method for ensuring that the models and analyses are valid, and the systems meet the requirements and operate safely and as desired. During the developmental cycle, ground tests are necessary to understanding and trading the core technology that will be used in the new vehicle. Typical tests include material properties, avionics architecture, structural strength, propulsion systems performance, thermal protection system concepts, aerodynamics, and many others. The next set of needed ground tests are used to verify that the design meets the requirements and to validate analysis and models. The discipline/component ground tests demonstrate lower-level requirements and, when combined with integrated tests and the other component/discipline tests, help validate the system. The first time many flight interfaces and interactions are demonstrated and verified is in integrated system tests. Therefore the analysis has, at best, limited ability to predict what the interactions will be. Integrated systems tests start at the subsystem level and progress to system-level tests on the vehicle. The requirements are verified and a critical evaluation is made of the subsystem operation. During the integrated testing, it is essential to test at the edges of the performance envelope. In structures this may involve testing at higher load conditions or inducing loads through unexpected paths. Often a full structural test will discover that the load paths are different than expected. The same is true for avionics, propulsion, and other subsystems.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 26 of 58	

The majority of the integrated testing generally requires complex test environments. Understanding the differences and capabilities of the test system is important for understanding the test results, especially when evaluating whether the system is operating as expected. Integrated systems testing for many systems (avionics, power, propulsion feed and cooling, environmental control and life support, and active/passive thermal control) requires a high-fidelity simulation to produce realistic data for the systems under test. All items that can be tested on the ground should be, including the integration testing of major elements. The behaviors of the integrated major elements are difficult, if not impossible to predict and often adversely affect safety. As with all complex systems, the vehicle's behavior and reactions may change over time based on interactions with the environment and between elements—often with unintended consequences. Many of these behaviors will require design and/or implementation changes. As a consequence, integrating the essential elements, especially those that are related to safety, reduces the uncertainty and subsequently the risk. As a rule, it is difficult if not impossible to fully test an integrated system on the full-up vehicle. Therefore, care should be taken to assess the impact on safety when integrated element testing is moved to the vehicle. It is critical to ensure that the fidelity of the test set-ups is at the level needed to understand the vulnerabilities of the systems.

Prior to any flight test, a set of integration tests must be performed on the vehicle to ensure that the vehicle matches the systems tested on the ground and the analysis result. These tests encompass ground assets as well as the flight vehicle. Subsets of those tests run on the ground are often used, as well as additional tests that can only be performed on the vehicle. Environmental qualification testing, another major part of ground testing, takes flight or preflight components, sub-systems, and systems and exercises them in an environment as similar to the actual flight environment as can be created on the ground. Typically, components are qualified separately and, depending on the maturity, validity of the analysis, and heritage of the component, the environmental testing will be extended to the system. It is important to understand the differences between the test and the flight environments. The tests should be testing the system at the extremes as well as in the “nominal” operating range. Typically environmental qualification tests include loads, thermal, pressure (internal and external), electromagnetic interface/electromagnetic control, vibration, and

*Multi-Element Integrated Tests (MEIT) were performed on International Space Station (ISS) elements during ground processing at Kennedy Space Center (KSC). MEIT was conducted to validate the operation of flight elements and associated systems in an environment that was as flight-like as possible—where practical, actual flight connections, flight hardware components, and flight software were used. If available, actual on-orbit operators (astronauts), ground controllers, and on-orbit procedures were also used. MEIT found problems such as an electrical component under-voltage condition that would have prevented start up of an element; an activation sequence that was nearly twenty times longer than specified; requirements that would have led to thermal loading and a loss of an element; and swapped video signals that would have required an additional extravehicular activity (EVA) which would have increased risk to the crew. MEIT found several significant issues that were corrected prior to launch, whereas resolution of those problems on orbit would have been more difficult or impossible to accomplish.*

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 27 of 58	

acoustics. Qualification testing and analyses should verify the design for all of the expected environments, performances, and life (cycle, shelf, and operating times) of each level of hardware (part, component, subsystem, and system). Acceptance testing should screen for workmanship, all testable failure modes, and performances at each level of hardware. The acceptance test should ensure that each following hardware copy was manufactured, processed, and assembled as the qualification test hardware.

### Uncrewed Flight Test

While knowledge of the vehicle and its systems is increased through ground testing, it is still necessary to further understand the uncertainty for the safety-critical elements. The main goal of most uncrewed flight tests is to verify those elements that can only be verified in the flight environment and to validate the full system. It is not possible for ground tests to fully match the flight environment, nor can all the system interactions and interfaces be fully tested on the ground. The induced environments are one set of environments that cannot be matched on the ground. Determining which systems can only be validated through flight tests and concentrating attention and instrumentation on those elements for the flight tests is essential. Capturing emergent behavior of the system prior to a crewed flight is another goal of the uncrewed flight test. Defining test conditions and instrumentation to capture the behavior of the system is critical.

Uncrewed flight tests can be conducted during any of the program phases: design and development, qualification and acceptance, and integration. Typically, the uncrewed flight tests performed during design and development are technology-feasibility tests, model, analysis, and process validation, and risk-reduction tests. During the development phase, an uncrewed flight test is added to verify and validate changes whose risk is considered too high for a crewed flight. Uncrewed flight tests have unique challenges. Without onboard observers, the only way to gain knowledge of how the system operated and identify any stress points is through data collected from extensive instrumentation systems. The definition of the instrumentation and data to be collected is

*The NASA Launch Services Program launches unmanned vehicles with high-value, one-of-a-kind payloads. Based upon desired risk levels and classes of payloads, NPD 8610.7D requires a minimum number of successful launch vehicle flights before a payload can be flown.*

critical to reducing the uncertainty and must be carefully chosen to ensure that the areas of uncertainty and those areas vital to model validation are adequately addressed. Flight and ground tests must have similar instrumentation and in the same locations, as much as reasonable, to be able to compare data and enable the flight test to validate the ground test and the analysis. Having enough instrumentation to define the system performance is a necessary and difficult task. There is always the push for more instrumentation against the limits of mass, time, and money. The impact of the added instrumentation on the test environment must be understood (i.e., wiring through insulation is a heat transfer path). Uncrewed testing covers all portions of the system, including the launch vehicle, spacecraft, and ground/mission operations. Special attention to a launch-abort system, when launch is part of the mission, is also essential prior to

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 28 of 58	

the first crewed flight. Because it is a “last chance” escape, additional ground and uncrewed flight testing will be necessary. Understanding the envelope and capability of the system through well-validated models and analysis is essential. Since a launch-abort system is complex and there are many unique interactions and interfaces with the launch system, a substantial portion of the validation needs to be done with flight testing.

### **Crewed Flight Test**

Validation testing may continue on crewed flights when the benefit of the crewed flight is greater than the residual risk. There will be systems that cannot be fully validated without a crew and there may be elements of the testing that can be safely delayed, if necessary. The introduction of a crew adds another set of interfaces and interactions that potentially change the performance of the system, often in unexpected ways. These flights, as with the uncrewed flights, will be used to gather important test data to verify and validate the vehicle and its systems. The test flights will also be used to gather data necessary to further validate the analysis and models. As the flight program progresses, the analyses and models will be relied on to plan future flights and assist in resolving any anomalies or understanding emergent behavior. While instrumentation may be reduced for crewed flight tests, it cannot be eliminated. Ensuring that sufficient data is gathered to continue validation of the system started during ground testing is essential.

Prior to a crewed flight, the system must be determined to be at an acceptable risk level. It is at this point that an understanding of the differences in ground and uncrewed flight environments is critical. All items required for safe flight should be tested prior to flight to provide sufficient safety margin to allow for unexpected events. Even those items that are not directly related to safety must be evaluated before flight to ensure they do not cause degradation in crew safety.

The mission of the crewed flight test must be clearly defined and well understood to increase safety and reduce risk. Each flight mission should be limited to essentials and, as much as practical, incremental missions utilized to clear the vehicle for its full operational mission. The first crewed flight should not try to clear the system as fully operational for all its missions. At the same time, the crew should be focused on only those objectives essential to safely completing the mission.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		29 of 58	

## Appendix B. Techniques for Risk Identification

The details of NPR 8705.2 (*Human Rating Requirements Document*) and other NASA Standards such as 8715.3 (*Safety and Mission Assurance Plan*) and 8000.4 (*Risk Management Plan*) provide guidance in risk management. It is essential to have the proactive mindset needed to assess what could go wrong, whether in the design phase (including model development and validation), testing phase, or operational phase. The purpose of the documentation on risk management is to be more than just a “checklist” to determine that all risks are eliminated. Importantly, the purpose is to help focus that proactive mindset in such a way that things do not ‘slip through the cracks.’ It is vitally important to maintain a balance between the ‘process’ and maintain an awareness of what the process is trying to help the team accomplish, namely, to ensure thorough risk identification and preclude either eliminating or reducing attention to items that could result in an undesirable outcome.

Over the years, several techniques for identifying risk have been developed. Because a single strategy that works in every situation has not been identified, multiple paths are pursued in parallel in an attempt to maximize the opportunity to identify risks at the earliest time.

Risk identification (and assessment) can be approached from a number of different perspectives. For instance, either a bottom-up or top-down perspective could be used. It is important to choose complementary approaches to achieve a more complete understanding of the risks. Top-down and bottom-up approaches each have their advantages and disadvantages. The biggest disadvantage of a top-down perspective is that the person doing the assessment may not have a sufficiently detailed knowledge of the systems. However, the top-down approach allows ‘out of the box’ ideas and perspectives that a person submerged in the details of the system may not have. One of the bottom-up approach’s biggest drawbacks is the lack of a wider perspective, which can miss critical interactions across subsystems. The strength of a bottom-up approach is that perspective is based on a solid knowledge of the details of the system which may not be evident to an outside reviewer. It is for these reasons that a variety of approaches and perspectives should be implemented.

The following information addresses some of the pros, cons, and comments for some of the more popular risk identification techniques.

**Simplify what must be assessed.** There are things that **MUST** work. So, what are they and what can go wrong? The objective of this mission is (fill in the blank), and what **MUST** happen to achieve that objective? Where can these few critical things go wrong and then how can I prevent those things from going wrong? This mindset can also be used to simplify the mission objectives and what has to be certified before flying a crew for the first time (see Figure 4.4.1).

**Design reviews.** In addition to a program representative, these reviews should include the engineering and S&MA community and representatives of the manufacturing, assembly, test and checkout, and operations teams. Independent reviewers should also be included. It is imperative

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		30 of 58	

that designs be fully integrated across systems and interfaces in order to achieve the desired level of confidence in risk identification.

**Failure modes and effects analysis (FMEA).** The FMEA was developed as a methodical way to examine each component to determine its failure modes and corresponding signatures and implications. This is a valuable technique but relies on judgment and can be labor intensive. This is a bottom-up approach.

**Fish bone diagrams.** These have proven to be extremely powerful tools, especially in conducting accident investigations. This technique starts with a symptom (e.g., an engine ignition failed). The analysis works backward to identify every step in the functional sequence that might cause such an outcome. It has helped find relationships that were overlooked during the FMEA process, but it can be labor intensive. An ideal approach would be to perform both FMEA and fish bone analyses on critical functional paths. This is a top-down approach.

**Mission simulations.** Simulations have been used for decades to prepare operational teams and validate mission rules. Their effectiveness is contingent on having the simulation supervisors aggressively search for unusual combinations of actions and events that would challenge the team's knowledge. The cost of such high-fidelity simulations has been reduced over time and provides a powerful technique for identifying unrecognized interactions. If such capabilities can be implemented in the early design stage, such simulations will help identify problems early and improve the utility of the operational inputs to the design team. In general, mission simulations are a bottom-up approach implemented by the operations community (fail a subsystem component and see how it affects overall operations), but can also be a powerful top-down approach to assess system interactions and dependencies (a lack of cooling requires powering down, but critical operations require staying powered up).

**Configuration management.** Most human spaceflight programs involve many people and organizations dispersed across the country. This decentralized approach can make the programs more vulnerable to miscommunication, oversights, and omissions. The importance of configuration management (control what is supposed to be there), configuration accounting (awareness of what IS there), materials and parts traceability, and the ability to ensure everyone is using the same data sets cannot be overemphasized as a front line risk reduction activity. In general this is a bottom-up approach.

**Checklists and surveys.** Checklists and surveys are probably the most common form of risk identification. They are used to systematically search and identify as many exposures, perils, and hazards as possible. Many people like them because they are standardized, they can be used by non-risk management personnel with minimal training, information can be easily categorized, and they can be used to create a history. On the down side, they cannot cover all areas or operations and provide limited, if any, financial impact effect. They also do not prioritize the risk exposures that they identify and may not identify new exposures. This is usually considered to be a top-down approach.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		<b>Readiness for First Crewed Flight</b>	
		Page #: 31 of 58	

**Policy and procedure reviews.** These are used to identify how an organization functions. They can be done either internally or externally or both. While there is an opportunity to identify exposures, organizational politics may prevent this from being effective. This is usually considered a top-down approach.

**Contract reviews.** This is a broad category and often there is the misconception that because an attorney or contract specialist wrote or blessed it, it is acceptable. Contract review includes a wide variety of material, including but not limited to: leases, hold harmless and indemnification agreements, purchase orders and sales contracts, bills of lading, warranties, advertising materials, employment contracts, service contracts, and insurance certificates. If a full contract review has not been conducted (regardless of the size of the program), it is safe to say there is unidentified (passive) risk in that program.

**Experts.** Experts bring additional technical depth, experience, and perspective to the risk identification process that may not exist internally. It may be difficult to find qualified experts in some disciplines and they could be expensive.

**Common-risk checking.** In most systems disciplines, lists of known risks unique to that type of system are available. Each risk on the list can be checked for application to a particular situation. Depending on the level of technical detail, this can be either top down or bottom up, but since it employs a generic type of approach, it is usually considered a top-down strategy.

**Event-based risk identification.** This refers to events that, when triggered, cause problems. Hence, risk identification can also start with the source of problems or with the problem itself. The chosen method of identifying risks may depend on culture, industry practice, and compliance to requirements. The identification methods are formed by templates or the development of templates for identifying the source, problem, or event. Three common perspectives of event-based risk identification are:

**Objectives-based risk identification.** Organizations and programs teams have objectives. Any event that may endanger partly or completely achieving an objective is identified as a risk.

**Scenario-based risk identification.** In scenario analysis, a functional decomposition is performed to identify and list each step required to be performed to achieve an objective or perform a task (similar to a fishbone diagram). However, then different scenarios that illustrate potential issues that may arise in performing that step are explicitly listed (e.g., a message must be received and acted upon. Scenarios are that the message was garbled, or not received, or not understood, etc.). The scenarios may be the alternative ways to achieve an objective or step, or an analysis of the interaction of systems that causes an issue. Any event or scenario that triggers a subsequent undesired scenario alternative is identified as a risk.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 32 of 58	

**Taxonomy-based risk identification.** The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks [CMU/SEI-93-TR-6 *Taxonomy-based risk identification in software industry* <http://www.sei.cmu.edu/library/abstracts/reports/93tr006.cfm>].

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		33 of 58	

## Appendix C. Discussion of Risk Contributors

There are many different sources of technical risk to a system—some are known and understood and many are not. These unknown risks are often referred to as epistemic or systemic uncertainties. Some of the most important sources of uncertainty include: variability in the processes (materials, manufacturing, measurements, etc.), complexity of the system, maturity of the hardware/software, reuse of hardware/software, and emergent behavior or unintended interactions. These factors are recognized and understood by the decision makers but may not be consciously considered during the decision-making process. In order to achieve the best possible results, decision makers should think through each of the sources of uncertainty before making a final decision.

Typically, concerns with variability, complexity, and maturity are addressed upfront in the design phase through conservative margins and requirements. For example, structural engineers may apply knock-down factors or electrical engineers will ensure larger power margins. This can accommodate some of the uncertainty. As development progresses, extensive testing at each stage will also help to identify any weaknesses or unexpected interactions. Testing of systems is more than just verifying requirements, it is also essential for understanding the true operation and limitations of a system. This is also addressed in Appendix A.

Most managers and decision makers recognize that new designs, technology, and interfaces create additional uncertainty, while previous testing increases confidence for the program. However, reuse of existing components in new applications may increase uncertainty. Decision makers may assume that reuse of a component of hardware or software will reduce the uncertainty level of the system. Unfortunately this is often not the case. The new application and new interfaces may in fact increase the uncertainty, unless enough time and effort are invested in a thorough review and analysis of the particular application. One example of the perils of software reuse without a thorough understanding of the implications was experienced by NASA's Mars Climate Orbiter (MCO). The MCO reused software code originally developed for another spacecraft for the thruster trajectory equation. The conversion code was in British units but the specification called for metric. The code was obscure and the specification was not well understood or reviewed with the reuse application. The subsequent mismatch of units resulted in the loss of the MCO.

An example that specifically relates to heritage hardware in a different application is Landsat 7. The instrument on Landsat 7 was the Enhanced Thematic Mapper Plus, which had many heritage components and a few new ones. One of the heritage components was the main power supply box which converted the spacecraft 28-V direct current power into the secondary voltages required for the instrument electronics systems. The power supply had an input filter that had fairly large inductors and capacitors and therefore large complex impedance. This was not an issue for previous Landsats that used this power supply design because these spacecraft had unregulated 28-V power supply buses. However, Landsat 7 had a regulated bus and when the instrument was powered, the bus would ring due to the large complex impedance at the

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 34 of 58	

instrument power supply input. The least expensive way to fix this problem at that point in the program was to develop and integrate a damping circuit in a separate box on the spacecraft.

These examples demonstrate a possible downside of reuse: decision makers may be lulled into a false sense of security due to successes in the past. Sometimes such reductions may be the appropriate action but a thorough review and analysis must take place first. Appropriate decision making must take into account that similar components will not necessarily behave identically.

The process of identifying emergent properties and unintended operations of human-rated spacecraft must begin at an early stage in the development process to ensure that as many issues as possible are recognized and addressed. Analytical methods can be applied to early systems to find and correct possible interactions before the design is complete. Analysis alone will not identify all unexpected emergent behaviors; testing is necessary to ensure that those interactions that do present themselves will not create an unsafe situation for the spacecraft or crew.

An example of this kind of unexpected behavior occurred during the Wide-Field Infrared Explorer (WIRE) experiment launch in March 1999. After the launch, a system anomaly occurred in which the telescope aperture cover was opened prematurely, resulting in the release of the spacecraft's cryogenic hydrogen. The subsequent report on the incident traces the behavior to a field-programmable gate array (FPGA) that was used in a circuit for which it was not well suited. The mishap investigation determined that a transient signal occurred after start up of the FPGA. The WIRE report indicated that the testing method used for the spacecraft was performed at the hardware-box level only, a method that would not have identified the transient. The report also stressed that the spacecraft should have been tested in its flight configuration to identify these types of behaviors.

Most engineers and managers recognize unexpected emergent behavior as a source of uncertainty in the system's operation yet few are able to describe a standard process for driving out such behavior. Most system and test engineers suggest additional testing in off-nominal and maximum-use conditions as a means of discovering unexpected behavior. Consciously addressing any potential unexpected emergent properties is important and the test program should be designed to uncover as much of this behavior as possible.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		35 of 58	

## Appendix D. Evaluation of Risk Analysis Tools

Just as a proactive mindset is important for the risk identification process, so is an awareness of analysis tool limitations and personal accountability and responsibility for the outputs of ‘accepted’ analysis tools. Any tool will give an incorrect answer if fed incomplete or inaccurate inputs, so any tool used must be given input based on real data whenever possible. Assumptions should only be used when clearly understood and accepted rationale exists for using them. One must always apply a common-sense litmus test to any result. This can be difficult because good judgment often comes from experience, but valuable experience often includes remembering the results of poor judgment. In addition, one must always remember that statistical results can be manipulated to tell any story, especially if someone is trying to justify an answer.

The following information addresses a number of different tools that can be powerful aids for making informed decisions about risk.

**System Modeling and Analysis.** This includes a broad variety of methods, including:

- Solid physical and computer-aided design (CAD)-based models of hardware
- Concept and flow evaluation tools such as network and event sequence diagrams
- Models describing physical processes such as stress models or flow dynamics models
- Probabilistic models that build on many of these tools by quantifying uncertainty

Techniques of varying effectiveness are available to model at almost any complexity level, from stresses on small regions of a single bolt hole through complex environmental effects on highly complex structures. Perhaps the most important strength of system modeling lies in the development of the models: the mere effort of putting the model together will reveal risk contributors, consequences, and mitigations during early design stages when changes are relatively inexpensive. Problems of modeling often stem from the fact that they are models, not the actual physical system or process. Assumptions, simplifications, design changes, interactions with unmodeled factors, and misunderstanding of the system can be significant, unquantified risk contributors.

NASA-STD-7009 (*Standard for Models and Simulations*) is a valuable reference that can help analysts design, use, and communicate results from many types of computer-based models. While adherence to this standard does not guarantee avoidance of the problems mentioned above, it can be effective in addressing problems, especially when used with other risk analysis methods. Other excellent tools can be drawn from other disciplines, such as systems engineering, operations research, human factors engineering, reliability, maintainability, and quality engineering.

Two important types of probabilistic modeling tools are Monte Carlo (MC) simulation and probabilistic risk assessment (PRA).

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP- 10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		36 of 58	

**Monte Carlo (MC) Simulation.** This technique gains its name from the city famous for its games of chance. Initially, a system model is constructed. Instead of deterministic inputs (simple point estimates, means, medians, allowables, etc.), important variable or uncertain inputs are modeled by probability distributions intended to explicitly reflect the variability or uncertainty of each of these inputs. The model is run (exercised) a number of times (trials). Each trial uses a different set of input values, chosen randomly from each input's assigned probability distribution. The output, then, is itself a distribution of values rather than a single number. If the model and inputs sufficiently reflect reality, the distribution from exercising the MC model will be the same as one would expect from operating actual hardware. For example, a drive to work might be modeled using an event sequence diagram. The model can then be perturbed by varying the speed of traffic, number of red lights, etc., according to appropriate probability distributions. Running the model a number of times using different traffic speeds weighted by how likely they are to occur will give an idea of not only how long it takes to make the drive, but also the range of drive times that might be expected.

Strengths of MC analyses include generally greatly reduced cost over physical testing and improved risk quantification due to gaining estimates of not only means, but also variability in responses and insight into drivers of variability of output (sensitivity analysis). Experienced practitioners can construct useful models early in the design process, even with extremely limited data. MC models are particularly useful in modeling stochastic processes, when there is a time component in the process or variability. Potential weaknesses need to be recognized and include unmodeled contributors to risk, sensitivity to incorrect assumptions and to probability distributions used, plus the significant resources and time that can be needed to assemble and exercise models of complex structures, physics, and processes.

**Probabilistic Risk Assessment (PRA).** A PRA is a structured analysis that presents a set of scenarios, frequencies, and associated consequences. A scenario contains an initiating event and one or more pivotal events leading to an end state, generally an undesired consequence such as loss of mission or loss of crew. The initiating event is typically an energetic event, failure, or other perturbation that requires response from one or more systems, or operators, (e.g., an explosion of a hydrogen tank). Pivotal events generally include failures of these responses, which enable the end state to occur when the initiating event occurs; an example might be the puncture of an oxygen tank due to debris from the initiating event at the hydrogen tank.

The logic of possible scenarios leading from the initiating event is shown using event trees or fault trees. Scenarios are classified into end states according to the kind and severity of consequences. Physics-based models are used for phenomena and dynamic events. The probabilities of the initiating event and the pivotal events are estimated—along with their uncertainties—to obtain the probability and associated uncertainty for the scenario. The scenario probabilities are then combined to obtain the total probabilities and associated uncertainties for the end states.

The technique is generally used for highly complex systems; however, smaller-scale applications can be carried out using simpler models. PRA on a highly complex system can be time- and

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		37 of 58	

resource-intensive, thus expensive; however, it can be more efficient than many other methods for modeling highly complex systems, particularly early in the design process when uncertainties are greater. The results of the tool will be no better than the accuracy of the input data and assumptions. For systems early in their design phase, extra care must be taken when assessing the inputs to the tool for their validity and applicability

A method known as Bayesian updating is often used in PRA analysis. This mathematical technique is a quantitative formalization of techniques used in engineering judgment. Bayesian updating is used to reconcile conflicts in data sources and explicitly quantify uncertainties related to the lack of credibility, strength, and/or similarity of sources in the analysis results.

The models and inputs can be drawn from many sources, including raw physics, test and historical data, experience from similar systems, and/or expert opinion. For models that reflect high complexity there is often a dearth of directly applicable data, low design maturity of the modeled system, and uncertainties about physics and other issues. In those instances, uncertainty analysis is an important part of the PRA and a healthy skepticism is needed when assessing the validity of the assumptions and data feeding into the model.

This leads to both its most important strengths and weakness. A PRA includes significant sources of uncertainty stemming from possibly more assumptions than are used in other modeling techniques. Assembling highly complex models using large numbers of assumptions, including uncertain inputs and quantification of their ‘goodness,’ is bound to cause disagreement. Disagreements between experts on assumptions and inputs can also be significant. However, explicit evaluations of the risk impacts of the uncertainties and disagreements can be made via uncertainty and sensitivity analyses. This is an important feature of a PRA.

For applications involving complex systems and new design, it is most likely true that PRA results do not exactly reflect accurate ‘absolute’ risk values because of the sheer complexity and uncertainties. In addition, the time needed to construct a PRA can mean the analysis lags design, so the ‘current’ design’s actual risk status can be different than the tool’s results. This said, PRA can be tremendously useful, especially as a comparative risk assessment tool for these particular applications. A well-constructed PRA can provide key information on:

- Quantification of uncertainty levels on risk estimates (example: 5<sup>th</sup>, mean, and 95<sup>th</sup> percentile estimates)
- Quantitative assessment of system risk contributors and measures of risk and reliability effects in trades between different system designs
- Sensitivities to problems, environments, stressors, age, etc.
- Quantitative importance and rank orders of contributors to risk
- Identification and relative importance of knowledge gaps for prioritization of test and design choices

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 38 of 58	

PRAs can also be tremendously useful for organizing thinking and suggesting priorities in the case of actual system problems, especially when the system is complex. A good starting resource on PRA containing further references is *PRA Procedures Guide for Managers and Practitioners*, currently in version 1.1 (NASA Office of S&MA, March 2002).

**Demonstrated Reliability Estimate and Associated Confidence.** A quick, useful, often misused, and frequently misunderstood summary quantitative method is the demonstrated reliability estimate. It would seem to make sense that if there have been 100 flights and no failures, then that program must have demonstrated high reliability. But there are important misconceptions in that short statement. First, a firm definition of ‘high reliability’ must be developed from the program’s acceptable risk posture *a priori*. For this example, suppose an acceptable mission failure rate of 1/200 was stated in the program’s risk-planning documents. Second, it must be remembered that each mission is a *sample* from a population of all possible missions. As such, the current collection of 100 missions is a collection of samples that *estimates* the failure rate in the population of all missions. It is quite possible to achieve 100 missions without a failure given a population failure rate of 1 in 70; in fact, the program could expect to get this result about ¼ of the time. Obviously, optimism regarding proof of acceptable risk is unwarranted.

Because the set of successful flights can only be used to obtain an estimate of the true risk, a required confidence level must be decided upon *a priori* and published along with the program’s acceptable risk document to bound the limit of acceptable estimation error on the value. The concept of statistical confidence will not be covered here. As a rule-of-thumb, a value between 70 and 95 percent confidence is recommended (closer to 95 percent for easy-to-estimate or high-risk values; the closer to 70 percent, the more derating by use of larger safety factors is necessary). Many specialized statistics software tools are available to calculate demonstrated reliability. An excellent and free tool for calculating not only true demonstrated reliability values but also sample sizes required to prove a reliability risk given a desired confidence level is Gary Pryor’s *Reliability Test Planner*<sup>3</sup>.

---

<sup>3</sup> Available at [www.midmozark.com/rtp.html](http://www.midmozark.com/rtp.html). A tutorial is available through NASA’s NESC Engineering Statistics Team (NEST) by contacting the NESC at [www.nesc.nasa.gov](http://www.nesc.nasa.gov).

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		39 of 58	

## Appendix E. Historical Perspective on First Crewed Flights

The purpose of this appendix is to provide a general discussion of the steps leading to the first human flights of all NASA crewed launch systems from Mercury through the Space Shuttle. The material in this appendix was synthesized from a survey of readily available public documents (listed in Appendix G) and personal experiences related to:

- Preparing for the first crewed flights of the Space Shuttle, Apollo spacecraft, and Saturn launch vehicles
- Working with those responsible for developing and flying Mercury and Gemini
- Developing and committing one-of-a-kind robotic systems to flight
- Executing experimental and developmental flight tests of aircraft and rockets

Team members used personal experience along with information published in applicable NASA special publications (SP) to infer the basis for management confidence in committing crews to flight during the Mercury, Gemini, Apollo, and Space Shuttle Programs. The material contained in this appendix reflects these observations but should not be taken as total evidence of the actual thought processes and logic that were used in making these historic decisions. Nevertheless, the team believes that the observations in this appendix are consistent with history and warrant consideration in planning for initial crewed missions for future human-rated systems.

A space launch/transportation system for the purposes of this discussion includes the launch vehicle, spacecraft, and components required to return humans safely to Earth from any point in a low Earth orbit (LEO) mission. The scope of this overview is limited to identifying the basis for confidence in the ability to execute functions that must be performed in order to send humans into space and return them to Earth with reasonable assurance.

### Early Human Spaceflight Programs

The three early human spaceflight programs (Mercury, Gemini, and Apollo) are reviewed as a single series of missions. While the mission and vehicle designs for each program were different, the management processes and technical approaches were very similar. This similarity likely reflects the fact that the same core government teams that led development of the Mercury spacecraft and Redstone launch vehicle also led development of Saturn, Gemini, and Apollo. In addition, following Mercury, each program leveraged the design and data from the previous program. The development and preparation for human flight was guided by experience gained along the way. Ultimately all three programs were focused on the same eventual Apollo goal of landing men on the Moon and returning them safely to Earth.

The “man in space” Program was introduced just 6 days after NASA was formed on October 1, 1958. The Program was renamed Project Mercury on November 26, 1958. Project Mercury involved three distinct systems: the Mercury spacecraft (capsule), the launch vehicles (Redstone and Atlas), and the launch escape system. The Mercury spacecraft (capsule) was a

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 40 of 58	

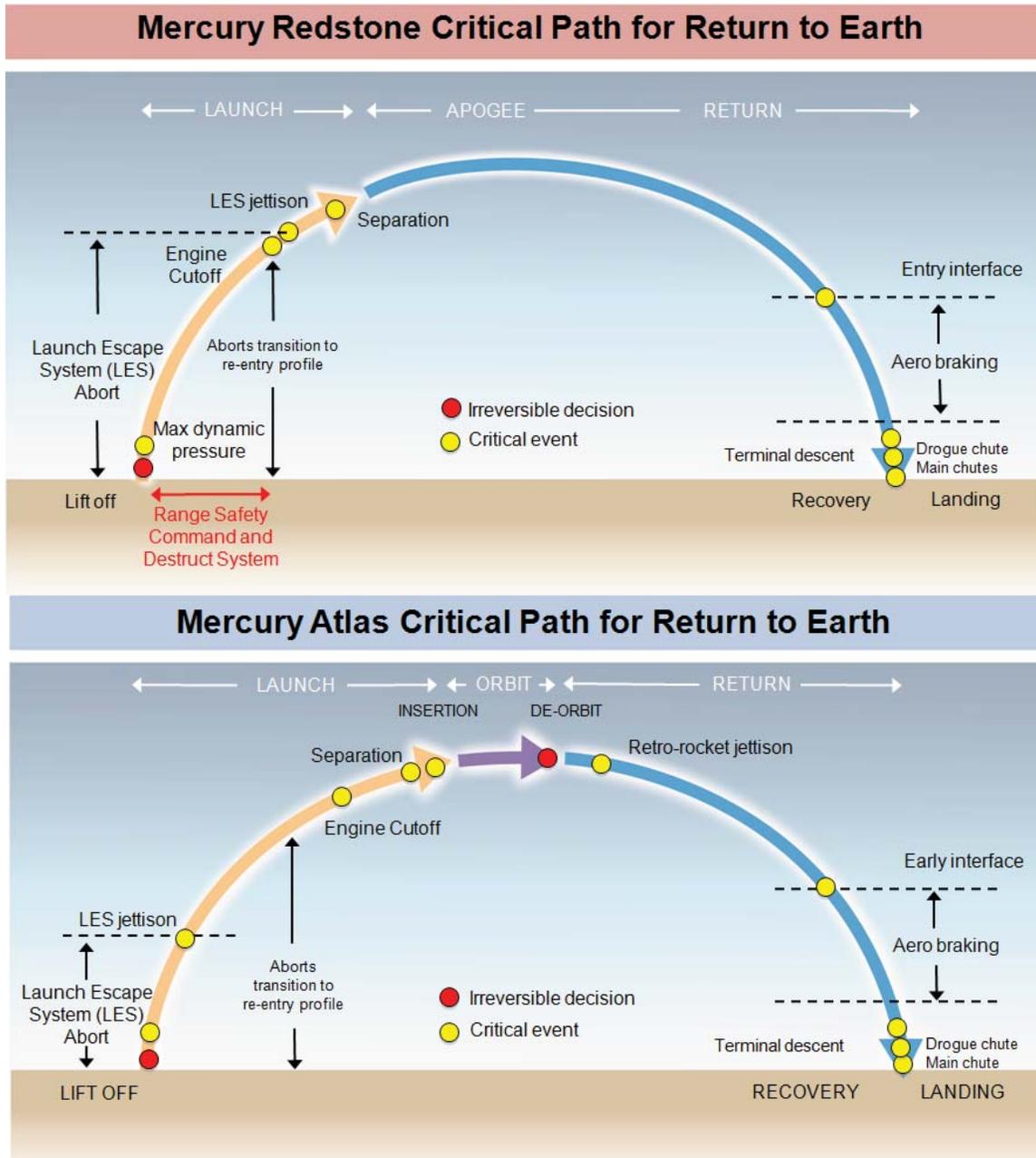
cone-shaped, one-man capsule with a cylinder mounted on top. It was 2 m (6 ft, 10 in) long and 1.9 m (6 ft, 2.5 in) in diameter. A 5.8-m (19-ft, 2-in) escape tower was fastened to the cylinder of the capsule. Project Mercury's design philosophy was based on practicality and relatively simple requirements. Basic guidelines and criteria were established and observed in the design and development of the Mercury spacecraft and further extended to the modification and accommodation of the two Mercury launch vehicles, the Redstone and Atlas. The Mercury Redstone (MR) and Mercury Atlas (MA) critical paths for a safe return to Earth are shown in Figure E-1.1.



Title:

**Readiness for First Crewed Flight**

Page #:  
 41 of 58



**Figure E.1-1. Mercury Redstone and Atlas Critical Path for Return to Earth**

With critical functions identified and a development strategy defined, the program prepared a flight test sequence that would validate all critical functions required for each manned mission at the earliest time. The first missions collected data needed to complete spacecraft and launch escape system (LES) designs. Boilerplate spacecraft were used to show that each launch vehicle was compatible with the spacecraft. Finally a series of envelope expansion flights was made

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		42 of 58	

with “production” spacecraft. A series of 18 uncrewed test flights of the Mercury spacecraft was conducted on various launch vehicles (Little Joe, Big Joe, Mercury, Atlas) to check out the performance of critical spacecraft systems. A primate named Ham was launched on Mercury Redstone 2 (MR-2) on January 31, 1961, prior to flying humans for the first time on May 5, 1961.

It should be noted that the Mercury launch vehicle development heavily leveraged previous systems and testing by the Army Ballistic Missile Agency. Mercury used classic flight envelope expansion techniques to demonstrate human compatibility with launch and entry environments before evaluating human utility in orbit. The build-up sequence began with qualifying Redstone for suborbital flight with the Mercury spacecraft, demonstrated compatibility with a primate, and concluded with crewed missions. The Atlas launch vehicle was qualified for orbital flight in parallel with the Redstone missions and then used a primate to validate the life support systems and compatibility with increased time in zero gravity. Human compatibility and utility were evaluated by a series of flights with increasing time in zero gravity. Qualification of the launch escape system and procedures for launch, flight operations, and recovery were pre-requisites for all human missions. Satisfactory completion of the flight-test sequence, hardware qualification, and validation of critical function fault tolerance was expected to provide sufficient evidence of readiness for first crewed flight.

Following the successful test of MR-2, consideration was given to launching a human on a suborbital trajectory on the next Mercury-Redstone launch. Dr. Wernher von Braun met with his leadership team at MSFC to develop a recommendation on how to proceed. The team, with one exception, was prepared to fly a human on the next launch. Typically, Dr. von Braun attempted to arrive at team consensus, but frequently decisions were made without unanimous agreement among the team members. The lone dissenter in this meeting believed that it would be wise to fly one more test that, if nearly perfect, would provide confidence to man the next flight. Dr. von Braun decided that the historical nature of launching the first American into space, dictated that his team agree unanimously on the recommendation. As a result, one additional flight test (MR-BD) with a boilerplate spacecraft was flown on March 24, 1961. The flight was fully successful. On May 5, 1961, a Redstone rocket launched astronaut Alan Shepard into space in a Mercury spacecraft designated Freedom 7. Just 15 days later, on May 20, 1961, President Kennedy announced the Apollo Program to a joint session of the U.S. Congress.

Because it was the first U.S. human spaceflight program, the first crewed flight decision for Mercury was arguably the most difficult—with the most unknowns. The man-rating program for the Redstone, Atlas, and Titan launch vehicles was characterized as follows: “The total man-rating program fell into the general categories of minimum redesign, an extensive quality program, the development of an abort sensing and implementation system, and a program discipline which insisted through meticulous attention to detail that we not fly when there were

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 43 of 58	

any unanswered problems concerning the status of any of the hardware.”<sup>4</sup> Only those changes necessary to adapt the vehicle to the requirements of the mission and those necessary for the improvement of safety were authorized.

Gemini was the next human spacecraft after Mercury. The spacecraft was an enlargement of the familiar Mercury capsule—5.8 m (19 ft) long, 3 m (10 ft) in diameter, and weighing about 3,810 kg (8,400 lb). Engineering changes simplified maintenance and made it more maneuverable for the pilots. The Titan II rocket, more powerful than the Redstone or Atlas rockets, placed the larger spacecraft into orbit. Sometimes referred to as Gemini-Titan for the craft and its launch vehicle, each flight was designated by a Roman numeral. The Gemini spacecraft had approximately 50 percent more volume than the Mercury for twice as many crewmembers. Aircraft-type ejection seats replaced the Mercury Project’s escape rocket. The Gemini spacecraft was designed with essentially the same type of redundancy features that had been employed in Mercury. One significant departure from Mercury was that the Gemini crew was given the capability to make the decision to abort based on inputs from selected sensors.

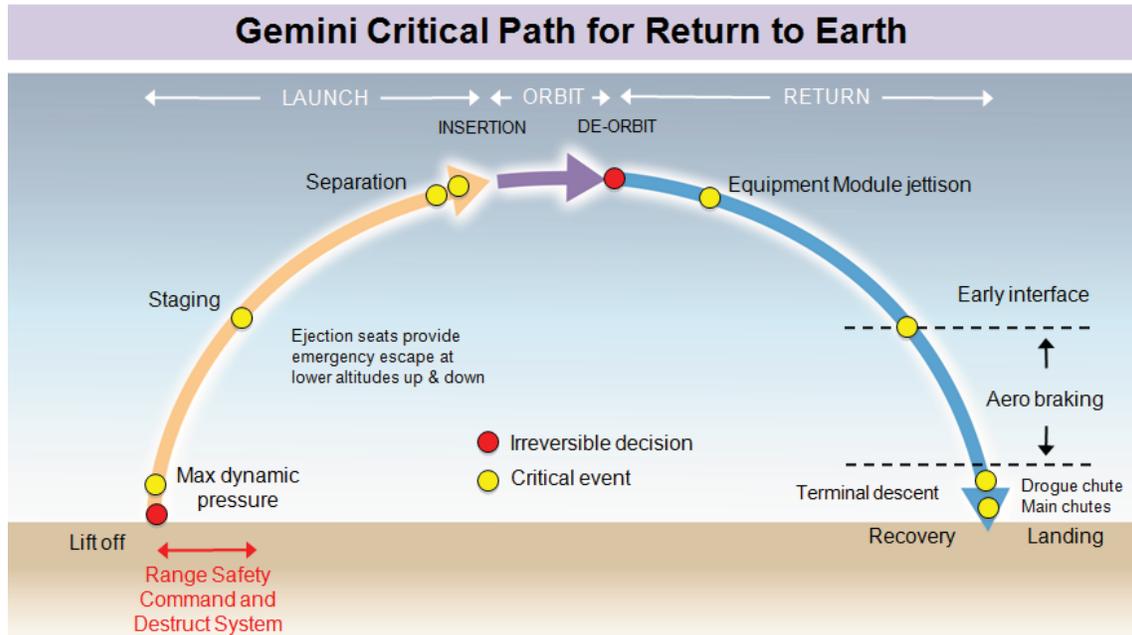
The launch vehicle for the Gemini missions was the Titan II. As with the Atlas, an intensive investigation of Titan performance and all past failures was undertaken in order to pinpoint the vehicle areas that needed to be modified, redesigned, or made redundant. As a result of these studies, it was determined that the flight control, propulsion, electrical systems, and hydraulic systems were the areas that needed reliability improvement and possible redundancy.

The first human Gemini launch occurred on March 2, 1965, after two successful test flights of Gemini I and Gemini II were conducted and all primary test objects achieved. The Gemini critical path for a safe return to Earth is shown in Figure E.1-2.

---

<sup>4</sup> Culbertson, “Man-rating the Atlas as a Mercury Booster,” America Institute of Aeronautics, paper No. 65-252, WAFLUASD Support for Manned Flight Conference, Dayton, OH, April 21–23, 1965.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:			Page #:
<b>Readiness for First Crewed Flight</b>			44 of 58

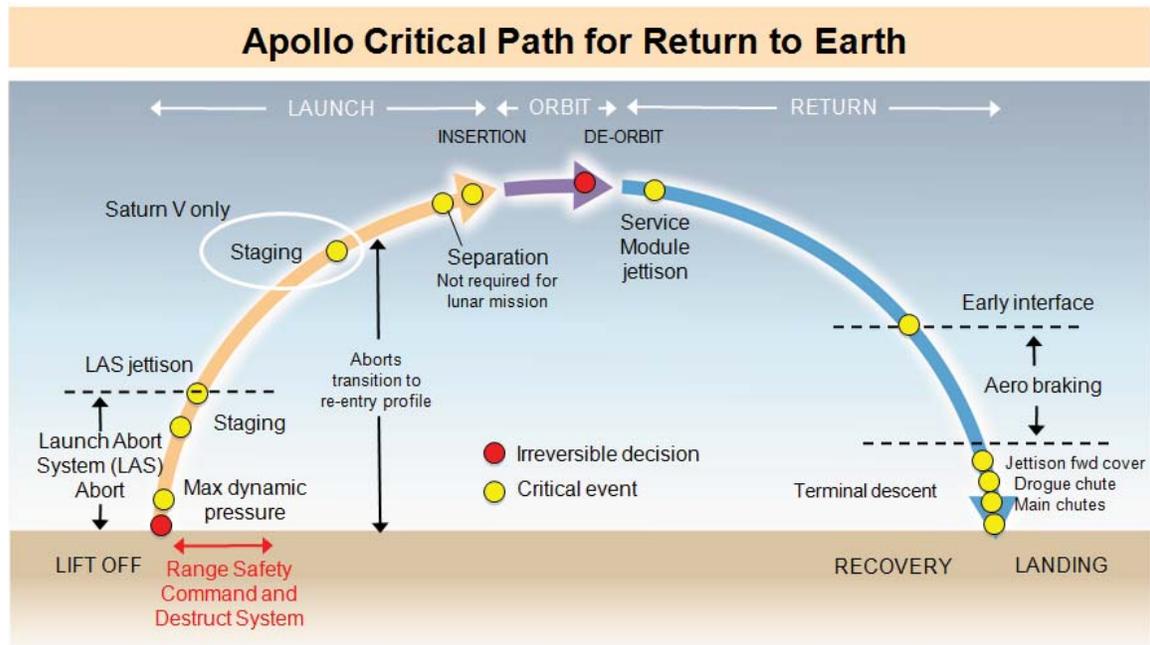


*Figure E.1-2. Gemini Critical Path for Return to Earth*

The 10 crewed Gemini flights demonstrated the capability to subject two men and supporting systems for the challenges of longer duration flights as required for the later trips to the Moon; to effect the rendezvous and docking with other orbiting vehicles for Apollo; to perfect methods of reentry and landing at a pre-selected landing point; and to gain additional information on the effects of weightlessness on crew members and to record the physiological reactions of the crew during long-duration flights.

The Apollo Saturn IB was the first launch vehicle developed specifically to carry humans into space. The Redstone, Atlas, and Titan systems all had their origins as ballistic missiles. In order to launch humans, a process called “man-rating” was followed that included various modifications which were subsequently validated through a combination of ground and flight testing. Although the Saturn IB would also be used to launch uncrewed payloads, it was designed from the outset to be able to safely launch crews into orbit. The Saturn IB flew four uncrewed flight tests, all considered fully successful. Based on the success of these 5 S-IB test flights and the 10 successful flights in the Saturn I test series, the decision was made that the Saturn IB was ready for its first crewed orbital flight test in October 1968. The Apollo critical path to a safe return to Earth is shown in Figure E.1-3.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		45 of 58	



*Figure E.1-3. Apollo Critical Path for Return to Earth*

In reviewing the previous human spaceflight programs, common traits became evident. First, clear definitions of the end result (objectives), the method by which they were to be achieved (guidelines), and development and verification that was required prior to flight (development tasks) were established at the outset. For all the early programs, the decision makers determined that the following conditions were met:

1. The development team was confident that the evidence of task completion was compelling.
2. There were no uncorrected, not understood, or unverified corrections to design-related anomalies.
3. The development team was confident that (a) the mission could be executed as planned and (b) no single credible failure could prevent returning the crew safely to Earth (as depicted in Figures E.1-1 through E.1-3).
4. Flight and mission systems replicated the certified design configuration and specifications.

The history of the early human spaceflight programs includes numerous developmental tests, both ground and flight. The development process focused on building and ground testing systems at the highest level of assembly and flying test articles at the earliest possible time to gather data needed for design refinement. As part of this build, test, and “fix what doesn’t work” approach, failure to fully achieve specific test objectives was not a showstopper unless the data

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 46 of 58	

were deemed insufficient for design and validation purposes. Hence, the development process included a robust ground test program that emphasized critical functionalities. A few examples include:

- Structural test article tests to demonstrate full design capabilities with appropriate margins
- Water-landing tests to demonstrate structural integrity and performance in worst-case scenarios
- Full-scale parachute deployment tests to demonstrate chute operation, strength, and the ability to reliably deploy and inflate the drogue and main parachutes
- Post landing flotation
- Water-drop tests to demonstrate effectiveness of air bags in reducing crew landing loads
- Crew couch tests to demonstrate non-injurious crew loads
- Mission simulated timelines with production spacecraft (and crew) in vacuum chambers
- Series of special space mission testing to exercise planned and contingency scenarios with all systems running
- 1,730 J-2 engine tests before Apollo 8
- Ground vibration tests for launch vehicle and spacecraft combinations

As part of the development cycle, classic flight envelope expansion techniques with prioritized building blocks were used to demonstrate human compatibility with launch and entry environments before evaluating human utility in orbit. The first missions collected the data needed to complete spacecraft and launch systems design/ratings using boilerplate spacecraft. Boilerplate spacecraft were initially used to show that each launch vehicle was compatible with the spacecraft. Finally a series of envelope expansion flights was made with ‘production’ spacecraft building up to a primate and then a human flight. The need to repeat or re-fly a test if a targeted test condition or component was modified was based on engineering judgment. A significant, yet unquantifiable factor that led to the overall success of the early human spaceflight programs was the strong, well-established technical and management teams. Working together so closely, for so long, and in such a fast-paced, pressure-filled environment built strong relationships and understanding. Each team member was accountable for their own system/components and related decisions. The senior managers were technically proficient and remained personally involved from inception through flight, continuously asking “what if” and “how do you know” questions.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 47 of 58	

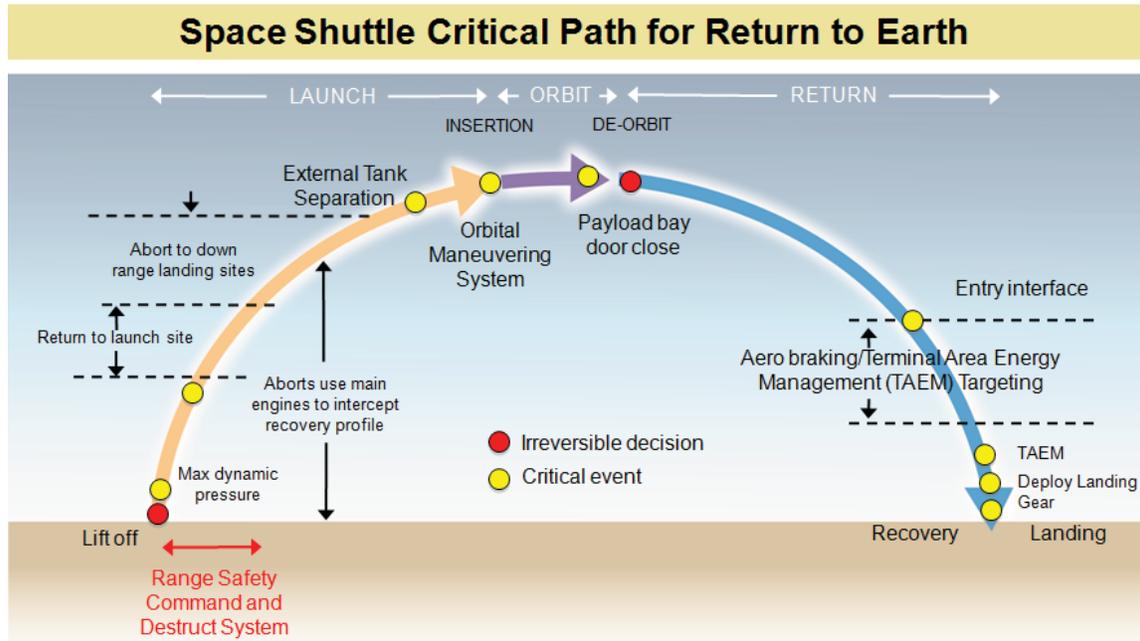
## The Space Shuttle Program

The Space Shuttle represented a significantly more complex system than the early human spaceflight programs. George Low, leader of the Apollo Spacecraft Program Office, noted after a Moon landing that only 100 wires linked the Saturn rocket to the Apollo spacecraft. He wrote, "The main point is that a single man can fully understand this interface and can cope with all the effects of a change on either side of the interface. If there had been 10 times as many wires, it probably would have taken a hundred (or a thousand?) times as many people to handle the interface."<sup>5</sup> This also meant that, in the preceding programs, contractors and NASA Centers could develop hardware in relative isolation from one another, which enabled work on multiple parts of the system to progress in parallel. The Space Shuttle, on the other hand, had to be highly integrated because of its requirements for re-usability and the ability to land like an aircraft on any 10,000-ft runway, among other reasons. The tight integration of the Space Shuttle also required intensive communication and good working relationships among the different organizations involved in its development. The aerodynamic shapes of the Orbiter and launch configurations were much different than the Mercury, Gemini, and Apollo spacecraft, which meant a significant set of new development challenges for even the experienced workforce involved in its design and development. The Space Shuttle critical path to Earth is shown in Figure E.1-4.

---

<sup>5</sup> SP-287, "What Made Apollo a Success." George M. Low, introduction. Accessed on 10/12/10 at: <http://klabs.org/history/reports/sp287/ch1.htm>; SP-4219, "The Space Shuttle's First Flight, STS-1," Henry C. Dethloff; SP-6104, "A perspective on the Human-Rating Process of U.S. Spacecraft: Both Past and Present," George Zupp, Editor, February 1995.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		48 of 58	



*Figure E.1-4. Space Shuttle Critical Path for Return to Earth*

Considerations for crew safety were a tremendous challenge over previous programs due to the vehicle’s complex launch and reentry configuration. One of the most significant challenges was how to address the issue of first-stage aborts (while the SRBs were thrusting). The unique Space Shuttle system design took the Program down a different solution path than previous programs. Several first-stage abort concepts were considered for the Space Shuttle but each introduced its own significant safety risks and complexities. As a result, the decision was made that these additional risks and complexities were of greater concern than the presumed low failure rates of the solid motors. For those areas deemed ‘high risk’ more stringent design requirements were derived to build in greater reliability. For example, simultaneous ignition, simultaneous thrust tail off, and similar thrust profiles were absolutely critical and received extraordinary attention and ground testing. Previous human spacecraft included additional safety through escape capsules or crew ejection in order to accept the less than desired launch vehicle reliability. The Space Shuttle, alternatively, used an historical solid rocket motor (SRM) performance database and extensive testing to minimize risk and deemed the vehicle acceptable for crewed flight without first-stage abort capability.<sup>6</sup>

<sup>6</sup> SP-6104, “A perspective on the Human-Rating Process of U.S. Spacecraft: Both Past and Present,” George Zupp, Editor, February 1995.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 49 of 58	

The Space Shuttle Program's significant emphasis on the approach of focusing on reliability and/or redundancy of high-risk areas relied on extensive testing and quality control processes being successfully implemented as part of the decision considerations to fly a crew on the first (or any) launch. The effective and appropriate use of test articles and test results was vital. The Space Shuttle *Enterprise* played a large role in supporting this approach.

The *Enterprise* was not designed to be capable of spaceflight. It was designed and built as a test bed for conducting the horizontal ground vibration tests (HGVTs) at the manufacturing plant. The HGVT activity was designed to test the structural integrity of Space Shuttle Orbiters with particular emphasis on launch and landing conditions.

Later, *Enterprise* was modified to support the approach and landing tests at Edwards Air Force Base in California. Many systems that would be required for an actual flight into space were either simpler versions or were not even aboard *Enterprise* for these tests. The *Enterprise* approach and landing tests included four categories (this is also an example of how to do incremental test build ups with aircraft):

1. Three Taxi Tests, intended to verify the taxi characteristics of the 747 Shuttle Carrier Aircraft (SCA) while carrying a Space Shuttle. These were runway taxi tests only and did not involve flight. No crew flew aboard *Enterprise* for these tests.
2. Five Captive-Inactive Flights, intended to verify the performance, stability, and control of the SCA while carrying a Space Shuttle in flight. No crew flew aboard *Enterprise* for these tests.
3. Three Captive-Active Flights, intended to determine the best separation profile that *Enterprise* could utilize as it separated from the SCA during upcoming Free Flights, refine crew procedures, and evaluate *Enterprise* flight systems. A two-man crew flew aboard *Enterprise* for these tests.
4. Five Free Flights, intended to verify the airworthiness, integrated system operations, pilot-guided landing systems, and automated landing systems of the Space Shuttle. A two-man crew flew aboard *Enterprise* for these tests. The first four glides to the Rogers Dry Lake runway provided real envelope expansion. The first three drops were conducted on the lake bed with a drag-reducing tail cone over the boat tail. Flight 4 removed the tail cone but used the long lake bed so that there was no pressure to try to land on the spot. Finally, flight 5 was targeted for the concrete runway without a tail cone to evaluate the braking and roll out control that would be representative of an operational return.

At the conclusion of the *Enterprise* approach and landing tests, NASA certified the Space Shuttle Orbiter as aerodynamically sound for subsonic flight and determined that no additional flight tests would be necessary. *Enterprise*, as a high-fidelity pathfinder, was then extensively used to test Kennedy Space Center (KSC) equipment and procedures that would be necessary to support processing operations of a Space Shuttle.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 50 of 58	

The use of the *Enterprise* in testing is only one example of the extensive hardware, avionics, software, and operations development and testing that were done in preparation for getting the Space Shuttle ready for its first launch. The complexity of the Space Shuttle introduced numerous additional interactions and dependencies (such as thermal and power management, GN&C and mechanical system dependencies, and complex software integration and management) and required much more integration and testing to ensure proper coordinated functionality.

The baseline plan in 1973 was to fly the first Space Shuttle mission with a crew, yet preserve an option to launch without a crew. However, at the Program Director’s Review in June of that year, two key issues were raised: Should the first flight be baselined with a crew, and if so, should ejection seats be used? The Program wanted to avoid dual mode vehicle design and focus the Program along a single path.<sup>7</sup>

Part of the rationale for deleting the uncrewed flight test options was that the successful return of the Orbiter was critical to the continuation of the vertical flight test program (one of a kind spacecraft), and the crew would significantly increase the probability of this success. There was a recognized risk to the crew, but the Space Shuttle design effort and test program was geared to establish confidence in the system. It was postulated that maintaining a dual path would detract from or compound the development effort of the baseline crewed system, thus reducing its reliability and robustness.

The major points discussed at this key review were the necessity of recovering the Orbiter, past experiences of crew members saving a mission from failure, confidence in ground-test programs, crew ability to deal with contingencies (i.e., landing at alternate sites), preventing hazards to over flight of population, capabilities of abort and ejection systems, and the impact of an uncrewed option on crewed design effort (uncrewed capability requires a successful auto land program). The decision from that review was to proceed with design, development, and testing of the Space Shuttle considering only a crewed first flight and to discontinue development of the uncrewed option. It was also stated that the decision would be reviewed again 18 months before the first orbital flight. The rationale was that as the benefits of crewed flight (greater probability of success, less risk to fly over populated areas, lower cost, and better operational system) far outweighed the crew and program risks involved.

In 1977, at the planned review 18 months prior to launch, the conclusion remained that the crewed first flight test was superior for reasons of mission success and avoidance of diluted program effort, and the crew risk was acceptable. The reasons supporting the original decision were essentially unchanged and the maturing of the Space Shuttle design and the test program experience increased the overall confidence.

---

<sup>7</sup> “Chronology of Decision, Manned versus Unmanned Vertical Flight Test for the Space Shuttle,” compiled by Code Q, NASA HQ, August 15, 2002.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
	Title: <b>Readiness for First Crewed Flight</b>		Page #: 51 of 58

Although program and Agency management decided that the first Space Shuttle flight would include crew, they had to ensure a safe and successful first flight. As a result, the team pushed the envelope in design analysis and ground testing. For example:

- Many wind tunnel years were devoted to building an aerodynamic database for each configuration over the entire range of Mach numbers
- Thousands of hours of super-computer time evaluating structural models combining thermal and dynamic loads
- Validation of redundant data systems involved years of hardware and software compatibility tests in dedicated facilities
- Development and validation of the stand-alone backup flight computer to protect against loss of the tightly synchronized redundant computer set
- Years of development testing for thermal protection systems
- Years of system operation simulations to develop and test flight procedures and rules
- Developed Shuttle training aircraft to support development of approach and landing techniques and crew training
- Space Shuttle Main Engines (SSME) had 726 starts and 110,000 seconds of testing before STS-1
- SSME certification tests demonstrated boundary of performance on ground before first flight
- External Tank structural test article with over 1,000 strain gauges
- Mated ground vibration test provided design information for guidance and control systems
- SRM underwent full-scale static tests before first flight that included four development motors and three qualification motors

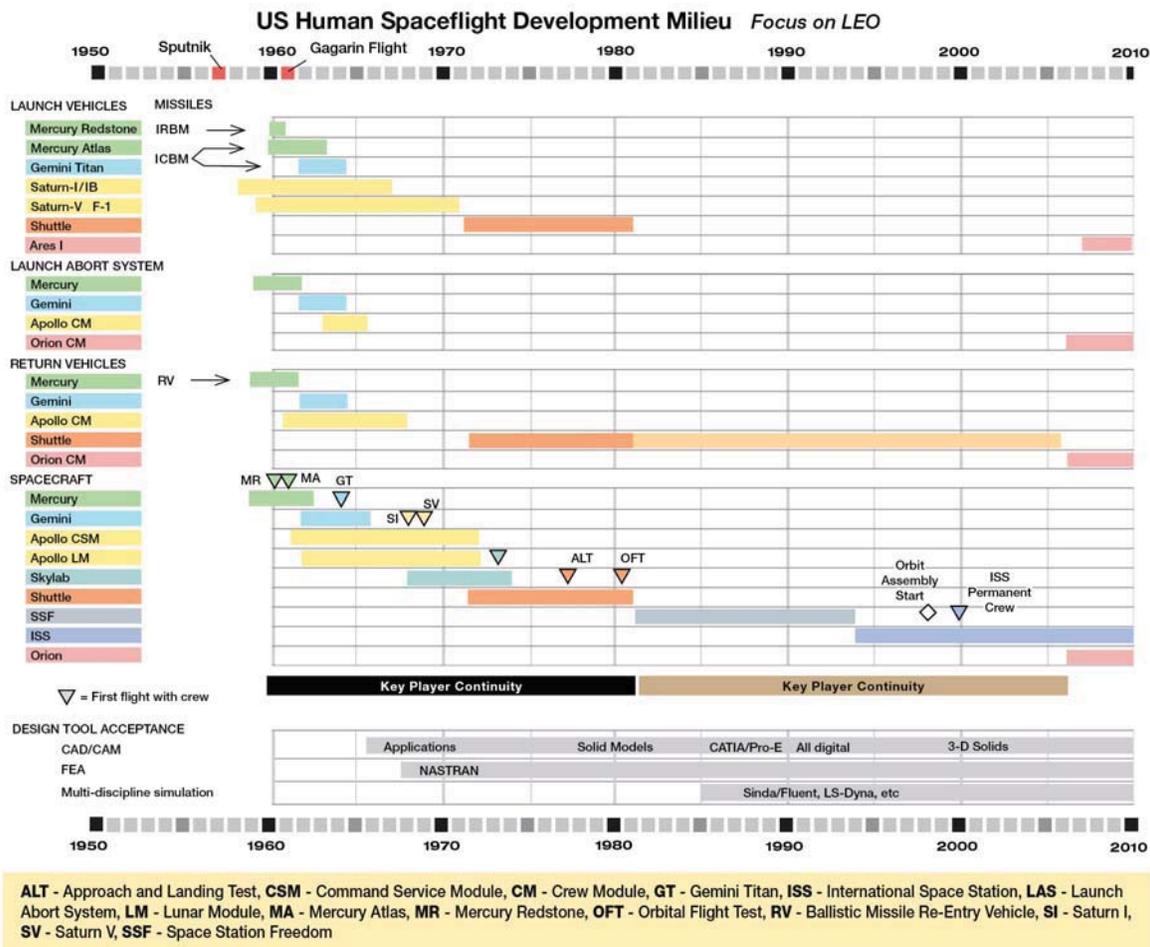
The first four Space Shuttle missions using *Columbia* were deemed to be orbital flight test (OFT) missions. The OFT configuration included thousands of pounds of development flight instrumentation. Each of the OFT missions included a minimum crew of two and employed ejection seats (which were later removed). The first crewed Space Shuttle launch occurred on April 12, 1981.

### **General Observations**

On the surface, it may appear that each of the four programs discussed did not follow the same approach to determining the first crewed flight, as each occurred at a seemingly different time in the test program. This is due, however, mainly to the differences in system design and mission. Though each decision was not reconstructed, it was evident that each program followed similar

thought processes outlined in the body of this report. Each event on the critical path to a safe return to Earth was thoroughly tested and the programs were continually questioning the results, data, and previous assumptions. The residual risks were discussed at all levels of management and open deliberations and communications were evident throughout the program teams.

While Mercury, Gemini, and Apollo were formally separate programs, in practice they functioned as one decade-long program leading up to the accomplishment of the mission set forth by President Kennedy in 1961 to send a man to the Moon and return him safely to Earth. The knowledge gained in each program informed all of the subsequent programs. The same held true for the workforce, which transferred relatively seamlessly from one program to the other. In one decade, for example, a group of engineers that had never before built a spacecraft went on to develop four (Mercury, Gemini, Apollo Lunar Module, and Apollo Command Module) (See Figure E.1-5).



*Figure E.1-5. U.S. Human Spaceflight Development*

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 53 of 58	

This previous workforce experience carried over beyond Apollo and Skylab to the development of the Space Shuttle and was invaluable in that development. Though the Space Shuttle posed altogether different technical challenges than the earlier programs, there was strong continuity of engineering design and operations personnel from the early programs to the design and development of the Space Shuttle. Few of these experienced engineers and managers have been a part of the development of the newer human spaceflight programs.

The second-generation workforce, on the other hand, did not have the benefit of developing and operating a new human-rated launch system for more than two decades between the first launch of the Space Shuttle and the establishment of CxP. It can be noted that there was some continuity in the design of human-rated spacecraft and significant upgrades within the launch vehicle. There were also other programs initiated, but not fully developed, tested, and put into operation. Another change that shaped the second-generation workforce was the growing role that information technology played in the work of engineering. The primary computational tools for the first-generation workforce that developed Mercury, Gemini, and Apollo were slide rules, pencils, and paper. NASTRAN, a finite element analysis (FEA) program, was introduced in the late 1960s, by which time the design and development of the Apollo Program was complete. Some of those tools were later used in an assessment of Apollo performance and flight data. By the mid-1980s, the use of modeling tools such as CAD and computer-aided manufacturing (CAM) had become standard practice and these tools grew increasingly sophisticated over the next decades. While modeling tools revolutionized the practice of aerospace engineering, they also distanced practitioners from fundamental calculations, making them dependent on the assumptions embedded in the software. The earlier work methods, while arduous, aided in the rapid development of engineering judgment by ensuring that practitioners understood the numbers that informed their designs.

While the technical and technological issues faced by previous and future human-rated space programs may be different, the same fundamental factors that are essential to mission success remain the same: sound engineering judgment, attention to detail, continuous questioning, technically competent engineers and managers, and constant vigilance.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		54 of 58	

## **Appendix F. Benchmarking with U.S. Navy and Air Force Flight Test Center**

In assessing when to fly a crew on a new vehicle for the first time, the inputs and experiences from other organizations with similar crew implementation requirements were sought. Personnel from the Air Force Flight Test Center (AFFTC) at Edwards Air Force Base in California and the U.S. Navy's Virginia-class Program Office (for submarines) were consulted on their respective processes and practices for putting into service first-in-class crewed vehicles. Both of these organizations have a history of developing and testing high-risk vehicles in severe environments: the U.S. Navy's nuclear submarines and the U.S. Air Force's advanced aircraft. Nuclear submarines operate in an extreme depth under high water pressure and at the edge of performance, and advanced aircraft operate in the extreme conditions of the atmosphere at the edge of performance. Both organizations develop and test new systems on a regular basis; the last new submarine class was in 2000 and the latest advanced aircraft is the F-35 (December 2006). While the advanced systems are developed primarily by industry, both government organizations are involved in the development process and have the final safety review and acceptance prior to a first use of the new systems. Therefore their experience and processes were considered relevant to this study.

Both organizations were asked to address the following questions:

- How is it determined when in the test program to add the crew for the first time? Can requirements be reduced if the configuration is similar to a previous vehicle? What tradeoffs, if any, are considered?
- How is it determined that the benefit of having a crew is greater than the risk to the crew?
- Have the processes been documented (such as standards or policies, etc.) that specifically outline what is required before a crew can be put on board to operate the vehicle? If so, what is the documentation and does it change for differing environments?

### **Air Force Flight Test Center Experience**

The AFFTC's mission is to developmental flight test a system to determine if it meets specifications, uncover any problem areas, and ultimately recommend whether the system is ready to proceed to operational testing. Their approach is based on the diversity of systems, from new state-of-the-art fighter aircraft to a fuselage tank on 50-yr-old aircraft, for which they are responsible for establishing flight safety. This broad spectrum of systems requires processes and requirements that can be tailored to meet the needs of each system. Rarely have there been vehicles that are flown first without a crew and then with a crew, therefore the decision process for adding a crew is in place for the first flight. A broad combination of ground analysis and test is required before a first crewed flight, with each unique program or system evaluated individually.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 55 of 58	

The AFFTC utilizes multiple reviews, including those for the developmental flight test, operational flight test, and operational use. There is a distinct difference in what level of risk and uncertainty may be acceptable prior to proceeding with a flight test program versus sending the system to an operational unit for routine use. For readiness to proceed to operational testing or deployment, the results from the flight test program are added to the results from the ground test and analysis to assess an overall risk. The AFFTC may decide the risk is acceptable to proceed with flight testing, but that the risk is not yet sufficiently low to proceed with operational deployment, including operational testing. A risk matrix is utilized, which attempts to identify specific risks along with the probability of occurrence and the consequences if they do occur. Many of the risks may be based on computed probabilities of occurrence, but many others are qualitative estimates of the probability of occurrence based on experience and engineering judgment. An extensive flight test and safety planning process is included to reduce the risk further by putting forethought into what needs to be tested. The testing addresses the most effective and safest approach, and what additional risk mitigation can be applied such as incremental testing (starting at the most benign conditions first), procedures, monitoring, etc. The flight test safety planning process is critical to ensuring all that is practical is done in order to safely proceed with flight test. The AFFTC has process documentation that outlines what is required prior to a first flight but can be tailored to a specific situation or system. The process tends to be very detailed and often utilizes standards but allows for some flexibility to account for varying systems requirements. Alternatively, the criteria for Air Worthiness Certification (MIL-HDBK--516B) for operational status is usually significantly more rigorous than the requirements to proceed with flight test.

### **U.S. Navy Nuclear Submarine Experience**

The U.S. Navy submarine development approach is an incremental process; each new submarine's specifications are built on the previous submarine's specifications. A three-tiered organization and process of program management, technical authority, and safety and quality, is used to determine when the ship is ready for its first sea trial. A combined complement of contractor and government, from these listed organizations, goes on the first sea trials where hull, propulsion systems, and safety systems are tested together as a system for the first time. A combination of contractor and Navy personnel operates the ship but nuclear power plant operations can only be operated by Navy nuclear personnel. The Navy's development process for submarines includes locating the ship's crew and Navy civilians at the contractor site throughout manufacture and testing. Prior to the sea trials, a "maximum reasonable assurance" that the ship is safe to go to sea is determined, based on the experience and judgment of the program management, technical authority, and safety and quality. The crew lives on-board during the initial testing, followed by dock trials and Fast Cruise. Fast Cruise is the operation of the ship as if it was at sea, concentrating on operations and safety systems. Once the primary systems required to return the crew safely to land are tested and the vehicle/ship is determined to be safe, the remainder of the ship is tested. Incremental testing and operation of systems is performed during sea trials that allow the crew to incrementally test up to operating capability.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP- 10-00619</b>	Version: <b>1.0</b>
Title: <b>Readiness for First Crewed Flight</b>		Page #: 56 of 58	

An independent assessment is performed prior to delivery that evaluates the ship to ensure it meets the needs of the Navy. The independent assessment includes a review of paperwork and underway trials. Once the review is completed at the end of testing, the ship testing results are presented to a board. The board evaluates two elements for unrestricted operations: Is the material sound and is the ship force trained? All mandatory deficiencies, as defined by the board, must be corrected prior to acceptance.

The team observed several commonalities between AFFTC and U.S. Navy approaches. Those commonalities and a brief discussion of how they might apply to a human spaceflight program are as follows:

1. Both AFFTC and the U.S. Navy are able to do incremental expansion of development, testing, and operational capability, and thus do not initially operate at full capability of the vehicle. It is more difficult for a crewed space system to do incremental expansion. To some extent, incremental testing of various components can be performed, however, incremental testing of an integrated vehicle is typically prohibitive due to cost and availability of one-of-a-kind hardware (unless features allowing for upgrades are part of the initial design).
2. Both AFFTC and the U.S. Navy have new development programs on a regular basis. This on-going development allows the organizations to consistently maintain their knowledge and experience base, building on lessons from program to program, rather than having to relearn. NASA may create a new crewed space system in multiple decade increments. It is much more difficult to maintain a knowledge and experience base and many lessons are lost.
3. Both AFFTC and the U.S. Navy stressed that the final evaluation was a judgment call and that the extensive design activities and testing that occurred prior to the first flight/sea trial provided information for that judgment. As noted in #2 above, that judgment is also based on experience in developing new systems.

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #:	Version:
		<b>NESC-RP-10-00619</b>	<b>1.0</b>
Title:		Page #:	
<b>Readiness for First Crewed Flight</b>		<b>57 of 58</b>	

## Appendix G. Selected References

The following selected references were deemed by the team to be informative and beneficial in addressing the question of first crewed flight.

### Human Rating:

NPR 8705.2B, Human-Rating Requirements for Space Systems

NASA-STD-3000, Man-Systems Integration Standards, July 1995

SSP 50808, ISS Commercial Orbital Transportation Services (COTS) Interface Requirements Document, Revision A, April 2008

T98-10212, A Review of Man Rating in past and Current Manned Space Flight Programs, A. Bond, 1998

### Historical:

Mercury Chronology, <http://history.nasa.gov/SP-4001/contents.htm>

Gemini Chronology, <http://history.nasa.gov/SP-4002/contents.htm>

Apollo Chronology, <http://www.hq.nasa.gov/office/pao/History/SP-4009/contents.htm>

Saturn Chronology (MSFC), <http://history.nasa.gov/MHR-5/contents.htm>

MSFC internal letter, Apollo 502 Anomaly Resolution and AS 503 Flight with Crew Decision, 1968

AIAA paper 3812, *ELV Human Rating, Atlas Heritage and Future Potential*, author Holguin, tracking number 33343

NASA TMX 57497, Pilot Safety Program for Mercury-Atlas Launch Vehicle, B A Hohmann, 1963

*History of Rocketry and Space Travel*, W. von Braun and F. I. Ordway III, (Thomas Y. Crowell, New York, 1969).

*Apollo Program Summary Report*, <http://history.nasa.gov/apsr/apsr.htm>

Apollo-Saturn 205 Mission, MSFC 70-30, 215 C.1, Jan 1966

Apollo links (KSC), <http://www-pao.ksc.nasa.gov/kscpao/history/apollo/apollo.htm>

NASA SP Series on Space Exploration, <http://history.nasa.gov/series95.html>

	<b>NASA Engineering and Safety Center Technical Assessment Report</b>	Document #: <b>NESC-RP-10-00619</b>	Version: <b>1.0</b>
	Title: <b>Readiness for First Crewed Flight</b>	Page #: 58 of 58	

**Safety/Risk:**

SSP 30309E, Safety Analysis and Risk Assessment Requirements, July 2009  
 NPR8000.4, Agency Risk Management Procedural Requirements, December 2008  
 NPR8715.3, Safety and Mission Assurance Plan  
 NPD 8610.7D, Launch Services Risk Mitigation Policy for NASA-Owned and/or NASA-Sponsored Payloads/Missions, January 2008  
 Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Version 1.1, Dr. Michael Stamatelatos, NASA OSMA, August 2002.  
 NASA/SP-2010-576, NASA Risk-Informed Decision Making Handbook, April 2010  
 JS-2010-017, Significant Incidents Human Spaceflight, Rev A

**Design, Test, and Verification:**

NESC RP-06-108, Design, Development, Test and Evaluation Considerations for Safe and Reliable Human Rated Spacecraft Systems  
 Science Applications International Corporation, A Study Of Commercial Industry Best Practices In Test & Evaluation Which are Potentially Applicable to DoD Developmental Test And Evaluation, 2002  
 NASA-STD-7009, Standard for Models and Simulations, August 2008

**Program/Project Management:**

7120.5D NASA Space Flight Program and Project Management Requirements  
 Aerospace Report TOR-2005(8617)-4204, *100 Questions for Technical Review*, September 2005

**Systems Engineering and Integration:**

NASA SP-2007-6105, NASA Systems Engineering Handbook  
 NPR 7123.1A, NASA Systems Engineering Processes and Requirements

**REPORT DOCUMENTATION PAGE**

*Form Approved  
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.  
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 01-04-2011			<b>2. REPORT TYPE</b> Technical Memorandum		<b>3. DATES COVERED (From - To)</b> March 2010 - April 2011	
<b>4. TITLE AND SUBTITLE</b> Readiness for First Crewed Flight					<b>5a. CONTRACT NUMBER</b>	
					<b>5b. GRANT NUMBER</b>	
					<b>5c. PROGRAM ELEMENT NUMBER</b>	
<b>6. AUTHOR(S)</b> Schaible, Dawn M.					<b>5d. PROJECT NUMBER</b>	
					<b>5e. TASK NUMBER</b>	
					<b>5f. WORK UNIT NUMBER</b> 869021.05.07.07.25	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> NASA Langley Research Center Hampton, VA 23681-2199					<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>  L-20026 NESC-RP-10-00619	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> National Aeronautics and Space Administration Washington, DC 20546-0001					<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>  NASA	
					<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>  NASA/TM-2011-217089	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> Unclassified - Unlimited Subject Category 16-Space Transportation and Safety Availability: NASA CASI (443) 757-5802						
<b>13. SUPPLEMENTARY NOTES</b>						
<b>14. ABSTRACT</b> The NASA Engineering and Safety Center (NESC) was requested to develop a generic framework for evaluating whether any given program has sufficiently complete and balanced plans in place to allow crewmembers to fly safely on a human spaceflight system for the first time (i.e., first crewed flight). The NESC assembled a small team which included experts with experience developing robotic and human spaceflight and aviation systems through first crewed test flight and into operational capability. The NESC team conducted a historical review of the steps leading up to the first crewed flights of Mercury through the Space Shuttle. Benchmarking was also conducted with the United States (U.S.) Air Force and U.S. Navy. This report contains documentation of that review.						
<b>15. SUBJECT TERMS</b> NASA Engineering and Safety Center; Human spaceflight; Low Earth orbit; First crewed flight						
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>	
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			STI Help Desk (email: help@sti.nasa.gov)	
U	U	U	UU	63	<b>19b. TELEPHONE NUMBER (Include area code)</b> (443) 757-5802	