An Investigation of Risk Management Approaches for NASA Piloted X-Plane Projects

By Steven Hirshorn and Guy Kemmerly

1.0 Executive Summary

NASA is resuming X-plane research. It plans to build a low-boom supersonic flight demonstrator (LBFD), an all-electric general aviation aircraft (X-57), and possibly an ultra-efficient subsonic transport (UEST) demonstrator. In an attempt to define what levels of risk are appropriate in piloted X-plane research, the NASA Office of the Chief Engineer (OCE) evaluated numerous NASA, Department of Defense (DoD), and industry project management and risk assessment tools. Provided are the results of the evaluations of NASA Procedural Requirements (NPR) 7120.5, 7120.8, and 8705.4; Langley Research Center (LaRC) Procedural Requirement (LPR) 7120.5; Dryden (Armstrong) Center Procedures S-002 and X-009; and Military Handbook 516C. Some of these were applied to the LBFD and X-57 aircraft. The impacts on risk of budgeting decisions and specialized flight conditions were also considered. None of the evaluated processes were found to be fully appropriate for governing experimental aircraft projects, but many useful elements were found in some of them. As such, the OCE offers nine recommendations:

1. Define "Experimental Aircraft" as a classification of NASA projects and explore tailoring the Federal Aviation Administration (FAA) Experimental Aircraft definition and regulations for NASA purposes.
2. Use the existing NASA aircraft design and airworthiness certification process to define the appropriate technical risk posture for NASA X-planes.
3. Include the Health Management Technical Authority (HMTA) in the X-plane design process to address the unique health risks associated with X-plane operations.
4. Hold discussions to develop consensus among the stakeholders to define "acceptable risks" early in the project lifecycle – at approximately Mission Concept Review.
5. Using existing models, such as NPR 8705.4, tailor a governance model for classifying piloted X-plane project risks.
6. Use military/industry/international standards for aircraft design philosophies and construction standards/guidelines. NASA need not develop and maintain its own.
7. Use the NPR 7120.5/7120.8 requirements that have been tailored for use with piloted X-plane projects to define the appropriate programmatic risk posture.
8. Maintain cost and schedule margins and reserves on all X-plane projects.
9. Clearly define the risk acceptance authority to enable project decision making. For example, delegate risk acceptance authority to the Center Director at the Armstrong Flight Research Center (AFRC) for flight risks created by X-planes operating in the Dryden Aeronautical Test Range (DATR).

2.0 Problem Description and Proposed Solutions

In aviation, the terms *safety* and *risk* are often used interchangeably, but in the flight research world they mean different things. In flight research, the primary motivation is to do everything possible to ensure mission success without compromising human safety. That includes the flight crew, the ground personnel, and the public/non-participants. To keep the operational risk low, technical risk might increase. Technical risk may include the possibility of a failure to meet mission objectives, failure of one or more aircraft systems, or maybe just the need to return to base with the mission incomplete and live to fly another day.

Experimental flight often carries a higher technical risk than operational flight. Obviously, experimental flights are conducted with systems that are less mature and have less demonstrated reliability. There may be no alternative ways to do some things in an experimental flight, so redundancy among elements may not be possible. Because the systems and components being used are often one of a kind, they may be salvaged and reused from other test aircraft systems rather than being tailored the exact needs of the current test aircraft. When off-the-shelf components are available, they are usually either excessively or minimally capable rather than perfectly matched to the need as they would be if developed for a production aircraft, and the integration of these parts in to the system can be a challenge. Finally, as "experimental aircraft" implies, a production prototype will not be built that can be used, for example, as a structural test article. On the other hand, experimental flight can also allow mitigations that are not available in routine operational flight. For example, experimental flight often has real-time system health and performance monitoring by a team of experts within a dedicated ground control room. The flight envelope and other mission-specific operating limits are often restricted and flight crews rely on carefully constructed procedures to stay out of trouble.

The NASA Aeronautics Research Mission Directorate (ARMD) is developing a series of piloted experimental aircraft (X-planes) for the first time in almost 30 years. These include the LBFD which has been designed to fly supersonically (M=1.4) with a significantly attenuated sonic boom (Figure 1), a subsonic aircraft (X-57) with a distributed electric propulsion system (Figure 2), and potentially even a UEST which is based on hybrid wing body or blended wing body design principles (Figure 3). The work on the LBFD has been proceeding in partnership with the Lockheed-Martin Corporation under the Quiet Supersonic Technology (QueSST) project. A preliminary design review (PDR) for a demonstrator was held in July 2017 and a request for proposals to complete the design and build the LBFD was released in August 2017. The X-57 concept underwent a critical design review (CDR) in November 2016 and a delta-CDR in February 2017. The first flight of the initial configuration is expected in 2018 with flights of additional configurations to follow. Work on the UEST is currently unscheduled.

Figure 1. Low-Boom Flight Demonstrator

Figure 2. X-57 Distributed Electric Propulsion Demonstrator

Figure 3. Ultra-Efficient Subsonic Transport

While the LBFD and X-57 designs appear to be consistent with previous piloted experimental aircraft development, to date, there is no NASA Agency-level consensus on how much risk (technical and programmatic) is acceptable on these projects. These are high-cost, high-complexity, and high-visibility vehicles that will have a crew (lower risk tolerance) and require integrated system-level development. Still, research aircraft are experimental in nature with options to 'Return to Field' and fly another day in the event of malfunctions, so they can generally accept higher risk. In this ambiguity, a full spectrum of opinions have been voiced. Some stakeholders say that the lowest level of risk acceptance - NPR 8705.4 (Ref 1) Risk Classification Class A - should be used because the vehicle has a crew and given the project's high visibility and importance to the Agency, and some say the highest level of risk acceptance - Class D - is appropriate because the project is research. Some say something in between is appropriate given the unique nature of this "one-off" experimental aircraft. Finally, some say that using NPR 8705.4 risk classifications is inappropriate because they are not created for use in aircraft development. A lack of consensus exists.

The purpose of this effort is to review NASA and DoD project management and risk analysis processes to see if they are useful for experimental aircraft projects. These processes will be applied to the LBFD and X-57 projects to determine whether the risk tolerance inherent in them is comparable to the risk

tolerance posture (technical and programmatic) being used by the LBFD and X-57 projects. This will indicate whether they are suitable for other X-plane projects working through risk management issues. Ultimately, the goal is to establish a common frame of reference and understanding among all NASA stakeholders on risk expectations for piloted flight research projects like the LBFD and X-57 projects.

3.0 NASA X-Plane Governance

Addressing risks requires some common language. Risk itself is defined in DCP-X-009, Armstrong Airworthiness and Flight Safety Review Process (Ref 2), as an event that could cause injury, loss, or damage to personnel, property, the environment, or mission accomplishment. It has an estimated probability of occurrence and severity of consequence. The task of identifying risks is the responsibility of all stakeholders, and the Project Manager manages the collection of identified risks. Different risks demand different levels of attention, so it is important that a system be adopted for characterizing or classifying the importance of the individual risks. This classification system should also be integrated with a system that describes the Project Manager's responsibilities for managing and mitigating the different classifications of risk. Managing the risks ensures they will not be overlooked and involves mitigation to reduce the likelihood of undermining the project or harming individuals or property. Some risks cannot be eliminated completely, and it may be necessary for the Project Manager to secure approval to proceed with unresolved risks. This risk approval process, if it exists, should also be integrated with the risk classification process. The evaluations of the documents listed below, are conducted using these actions (identification, classification, management, and approval) related to risks.

Numerous procedures describe ways to classify and effectively manage risk within a project management structure. Several procedures were reviewed and evaluated in this study including NPR 7120.5, NASA Space Flight Program and Project Management Handbook (Ref. 3), NPR 7120.8, NASA Research and Technology Program and Project Management Requirements (Ref 4), DCP-X-009, Armstrong Airworthiness and Flight Safety Review Process (Ref. 2), NPR 8705.4, Risk Classification for NASA Payloads (Ref. 1), MIL-HDBK-516C, Airworthiness Certification Criteria (Ref 5), DCP-S-002, Armstrong Hazard Management Procedure (Ref. 6), LPR 7120.5, NASA Langley Space Flight Project Practices Handbook (Ref. 7). In addition to these, numerous subsystem and component design, development, and certification standards were also considered (Refs. 8-39).

Risk is often broken into two categories – technical and programmatic. Though the line between these categories is often unclear, technical risk typically involves hardware, software, facilities, analysis, and the abilities of individuals. Programmatic risk includes more overarching elements such as political priorities, plans, or resource availability. Confusion can arise when both of these contribute to the obstacle. For example, hardware design features may be eliminated because resources are cut or facilities may be made unavailable because priorities change. Nevertheless, an attempt has been made to separate these risks in this analysis.

3.1 Technical Risk

3.1.1 NPR 7120.5, NASA Space Flight Program and Project Management Handbook and 7120.8, NASA Research and Technology Program and Project Management Handbook

Neither NPR 7120.5 nor NPR 7120.8 is fully appropriate for governing NASA X-plane projects. NPR 7120.5 was developed for spaceflight programs and NPR 7120.8 was developed for relatively low-risk research and technology development projects.

For classifying risk, NPR 7120.5 points to NPR 8705.4. For managing risk, NPR 7120.5 and 7120.8 both point to NPR 8000.4b (Ref 40), Agency Risk Management Procedural Requirements, and NPR 7120.5 also points to NASA/SP-2011-3422, NASA Risk Management Handbook (Ref 41). NPR 7120.5 also raises the issue of engaging the expertise of the NASA Chief Health and Medical Officer (CHMO) when issues arise related to the health of NASA personnel. Piloted operations at very high altitudes could generate medical issues and the CHMO should be alerted to the possible need for a HMTA. However, none of these NPRs or handbooks discuss the unique aspects of technical risk for experimental aircraft, and thus are not useful sources.

3.1.2 NPR 8705.4, Risk Classification for NASA Payloads

The applicability of NPR 8705.4 to New Aviation Horizons (NAH) X-plane projects was discussed within the ARMD Governance Working Group (GWG) and within the NASA Program and Project Management Board (PPMB) Tiger Team. The GWG and PPMB Tiger Team were set up to identify governance for the NAH projects and were populated by senior NASA managers and engineers from the four NASA Research Centers and offices at NASA Headquarters. Both entertained the question of whether NPR 8705.4 should be applied to NASA piloted X-plane development and both recommended not applying it, as is, to these projects. Both the GWG and PPMB Tiger Team completed their work over the course of 2016. The Tiger Team recognized that these Risk Classification definitions and the associated guidance were generated with spaceflight projects in mind, not aircraft, and that the applicability of the Risk Classification system within NPR 8705.4 should be determined during the design process and assessed on a case-by-case basis. That is the standard process used at AFRC and LaRC for research aircraft design. However, while the guidance provided in 8705.4 was not considered applicable to NASA experimental aircraft development, it was noted that certain generic precepts of Risk Classification, described in the first chapter of NPR 8705.4, should be followed. These include:

- Risk is understood and agreed to by the program/project, Governing Program Management Council, Mission Directorate, and other customer(s). (NPR 8705.4 ¶ 1.1.1)
- All parties are … able to understand the acceptable risk associated with a program or project. (NPR 8705.4 ¶ 1.1.2)
- As early in the formulation process as possible, the Mission Directorate establishes the acceptable risk classification level (NPR 8705.4 ¶ 1.2.1)
- The project can define and apply the appropriate design and management controls, systems engineering processes, mission assurance requirements, and risk management processes. (NPR 8705.4 ¶ 1.3.1)
- The guidelines (are) … intended to serve as a starting point for establishment of assurance criteria, mission design, and test programs tailored to the needs of a specific project. The intent is to generate discussion of implementation methodologies in order for the programs, projects, Centers, the Governing Program Management Council (GPMC), and the Mission Directorate to make informed decisions. (NPR 8705.4 ¶ 1.3.2)

Clearly, using NPR 8705.4 involves a discussion of "acceptable risk" tolerance early in the life of a project, typically at the first key decision point, KDP-A. This risk tolerance is then promulgated through NPR 8705.4 to determine which Risk Classification should be used in conducting the project. NPR 8705.4 was developed for spaceflight projects, though, and is not required for use by the NASA aircraft community, so this discussion has not historically occurred on ARMD projects. As a research portfolio,

ARMD projects normally carry higher inherent risk and could benefit from the understanding and commitment this early discussion generates.

When considering the usefulness of the Risk Classifications in NPR 8705.4, two sets of evaluation criteria are provided for characterizing risk. One addresses Technical Risk attributes and the other addresses Programmatic Risks (see Section 3.2.3). The Programmatic Risk attributes are listed below. These are described in NPR 8705.4 as "safety, mission assurance, design, and test" risks.

- Single point failure acceptability
- Engineering model, Prototype model, and Flight and Spare hardware availability
- Qualification, Acceptance, and Protoflight Test Program planned
- EEE[1] parts use
- Reviews planned
- Materials characterizations/experience availability
- Compliance with Reliability NPD 8720.1 – Level of failure effects analysis that is available
- Level of Fault Tree Analysis that is available
- Maintainability requirements
- Compliance with Quality Assurance NPD 8730.5
- Software Verification and Validation requirements
- Compliance with Risk Management NPR 8000.4b
- Telemetry Coverage for mission critical events

While NPR 8705.4 as a whole is not considered applicable to NASA's piloted X-planes, the above design criteria are examples of design aspects that should be considered in the development of experimental aircraft. Appendix A describes how the LBFD project is approaching these criteria. Furthermore, it was noted that there are likely similar design criteria to those discussed in 8705.4 that, while not included, are good design criteria applicable to aircraft development. Those aircraft-specific design criteria should be identified.

3.1.3 MIL-HDBK-516C, Airworthiness Certification Criteria

As there is no NASA-owned technical standard for airworthiness certification, the MIL-HDBK-516C was investigated for applicability. This DoD standard provides the airworthiness authority in all branches of the service with criteria to determine the airworthiness of all air vehicles including, but not limited to, manned or unmanned, fixed or rotary wing. Users are encouraged to tailor the entire set of criteria to a set that is applicable to the airworthiness of the aircraft system being assessed. Following the tailoring rules provided in the document, such a tailoring was performed for the LBFD. Table 1 shows the results as described at PDR. Nearly 40% of the criteria in MIL-HDBK-516C were found to not apply to this technology demonstrator. The tailoring of the criteria contained within MIL-HDBK-516C is

[1] NASA's Electrical, Electronic and Electromechanical (EEE) Parts discipline seeks to evaluate newly available and advanced electronic parts for NASA programs and projects and maximize effectiveness and efficiency by collaborating with industry and other agencies.

based on three factors: 1) the subject matter of the criterion, 2) how high or low the safety bar needs to be set for success, and 3) the methodology used to verify compliance.

Table 1. MIL-HDBK-516C Tailoring for LBFD

	Section Heading	Total Criteria	Applicable Criteria	Non-Applicable Criteria
4	Systems Engineering	21	19	2
5	Structures	29	22	7
6	Flight technology	206	125	81
7	Propulsion & Propulsion Inst'l	99	36	63
8	Air Vehicle Subsystems	295	187	108
9	Crew Systems	57	46	11
10	Diagnostic Systems	7	7	0
11	Avionics	30	29	1
12	Electrical Systems	26	24	2
13	Electromagnetic Environ Effects	12	11	1
14	System Safety	39	36	3
15	Computer Systems & Software	42	41	1
16	Maintenance	12	12	0
17	Armament /Stores Integration	22	0	22
18	Passenger Safety	19	0	19
19	Materials	18	0	18
20	Air Transportability, etc.	18	2	16
	Totals	952	597	355

3.1.4 DCP-S-002, Armstrong Hazard Management Procedure

This NASA procedure applies to the aerospace and ground systems for which AFRC assumes ground, range, flight safety, or mission success responsibility. It includes all elements of flight research operations. At a minimum, the test article or vehicle, support subsystems or vehicles, and ground research capabilities are included unless specifically waived by the Independent Technical Authority or by the AFRC Center Director.

Risk assessment within this process is based on two matrices that assess the probability and severity of any possible mishap. The combination of the probability and severity associated with a possible mishap is designated a risk. This document defines a mishap as “an unexpected, unforeseen, or unintended event that causes injury, loss, or damage to personnel, equipment, property, the environment, or mission accomplishment.” The two matrices are presented in Figure 4. One deals with the impact of a mishap on the loss of a valuable asset and the other deals with injury or even the loss of human life. They differ in the level of approval required to accept specific levels of risk. Within DCP-S-002, the bounds on the different categories of both Probability and Severity are defined.

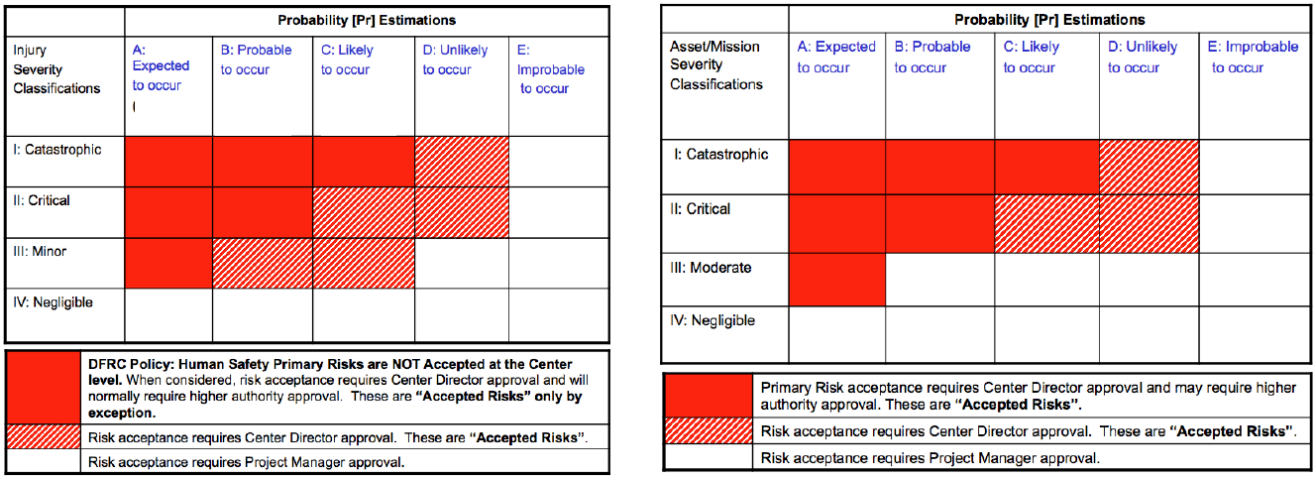

Figure 4. DCP-S-002 Human Injury Risk Assessment Matrix and Asset/Mission Risk Assessment Matrix

3.1.5 DCP-X-009, AFRC Airworthiness and Flight Safety Review Process

DCP-X-009 (Ref 2) defines the process by which reviews are used to approve all flight activities and hazardous ground tests at AFRC, as well as testing involving AFRC personnel using non-NASA facilities. For airworthiness and safety matters, it recommends that G-7900.3-001 (Ref 42) be used as guidance.

G-7900.3-001 advises reviewers to consider all aspects of the project including personnel, process and execution, technology, and technical areas, but it provides no guidance for how the areas should be judged. Risk Management falls under the heading of Process and Execution and G-7900.3-001 simply advises that the following elements should be evaluated:

- Assessment of residual risk
- Accepted Risk list
- Risk/Hazard identification
- Severity and Probability matrix
- Pre-mishap contingency plan
- Pre-declared risk list

Though this is a good place to start in evaluating how much attention a Project Manager has given to Risk Management, it is not an exhaustive list. It neither provides objective criteria for the evaluation nor describes what levels of risk are acceptable. Elements such as the Severity and Probability matrix must be found in other documents. Terms such as "residual risk" and "pre-declared risk" are undefined. As an advisory document, G-7900.3-001 is useful, but it must be used in partnership with other unspecified documents.

3.1.6 Unique Hazards

Most X-planes will also have unique hazards that will require risk analysis beyond any standard process used in the development of other aircraft. Communication is the key to addressing these unique challenges. Some level of risk must be accepted, and the goal is consensus among the stakeholders about

the appropriate level of risk. As described in Reference 1, that consensus should be reached early in the design process before options are eliminated.

3.2 Programmatic Risk

Some risks are unrelated to the technology development, hardware, or conduct of the experiment. A project can also fail because of management issues such as poor planning, inappropriate resource allocation, and unforeseen obstacles. These are programmatic risks. Several guides and procedures address these types of risks.

3.2.1 NPR 7120.5, NASA Space Flight Program and Project Management Handbook and 7120.8, NASA Research and Technology Program and Project Management Handbook

Though the preface of NPR 7120.5 describes it as being applicable only to spaceflight projects, the document offers programmatic risk management practices that may be equally applicable when developing a risk management system for experimental aircraft. It describes NASA-specific program and project management language and practices in detail. Those descriptions emphasize the need for scheduling periodic external project reviews and for building margin and reserve into resource and performance plans.

As the title implies, NPR 7120.5 (Ref 3) was not developed for experimental aircraft projects but it does outline that:

- **2.4.4.** Mission Directorates shall plan and budget tightly coupled and single-project programs (regardless of life-cycle cost) and projects with an estimated life-cycle cost greater than $250 million based on a 70 percent joint cost and schedule confidence level (JCL), or as approved by the Decision Authority.
- **2.4.4.1.** Any JCL approved by the Decision Authority at less than 70 percent shall be justified and documented.
- **2.4.4.2.** Mission Directorates shall ensure funding for these projects is consistent with the Management Agreement and in no case less than the equivalent of a 50 percent JCL.

NPR 7120.8 states that it is applicable to all NASA Research and Technology projects not covered under NPR 7120.5 and which are not Infrastructure or IT projects. It is generally applied to projects smaller than $250M, though, and even suggests that large-scale projects follow the management practices required in NPR 7120.5. Both the GWG and PPMB Tiger Team mentioned in Section 3.1.2 advised that the appropriate Project Management approach for NAH X-planes appears to be a combination of the management rigor of NPR 7120.5 and the technology development focus of NPR 7120.8.

3.2.2 LPR 7120.5, NASA Langley Space Flight Project Practices Handbook

As was the case for NPR 7120.5, LPR 7120.5 (Ref 7) was developed with spaceflight projects in mind. Still, it provides good guidance for reducing programmatic risk. LPR 7120.5 states:

- The Project shall include reserves in the cost estimate based on assessed implementation risk. The standard level of reserves is 30 percent at the time of PDR, and a waiver is required for a smaller level of reserves in the cost estimate. The Center will not allow less than 15 percent reserves at the time of PDR.

- Projects shall include funded schedule margin along the critical path of the Integrated Master Schedule. Guidance for funded schedule reserve margin that should be validated by assessment of implementation risk is:
  - Formulation through subsystem development = 1 month margin per year
  - System integration and testing through delivery to launch site (or storage) = 2 months margin per year

3.2.3 NPR 8705.4, Risk Classification for NASA Payloads

In addition to the technical risks categories described in Section 3.1.2, NRR 8705.4 also provides a matrix for assessing more programmatic risks. They are described as defining "risk combinations for NASA payloads by considering such factors as criticality to the Agency Strategic Plan, national significance, availability of alternative research opportunities, success criteria, magnitude of investment, and other relevant factors." Figure 5 shows the NPR 8705.4 Risk Characterization model applied to the LBFD and the X-57. While this application represents the judgement of the author and required a subjective interpretation of the intent of each category and the associated descriptors to apply this spacecraft tool to experimental aircraft, it is intended to show that not all piloted X-plane projects are the same. While they are both piloted X-planes, the LBFD and the X-57 may fall within different risk classifications using the definitions in this matrix. Though the LBFD is planned to cost ~$400M and to operate at M=1.4 over public lands, the X-57 is planned to cost only ~$30M and to operate at just 150 knots within the confines of the DATR. It is appropriate that their risks are different.

		LBFD		
Characterization	**Class A**	**Class B**	**Class C**	**Class D**
Priority (Criticality to Agency Strategic Plan	High priority	High priority	Medium Priority	Low priority
National significance	Very high	High priority	Medium Priority	Low to medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long, >5 years	Medium, 2-5 years	Short, <2 years	Short, <2 years
Cost	High	High to medium	Medium to low	Low
Launch Constraints	Critical	Medium, 2-5 years	Few	Few to None
In-Flight Maintenance	N/A	Not feasible or difficult	Maybe feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities

		X-57		
Characterization	**Class A**	**Class B**	**Class C**	**Class D**
Priority (Criticality to Agency Strategic Plan	High priority	High priority	Medium Priority	Low priority
National significance	Very high	High priority	Medium Priority	Low to medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long, >5 years	Medium, 2-5 years	Short, <2 years	Short, <2 years
Cost	High	High to medium	Medium to low	Low
Launch Constraints	Critical	Medium, 2-5 years	Few	Few to None
In-Flight Maintenance	N/A	Not feasible or difficult	Maybe feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities

Figure 5. Author's Estimates of NPR 8705.4 Applied to LBFD and X-57

Apparent in this risk matrix is the emphasis on spacecraft. For example, most spacecraft are not serviceable after launch so the possibility of performing "In-Flight Maintenance" significantly affects the likelihood of mission success. Aircraft, however, are available for service before and after every flight, even though "In-Flight Maintenance" may not be a desirable design feature. "Launch Constraints" also have little meaning. That attribute appears to be asking the question, "How narrow is the time window in which this research must be done?" It aims to assess whether schedule slips will

destroy the entire project. Finally, “Mission Lifetime” is more an assessment of the reliability that has been built into the system. The comparable mission lifetime for an experimental aircraft may be an hour (beyond that, many things can be serviced) or it may be the 1000-hour service life designed into components that are more difficult to service, such as the primary structure and engine bearings. On the other hand, because these aircraft are piloted, there is a new need for aircraft specific reliability not covered in NPR 8705.4. As a result of this difference in needs, LaRC has mapped the NPR 8705.4 Risk Classification criteria into a set more applicable to flight-test aircraft. That assessment matrix was applied to the LBFD in 2014 and again in 2017 (Fig 6). The risk classification can be seen to change from 2014 to 2017. As the priority of the work grew within ARMD, as alternative ways of conducting the research decreased, and as the risks associated with achieving mission success became better understood, the overall risk assessment increased.

	Select from the criteria drop-down lists below:	Type A	Type B	Type C	Type D	Type E	Type F
2014	Mission Type: Aircraft based mission					X	X
	Priority: Low				X	X	
	National Significance: Med to Low				X		
	Complexity: Medium to low			X	X		
	Mission Lifetime: N/A					X	X
	Cost Estimate: Medium to Low (~$100M -			X			
	Launch Constraints: N/A						X
	In-Flight Maintenance: N/A						
	Alternative Research: Significant				X	X	X
	Medium or significant risk of not achieving mission success is permitted. Minimal				X		
	Select from the criteria drop-down lists below:	**Type A**	**Type B**	**Type C**	**Type D**	**Type E**	**Type F**
2017	Mission Type: Aircraft based mission					X	X
	Priority: Medium			X			
	National Significance: Med to Low			X			
	Complexity: Medium to low				X		
	Mission Lifetime: Short <2years				X		
	Cost Estimate: Medium to Low (~$100M -			X			
	Launch Constraints: Few to None				X		
	In-Flight Maintenance: May be feasible				X		
	Alternative Research: Some or few alternatives or reflight opportunities			X			
	Medium or risk of not achieving mission success is permitted. Reduced assurance			X			

Figure 6. Evolving QueSST Perspectives on Risk from Spring 2014 to Summer 2017 (using the LaRC tailoring tool)

3.2.4 De-Scope Strategies

If resources are set and reserves are exhausted, it may be necessary to reduce the scope of a project. This should be performed with great care and should be based on a prioritization of the project objectives performed early in the project planning.

3.2.5 Project Review

It is important to build regular reviews into project schedules to ensure that the project team does not become too narrowly focused. Day-to-day challenges can draw attention to near-term concerns at the expense of maintaining a big-picture perspective. Occasionally, events outside the project can increase or decrease the importance or urgency of the project goals. Outside reviews can return the focus to an appropriate balance, even if only momentarily. These reviews should be scheduled with line management and with members of the broader stakeholder community.

4.0 Risk Management Lessons Applied to LBFD

Following the consideration of the risk management references, the Integrated Aviation Systems Program (IASP) within the NASA's Aeronautics Mission Directorate has developed the LBFD governance model. Largely, that was by tailoring both NPR 7120.5 (Ref 3) and NPR 7120.8 (Ref 4, as applicable, and adding elements to address experimental aircraft development not found in these NPRs. Specifically, these additional elements address airworthiness certification and were drawn from the Dryden Airworthiness and Flight Safety Review Process (Ref 4). This Governance and Decision Authority approach was approved by the NASA Agency Program Management Council on July 19, 2017.

4.1 Project Documentation

Part of effective communication is extensive documentation. Since the LBFD project was born of the QueSST project, considerable documentation existed that represented consensus among the stakeholders. It would be wasteful to abandon these documents without good cause. These documents include, among others:

- Project Management Plan
- Concept of Operations
- Requirements Documents (system/subsystem)
- Configuration Management Plan
- Risk Management Plan
- Configuration Control Board Charter
- Security Plan
- System Acceptance Plan
- Systems Engineering Management Plan
- Aircraft Requirements and Assumptions
- Airworthiness Requirements and Criteria
- Software Management Plan
- Life Support to Aircraft Interface Control Document
- Airworthiness Certification Plan
- Safety and Mission Assurance Plan
- System Safety Plan
- Quality Assurance Plan
- Mishap Preparedness/Contingency Plan

4.2 Project Reviews

Extensive reporting and review requirements have been built into the LBFD Plan to minimize programmatic risk. This project oversight and insight includes:

- Program/Center:
  - Key Decision Points (as required)
  - IASP Tag-up (every 2 weeks)
  - ARMD Quarterly Status Review (4 times a year)
  - ARMD Annual Review (annually, if no KDP that year)
  - Integrated Center Management Council (monthly)
  - IEPTR (Integrated Engineering Project Technical Review (monthly)
- Project (QueSST structure):
  - Project Management Review Board (monthly)
  - Engineering Review Board (TBD)
  - Project Configuration Control Board (CCB) (monthly)
  - Project RMB (monthly)
  - Aircraft CCB (TBD)
  - Engineering Tag-up (TBD)
- AFRC Airworthiness Certification process
  - Flight Readiness Review (FRR) (~3 months prior to first flight)

- Airworthiness & Flight Safety Review Board (AFSRB) (6-10 weeks prior to first flight)
- Tech Brief (~2 days prior to first flight)

4.3 Resource Management

ARMD created an Inter-Center Planning Team for the transition from the QueSST project to the LBFD project. Among other things, the team explored best practices for program and project management and considered how those might be applied to the LBFD project. Resource management was a main topic and the team recommended that funding to 50% JCL (Ref 43) and a 15% reserve (both contract and in-house) and 5 months funded schedule reserve should be secured before baselining the budget. In this context, margin and reserve are defined as follows:

- *Margin* is schedule and budget conservatism built into the plan to allow for "known" uncertainties.
- *Reserve* is resource conservatism built into the plan to allow for "unknown" uncertainties (things that cannot be predicted).

> *"Establish adequate program reserves—and double them."*
> *– Vince Rausch, X-43 Project Manager*

> *"Eliminate zero margin concept – establish risk and uncertainty reserves."*
> *– Fay Collier, ERA Project Manager*

4.4 De-Scope Plans

The primary technology being investigated by the LBFD project is the outer mold line (OML) of the aircraft and the LBFD Project Plan development effort is focused on meeting this primary objective while minimizing all other areas. As such, very few technologies can be abandoned without adding increased risk to the project. Nevertheless, the LBFD Project Office will be required to develop a de-scope strategy prior to the KDP-C, at which time the project's plans will be confirmed and baselined. This de-scope strategy will be important to the success of the project in the event resources are consumed more rapidly than anticipated.

4.5 Decision Making Authority

It is important, when accepting the responsibility for project results, to understand where the decision-making authority rests. Overall decision authority for the LBFD has been delegated to the ARMD Associate Administrator by the NASA Associate Administrator. Risk acceptance should follow. Safety risk is typically delegated to the AFRC Center Director, who formally accepts the risk for all test flights, both in restricted airspace and in FAA-controlled airspace. NPR 7900.3D, "Aircraft Operations Management Manual," requires that aircraft be certified airworthy under the authority of the Center Director through a Certificate of Airworthiness Process. Both Phase 1 (Initial Airworthiness and Envelope Expansion) and Phase 2 (Initial Acoustic Response) of the LBFD Project will be conducted in restricted airspace (DATR). Phase 3 is planned to be conducted in FAA-controlled, but unrestricted, Class A airspace above 55,000 ft. over populated areas. NPR 8000.4b, Agency Risk Management Procedural Requirements states:

> *– 2.3.4 When there is risk to humans, the actual Risk Takers (e.g., astronauts) (or official spokesperson[s] and official supervisory chain) are accountable for consenting to assume the risk.*
>
> *Note:* The NASA Administrator is the official Agency spokesperson to consent to any exposure to human safety or property risk on behalf of the general public.

It has not yet been determined how far risk acceptance authority will be delegated. The rationale for maintaining that authority at the NASA Associate Administrator level is based on the following considerations.

- The inclusion of a human on board raises the risk of the project to the agency level in all phases of the project.
- Piloted X-planes will garner nationwide interest, especially for anomalies.
- Many legacy subsystems will be used which were not originally rated for the QueSST/LBFD flight parameters.

The rationale for maintaining risk acceptance authority at Center Director level is based on the following considerations:

- Flight envelope will be flight-tested and set, with practiced operational test flights rehearsed in restricted areas before going out for operational runs.
- The mission profile of the flights is benign, straight and level at a constant Mach number.
- NASA aircraft presently fly in FAA-controlled airspace.

The uncertainty surrounding this decision-making authority must be resolved before the project proceeds.

4.6 Unique Hazards

Because of the requirement that the LBFD conduct sustained flight at M=1.4, flight testing requires both a large test area and an area free of slower traffic. The aerothermodynamics at high altitudes also contribute to sonic boom attenuation. The LBFD will, therefore, be flown in the airspace above commercial transports between 55,000 ft. and 58,000 ft. above mean sea level. Flight above 50,000 ft. requires that the cockpit be pressurized to no higher than 25,000 ft. equivalent air pressure and that the crew wear partial-pressure suits and use supplemental oxygen. No commercially available partial pressure suits and oxygen regulation systems exist for operations above 50,000 ft. except those that use emergency oxygen generation systems known as on board oxygen generation systems (OBOGS). These have historically been unreliable. To avoid problems with OBOGS, the design of the LBFD supplemental oxygen system will use bottled liquid oxygen (LOX). The seal that will maintain cockpit pressure at 25,000 ft. comes from the T-38 and is not currently qualified for operations above 50,000 ft.

The approach being taken by the project team is to ensure that cabin pressure can be maintained at or below 25,000 ft. equivalent air pressure while operating at altitudes between 55,000 ft. and 58,000 ft. Because the cockpit is a small volume, small leaks will be significant. As a second line of defense, a qualified Pilot Life Support ensemble must be identified or developed. Such a system would include a pressure suit and LOX with a regulator all capable of supporting ejection at approved altitudes. As an additional line of defense, the cabin pressure will be monitored and the pilot will be alerted to low pressure using an integrated caution, alerting, and warning system and panel cockpit display guiding a manual descent to a lower altitude.

The design and verification efforts needed for systems such as these include:

1) A cockpit pressurization schedule must be designed such that cockpit pressure can be maintained at or below 25,000 ft. altitude to support operations at LBFD mission altitudes.

2) A life support ensemble (partial pressure suit with LOX regulator and secondary oxygen supply) capable of supporting ejection at approved altitudes must be identified or developed.
3) A cockpit pressurization monitoring system capable of alerting the pilot through ICAWS and panel cockpit display must be developed for a manual altitude descent initiated action.
4) The performance of the life support ensemble must be validated through test and analysis.
5) The performance of the cockpit pressurization system must be validated through test and analysis.

This approach has been discussed with and accepted by the LBFD stakeholders. That consensus does not ensure mission success or guarantee safety, but it ensures that no obvious options have been overlooked and that everyone related to the project has had the opportunity to stop the process if they believe the risk to be unacceptable.

4.7 LBFD Overall Risk Conclusions

The LBFD Inter-Center Planning Team (ICPT) reached following the overall conclusions on risk:

- Current budget is high risk due to the lack of reserves.
- Robust programmatic documentation, reporting, and insight/oversight exists.
- NPR 8705 is difficult to apply to an X-plane application.
- The best fit for the LBFD Project is a tailored Class C/D categorization.

In addition to the overall conclusions from the ICPT, the survey conducted for this report leads to the following additional conclusions:

- Availability of cost/schedule margins and reserves will be critical to successful completion of this aircraft development effort.
    - While the data collected on sonic boom attenuation is for research purposes, the design/build of this aircraft should not be considered a research project but a more standard complex system-level development effort.
    - Strategy on margins and reserves is still in development.
    - For the LBFD project, conservatism may be less than for similar cost/visibility NASA projects because:
        - Standard manufacturing and testing processes will be used. No new materials or manufacturing processes are required.
        - Significant use of commercial off-the-shelf hardware/software will be possible, reducing development risk.
        - The mission profile is relatively low-risk compared with X-planes investigating new flight regimes.
- De-scope options will be limited.
    - The technology being investigated is the aircraft OML itself.
    - The design is already simplified for cost but adequate for safety/airworthiness.
    - There are few objectives that can be removed from the project.
- Depth of document tree and levels of oversight/insight appear to be rigorous and appropriate for a project of this complexity/cost/visibility.

- Where the authority to accept risk during flight, be it with the Project Manager, Center Director, Mission Directorate Associate Administrator, or with the NASA Associate Administrator, is still undetermined and with differences of opinion.

5.0 OCE Recommendations

Because of this study, the NASA OCE proposed the following recommendations:

5.1 Language

NPR 8705.4 is not used by the NASA aircraft development community because it is primarily focused on spaceflight. However, those outside the NASA aircraft development community use it when discussing LBFD. To avoid confusion of expectations, a language is needed for the aircraft development community.

OCE Recommendation: The FAA maintains a category for aircraft certification called "Experimental Aircraft." Adopt "Experimental Aircraft" as a classification of NASA projects when discussing NAH X-plane risk posture. It is not recommended that ARMD modify NPR 8705.4, rather that it continue to investigate the FAA Experimental Aircraft definition and regulations (and potentially DoD) and tailor those to NASA purposes.

5.2 Technical Risk Management

5.2.1 Airworthiness Certification

The existing NASA aircraft design and airworthiness certification process is rigorous, appropriate, best-in-class, and will produce safe aircraft that meet mission objectives within the parameters of "experimental aircraft."

OCE Recommendation: Use the inputs and outputs of that process to define the appropriate LBFD technical risk posture. Do not change the existing NASA aircraft design and airworthiness certification process. It is effective, as is.

5.2.2 HMTA

Experimental aircraft operations can present unique health risk that must be carefully analyzed.

OCE Recommendation: The HMTA should participate in the LBFD design process and should be formally included in the LBFD project team. ARMD and HMTA should discuss ways to ensure this.

5.2.3 Acceptable Risk

The precepts of consensus on acceptable risk early in the project life cycle are applicable to NAH X-planes.

OCE Recommendation: This type of discussion is needed at the Agency-level for each NAH project. Insert an AFSRB-led risk discussion at approximately the time of Mission Concept Review or KDP-A.

5.2.4 Risk Classification

The existing NPR 8705.4 classification categories are not applicable to experimental aircraft development.

OCE Recommendation: ARMD should tailor a governance model from existing models for use with piloted X-plane projects conducted by the IASP.

5.2.5 NASA Design and Construction Standards

Aircraft design philosophies and construction standards/guidance influence some risk decisions, yet NASA-owned standards are not needed.

OCE Recommendation: MIL/industry/international standards and AFRC/LaRC institutional processes are sufficient. However, the process QueSST used to determine applicability and levels of those standards should be captured for use on future X-plane projects.

5.3 Programmatic Risk

5.3.1 NPR 7120.5 and NPR 7120.8 Tailoring

ARMD conducted a thorough NPR 7120.5/7120.8 tailoring process, which has produced a set of programmatic requirements for NAH X-plane projects.

OCE Recommendation: Use that requirement set to define LBFD programmatic risk posture. Other sources, such as the Project Manager's Acquisition Strategy, must also be used to define specific aspects of LBFD programmatic risk posture.

5.3.2 Resource Planning

Cost and schedule margins and reserves will be critical to the success of NAH X-plane projects.

OCE Recommendation: NAH X-plane projects should maintain cost/schedule margins and reserves.

5.3.3 Risk Acceptance Authority

Clear risk acceptance authority is essential for project decision making.

OCE Recommendation: Delegate authority to the AFRC Center Director for flight risk acceptance while NAH X-planes are operating in restricted airspace (DATR). Initiate a broader discussion to determine the authority for flight risk acceptance in unrestricted airspace (National Airspace System).

6.0 Acronyms and Nomenclature

AA	Associate Administrator
A/C	Aircraft
AFRC	Armstrong Flight Research Center
AFSRB	Airworthiness & Flight Safety Review Board
ARMD	Aeronautics Research Mission Directorate
CCB	Configuration Control Board
CD	Center Director
CDR	Critical Design Review
CE	Chief Engineer
CHMO	Chief Health and Medical Officer
DATR	Dryden Aeronautical Test Range
DoD	Department of Defense
EEE	Electrical, Electronic, and Electromechanical
ERA	Environmentally Responsible Aircraft
FAA	Federal Aviation Administration
FMEA/CIL	Failure mode and effects analysis/critical items list
FRR	Flight Readiness Review

GIDEP	Government-Industry Data Exchange Program
GPMC	Governing Program Management Council
GWG	ARMD Governance Working Group
HDBK	Handbook
HMTA	Health and Medical Technical Authority
IASP	Integrated Aviation Systems Program
ICPT	Inter-Center Planning Team
IEPTR	Integrated Engineering Project Technical Review
IPAO	Independent Program Assessment Office
ITAR	International Traffic and Arms Regulations
IV&V	Independent verification and validation
JCL	Joint cost and schedule confidence level
KDP-A	First key decision point
KDP-B	Second key decision point
KDP-C	Third key decision point
LaRC	NASA Langley Research Center
LBFD	Low Boom Flight Demonstrator
LOX	Liquid oxygen
LPR	Langley Procedural Requirement
M	Mach Number
MD	Mission Directorate
MIL	Military
MRB	Management Review Board
NAH	New Aviation Horizons
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NPR	NASA Procedural Requirement
NRB	NESC Review Board
OBOGS	On-board oxygen generation system
OCE	Office of Chief Engineer
OML	Outer mold line
OSMA	Office of Safety and Mission Assurance
PDR	Preliminary Design Review
PLOA	Probability of loss of aircraft
PM	Project Manager
PPMB	NASA Program and Project Management Board
QueSST	Quiet Supersonic Technology
RMB	Risk Management Board
SCD	Source Control Drawing
SPF	Single Point Failures
TBD	To be determined
TSO	Technical Standard Order
UEST	Ultra-efficient subsonic transport
X-planes	Experimental aircraft

7.0 References

1. NPR 8705.4, Risk Classification for NASA Payloads
2. DCP-X-009, AFRC Airworthiness and Flight Safety Review Process
3. NPR 7120.5, NASA Space Flight Program and Project Management Handbook
4. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements
5. MIL-HDBK-516C, Airworthiness Certification Criteria
6. DCP-S-002, Armstrong Hazard Management Procedure
7. LPR 7120.5, NASA Langley Space Flight Project Practices Handbook
8. AFRC G-7123.1-001
9. JSSG-2009A, Specification Guide for Air Vehicle Subsystems
10. JSSG-2006, Aircraft Systems
11. JSSG-2008, Vehicle Control and Management System
12. JSSG-2010, Joint Service Specification Guide, Crew Systems
13. JSSG-2010-5, Crew Systems Aircraft Lighting Handbook
14. MIL-A-8862A, Airplane Strength and Rigidity, Landing Loads
15. MIL-STD-411F, Design Criteria Standard, Aircrew Station Alerting Systems
16. MIL-STD-882E, System Safety
17. MIL-STD-1333B, Military Standard Aircrew Station Geometry for Military Aircraft
18. MIL-STD-1797B, Flying Qualities of Piloted Aircraft
19. MIL-STD-3050, Aircraft Crew Breathing System using On-Board Oxygen Generating System
20. MIL-W-5008, Aerospace Vehicle Wiring
21. MIL-PRF-83282, Hydraulic Fluid, Fire Resistant, Synthetic Hydrocarbon Base
22. Engineering Design Handbook CALAC
23. AS5440, Hydraulic Systems, Aircraft, Design and Installation Requirements
24. SAE-AS90362, External Electrical Receptacle
25. NFPA 1 – Fire Code
26. SAE AIR 1168, Applied Thermodynamics Manual
27. AIR-STD-1052, Minimum Protection for Aircrew Exposed to Altitude Above 50,000 Feet
28. AIR-STD-4039, Minimum Physiological Requirements for Aircrew Demand Breathing Systems
29. AS94900, Aerospace – Flight Control System – Design, Installation and Test of Piloted Military Aircraft, General Specification
30. 6C5-DG-2, Lockheed Martin Aircraft Lighting Systems Design Guide
31. PM-4007, Lockheed Martin Design Manual
32. 6C1-DM-4A, Hydraulic System Design Manual
33. PM-4001, Lockheed Martin Software Design Manual
34. PM-4001, Lockheed Martin Software Engineering Process Manual
35. 14 CFR Part 23.1381-1401
36. MIL-PRF-83282, Hydraulic Fluid, Fire Resistant, Synthetic Hydrocarbon Base

37. 14 CFR-91
38. NPR 7150.2B, NASA Software Engineering Requirements
39. NASA-HDBK-2203, NASA Software Engineering Handbook
40. 8000.4b, Agency Risk Management Procedural Requirements
41. NASA/SP-2011-3422 NASA Risk Management Handbook
42. G-7900.3-001, Airworthiness And Flight Safety Review, Independent Review, Technical Brief And Mini-Tech Brief Guidelines
43. https://www.nasa.gov/pdf/394931main_JCL_FAQ_10_12_09.pdf

Appendix A. Application of NPR 8705.4 Programmatic Risk Criteria to LBFD

	Class A	Class B	Class C	Class D	Rationale
Single Point Failures (SPFs)	Critical SPFs (for Level 1 requirements) are not permitted unless authorized by formal waiver. Waiver approval of critical SPFs requires justification based on risk analysis and implementation of measures to mitigate risk.	Critical SPFs (for Level 1 requirements) may be permitted but are minimized and mitigated by use of high reliability parts and additional testing. Essential spacecraft functions and key instruments are typically fully redundant. Other hardware has partial redundancy and/or provisions for graceful degradation.	Critical SPFs (for Level 1 requirements) may be permitted but are mitigated by use of high reliability parts, additional testing, or by other means. Single string and selectively redundant design approaches may be used.	Same as Class C.	We will always have some critical items (coined "Jesus Bolts" by Mark Mangelsdorf in our project) that, if they fail, the airplane will crash. We try to be robust, we try to identify any systems or components in which a single failure or combination of likely failures could lead to catastrophic results, and then design those points with high-reliability parts, inspections/service plans, etc. We are selectively redundant.
Engineer-ing Model, Proto-type, Flight and Spare Hardware	Engineering model hardware for new or modified designs. Separate prototype and flight model hardware. Full set of assembled and tested "flight spare" replacement units.	Engineering model hardware for new or significantly modified designs. Protoflight hardware (in lieu of separate prototype and flight models) except where extensive qualification testing is anticipated. Spare (or refurbishable prototype) hardware as needed to avoid major program impact.	Engineering model hardware for new designs. Protoflight hardware permitted (in lieu of separate prototype and flight models). Limited flight spare hardware (for long lead flight units).	Limited engineering model and flight spare hardware.	We will test components to qualify them for the environments they will see, but certainly not the airplane as a whole, until it flies. We will have some spares of line-replaceable units. We will build various mock-ups of any new equipment, but most of the components we are using (except some of the NASA systems) will be off-the-shelf systems. We believe the closest to us might be Class C, but this is one that we think should be re-written to be more airplane-centric if we were to keep these kinds of tables for airplane research. Spares approach leans more towards Class B, but overall Class C is the best fit.
Qualifica-tion, Accept-ance, and Proto-flight Test Program	Full formal qualification and acceptance test programs and integrated end-to-end testing at all hardware and software levels.	Formal qualification and acceptance test programs and integrated end-to-end testing at all hardware levels. May use a combination of qualification and protoflight hardware. Qualified software simulators used to verify software and system.	Limited qualification testing for new aspects of the design plus full acceptance test program. Testing required for verification of safety compliance and interface compatibility.	Testing required only for verification of safety compliance and interface compatibil-ity. Acceptance test program for critical performance parameters.	We will do a number of qualification tests for individual components, as discussed above, and integrated system testing before going to flight, as the systems start being assembled. The FRR/AFSRB/Tech Brief process results in what could be called "formal" qualification and acceptance functions. We will not be doing the FAA-level qualification testing, such as is needed for getting a new avionics system TSO'd for use in the airplane. Since this is a one-off airplane, we do not need to qualify things to the same robust, fool-proof status that a system needs to be if being used in a largely uncontrolled environment with a large range of operator experience and training levels. This is another one that might use some re-write to make more airplaneish. We believe LBFD should be in the Class C/D range.

	Class A	Class B	Class C	Class D	Rationale
EEE Parts	NASA Parts Selection List (NPSL) Level 1, Level 1 equivalent source control drawings (SCDs), and/or requirements per Center Parts Management Plan.	Class A requirements or NPS Level 2, Level 2 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B or NPSL Level 3, Level 3 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B, Class C requirements, and/or requirements per Center Parts management Plan.	EEE Parts Plan part of the Performance Work Statement, project will be Class D. Need to focus on A/C quality parts.
Reviews	Full formal review program. Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and code.	Full formal review program. Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and peer reviews of code.	Full formal review program. Independent reviews managed at Center level with Mission Directorate participation. Include formal inspections of software requirements, peer reviews of design and code.	Center level reviews with participation of all applicable directorates. May be delegated to projects. Peer reviews of software requirements and code.	The LBFD review process is closest to Class C.
Safety	Per all applicable NASA safety directives and standards	Same as Class A	Same as Class A	Same as Class A	Same as all of them – we try to be a safe project within the accepted probability of loss metric, at least. Project observes all the applicable safety directives and standards.
Materials	Verify heritage of previously used materials and qualify all new or changed materials and applications/ configurations. Use source controls on procured materials and acceptance test each lot/batch.	Use previously tested/flown materials or qualify new materials and applications/ configurations. Acceptance test each lot of procured materials.	Use previously tested/flown materials or characterize new materials. Acceptance test sample lots of procured materials.	Requirements are based on applicable safety standards. Materials should be assessed for application and life limits.	We are not aware of any new materials in the design, so we are C/D.
Reliability NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.	Various systems will have different levels of failure effects analyses, depending on criticality. These have been somewhat defined in the Airworthiness Requirements and Criteria. We are in the C range.
	Class A	Class B	Class C	Class D	Rationale

Fault Tree Analysis	System level qualitative fault tree analysis.	Same as Class A	Same as Class A	Fault tree analysis required for safety critical functions.	Again, different systems will get different treatment – we expect to have some system-level fault tree analysis, as has already been done to help recognize the problem children. So, depending on how we read the Class A description, we could be anywhere on the spectrum; Class C/D is best fit.
Probabil-istic Risk Assess-ment NPR 8705.5	Full Scope, addressing all applicable end states per NPR 8705.5.	Limited Scope, focusing on mission-related end-states of specific ~~decision making~~decision-making interest per NPR 8705.5.	Simplified, identifying major contributors. Other discretionary applications.	Safety only. Other discretionary applications.	Probability and reliability predictions will be done for the entire aircraft system to arrive at the probability of loss statistic, which we have set a requirement to. This involves a complex understanding of the interaction of the subsystems in the airplane and results in the overall PLOA, and shows the contribution to that from each factor in the airplane design. Project is most likely a Priority II, therefore NPR 8715.3 requires "qualitative system safety analysis, supplemented by probabilistic risk assessment where appropriate." For LBFD, "where appropriate" would be the PLOA-related analyses.
Maintain-ability NPD 8720.1	As required by NPD 8720.1	Application of NPD 8720.1 determined by program. (Typically ground elements only).	Maintainability considered during design, if applicable.	Requirements based on applicable safety standards.	We have the design being conducted with a long flight campaign (1000 flight hours) in mind. Since that is the case, we are designing for reliability and maintainability. We are Class C since we are doing what we need to do to be able to operate for several years and lots of flying, so that is applicable
Quality Assurance NPD 8730.5, NPR 8735.2 (NPR 8735.1)	Formal quality assurance program including closed loop problem reporting and corrective action, configuration management, performance trending, and stringent surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and moderate surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and tailored surveillance. GIDEP failure experience data and NASA Advisory process.	Closed-loop problem reporting and corrective action, configuration management, GIDEP failure experience data and NASA Advisory process. Other requirements based on applicable safety standards.	There is strong collaboration between NASA and the contractor; we do have a quality assurance plan at NASA and for the contractor. Only difference between B and C seems to be moderate vs. tailored surveillance; Class C is the best fit.
Software	Formal project software assurance program. Independent verification and validation (IV&V) as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance insight.	We do NOT plan to subject our software to the IV&V in West Virginia, so we are Class D.
	Class A	Class B	Class C	Class D	Rationale

Risk Manage-ment NPR 8000.4b	Risk Management Program. Risk reporting to GPMC.	Same as Class A	Same as Class A	Same as Class A	We are the Governing Program Management Council (GPMC) at the QueSST CCB, so looks like we can be any of the classes there.
Telemetry Coverage for mission critical events	During all mission critical events to assure data is available for critical anomaly investigation to prevent future recurrence.	Same as Class A	Same as Class A	Same as Class A	There are no differences in the table (should be for airplane projects, I would think). We will vary telemetry requirements based on phase of flight project and the objective of each individual flight.

Mr. Steven R. Hirshorn

National Aeronautics & Space Administration Headquarters, Office of the Chief Engineer

Aeronautics Research Mission Directorate Chief Engineer

Mr. Hirshorn began working at the NASA in 1990. Presently, he resides at NASA HQ in Washington D.C. within the Office of Chief Engineer where he is the Chief Engineer for the Aeronautics Research Mission Directorate (ARMD).

After earning a Bachelor of Science degree in Aeronautical Engineering from Embry-Riddle Aeronautics University in 1986 and a Masters of Science degree in Aerospace Engineering at The University of Texas – Austin in 1989, Mr. Hirshorn began his NASA career at the Johnson Space Center in Houston, TX, joining the ranks of Space Shuttle flight controllers in the eponymous Mission Control. Serving as an EGIL, Mr. Hirshorn supported 55 Space Shuttle missions on console over the next eleven years, including ten launches and landings, on some of the Space Shuttle Program's most historic missions. Working side-by-side with many of the Mission Control "fore fathers", veterans of the Apollo Moon landing missions who were approaching retirement, Mr. Hirshorn was able to gain from the experience and wisdom of these space-age greats.

From 2001-2006, Mr. Hirshorn moved on to technical management responsibilities as the Mission Operations Directorate (MOD) representative to the Space Shuttle's Orbiter project, and from 2006-2011 as the MOD Lead Engineer for the Constellation Program. Both roles necessitated representing all of the shuttle flight operations community to larger elements within NASA.

At the end of both the Shuttle and Constellation Programs, Mr. Hirshorn moved to NASA HQ, first serving as the Systems Engineering & Integration Manager in one of the ARMD's aeronautics research programs. In 2013, Mr. Hirshorn transferred to the Office of Chief Engineer, first serving as Deputy Chief Engineer for both ARMD and the Space Technology Mission Directorate (STMD) before becoming ARMD Chief Engineer. In this capacity, Mr. Hirshorn has led efforts to better align NASA's R&T governance with program and project implementation. Mr. Hirshorn is also responsible for NASA's Systems Engineering (SE) policies, and continues to investigate the role of SE in R&T.

Mr. Hirshorn resides in pastoral Mt. Airy, MD, with his wife, four cats, two koi ponds and various other critters. Beyond a lifelong passion for spaceflight, Mr. Hirshorn also enjoys mountaineering and painting.

Mr. Guy T. Kemmerly

Analytical Mechanics Associates, Inc

Technical Writer

BS, Aerospace Engineering from Virginia Tech
MS, Flight Sciences from GWU

Mr. Kemmerly worked for NASA at the Langley Research Center from 1979 to 2016. Presently, he works for Analytical Mechanics Associates at the NASA Langley Research Center as a Technical Writer. He began his career conducting subsonic aerodynamic research on military configurations and on a new Supersonic Civil Transport. During this time, he developed a new test technique for modeling aircraft in ground effect. He has also supervised branches that developed new test techniques and other research tools that support ground-based testing. He was the Manager of NASA's Small Aircraft Transportation System Project and of NASA's Airportal Project, both aimed at moving people and products more efficiently and, near the end of his NASA career, was the acting Deputy Director of the Langley Aeronautics Directorate and the New Business Development Manager for Langley Aeronautics. In 2017, he became a Technical Writer with Analytical Mechanics Associates primarily supporting research teams working with the NASA Engineering and Safety Center.