Balancing Public & Private Partnerships for Future Human Spaceflight

JOHN J KENNEDY
12/3/2018

Table of Contents:

1.0 Introduction:

Privatization is key to America's current and future interests in Space and is consistent with the 2010 Title 51 ''National Aeronautics and Space Act'' which states "COMMERCIAL USE OF SPACE.—Congress declares that the general welfare of the United States requires that the Administration seek and encourage, to the maximum extent possible, the fullest commercial use of space."[1] With this thought in mind, this paper discusses several key considerations when entering into a Human Spaceflight Public/Private partnership, with particular attention to the engineering team engagement.

NASA's historically develops technology and capability in areas that are not commercially profitable but can enable future commercial opportunities. By leveraging the experiences and lessons learned from the past, we can improve our opportunities for success in the future. We have made great strides in these areas, but there is significant room for improvement.

2.0 Purpose/Objective:

This paper intends to highlight many of the thoughts and considerations, which are necessary when developing a public/private partnership for "*Human Spaceflight"*. Although this paper is being developed with an emphasis on "Human Spaceflight", many of the thoughts may have applicability to un-crewed missions. This paper does not attempt to define specific lines between government and private entities, since those lines vary based on many factors such as allocation of roles, responsibilities and accountabilities between participants and risk tolerance for both safety of flight and mission success. It should be recognized that "Safety of Flight" and "Mission Success" are two very separate and distinct areas of consideration, particularly when dealing with Public/Private partnerships. In this context, "Safety of Flight" focuses on potential failures or performance deficiencies that can result in loss of life or a permanent disability injury, while "Mission Success" addresses deficiencies that can prevent successful completion of key mission requirements and objectives.

3.0 Models in the Past / Present / Future:

The use of a joint Public/Private partnership between NASA and the Private Industrial community is not a new concept and dates back to the beginning of the U.S. Space Program. Previously flown U.S. spacecraft were products of private industry Design, Development, Testing and Evaluations (DDT&E). The levels of government technical and programmatic involvement has been the changing variable in the different models used in the past. The balance between insight and oversight (as defined in section 6.0)

[1] Public Law 111–314 : 111th Congress; "ENACTMENT OF TITLE 51—NATIONAL AND COMMERCIAL SPACE PROGRAMS" https://www.nasa.gov/sites/default/files/atoms/files/public_law_111-314-title_51_national_and_commercial_space_programs_dec._18_2010.pdf page 5 –section (C) [cited 18 December 2010]

has varied from program to program. NASA's engineering teams, have historically been deeply involved in the technical design and development commensurate with the level of safety and mission success risk involved in a specific project.

More recent models are taking on a particularly different flavor in several key aspects. In the case of the Commercial Crew Program (CCP), the government is procuring a service (or a ride) on a privately owned and operated transportation system. This is a significant departure from previous models which were based on the government owning and operating the space transportation system, with support from the private sector. This newer model carries with it a significant reduction in the NASA/government engineering engagement and penetration into the vehicle Design, Development, Testing and Evaluation (DDT&E). This reduced engagement and penetration limits the NASA engineering teams level of support for the Certification of Flight Readiness endorsement (commonly referred to as CoFR). The CoFR process focuses on ensuring that all elements involved in a particular flight/mission are ready to proceed with launch. Key to this process is the review and focus on "Safety of Flight" and "Mission Success" as it relates to the particular flight/mission under review. As was previously noted, "Safety of Flight" focuses on potential failures or performance deficiencies that can result in loss of life or a permanent disability injury, while "Mission Success" addresses deficiencies that can prevent successful completion of key mission requirements and objectives.

For CCP, the engineering CoFR is limited to the Safety of Flight areas where data has been reviewed, and does not address Mission Success. While the Safety of Flight is a shared responsibility, the accountability for mission success rests solely on the private company and the NASA Program Management. The CCP relies heavily on a concept known as "Shared Accountability" where in theory, the accountability for success and/or failure is shared between the government and private entity (see figure 3-1). The definition of shared accountability has continually evolved as the CCP has matured. Per the CCP Program Certification Plan (CCT-PLN-2000)[2], shared accountability is defined as "… under a shared accountability model between NASA and the Commercial Provider. The Commercial Provider is responsible for the design, development, test, and evaluation (DDT&E) which supports their assertion of meeting the CTS (*Crew Transportation System)* requirements and NASA is responsible for approving the compliance evidence to NASA's requirements. This presents a significant challenge in the NASA engineering team's reasonability for endorsing safety of flight while not having an oversite and approval role in the design certification. The CCP Program has decided to address this by assigning NASA levied requirements to NASA program office personnel who then in turn must approve the Verification Closure Notices (VCN's) submitted by the commercial provider to support their assertion of satisfying NASA requirements. In the case of several specifications and standards, those owners and VCN approvers may be NASA engineering team members in support of the program approval authority. These VCN's reference analysis, test, similarity and inspection to differing levels of fidelity in supporting their assertions of requirements compliance. In some cases, the testing referenced in these VCN's may, or may not,

[2] CCT-PLN-2000, Rev_A-NASA Crew Transportation System Certification Plan, Section 3.0, p-7

have been witnessed by NASA engineering team members. The analysis referenced will have varying levels of detail and fidelity. This presents unique challenges in attempting to establish consistent expectations across multiple system and technical disciplines.

In addition to the VCN review and approval process, the NASA program employed the review and approval of "Hazard Reports" as a means to assess safety of flight. Hazard Reports (HR's) are a tool used by various NASA programs to identify and analyze potential risk situations caused by an unsafe act or condition, from a top down perspective. The reports identify the hazards, note the controls used to address the hazard, and define the method of verification of these controls. In the case of CCP, Hazard Reports are presented and reviewed in a forum knowns as the Safety Technical Review Board (STRB) which is chaired by the NASA Program office representative and supported by various organizations including engineering, safety and flight operations. Since NASA involvement in system/subsystem design reviews has been limited to submitting comments for the partner's consideration, the Hazard Review process took on additional significance as a tool to identify design non-compliance and drive necessary design changes where the risk was deemed unacceptable. The timing of the Hazard Review process occurred late in the design cycle, so it's benefit of informing the design in a timely manner was challenging.

The CCP program briefing to the NASA Headquarters offices (including the NASA Administrator) conducted in June of 2015, helped define NASA's proposed engagement in the CCP partnership. The diagram in figure 3-2 was used to provide a graphic representation of the programs planned level of engagement for mission success. Although not explicitly stated, it is reasonable to assume the commitment for safety of flight would be even greater than the level identified for mission success. As noted previously, the engineering CoFR is limited to safety of flight and does not address mission success. Also note the commercial crew selection announcement[3] (September, 2014) stated "NASA's expert team of engineers and spaceflight specialists is facilitating and certifying the development work of industry partners to ensure new spacecraft are safe and reliable."

As difficult as it can be to reconcile these statements to clearly define and understand the government's involvement, it has been equally challenging to the technical workforce to reconcile their roles, responsibilities, and accountabilities. These challenges and varying levels of interpretation were clearly displayed during the development of the engineering CoFR statements and expectations in 2017.

Clearly and explicitly defining the various roles and responsibilities for both government and contractor teams must be addressed early in the program/project formulation phase in order to avoid a numbeous issues including communication and data exchange requirements. Establishing these ground rules, along with clearly defining the project/program risk posture, is critical to enabling the public/private partnership teams to maximize their efficiency and effectiveness.

[3] NASA Press release 14-256: "NASA Chooses American Companies to Transport U.S. Astronauts to International Space Station"
[https://www.nasa.gov/press/2014/september/nasa-chooses-american-companies-to-transport-us-astronauts-to-international] [cited 16 September, 2014]

Figure 3-1[4]

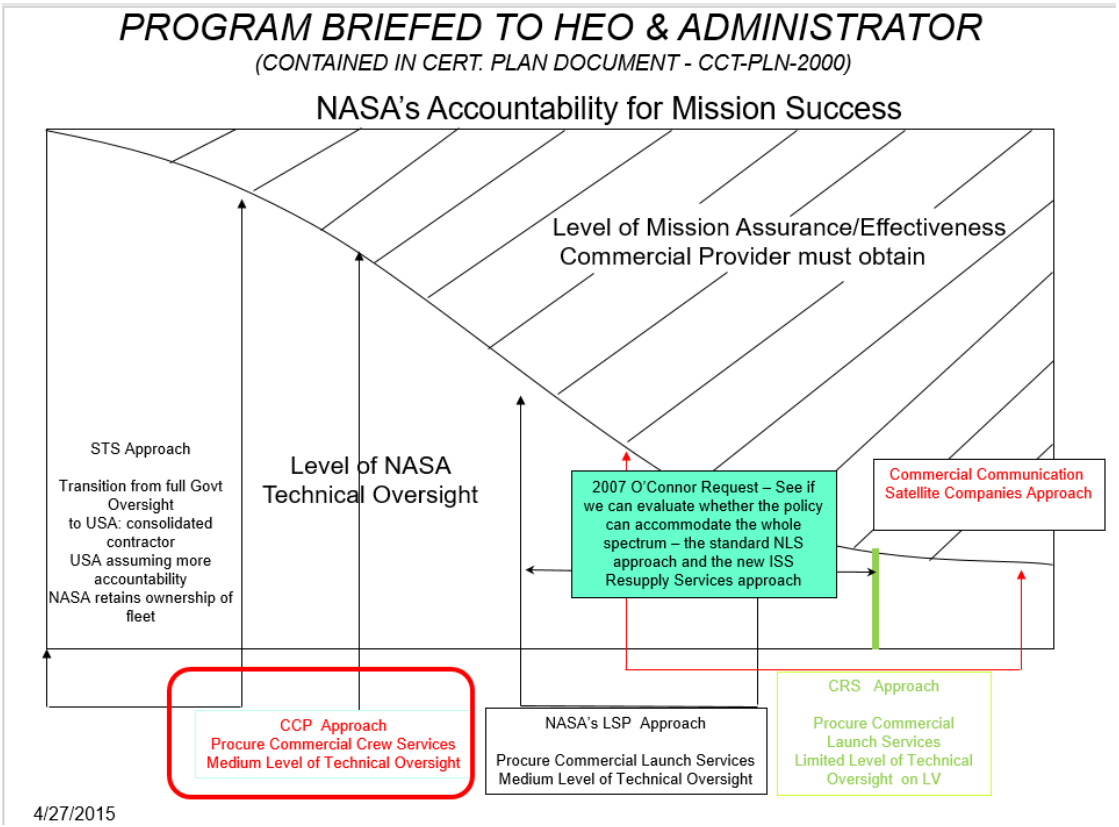


Figure 3-2

4.0 Differences in Consequences for Crewed and Un-Crewed Missions:

In evaluating Public/Private partnerships for human spaceflight, it is important to note the differences in consequences between crewed and un-crewed flight. Since "Risk" is the product of probability x consequence, a higher consequence carries with it a higher level of risk. This is often a point

[4] CCT-PLN-2000, Rev_A – NASA Crew Transportation System Certification Plan, Section 3.0, p-7. [cited 11 February 2016].

of contention between those that have been engaged in human spaceflight and those that are new and/or are coming in from the cargo or satellite community. Occasionally the statement is made "…but it's good enough for cargo…" Good enough for cargo is not however good enough for crewed flights. While many satellite launches carry extremely important and expensive pieces of equipment, the consequences of their failure do not measure up to the consequences of losing a crew. Never have we seen a period of national mourning for the loss of a satellite, nor have we flown our flags at half-staff for such an occurrence. Losses of crewed flights are extensively addressed in media coverage and front-page press headlines for months, whereas coverage of a satellite loss may or may not make the headlines and will disappear or be quickly relegated to back page articles. United States crewed vehicle losses also result in presidentially appointed accident investigation committees and the associated system down time measured in years versus the un-crewed failures, which require no such investigation and oversight, often resulting in recovery time on the order weeks to months.

Human Spaceflight Accident & Recovery			
Incident	**Incident date**	**Next Flight**	**Next Flight Date**
Apollo 1 Fire	1/27/1967	Apollo 7	10/11/1968
Challenger Accident (STS-51L)	1/28/1986	STS-26	9/29/1988
Columbia Accident (STS-107)	1/16/2003	STS-114	1/26/2005

Figure 4-1[5]

Un-crewed Spaceflight Accident & Recovery			
Incident	**Incident date**	**Next Flight**	**Next Flight Date**
Titan IV A-20	8/12/1998	Titan IV B-27	4/9/1999
Titan IV B-27	4/9/1999	Titan IV B-32	4/30/1999
Titan IV B-32	4/30/1999	Titan IV B-29	5/8/2000
Delta III 259	8/27/1998	Delta III 269	5/5/1999
Delta III 269	5/5/1999	Delta III 269	8/23/2000
Falcon F9-19 (CRS-7)	6/28/2015	Falcon F9-20	12/22/2015
Falcon F9-29	9/1/2016	Falcon F9-29	1/14/2017

Figure 4-2[6][7][8]

[5] NASA – Mission Information (Space Shuttle) www.nasa.gov/mission_pages/shuttle/shuttlemissions/index.html [cited 29 August 2011]
[6] Wikipedia – List of Falcon 9 and Falcon Heavy Launches - https://en.wikipedia.org/wiki/List_of_Falcon_9_and_Falcon_Heavy_launches [cited 3 June 2018]
[7] GlobalSecurity.org – Space – Titan-4 Launch History https://www.globalsecurity.org/space/systems/t4table.htm [cited 21 July 2011]
[8] Space Launch Report : Delta III Data Sheet - http://www.spacelaunchreport.com/delta3.html [cited 5 September 2010]

Previous Human Spaceflight programs have emphasized this different in their reference to system criticality. In the case of the Space Shuttle, Criticality 1 was the highest level and was reserved for Loss of Crew or Vehicle, which in the case of the Shuttle program, loss of vehicle would reflect the loss of 25% of the programs future capability and carry the risk of program termination. Criticality 2 was related to Loss of Mission. Significantly, more effort, energy and resources were expended on Criticality1 items than Criticality 2 or Criticality 3.

Criticality Categories. / Category Definition (Per NSTS 22254 - Methodology for Conduct of Space Shuttle Program Hazard Analysis)[9]

1 **-Loss of life or vehicle.**

1R -Redundant hardware element the failure which could cause loss of life or vehicle.

1S - Potential loss of life or vehicle due to failure of a safety or hazard monitoring system to detect, combat, or operate when required.

2 **- Loss of mission**; for GSE, loss of vehicle system.

2R - Redundant hardware elements the failure of which could cause loss of mission.

3 **- All others.**

In some cases, the consequence associated with un-crewed flight are mitigated by procuring spares, such as the two National Reconnaissance Office (NRO) satellites kept in storage in Rochester New York and offered as surplus to NASA in 2012[10]. This concept is also reflected in the DoD Broad Area Review (BAR) findings, which noted, "Given the historical record, satellite constellation planning and budgeting based on 100% launch success (no spares) is unrealistic."

As to the comparison of high level accident investigations, perhaps the closest un-crewed flight investigation would be the "Broad Area Review"[11,12] (BAR) initiated by the President and Secretary of Defense following a string of Titan IV and Delta III failures. The BAR culminated in a final report completed in November 1999. The failures addressed in this report were heavily influenced by the transition of the governments Oversite-Insight role, which is further addressed in section 5.1.

[9] NSTS 22254 Methodology For Conduct of Space Shuttle Program Hazard Analysis F−4 CHANGE NO. 15 Revision B - Retired (Final Version)

[10] Joel Achenbach "NASA gets two military spy telescopes for astronomy" The Washington Post, URL: https://www.washingtonpost.com/national/health-science/nasa-gets-military-spy-telescopes-for-astronomy/2012/06/04/gJQAsT6UDV_story.html?utm_term=.e72af0ef8eb7 [cited 4 June 2012].

[11] Maj Gen Ellen M. Pawlikowski (USAF) "Mission Assurance – A Key Part of Space Vehicle Launch Mission Success", Air Force Space Command – High Frontier – Journal, URL: http://www.nro.gov/news/articles/2008/2008-05.pdf [cited 26 August 2008]

[12] General Thomas S. Moorman, Jr (USAF, retired) "Framing the Assured Access Debate: A Brief History of Air Force Space Launch". Air Force Space Command – High Frontier – [online Journal], Vol 3, No. 1 URL: http://www.afspc.af.mil/Portals/3/documents/HF/AFD-061128-043.pdf [cited 21 November 2006]

5.0 Lessons Learned:

The content of this paper is based on experiences and lessons learned from direct participation in multiple programs including, but not limited, the Space Shuttle, International Space Stations (ISS), Orbital Space Plane, Constellation, Orion, and Commercial Crew Programs. There are however, several specific cases where lessons learned have been extensively studied, reviewed and documented. The following subsections touch on three of these areas. Links are provided to the reports and findings, which will allow for a more thorough review and appreciation than can be properly conveyed in this paper alone.

5.1 Department of Defense (DoD) Expendable Launch Vehicle Broad Area Review (BAR):

In the late 1990's, five (5) launch vehicle failures occurred over a 10 month period, consisting of three (3) Titan IV's and Two (2) Delta III's (5 failures in 25 launches) This fell on the heels of a change in acquisition strategy, an upcoming end to some key launch vehicles and sharp reductions in government engagement and oversite. The resultant launch failures prompted the President to task the Secretary of Defense with conducting a detailed review to identify the failure causes and to produce recommendations for changes to prevent reoccurrence. This 1999 Broad Area Review (BAR) provides a unique opportunity to see an actual example of what can happen when a significant change in culture and reduction in government technical engagement is applied and how it can/has resulted in a series of launch failures. It is often easier to talk and accept major changes in Roles and Responsibilities (R&R's) and levels of government technical engagement when operating in the theoretical "space" (unencumbered by reality). The BAR provides an opportunity to see what can happen when reality is applied to a theoretical situation. This report provides information and insight based on past experience which can prove beneficial and should be taken into consideration when making major changes to the public/private partner relationships. That is not to say that we should not make changes and continue to evolve the partnership, but it does say we should recognize what can happen and put proper checks and balances to prevent reoccurrence of the experiences of the late 1990's. Recall the famous quote "Those who fail to learn from history are doomed to repeat it"[13]. It is for that reason that particular attention should be taken to review the lessons learned from this activity. The BAR noted that System design and process engineering deficiencies have played a key role in failures and near misses.

Some of the key takeaways from that activity include, but are not limited to, the following excerpts:

- Systems Engineering required strengthening to reflect a more disciplined approach.
- Clear authority and accountability are necessary.
- Maintaining engineering and technical support expertise is critical.
- Process discipline is necessary.

[13] Nicholas Clairmont, "Those Who Do Not Learn History Are Doomed To Repeat It. Really?" URL: http://bigthink.com/the-proverbial-skeptic/those-who-do-not-learn-history-doomed-to-repeat-it-really

- Independent reviews are essential.
- Mission success is both a process and a culture.
- Mission assurance includes a disciplined application of systems engineering, risk management, quality assurance and program management principles.
- Risk management processes and practices degraded over time and needed to be re-emphasized.
- All technical issues need to be assessed and resolved with residual risk assessed and accepted or mitigated.
- An in-depth review and validation of launch vehicle design should be conducted.
- An in-depth review of manufacturing and preparation should be conducted.
- Independent technical assessment of the system design should be conducted to increase confidence that no issues have been missed or incorrectly dispositioned.
- The government needs clear visibility into the change control process.
- The government needs clear visibility into the technical and Independent Verification & Validation (IV&V) baselines to ensure being a smart and involved customer.
- A "…third set of eyes to ensure the contractor's and program office's technical and quality assurance processes have been adequately performed and all significant mission risks have been independently assessed…" is critical.

5.2 Challenger Accident:

A Flight Readiness Review (FRR) for STS-51-L was conducted on January 15, 1986 in preparation for the upcoming flight of the Space Shuttle Challenger (OV-99). The highlights of the planned 7-day mission were to include deployment of two satellites and two live teaching lessons telecast from the 1st "Teacher in Space", Ms. Christa McAuliffe.

Liftoff occurred on the morning of January 28, 1986 at 11:38 AM Eastern time. 73 seconds after liftoff, the vehicle was engulfed in an "explosive burn" resulting in the loss of the Orbiter Vehicle and her crew of seven.

In response to this incident, President Reagan announced the formation of a commission on February 3rd to investigate the accident. Executive Order 12546 required the commission to:

1) Review the circumstances surrounding the accident to establish the probable cause or causes.

2) Develop recommendations for corrective or other action based upon the commission's findings and determinations.

The Presidential Commission on the Space Shuttle Challenger Accident (aka. The Rogers Commission, named after the commission chairman Mr. William Rogers) generated a 261 page report[14] on the matter. The commission concluded that the physical cause was a failed seal in the joint between the two lower segments of the solid rocket booster. This design flaw resulted in a flame from the SRB's impinging on the external tank. This impingement initiated a series of events beginning with a breach of the external tank, allowing the hydrogen fuel to flow overboard thereby increasing the intensity of the flame emanating from the SRB. This flame then impinged on the SRB lower structural attachment to the external tank, which resulted in the attachment structural failure. From there the SRB rotated into the external tank damaging the tank structure and causing rupture of the fuel and oxidizer elements, creating a massive fireball. The commission also concluded that "The decision to launch the challenger was flawed" (chapter V, para 1) and noted several institutional and process issues that contributed to the accident. The commission's report noted several issues, including (but not limited to) the following:

- Project management failed to provide full and timely information related to safety of flight to program management. These failures in communication resulted in decisions being made based on incomplete and sometimes misleading information. This resulted in a conflict between engineering data and management judgement. The commission recommended NASA take action to eliminate this tendency. Additionally, they recommended recording of Flight Readiness Reviews and Mission Management Team meetings.
- Installation, test, and maintenance procedures must be especially rigorous for items designated criticality 1 (loss of crew). The commission recommended NASA establish a system of analyzing and reporting performance trending of such items. Additionally, they recommended NASA develop and execute a comprehensive maintenance inspection plan.
- Relentless pressure on flight rate. The commission noted that this concern might have been adequately handled if NASA insisted on thourough procedures that were "…hallmark during the Apollo program". The commission recommended NASA establish a flight rate that is consistent with the supporting resources.
- Level II management was unaware of Level III safety, operational and flight schedule issues. The Marshall Space Flight Center (MSFC) monthly problem reports were not distributed to Level II management. The commission recommended an independently staffed (workforce independent of other NASA functions and program responsibilities) SR&QA office to take responsibility for documentation of problems, problem resolution and trending associated with flight safety.

[14] Report to the President By the Presidential Commission on the Space Shuttle Challenger Accident, https://history.nasa.gov/rogersrep/genindex.htm [cited 6 June 1986]

- Problems, and reoccurrences of problems, can be prevented with an accurate reporting, analysis, and testing program. They noted an "…effective program, reporting, testing and implementation of corrective measures must be fully documented." Additionally, they noted that for criticality 1 equipment anomalies, communication must reach all levels of management.

As part of the investigation process, the Space Shuttle Program Manager (Arnold Aldrich) noted several communication and organizational failures during testimony with the commission on April 3rd, 1986. These included:

- A lack of problem reporting requirements.
- Inadequate trending analysis.
- Misrepresentation of criticality.
- Lack of involvement in critical decisions.

The commission noted that a properly staffed and robust safety organization might have avoided these faults and eliminated the communications failures.

NASA in turn generated a series of responses to the commission's report and findings[15]. Both detail design changes and institutional changes were noted, including, but not limited to, the following:

- Implement changes in the Program management structure to improve lines of authority and communication.
- Review all criticality 1 waivers.
- Reviewed all Failure Modes and Effects Analysis (FMEA's) and Hazard Reports (HR's).
- Removed reliability and quality assurance from engineering and combining them with the Safety Organization
- Implemented a series of System Design Reviews (SDR's) to understand all instances of in-flight anomalous behavior and failures related to mission critical flight hardware. This included design issues, test issues, pre-launch operations issues, in-flight anomalies, post flight inspections and analysis, and any other design or operations assessments.
- Re-emphasis that engine limits testing and malfunction testing are required to properly characterize engine margins.
- Increased emphasis on fracture mechanics analysis relative to engines with emphasis on turbopump blade cracks.
- Establishment and designation of critical processes for production of critical items (crit 1). Also, emphasize to primary and secondary suppliers the criticality of the item associated with their production process.

[15] Report to the President – Actions to Implement the Recommendations of The Presidential Commission on the Space Shuttle Challenger Accident https://history.nasa.gov/rogersrep/actions.pdf [cited 14 July 1986]

- Related to return to flight, “NASA will not permit “pressure to launch” or any other form of schedule pressure to compromise flight safety.”
- The safety organization will provide oversight to include evaluation of operating practices such as safe overtime rates.
- Conducted a total review and implemented changes to the risk management system, recognizing it as a continuous process assessing safety, performance, cost, and schedule, “…but safety is the primary consideration.”
- Waiver approvals to include a thorough review of the rationale for the original criteria, the nature of the violation and potential consequences.
- Process changes to ensure Configuration Management effectively assures all hardware changes are done in a safe and reliable manner.
- Etc…

5.3 Columbia Accident:

Unfortunately, the Challenger incident was not to be the only accident to occur during the life of the Shuttle Program. On the morning of February 1, 2003, we again faced the loss of a crew and vehicle. This time the incident did not involve the launch vehicle or ascent phase of the mission, but instead occurred during the Orbiter Vehicle Columbia (OV-102/STS-107) re-entry in preparation for landing. Communication with the Orbiter was lost at 8:59 am followed by Shuttle contingency plan engagement shortly after the planned landing time of 9:16am.

As with the loss of Challenger, an investigation team was established. This team is referred to as the Columbia Accident Investigation Board (CAIB). The board concluded that the physical cause of the accident was due to external tank thermal foam insulation separating from the external tank, impacting and structurally failing the left wing leading edge. This compromised the wing thermal protection system and led to a catastrophic failure of that Thermal Protection System (TPS). As with the Challenger accident, a number of recommendations (29) related to both specific design characteristics and program management practices were presented to the President[16]. The board noted, “We are convinced that the

[16] Columbia Accident Investigation Board, https://history.nasa.gov/columbia/CAIB_reportindex.html [cited August 2003]

management practices overseeing the Space Shuttle Program were as much a cause of the accident as the foam that struck the left wing." Their recommendations include, but are not limited to, the following:

- For ISS missions, there should be a capability to inspect and effect emergency repairs to the Thermal Protection System (TPS).
- Maintain a flight schedule that is consistent with the available resources. Deadlines must be regularly evaluated to ensure any additional risk incurred to meet schedule are recognized, understood and accepted.
- Form an independent Technical Authority responsible for technical requirements and waivers for those requirements. This Technical Authority will build a disciplined and systematic approach to analyze and control hazards.
- The Technical Authority should be funded directly from NASA Headquarters and separate from the Shuttle Program. The Technical Authority should have no responsibility for schedule or program costs.
- NASA Headquarters Office of Safety and Mission Assurance should have direct line authority over the program safety organization and should be independently funded.
- Digitized close-out photo images should be immediately available for on-orbit trouble shooting.

6.0 Roles, Responsibilities, and Accountabilities (RRA's):

Clearly defining the Roles, Responsibilities, and Accountabilities (RRA's) for the engineering team, is critical to establishing the appropriate working relationship between NASA and the private entity. Defining RRA's related to key characteristics, provides the foundation necessary to establish the levels of engagement on the part of both NASA and the private entities. This helps to inform the levels of insight and oversight required. Delineation for who is in charge of what aspects of the partnership must be clearly defined and documented. Where does the government have a role of insight, and where does it have a role of oversight? In this context, Insight is having clear understanding and awareness of the issues, situations and activities worked by the provider without having authority and responsibility to direct and manage those activities. Oversight is having responsibility with authority to direct and manage work.

Too often, the establishment of these defining characteristics are considered "forward work", thereby deferring any clear decision making and instead waiting to see how it "works itself out". This has led to conflicts in communication and data exchange. In some cases, the private entity does not wish to be encumbered by responding to what they see as unnecessary requests for information and has responded on occasion with statements that the government does not need that data. On the receiving end, the NASA engineering team focuses on what they believe are their accountabilities for endorsing/certifying the design and endorsing the mission/flight through the Certification of Flight Readiness (CoFR) process. These endorsements and certifications cannot be properly supported without the appropriate data and related insight. The technical insight provided and documented in the

engineering CoFR is key to ensuring Program and Agency management has the information necessary to make an informed decision on the readiness to proceed with a specific flight/mission.

The sections that follow provide a description of some key areas requiring attention in establishing the partnering arrangements. The detailed specifics for each of these topics will be governed by the RRA's established by the specific Program/Project.

6.1 Rules of Engagement

As the RRA's are established, it is important to address the rules of engagement for meeting these expectations, and provide a framework to help guide the workforce. This next level of detail is critical to taking generally broad statements on RRA's and breaking them down into executable direction at the detailed technical engagement level.

As the NASA Administrator noted in a recent Town Hall meeting at the Johnson Space Center (JSC) [August 2nd, 2018]. NASA's expectation is for the NASA engineering technical team to be embedded with the commercial provider. He noted this is necessity to ensure the government maintains a "Smart Buyer" position.

In order to be compliant with these expectations, both the RRA's and rules of engagement at the basic engineering technical level need to be defined, established, and mutually agreed to early in the projects/programs development. These rules of engagement must include, but are not limited to, the following:

- Establishing guidelines and expectations for day-to-day technical interchange. Are there regular and unregulated technical exchange between private entity engineers and NASA technical experts? Are there limits on this technical interchange and if so, what are those limitations?
- Identify what rules will be applied at design reviews. Are issues/concerns identified by the NASA technical expert treated as comments and suggestions, or are they treated as formal documented issues/concerns requiring written technical based responses with rationale and forward work action plans?
- What are the rules for NASA government insight into the various vendors and sub-tier vendors?
- What standard meetings and technical forums will be established for interactions? What will be the frequency and schedule for such forums?
- What insight will NASA technical experts have into the providers Problem Reporting And Corrective Action (PRACA) reporting system? Will there be some type of filter on what items are elevated to NASA or will all items be available for review? What if any items will require NASA approval ?
- What will be the NASA role in failure investigations? Will NASA technical experts be active in the investigation or will they be limited to reviewing summary reports following a provider investigation?

- How will risks and risk management be treated and shared between the provider and the government team? Who will be authorized to create and close out a risk in the system?
- How will Unexplained Anomalies (UA's) be treated and what role does the government have in authorizing the mission to proceed with open UA's.
- What if any role does the engineering technical team have in endorsing a Certification of Flight Readiness (CoFR)? Are they certifying the system are good to go forward for flight based on an in-depth knowledge of the system and its current state? Are they endorsing based on a limited set of information they have been provided? Is their endorsement limited to safety of flight or are they endorsing for mission success as well?
- Etc…

The above list represents just a few of the many areas which require the establishment of clear rules of engagement early in the project/program development.

6.2 Certification of Flight Readiness (CoFR):

The impact and effect of variations in Roles, Responsibilities, and Accountabilities for crewed flight vehicles can be seen when comparing the differences in engineering CoFR endorsements between the Space Shuttle, Commercial Crew, and Orion Programs. Each of these programs relies on a government and private industry partnership, but each has a very different set of RRA's, which can be seen in the variations in breadth and depth for the CoFR related areas of emphasis.
Figure 6-1 shows an abbreviated and compressed representation of how these differences manifest themselves in the government's engineering CoFR engagement. The figure is based on a 2017 comparative assessment for the spacecraft portion of the architectures.

In the case of the Commercial Crew Program, a comparison between the actual engineering engagements is significantly different from the "NASA Accountability for Mission Success", captured in figure 3-2 and shared with senior management in 2015. While figure 3-2 indicates a significant accountability for NASA related to mission success, the NASA engineering Certification of Flight Readiness (CoFR) endorsements are limited to safety of flight and do not address mission success at all. Clear definition and delineation of RRA's early in a project/program are key to guiding and maintaining consistent expectation at all levels throughout the project/program life cycle.

CoFR/Endorsement Statement	Review/Concur			Audit/Surveillance			No Task			Notes
	SSP	CCP	MPCV	SSP	CCP	MPCV	SSP	CCP	MPCV	
Requirements Compliance		Less thorough than MPCV								**CCP** requirements compliance limited to fligth safety, not mission success. Addresses Hundreds of requirements for **CCP** vs Thousands of req for **MPCV**.
Certification		Less thorough than MPCV								**SSP** had comprehensive prime and sub-vendor penetration/insight to process changes. **SSP** reviewed all Rockwell analysis, extensive IV&V, independent review methods - assumptions - qualitative checks comprehensive and comprehensive independent analysis. **CCP** Enginering Approve Design Construction Standard Certification changes…reviews CCP 1100 series requirements compliance. Limited insight to sub-vendors. **MPCV** has less insight to sub vendors than SSP, but greater insight than CCP **MPCV** spot check prime methodology - significant NASA analysis checks and in-line analysis work for prime.
Risk Management										**SSP** had comprehensive prime and sub vendor penetration/insight to identify and track risks. **CCP** Enginering has insight to provider risk system and risk awareness based on varying levels of provider penetration/insight. - Limited insight to sub-vendors **MPCV** has insight to prime risks but less insight into sub vendor risks.
Hazard Reports/Analysis										For **SSP**, the main role reside in S&MA. Engineering engages as necessary. **CCP** detailed involvement in Hazard report review, but not involved in hazard analysis review. **MPCV** tracks verification of controls - flags verification controls for tracking
Acceptance Plans		Less thorough than MPCV								**CCP** does not review individual ADP's as part of CoFR. Ensure process is properly defined and validate implimentation as part of the design phase. **MPCV** has CE dedicated to production and production activities.
Anomaly Resolution		Less thorough than MPCV								**CCP** one provider challenged with concept of working resolution to root cause. Mitigates to most probable causes. **MPCV** has extensive engagement in Anomalies resolution. Looks at all PRACA items (Safety & Mission success - form-fit-function) - Provided "Q-notes" from provider and review list every week. Engr Sign @ PMRB (Engr-Prgm-Safety). Break req. => PMRB & waiver. CE discretion to add item to PMRB as they see fit.
FMEA										**SSP** required FMEA's and these were reviewed by engineering. **CCP** does not require FMEA deliverables. Expectation is to review available FMEA's. **MPCV** reviews all FMEA's.
Mission - Flight Specific requirements										
Mission Operations, Flight Rules, LCC										
Production Insight	**NA**		**Yes** See Note							**SSP** deep control of prime and sub-vendor change control during veicle build - Re-used vs new production vehicle per flight for SSP. **CCP** focus on PAA (Product Asurance Activites) - Risk Based Assessment (RBA). **MPCV** Engineering deep contorl of prime, with less sub vendor control than SSP. **MPCV** assigned production CE CoFR required.
Flight Software		Less thorough than MPCV								**MPCV -** NASA involved in code coverage - NASA embedded in LM SW development team. NASA review LM SW. West Virginia IV&V used for program. SW partner with in HW mgr, integration mgr. Review infrastructure loading and test cases.
Open Paper										
CHIT's (MER to Flt Control Center Info Exchange)		Under review	**Yes** See Note							**CCP** to provider interface still in development. **MPCV** CHIT Mechanism in development - will apply - will embed in CoFR statement.
Facility Certifications			Review							**MPCV** engagement risk based, less than SSP.
Vehicle Processing Changes			In work							
Limited Life Items			**NA**							
Packaging, Handling, and Transportation			**NA** See Note							**MPCV** engineering follows this through flight test element tracking - No CoFR statement item
Facilities are Ready to Support the Mission										GSDO CoFR and select **MPCV** engieering engagement.
Payload/Cargo Integration and Checkout			TBD							**MPCV** scope maturign to include this - CoFR update under review
Alerts/GIDEP										Review items identifed by S&MA as areas of concern
Trending Analysis			See Note							**MPCV** will do - not explicitly outlined in COFR- CoFR statement under review
Mass Properties			See Note							**MPCV** will do - not explicitly outlined in COFR- CoFR statement under review

Figure 6-1

6.3 Design Certification:

It is important to understand the difference between CoFR and Design Certification to avoid confusion and duplication of efforts. The “Design Certification” is a step that occurs prior to initiating the Flight Readiness Review process. At “Design Certification Review” (DCR) completion, the vehicle baseline design is “Certified”, meaning that requirements compliance have been successfully completed when measured against an established design baseline. All verifications activities (analysis, test, demonstrations and design related inspections) are successfully completed and the program/project is ready to apply this design to specific missions/flights. In reality, there are likely to be some remaining issues with forward work and actions coming out of a DCR, but in general, the design has been established and verified. The CoFR plan leverages the assurance provided in the DCR process and addresses changes and/or updates in the vehicle design and certification subsequent to establishing the vehicle certified baseline. The Engineering CoFR and related Flight Readiness Review (FRR) process provides the technical assessment on readiness of the systems *for a particular flight/mission.* This would includes review of any unresolved issues or actions coming out of the DCR. In subsequent CoFR assessments and FRR cycles, only changes realized from the previous flights are reviewed from a vehicle design perspective. This CoFR review includes, but is not limited to, the following:

- Mission profiles and particular characteristics for the specific flight/mission under review.
- That particular vehicle production, build, and processing.
- Review of lessons learned from previous flights, including any in flight anomalies.
- Review Issues with vehicle design certification identified since last flight.
- Review changes to design certification since last flight or last certification review.
- Review those cases where the design certification and verification have not been completed but there is enough data and evidence to support a limited use for one or more flights. This is also referred to as a limited flight effectivity or limited flight certification..
- Review new discoveries of system performance and risks since the last flight.
- Review vehicle configuration changes since last flight.
- Review Changes in how we operate the vehicle since last flight (flight rules, envelope expansion, new capabilities, etc…).
- Review Key issues and their resolution status from last flight FRR.

The CoFR effort feeds into the FRR process, while the Design Certification Review (DCR) is used to establish the design “Certified Baseline.”

Here again it is critical to understand and establish the Roles, Responsibilities and Accountabilities for the various parties going into the Design Certification Milestone Review. This definition will drive the depth and breadth of the government engineering team involvement, which directly affects the level of engagement with the private entity and establishes the technical data exchange

requirements. Simple questions such as who is in charge of the milestone review and who has authority to approve or reject the assertions of successful design certification completion must be addressed. Is the government technical team responsible for:

- Signing off on the vehicle, system, subsystem and component certification?
- Providing an endorsement based on a limited set of information that has been provided directly to them?
- Providing an endorsement based on the information that has been made available for possible review?
- Substantiating the private entity certification, and what is meant by "Substantiation"?

Many questions affect the various parties engaged in the partnership. Failure to establish these Roles, Responsibilities, and Accountabilities early in the development of the partnering relationship will result in reduced team efficiencies, gaps in assignments of RRA's, and distract focus and attention from other key technical areas. Up-front definitization will minimize unnecessary conflicts and the related resolution forums that must be held to address these conflicts. As unpleasant as the question may be, when considering RRA's, the question of whom do we hold accountable when a bad day happens must be asked and addressed. Historically speaking, as we get closer to flight there is a tendency to broaden the accountability and ownership of risk. When formulating budget and staffing plans early in a program/project, it is often easy to rationalize why some areas can be minimized based on up front perspectives of who will be accountable for what. These perspectives and expectations are often re-visited and modified as we approach flight to broaden the accountability for the various risks.

6.4 Creating and Maintaining a Health Tension Environment:

"Healthy Tension" is a term used in the past to describe a relationship often between NASA/Government Supporting Institutions (Engineering, Health and Medical, Safety, Flight Operations, Flight Crew, Program Offices) and the private entity under contract. While all parties are engaged in providing goods and services to meet and exceed expectations for safety, performance, cost, and schedule, the weight of these pressures can be different on different parties and can bias their decision process in one direction or another. While everyone has a particular sensitivity to safety, the definition of what is "safe enough" can be strongly influenced by pressures of cost and schedule. This balancing act is challenging in a "Cost Plus" contract environment, and can be even more challenging in a "Fixed Price" contract environment. Historically, this push/pull between those emphasizing high ideals for safety and performance vs. those attempting to balance cost and schedule have resulted in meeting somewhere in the middle. This final resolution occurs after healthy technical discussion, which include impact assessments for the various option under consideration. These technical presentations in management decision forums include technical experts and the actual risk takers (astronauts) being heavily engaged in the discussions and final decision. When establishing RRA's, care should be taken to establishing and maintaining a healthy tension environment, as well as determining where the center of gravity should be to provide the most benefit to the project/program. It has proven to be a beneficial check and balance in past applications. This is particularly true when developing verification test programs where discussions

of cost versus benefits, and associated risk acceptance, regularly occur. These discussions evolve as new information is uncovered from post test data analysis. An example of this are evident in the initial definition and evolution of the parachute test programs for the current spacecraft under development.

Ensuring there is an engineering team separate and independent from the pressures of cost and schedule, working with another team that is not completely removed from the pressures of cost and schedule, can help establish a healthy tension environment. This can occur so long as both teams have the ability and authority to influence the DDT&E.

7.0 Risks and Risk Management:

Today's NASA engagement models use significantly less government provided resources when compared to those employed in past programs/projects. Proper application of a risk management system is particularly beneficial in determining where to apply these limited resources to buy down risks. It provides an opportunity to assess the cost vs benefits looking at the overall program/project risk posture. This comparison of risk across multiple areas and disciplines is key to providing program/project management with the information necessary to make a risk informed decision on where to accept risk and where to apply resources to further mitigate risk. A mutually agreed to, and well integrated, risk management system is key to ensuring all parties/partners have a clear understanding of the risks being accepted. This includes the criteria for accepting risks, and a mutual understanding of what is considered acceptable and/or unacceptable from a risk posture perspective.

It should go without saying that there is an inherent risk in human spaceflight. Space is a challenging environment, and one where we are still learning about the detrimental effects it can have on the human body. The lack of air to breath, the effects of zero gravity, extreme variations in temperature, effects of radiation, potential for micrometeorite impacts are just some of the environmental challenges that make human spaceflight an inherently dangerous endeavor.

These on-orbit effects are separate from the fact that in order to access space, one must ride on a set of massive fuel and oxidizer tanks which feed a prolonged series of contained and controlled explosions, focused in a particular direction, to provide the prolonged thrust necessary to achieve a desired orbit. These environmental effects can adversely affect a multitude of systems and piece parts necessary to safely reach orbit. Failure or off nominal performance can have catastrophic consequences for both safety of flight and mission success.

On the other side of the equation, the safest thing to do is to stay on the ground and do nothing, which is equally unacceptable. This leaves us in the position of regularly making decisions on the risks vs benefits in a consistent manner, across multiple systems and disciplines. This is often referred to as Risk Informed Decision Making, also known as RIDM. A more detailed discussion of RIDM can be found in the NASA Spaceflight Program and Project Management Requirements document (NPR 7120.5E), and the NASA Systems Engineering Handbook (NASA/SP-2007-6105, section 6.4.2.2). RIDM is applied when evaluating the design of components, subsystems, systems, and higher-level assemblies. We also make

risk vs benefit decision when defining our verification plans and strategies, including establishing the fidelity of analysis and test necessary to provide an acceptable level of confidence that the design satisfies the requirements. Balancing safety, performance, cost and schedule risks is challenging since reductions of risk in one area may lead to an adverse consequences in another. There should be healthy discussions between those pushing to maximize a test like you fly campaign, (a philosophy that maximizes the drive to make the test program as representative of the actual flight environment as possible) balanced by those looking to control cost and schedule. Again, this is where a healthy tension can be beneficial in driving out the pro's and con's necessary to make an informed decision. Both camps are key players is establishing the right balance of analysis, test, demonstration, checkout, and inspections while recognizing we do not operate within an unlimited budget and infinite timeline. Here again, the key is balancing the risk vs benefit in the decision making process.

We must be very clear on what defines a "Risk" and what "Risk management" means in practice. A Risk in NASA terminology is potential of a problem with negative consequences occurring. Managing risk is managing the potential for a problem to occur and/or managing the consequence of the problem occurrence, i.e. what steps and mitigations are going to be applied to avoid a potential problem from occurring or mitigating it's adverse effects. Mitigations may include things such as additional testing, addition of redundancy, design modifications, additional acceptance screening, etc…The higher the severity and the higher the probability of the risk occurring, the higher its ranked in a risk management system. We define Risk as the product of "Probability" and "Consequence" (Risk = Probability X Consequence). In ranking risks, we often use "Risk Scorecards" following the basic principles noted in figure 7-1 from section 6.4 of the NASA Systems Engineering Handbook (NASA/SP-2007-6105, rev 1). This diagram shows how we group risks into Low, Medium, and High categories based on how they are scored on the matrix. Note that the higher the severity/consequence of the risk, the wider the likelihood range to categorize it as a high risk. Figure 7-2 provides some additional context to the likelihood and consequences legends. This provides some general context for the ranking ranges, while Figures 7-3 and 7-4 show how these principles are applied to specific program ranking and scoring. Note that the program/project applies more specific and measurable values to the categories in the matrix. Using cost as an example, what may be a high dollar value for one program/project may not be as high a consequence for another program/project. In general, when dealing with safety related issues, a consequence of "5" is associated with loss of life, while permanent disability and temporary injuries may be ranked in the 3-4 category.

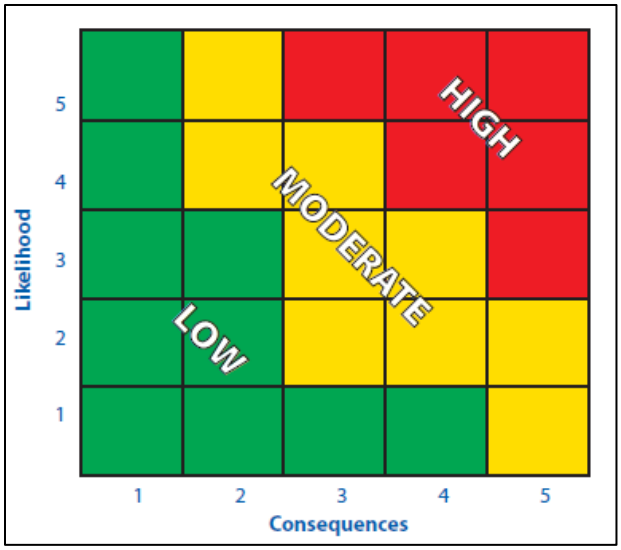


Figure 7-1[17]

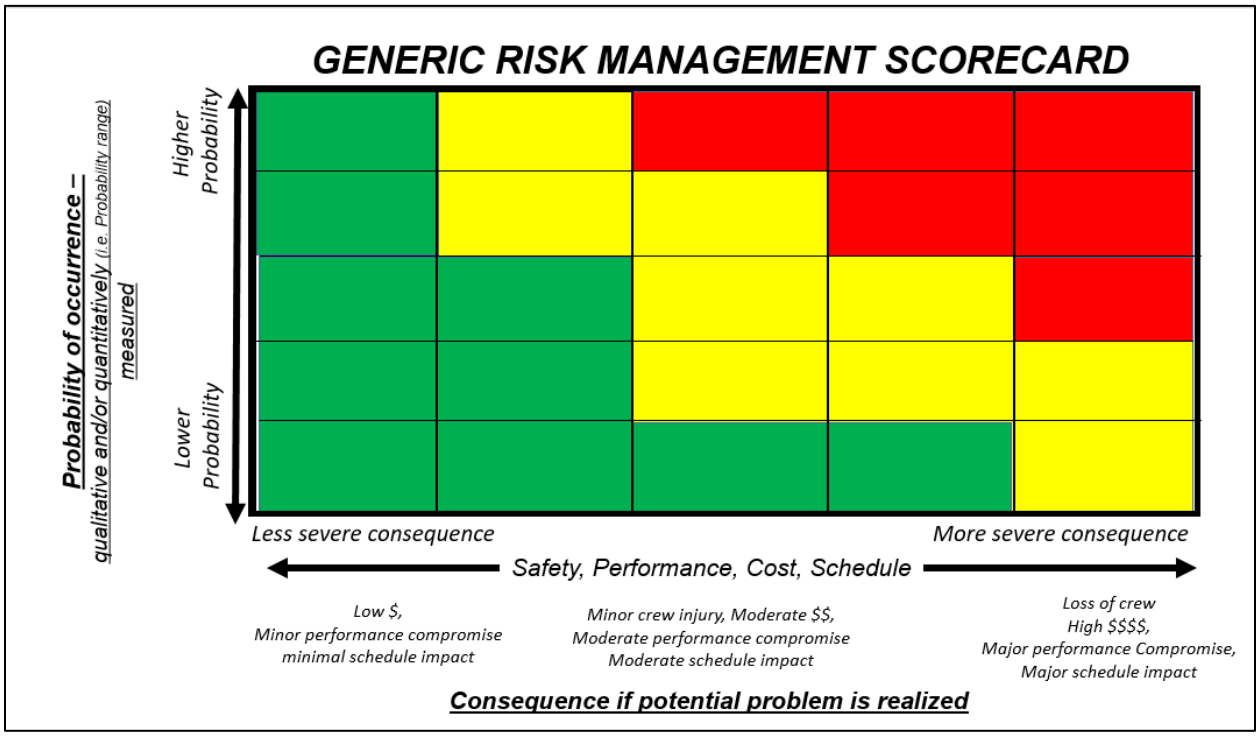


Figure 7-2

[17] *System engineering handbook, section 6.4 Technical Risk Management, figure 6.4-7 page145.*

CCP Risk Management Scorecard

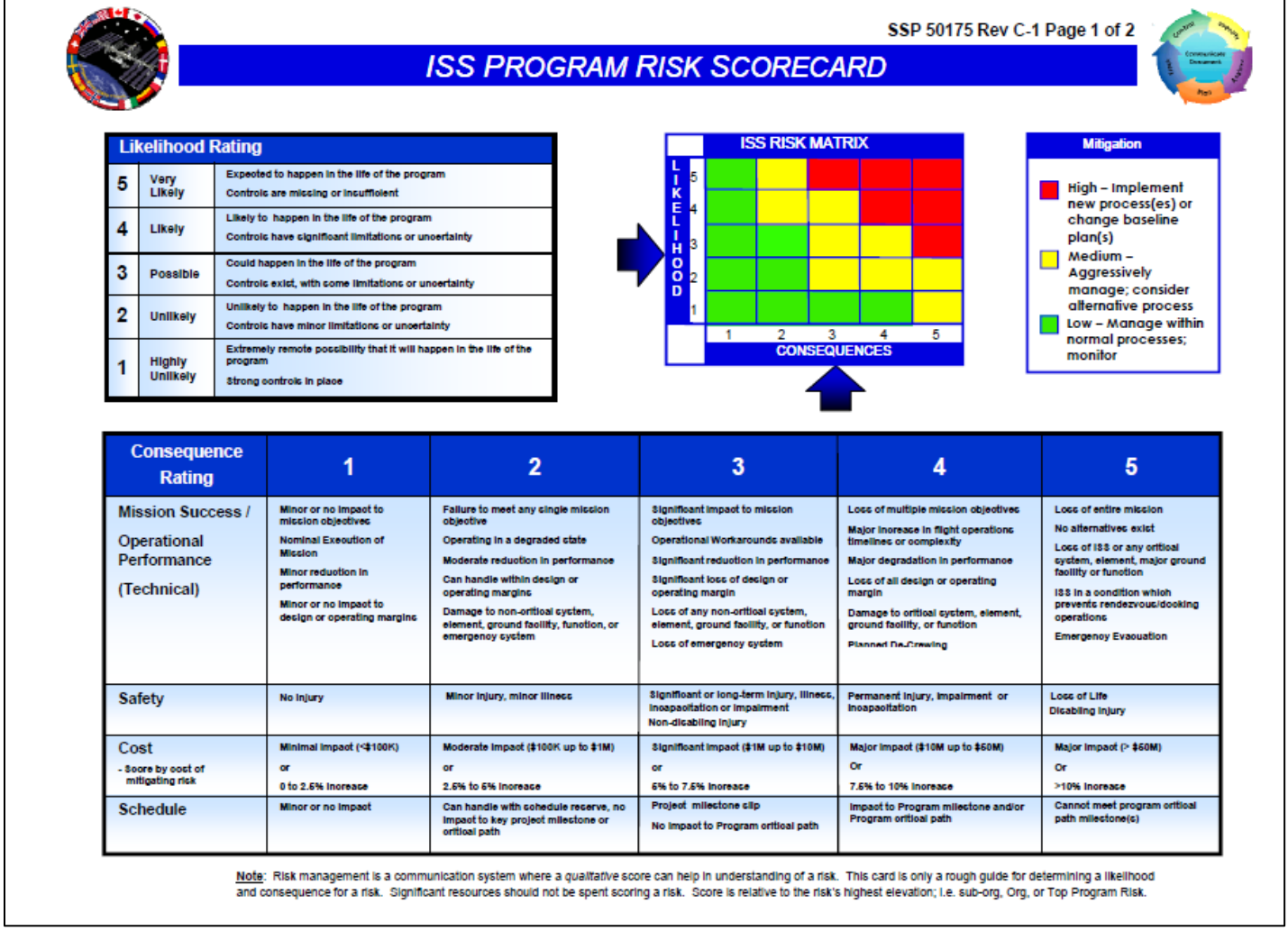
Likelihood		Performance, Cost, and Schedule	Human Safety
5	Qualitative	Very Likely to occur. Controls have significant uncertainties or have little to no effect.	Very Likely to occur. Controls have significant uncertainties or have little to no effect.
	Quantitative	Probability of occurrence is >90%.	Probability of occurrence is equal to or greater than 1/500.
4	Qualitative	Likely to occur. Controls have large uncertainties or have little to no effect.	Likely to occur. Controls have large uncertainties or have little to no effect.
	Quantitative	Probability of occurrence is 60-90%.	Probability of occurrence is greater than or equal to 1/1,000 and less than 1/500.
3	Qualitative	Possible to occur. Controls exist with moderate uncertainties.	Possible to occur. Controls exist with moderate uncertainties.
	Quantitative	Probability of occurrence is 40-60%	Probability of occurrence is greater than or equal to 1/10,000 and less than 1/1,000.
2	Qualitative	Unlikely to occur. Controls are strong or have minor limitations and uncertainties.	Unlikely to occur. Controls are strong or have minor limitations and uncertainties.
	Quantitative	Probability of occurrence is 10-40%.	Probability of occurrence is greater than or equal to 1/100,000 and less than 1/10,000.
1	Qualitative	Highly Unlikely or very unlikely to occur. Controls are strong or have negligible limitations and uncertainties.	Highly Unlikely or very unlikely to occur. Controls are strong or have negligible limitations and uncertainties.
	Quantitative	Probability of occurrence is <10%.	Probability of occurrence is less than <1/100,000.

Likelihood					
5	15	10	6	3	1
4	19	14	9	5	2
3	22	18	13	8	4
2	24	21	17	12	7
1	25	23	20	16	11
	1	2	3	4	5

Consequence

Consequence	1	2	3	4	5
Safety (Personnel)	Minor injury not requiring first aid treatment, minor crew discomfort.	Moderate injury requiring first-aid treatment, moderate crew discomfort	Severe Injury, occupational illness requiring medical treatment.	Critical Injury or occupational illness requiring definitive/specialty hospital/medical treatment, resulting in loss of mission	Loss of life or permanently disabling injury
Safety (Facilities, equipment, or other assets)	No more than slight damage to flight/ground assets.	Minor damage to flight/ground assets. Major damage to non-critical assets.	Moderate Damage to flight/ground assets prior to or during mission/test. No loss of mission/test.	Major damage to flight/ground assets prior to or during mission/test. No loss of mission/test.	Severe damage to flight/ground assets prior to completing its mission/ critical test. Loss of mission/test.
Safety (Environment)	No more than a slight reportable OSHA/EPA violation.	Minor reportable OSHA/EPA violation	Moderate OSHA/EPA violation which requires remediation.	Major OSHA/EPA violation which requires immediate remediation.	Severe OSHA/EPA violation(s) causing temporary stoppage or termination of project.
Performance	No more than a slight impact to requirements, design margins, or mission objectives.	Minor impact to requirements, design margins, or mission objectives.	Moderate impact to requirements, design margins, or mission objectives.	Major impact to requirements, design margins, or mission objectives. Milestone is likely not achievable with existing Commercial Provider engineering capabilities/ technologies.	Severe impact to requirements, design margins, or mission objectives. Milestone is not achievable with existing Commercial Provider engineering capabilities/ technologies.
Cost	≤ $1M	$1M-5M	$5M-10M	$10M-50M	> $50M
Schedule	Slight Impact to Program Controlled Milestone (≤1 month)	Minor impact to Program Controlled Milestone (1-2 Month impact)	Moderate impact to Program Controlled Milestone (2-4 Month impact)	Major impact to Program Controlled Milestone (4-6 Month impact)	Severe impact to Program Controlled Milestone (>6 Month impact)

Figure 7-3



SSP 50175 Rev C-1 Page 1 of 2

ISS PROGRAM RISK SCORECARD

Likelihood Rating

5	Very Likely	Expected to happen in the life of the program Controls are missing or insufficient
4	Likely	Likely to happen in the life of the program Controls have significant limitations or uncertainty
3	Possible	Could happen in the life of the program Controls exist, with some limitations or uncertainty
2	Unlikely	Unlikely to happen in the life of the program Controls have minor limitations or uncertainty
1	Highly Unlikely	Extremely remote possibility that it will happen in the life of the program Strong controls in place

Mitigation

- High – Implement new process(es) or change baseline plan(s)
- Medium – Aggressively manage; consider alternative process
- Low – Manage within normal processes; monitor

Consequence Rating	1	2	3	4	5
Mission Success / Operational Performance (Technical)	Minor or no impact to mission objectives Nominal Execution of Mission Minor reduction in performance Minor or no impact to design or operating margins	Failure to meet any single mission objective Operating in a degraded state Moderate reduction in performance Can handle within design or operating margins Damage to non-critical system, element, ground facility, function, or emergency system	Significant impact to mission objectives Operational Workarounds available Significant reduction in performance Significant loss of design or operating margin Loss of any non-critical system, element, ground facility, or function Loss of emergency system	Loss of multiple mission objectives Major increase in flight operations timelines or complexity Major degradation in performance Loss of all design or operating margin Damage to critical system, element, ground facility, or function Planned De-Crewing	Loss of entire mission No alternatives exist Loss of ISS or any critical system, element, major ground facility or function ISS in a condition which prevents rendezvous/docking operations Emergency Evacuation
Safety	No injury	Minor injury, minor illness	Significant or long-term injury, illness, incapacitation or impairment Non-disabling injury	Permanent injury, impairment or incapacitation	Loss of Life Disabling injury
Cost - Score by cost of mitigating risk	Minimal impact (<$100K) or 0 to 2.5% increase	Moderate impact ($100K up to $1M) or 2.5% to 5% increase	Significant impact ($1M up to $10M) or 5% to 7.5% increase	Major impact ($10M up to $60M) Or 7.5% to 10% increase	Major impact (> $60M) Or >10% increase
Schedule	Minor or no impact	Can handle with schedule reserve, no impact to key project milestone or critical path	Project milestone slip No impact to Program critical path	Impact to Program milestone and/or Program critical path	Cannot meet program critical path milestone(s)

Note: Risk management is a communication system where a qualitative score can help in understanding of a risk. This card is only a rough guide for determining a likelihood and consequence for a risk. Significant resources should not be spent scoring a risk. Score is relative to the risk's highest elevation; i.e. sub-org, Org, or Top Program Risk.

Figure 7-4

The Risk Management System is a valuable tool used by management help identify where best to apply resources to achieve maximum benefit. Equally important is its function of documenting risks that have been accepted (with appropriate data and rational) and to track the continuation of mitigation activities to reduce the probability and/or consequence of occurrence. It may also address any work necessary to better understand and quantify a risk which will better informed decision-making process. Risk management does not necessarily equate to elimination of risks, but can provide for an acceptance a risk once it has been mitigated to an acceptable level. As an example, the MicroMeteorite and Orbital Debris (MMOD) presents a significant risk to earth orbiting spacecraft. While we can reduce he probability of a catastrophic event by designing robustness into our vehicle exterior, we cannot reasonably eliminate the orbital debris environment and the risk it poses to spacecraft. The same can be said for parachute landing systems. Apollo conducted well over 100 parachute tests, yet parachutes performance remained

one of the highest risk items on the vehicle. The question must be asked of how much it costs to further buy down risk in a particular areas vs can those resources be better and more efficiently applied in reducing risks in other areas.

The risk system is also not a "worry list". Risk management is intended to documenting accepted risks and forward work or actions being planned to buy down risk to an acceptable level. If there is a worry that you are not willing to accept, and not willing to work to mitigate, then it has no place in the risk management system. If for example, you are worried about a budget to fund a program and there is nothing you can do about it, it does not belong in the risk management system. Also, if you have a critical system or element that is broken, then it should be characterized as a problem, not a risk. A risk is something that can be avoided whereas a problem is a risk that has been realized.

An additional caution when dealing with risk is being aware of (and resisting) a phenomenon often referred to as "Go/Launch Fever". The closer a vehicle get to the launch pad and/or its launch date, the greater the temptation and tendency to accept increases in risk. Swapping out of a suspect component that would have been part of standard work in the assembly and processing flow, becomes more of a risk acceptance/acceptability discussion as the vehicle moves closer to the pad. This also occurs by deferring decision and discussion on technical issues. Deferring a technical discussion can often result in coming to a head with statements along the lines of "If you make me do this you will be responsible for slipping the launch" or "Is it worth slipping the launch for this thing that probably won't occur?" Again, as a vehicle moves closer to the pad and to launch date, there is often an increased willingness to take on additional risks, which would not have been considered earlier in the flow.

One final note on risks. We often hear the drum beat for "accepting more risk" or challenges to being too risk averse. There may indeed be some truth in these statements. However, it is much easier to talk of increased risk tolerance when things are going well and no losses have occurred in recent history. We tend to be less sensitive to risks when no one has had to answer the question of "How could you have let this happen" recently. When determining risk acceptance posture, it is worth noting that a key driver for termination of the Space Shuttle Program was tied to the risk of a system that suffered two (2) accidents over a 100+ flights. This cancellation happened in spite of the fact that corrective actions were implemented to prevent reoccurrence of these technical problems and thereby making the system safer as it continued to mature. A large selling point for the CCP was the promise of increased safety for human spaceflight. These considerations should not be ignored when considering increasing risk tolerance.

8.0 Other Key Relevant Topics:

8.1 Crew Survival Analysis (CSA):

Crew survival Analysis or CSA, is a term given to a key safety analysis product which identifies additional opportunities and capabilities to enhance crew survival above and beyond satisfying the

program/project documented requirements. Having a long list of items in a crew survivability analysis report is not an indictment of the design, but is a method to recognized opportunities to provide the crew with a reasonable chance of survival in the event of some low likelihood failures. This product may identify the potential application of hardware and systems in ways they were not originally intended and were not certified to be used, but in an extreme scenario, can provide the crew with an opportunity to improve their chances of survival. It may also include incorporating capabilities such as manual control of some elements that are not the key focus or pre-mission training exercises. It may or may not require hardware and systems to be tested or certified to accomplish this additional functionality. In some cases it may result in design changes being made to a system, or the addition of components to a system if there is a clearly recognized benefit to overall safety and it is determined to be warranted based on a cost vs. benefit trade. This trade may also be a key driver in determining the level of rigger and effort put into any required verification activity.

Per NASA Program requirement document "NPR 8705.2C Human rating requirements for Space Systems"[18], having a documented strategy for crew survival is one of many required element to be included in the Program/Project Human Rating Certification Package (HRCP).

8.2 Probabilistic Risk Assessments (PRA's) – aka Probabilistic Safety Assessment (PSA):

Probabilistic Risk Assessments or PRA's are another useful tool to identify where resources can be most effectively allocated to provide the most benefit to enhancing crew survival or mission success. When dealing with crew safety we refer to the scoring associated with the potential "Loss Of Crew" or LOC. When dealing with mission success, we may have different values for the same systems and may also be including different systems in determining the potential "Loss Of Mission" or LOM. An example of this might be a docking system malfunction where the spacecraft may not be able to latch to an orbiting space station. This may result in a loss of mission and a need to return to earth, but does not necessarily present a safety risk to the crew.

These values represent a relative term and are useful in relative comparisons between different opportunities, but should not be considered as exact numbers. The value referenced are often mean values that covers a very wide range of potentials values. A failure of a system anywhere in this wide range of numbers can be considered a PRA predicted occurrence. The figure 8-2a below shows the typical range of failure probabilities for a particular component, while figure 8-2b shows how it can be used to compare across system to better inform the allocation of resources. Again, failure anywhere within this range constitutes a successful PRA prediction. In this way, care should be taken when relying on a specific PRA mean value, and it should not be considered to have decimal place accuracy. The

[18] 8705.2C, Appendix A (sec 1.3, bullet "b")
https://nodis3.gsfc.nasa.gov/npg_img/N_PR_8705_002C_/N_PR_8705_002C_.pdf

PRA provides a relative risk comparison across multiple areas. This tool provides a valuable resource when properly utilized to show where one may find the most bang for the buck.

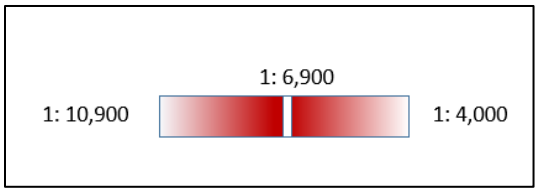


Figure 8-2a

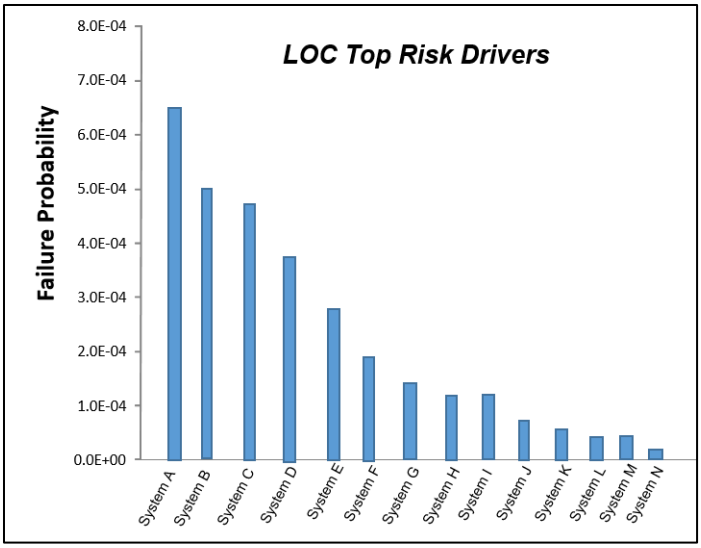


Figure 8-2b

8.3 "Tailoring" Requirements, Standards and Milestones:

"Tailoring" of requirements, standards, and milestones can be a very powerful and useful tool in streamlining development and ensuring the appropriate set of requirements are applied to a specific application. Equally important however, is ensuring that "tailoring" is not used as an excuse to ignore requirements, delete necessary analysis and tests of the design, or defer this work until it is too late to reasonably inform the design. NASA development and documentation of the program/project design cycle has been developed based on experience and costly lessons learned from numerous programs and projects conducted over many years. As former Astronaut and NASA Administrator Charles Bolden noted in a September 2016 article in the Journal of Space Safety Engineering[19]…"We have 50 years of history launching humans to space, and there's an incredible knowledge base in there….We've always been about lessons learned – both good and bad."

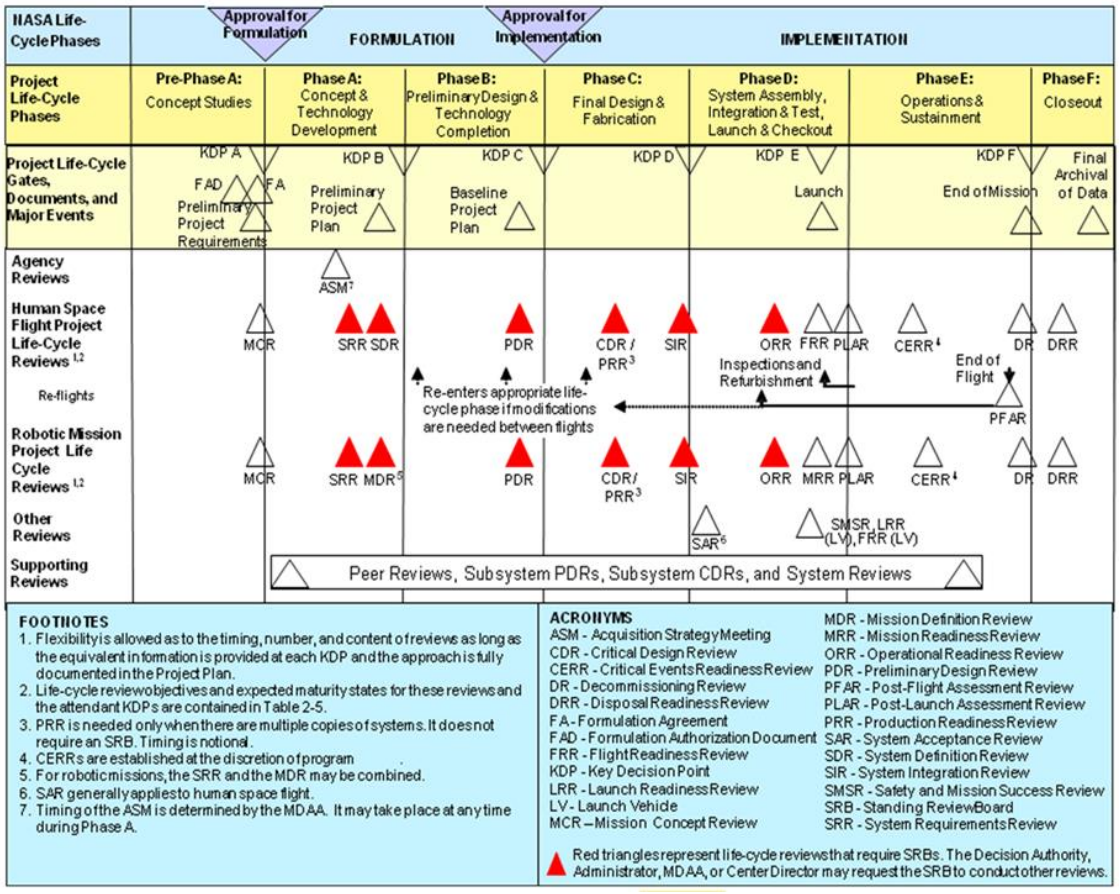
The program life cycle description can be found in several references including section 3 of the NASA Systems Engineering Handbook ((NASA/SP-2007-6105, rev 1), and NASA Procedural Requirements (NPR) document "NPR 7120.5 NASA Space Flight Program and Project Management Requirements". While Figure 8-3 (from NPR 7120.5E) may at first look onerous, it should be pointed out that this figure contains separate milestone review paths for both human and non-human projects. This map, when combined with description of the content expected at each milestone (captured in NPR 7123,

[19] Charles Bolden – NASA Administrator – "NASA Administrator Bolden Opening remarks". URL: http://iaass.space-safety.org/wp-content/uploads/sites/24/2015/07/JSSE-VOL.-3-NO.-2-SEPTEMBER-2016-HR-NASA-ADMINISTRATOR-CHARLES-BOLDEN-OPENING-REMARKS.pdf - Journal of Space Safety Engineering, Vol 3, No. 2 [cited September 2016]

Appendix –G) provides a strong basis for establishing the appropriate framework for a Human rated flight project/program. Using this as a starting point allows for making informed decisions on tailoring of both process and content. Tailoring should not be used as a matter of convenience to delete content without a thoughtful and deliberate assessment of the applicability to a specific project/program. It should also include any appropriate up-front acknowledgement and disclosure of risks that will be incurred through the specific tailoring application. As new tools and capabilities continue to be developed, both the established processes and milestones captured in the NASA NPR's should also be matured. Care should be taken to show how new tools and processes meet the intent of these key experience based milestones. This should include addressing the technical assessments included in the experience-based milestones and ensuring this information is provided in an appropriate time frame to inform the design.

In addition to tailoring at the NPR document level, tailoring may also be appropriate for detailed technical Design and Construction (D&C) standards. These detailed technical standards may be levied as requirements or guidelines on the project/program. Examples of these are items such as mechanical design standards, electrical bonding standards, and pyrotechnical standards just to name a few.

Tailoring can be a very useful tool when appropriately applied, but can also have catastrophic consequences when applied purely as a matter of convinces without a thoughtful and deliberate assessment on the potential impacts to flight safety



FOOTNOTES

1. Flexibility is allowed as to the timing, number, and content of reviews as long as the equivalent information is provided at each KDP and the approach is fully documented in the Project Plan.
2. Life-cycle review objectives and expected maturity states for these reviews and the attendant KDPs are contained in Table 2-5.
3. PRR is needed only when there are multiple copies of systems. It does not require an SRB. Timing is notional.
4. CERRs are established at the discretion of program
5. For robotic missions, the SRR and the MDR may be combined.
6. SAR generally applies to human space flight.
7. Timing of the ASM is determined by the MDAA. It may take place at any time during Phase A.

ACRONYMS

ASM - Acquisition Strategy Meeting
CDR - Critical Design Review
CERR - Critical Events Readiness Review
DR - Decommissioning Review
DRR - Disposal Readiness Review
FA - Formulation Agreement
FAD - Formulation Authorization Document
FRR - Flight Readiness Review
KDP - Key Decision Point
LRR - Launch Readiness Review
LV - Launch Vehicle
MCR – Mission Concept Review
MDR - Mission Definition Review
MRR - Mission Readiness Review
ORR - Operational Readiness Review
PDR - Preliminary Design Review
PFAR - Post-Flight Assessment Review
PLAR - Post-Launch Assessment Review
PRR - Production Readiness Review
SAR - System Acceptance Review
SDR - System Definition Review
SIR - System Integration Review
SMSR - Safety and Mission Success Review
SRB - Standing Review Board
SRR - System Requirements Review

Red triangles represent life-cycle reviews that require SRBs. The Decision Authority, Administrator, MDAA, or Center Director may request the SRB to conduct other reviews.

Figure 8-3[20]

8.4 Data and Data Access:

Data and data access needs to be consistent with the roles, responsibilities, and accountabilities established for both NASA and the private entity. The more accountability placed on the NASA engineering team, the deeper the depth and insight of the private entity is necessary to fulfil those expectations. Any "Shared Accountability" must be clearly defined for both the NASA and private entity teams. Experience has shown data access to be particularly challenging. Even with broad access privileges to a private company's data storage location, often finding the right data has been referred to as "Finding a needle in a haystack" or "Dumpster Diving". The appropriate data must be stored, searchable, and retrievable in a logical and systematic manner. Efficient and effective use of time must be considered for both NASA and private entity team members. Experience has shown that lacking a well-organized and properly maintained data repository has detrimental effects in multiple areas including, but not limited to, the following:

- Inefficient use of time and resources for both the NASA and private entity technical team.
- Compromising agreed to technical data review times prior to major project/program reviews.
- Creating cumbersome, complicated and de-centralized data retrieval environment will limit the team's ability to effectively utilize the data in a timely manner.
- Denial of access to necessary review products.
- Time wasted on review of obsolete technical information.
- Hyperlinks pointing to material not applicable to the subject at hand.
- Cross-referencing to incomplete and erroneously data areas with missing data, not appropriate subject/content, or a combination of the two.
- Data summaries provided without the granularity and level of detail necessary to support flight decision making.
- Inadequate access to necessary subcontractors/third party data including issues, concerns, and anomalies.
- Inconsistent and limited awareness of testing and test results.
- Lack of team awareness of when information is made available.
- Lack of access to anomalies, corrective actions, anomaly dispositions, and root cause.

The latter items are particularly important when dealing with anomalies and non-conformances in system, subsystem and component performance with significant implication to flight safety and mission success.

[20] NPR 7120.5E NASA Space Flight Program and Project Management Requirements, figure 2-5 NASA Project Life Cycle

It is worth noting that “Engineering Judgement” is not considered as equivalent to a sound technical based justification. As the phrase in the mission evaluation room used to say “In God We Trust, All Others Bring Data”. A judgement or opinion may be useful in predicting which path may be most advantageous, but in the end, the flight rationale must be supported by technical data rather than opinion or judgement.

8.5 Documentation:

Documentation is unavoidable when dealing with complex engineering designs and implementation of those designs. Advances in documentation tools have greatly enhanced the ability to develop, maintain, and search for relevant information. This reduces the burden of storage, updating, and tracking revisions. Whether by electronic database or other means, clear documentation and process controls are critical to ensuring flight safety and resolving anomalies including, but not limited to:

- In Flight Anomalies (IFA’s).
- Qualification anomalies
- Hardware acceptance anomalies.
- Vehicle processing anomalies
- Flight hardware non-conformances and associated dispositions
- Corrective and preventative actions

Without proper document control (including configuration management and documentation management), we cannot ensure the design documentation reviewed is representative of the flight vehicle design. The ability to provide an endorsement for flight relies heavily on the ability to ensure the documentation presented for flight is up to date and accurate. Last minute updates or revisions released just prior to flight increase the risk of schedule pressures overshadowing a proper technical review. Additionally, inaccurate documentation compromises the integrity of any flight endorsement. This has proven challenging in the past when a system has a high frequency of design changes. In these cases, many design changes considered “minor” may be overlooked in an attempt to focus attention on the “major” high visibility changes. This can be particularly concerning when dealing with a crewed ascent/decent vehicle where the majority of system are critical to maintaining flight safety and mission success.

There are however, “opportunities” that can significantly reduce the documentation burden, if we can leverage off a well-established and mutually beneficial insight/oversight relationships. Combining this with an adjustment to our joint teams approach of how to meet the intent of proper documentation can result in less onerous methods compared to those of previous programs. There may be opportunities to collaborate on the documentation when executed in good faith. The following opportunities leverage heavily from approaches already being applied by the Orion/MPCV program. They include, but are not limited to the following:

- Providing direct technical communications at the system, subsystem, and component engineering level between government and private entity to resolve and clarify understanding before generating actions and associated paper prior to key design milestones.
- Focus documentation on key issues and concerns that have hit an impasse and require management engagement.
- Refrain from generation of paper based on editorial changes.
- Rather than review and reject documentation for clerical issues or insufficient rationale, if a reviewer is aware of additional info and corrected information that would provide acceptable justification to accept and close an issue, allow that reviewer to augment the submitted documentation with the complete story to allow proper closure.
- Once a project has passed a Critical Design Review (CDR) level of maturity, limit changes to those that are necessary to make the system work vs changes to make the system "better". If the change were not implemented, would we refrain from launching?
- When dealing with an uncrewed test flight of a system, consider greater risk acceptance posture for items that will be mitigated when crew is introduced into the system. Recognize the difference in consequence of un-crewed vs crewed flight as risk mitigations are matured over time. Maturing mitigation may be the result of more extensive analysis and test activities occurring in parallel or following the uncrewed flight. Care must be taken when increased risk is accepted for an uncrewed flight, to ensure that uncrewed flight risk acceptance is not used to justify acceptance of that same risk on a crewed flight. In each case, the risk must be evaluated based on the applicable consequence for that particular flight.
- If a large activity is ~95% complete but is held open for a lingering 5% of additional information or activity, consider closing the 95% portion and track the 5% closure separately. Take credit for the actual work complete and keep focus on the remaining open work. Key to this approach is maintaining focus on the remaining work to ensure it is not overlooked or lost in a tracking system.
- Do not let disagreements on defining what level of data is "good enough" linger. Ensure there is an expedited elevation to proper management decision forum to resolve this discrepancy and mitigate the "churn" and wasted time in arguing at the lower levels. When applying this approach, care must be given to ensure this path is not used as a mechanism to bypass engineering technical reviews and provide a strong technical base for decision-making. It should be reserved for addressing impasses driven by disagreements on "good enough" level of data.

Clear and accurate documentation is critical to determining the root cause of any catastrophic event, and ensuring proper corrective action will prevent reoccurrence. Lacking this level of information will adversely affect attempts to return to flight status following an accident or significant incident.

8.6 Determination of Root Cause:

Root cause is defined as events, conditions and/or organizational factors that contributed or created the proximate cause, resulting in the undesired outcome. The Proximate cause (aka direct cause) is defined as the events that occurred immediately before the undesired outcome.

In order to ensure the prevention of reoccurrence, Human spaceflight strives to identify not only proximate cause, but also root cause where safety of flight is concerned. Failure to do so increases the risk of reoccurrence, which may impact the ability to proceed with future missions. While this determination of root cause (and implementation of corrective action) is clearly demonstrated in the Challenger and Columbia investigations, it is also applied to resolution of safety of flight items that have not received that same level of visibility but also have the potential for catastrophic consequences. In the case of the Challenger and Columbia investigations, a strong emphasis was placed on the organizational and institutional deficiencies, which contributed to the accidents. The resultant corrective actions included detained technical recommendations along with organizational and institutional changes, all of which were implemented to prevent reoccurrence. Failing to identify, and directly address, root cause brings into question the effectiveness of corrective action taken to prevent reoccurrence. This in turn compromises the CoFR process.

Key to determination of root cause is the rigorous application of a Root Cause Analysis. “Fault Tree’s” and/or “Fishbones” are analysis tools that have been utilized to identify the potential failure causes and to help guide the application of resources to determine the likelihood of specific items being contributing factors. The specific items identified by these tools are reviewed in detail to determine what information is necessary to either remove them from consideration as a potential contributor, or what information is necessary to confirm they did contribute to the failure so preventative action can be taken to prevent future reoccurrences.

9.0 Finding the Right Balance:

Leveraging from the engagement scale from figure 3-2, and making some adjustments for setting minimum bars for safety and accountability, we can generate a notional figure to help guide the discussion of how transitioning ISS to the private sector might be partnered. Considering the recent stated goals of adjusting the current government model for ISS management and operations, we can envision a wide range of options and opportunities for the International Space Station (ISS) in the post 2024 period (Figure 9-1). Similarly, this thought process might aid in guiding partnering discussion and expectations for NASA’s announced “Gateway” activities and other yet to be determined exploration initiatives. There is a wide range of potential partnering arrangements based on how the RRA ground rules and assumptions are defined.

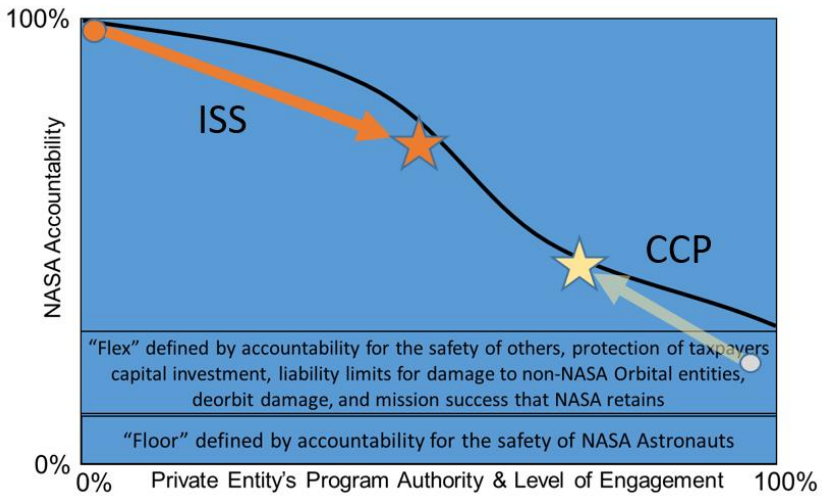


Figure 9-1

10. Summary/Conclusion:

Today's environment offers a wide array of opportunities to engage in human spaceflight partnerships between the government and private sectors. Up front and early definition of Roles, Responsibilities, and Accountabilities is key to building and understanding the Program/Project relationships. Clear establishment here will naturally drive out decision in other areas such as data access, documentation, risk management, certification approvals, etc… Additionally, it is important to understand and appreciate the differences between crewed and un-crewed spaceflight since the consequences associated with the loss of a crew are significantly different from un-crewed missions. Failure to properly apply these fundamental principles and lessons learned can have dire consequences to the success of a project/program. The adverse impacts to safety, performance, cost and schedule can lead to termination and/or failure of a program that began with a strong promising potential for success.

New technologies and capabilities present impressive growth opportunities for both space exploration and commercialization of space. We can and should move forward to develop these partnerships, but should also not forget the lessons we have learned in the past. We have paid a very high price (both monetarily and in human lives) for many of these lessons. The knowledge gained from these experiences can be used to better inform us as we engage in future partnerships. Change is necessary to remain relevant and competitive in an evolving market such as space. However, changes must be made with an eye on the risks vs benefits involved, and ensuring we know why we are deviating from established process or procedure. Why was that process or procedure put in place to begin with and how are we meeting the intent, or are we acknowledging openly and with supporting data that there is a reason to accept the risk of deviating from lessons learned based content. What has changed to make it acceptable? It is easy to ignore things we find too imposing. Indeed, it is more work to fully integrate lessons learned from the past as we formulate a program or partnership for the future. Taking

this time and effort up front offers the opportunity to avoid the pitfalls encountered in the past as we move forward with new and evolving partnerships.

Appendix A – References

Government Documents

CCT-PLN-2000, Rev_A – NASA Crew Transportation System Certification Plan

CCT-PLN-2100, Rev Basic – NASA Commercial Crew Program Crew Transportation System Certification of Flight Readiness Plan

Public Law 111–314 : 111th Congress; "ENACTMENT OF TITLE 51—NATIONAL AND COMMERCIAL SPACE PROGRAMS" https://www.nasa.gov/sites/default/files/atoms/files/public_law_111-314-title_51_national_and_commercial_space_programs_dec._18_2010.pdf page 5 –section (C) [cited 18 December 2010]

NASA Press release 14-256: "NASA Chooses American Companies to Transport U.S. Astronauts to International Space Station"

[https://www.nasa.gov/press/2014/september/nasa-chooses-american-companies-to-transport-us-astronauts-to-international] [cited 16 September, 2014]

NASA/SP-2007-6105 rev 1 – NASA Systems Engineering Handbook

NPR 7120.5E – NASA Space Flight Program and Project Management Requirements

NPR 7123.1B – NASA systems Engineering Processes and Requirements

NPR 8705.2C – Human-Rating Requirements for Space Systems

https://nodis3.gsfc.nasa.gov/npg_img/N_PR_8705_002C_/N_PR_8705_002C_.pdf

NSTS 22254 Methodology For Conduct Of Space Shuttle Program Hazard Analysis F−4 CHANGE NO. 15 Revision B - Retired (Final Version)

Articles, Publications

Charles Bolden – NASA Administrator – "NASA Administrator Bolden Opening remarks". URL: http://iaass.space-safety.org/wp-content/uploads/sites/24/2015/07/JSSE-VOL.-3-NO.-2-SEPTEMBER-2016-HR-NASA-ADMINISTRATOR-CHARLES-BOLDEN-OPENING-REMARKS.pdf - Journal of Space Safety Engineering, Vol 3, No. 2 [cited September 2016]

Electronic Publications

Columbia Accident Investigation Board, https://history.nasa.gov/columbia/CAIB_reportindex.html [cited August 2003]

Nicholas Clairmont, "Those Who Do Not Learn History Are Doomed To Repeat It. Really?" URL: http://bigthink.com/the-proverbial-skeptic/those-who-do-not-learn-history-doomed-to-repeat-it-really

General Thomas S. Moorman, Jr (USAF, retired) "Framing the Assured Access Debate: A Brief History of Air Force Space Launch". Air Force Space Command – High Frontier – [online Journal], Vol 3, No. 1 URL: http://www.afspc.af.mil/Portals/3/documents/HF/AFD-061128-043.pdf [cited 21 November 2006]

GlobalSecurity.org – Space – Titan-4 Launch History https://www.globalsecurity.org/space/systems/t4table.htm [cited 21 July 2011]

Joel Achenbach "NASA gets two military spy telescopes for astronomy" The Washington Post, URL: https://www.washingtonpost.com/national/health-science/nasa-gets-military-spy-telescopes-for-astronomy/2012/06/04/gJQAsT6UDV_story.html?utm_term=.e72af0ef8eb7 [cited 4 June 2012].

Maj Gen Ellen M. Pawlikowski (USAF) “Mission Assurance – A Key Part of Space Vehicle Launch Mission Success”, Air Force Space Command – High Frontier – [online Journal], URL: http://www.nro.gov/news/articles/2008/2008-05.pdf [cited 26 August 2008]

NASA – Mission Information (Space Shuttle) www.nasa.gov/mission_pages/shuttle/shuttlemissions/index.html [cited 29 August 2011]

Nicholas Clairmont, “Those Who Do Not Learn History Are Doomed To Repeat It. Really?” URL: http://bigthink.com/the-proverbial-skeptic/those-who-do-not-learn-history-doomed-to-repeat-it-really

Space Launch Report : Delta III Data Sheet - http://www.spacelaunchreport.com/delta3.html [cited 5 September 2010]

Report to the President By the Presidential Commission on the Space Shuttle Challenger Accident, https://history.nasa.gov/rogersrep/genindex.htm [cited 6 June 1986]

Report to the President – Actions to Implement the Recommendations of The Presidential Commission on the Space Shuttle Challenger Accident https://history.nasa.gov/rogersrep/actions.pdf [cited 14 July 1986]

Wikipedia – List of Falcon 9 and Falcon Heavy Launches - https://en.wikipedia.org/wiki/List_of_Falcon_9_and_Falcon_Heavy_launches [cited 3 June 2018]

Appendix B – Acronyms

BAR - Broad Area review
CAIB - Columbia Accident Investigation Board
CCP - Commercial Crew Program
CCT - Commercial Crew Transportation
CDR - Critical Design Review
CoFR - Certification of Flight Readiness
CSA - Crew Survival Analysis
CTS - Crew Transportation System
D&C - Design and Construction
DCR - Design Certification review
DDT&E - Design, Development, Testing and Evaluation
DoD - Department of Defense
FMEA - Failure Modes and effects Analysis
FRR - Flight Readiness Review
HEO -
HR - Hazard Reports
IFA - In-Flight Anomalies
ISS - International Space Station
IV&V - Independent Verification and Validation
JSC - Johnson Space Center
KSC - Kennedy Space Center
LOC - Loss Of Crew
LOM - Loss of Mission
MPCV - Multi-Purpose Crew Vehicle
MSFC - Marshall Spaceflight Center
NASA - National Aeronautics and Space Administration
NPR - NASA Procedural Requirements
NSTS - National Space Transportation System
NRO - National Reconnaissance Office
OV - Orbital Vehicle
PRA - Probabilistic Risk Assessment
PRACA - Problem Reporting And Corrective Actions
PSA - Probabilistic Safety Assessment
R&R - Roles and Responsibilities
RIDM - Risk Informed Decision Making
RRA - Roles, Responsibilities and Accountabilities
SDR - System Design Review
SSP - Space Shuttle Program
TPS - Thermal Protection system
UA - Unexplained Anomaly
VCN - Verification Closure Notice