NASA'S COMMERCIAL CREW PROGRAM, THE NEXT STEP IN U.S. SPACE TRANSPORTATION FOR THE 6TH IAASS CONFERENCE

Edward J. Mango, [1], Rayelle E. Thomas [2]

[1] National Aeronautics and Space Admnistration, Kennedy Space Center, Florida, US, edward.j.mango@nasa.gov
[2] National Aeronautics and Space Admnistration, Kennedy Space Center, Florida, US, rayelle.e.thomas@nasa.gov

ABSTRACT

The Commercial Crew Program (CCP) is leading NASA's efforts to develop the next U.S. capability for crew transportation and rescue services to and from the International Space Station (ISS) by the mid-decade timeframe. The outcome of this capability is expected to stimulate and expand the U.S. space transportation industry. NASA is relying on its decades of human space flight experience to certify U.S. crewed vehicles to the ISS and is doing so in a two phase certification approach. NASA Certification will cover all aspects of a crew transportation system, including development, test, evaluation, and verification; program management and control; flight readiness certification; launch, landing, recovery, and mission operations; sustaining engineering and maintenance/upgrades. To ensure NASA crew safety, NASA Certification will validate technical and performance requirements, verify compliance with NASA requirements, validate the crew transportation system operates in appropriate environments, and quantify residual risks.

1. INTRODUCTION AND BACKGROUND

1.1 Objective of this Paper

The objective of this paper is to define the framework for Certification of a commercially-provided transportation system to carry NASA crew to and from the ISS. A certification approach is needed that will allow CCP to work closely with the Commercial Provider (Provider) in order to efficiently and effectively focus CCP resources on certification completion, and minimize the duplication of effort and safety critical forward work late in the design cycle. This paper outlines a framework for Certification that is independent of the acquisition process and contains overarching guidance for the CCP team.

1.2 Framework for Certification of Commercial Crew System

In general, Certification is the confirmation that critical characteristics of an object or system have been achieved. Crew Transportation System (CTS) Certification is the documented authorization granted by the NASA Associate Administrator (AA) that allows the use of the CTS to transport NASA crew. The focus of this paper is Certification of the CTS for use in transporting NASA crew in accordance with the ISS Design Reference Mission (DRM). The verification of these requirements is an essential focus of the CTS Certification. As shown in Figure 1.1, CTS Certification consists of three elements: design, production, and operations Certification. NASA will review and approve the Provider's Certification plan which explains how the Provider intends to achieve Certification of their CTS. Where NASA finds that their requirements are not contained in the Provider's Certification Plan, or planned verifications of requirements are not rigorous enough to meet Certification, NASA will reserve approval of the plan until the gaps are resolved to an acceptable level of risk. After NASA approves the Certification plan, the Provider will execute the plan, and generate the data required to confirm that the CTS meets NASA's requirements.

Certification of each of these is described as a three step process:

1) The Provider develops a CTS that they assert meets NASA's safety, crew, and technical requirements and is managed to an acceptable level of risk for transporting NASA crew.
2) NASA substantiates the Provider's assertion.
3) NASA grants Certification.

This is a complex and iterative process that requires considerable effort on the part of both NASA and the Provider. To support this effort, the Provider will provide access to the facilities, products, data, and models necessary for NASA to substantiate their assertion of certification. Provider certification activities and NASA review should be concurrent to the greatest extent possible.

An interim Certification will be granted by NASA prior to the first low Earth orbit (LEO) crewed flight, whether crewed by NASA or the Provider, upon successful completion of a Design Certification Review (DCR). The DCR will formally document the configuration baseline and the conditions under which the system is certified, the verification of the system, as well as the baselined risks. A delta DCR may be necessary to review completion of residual open work from the DCR before full Certification for the ISS DRM is granted.

Upon successful completion of the crewed flight test phase, an Operational Readiness Review (ORR) will be conducted by the Provider. The ORR is a key part of CTS Certification for the operational ISS transportation

missions. It occurs once during the program life cycle (or at the introduction of new or significantly modified systems/facilities) and marks a transition time from a design, development, and test phase to an operational phase where the CTS is expected to perform standard crew transportation services missions to the ISS.

With successful completion of DCR (and any delta DCRs) and the ORR, the CCP will conduct a certification review to determine that the CTS can safely transport crew to and from the ISS and that the CTS can meet the DRM for which it was developed. The baseline configuration of the hardware, software and processes used in design, production and operations will be documented and maintained by the Provider.

Certification maintenance will be performed for all crewed flights. It ensures that new understanding of hazards/risks, modifications to design, production, and operations which could violate the CTS Certification are understood and accepted prior to subsequent flights. NASA will evaluate and grant Certification addendums for any modifications to the design, production and operations that invalidate the CTS Certification or determine the need for re-Certification.

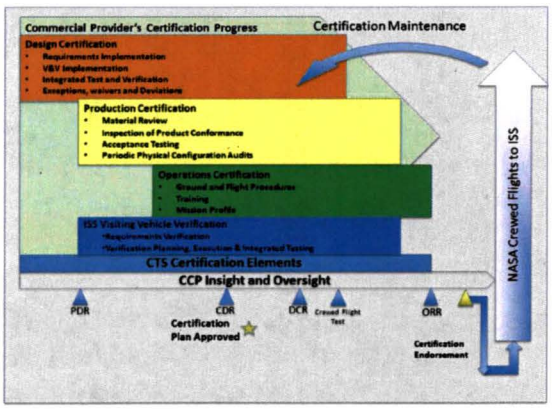

Figure 1: Elements of CTS Certification.

2. CTS CERTIFICATION

While Certification is discussed in terms of design, production and operations throughout this document, it should be noted that multiple certifications are not performed or granted for a single mission. As the CTS design matures, the primary focus of the Providers and NASA will shift from design to production, and then to operations, and portions of these elements are executed concurrently.

Broken down into fundamental elements, the design portion of certification encompasses:

1) verification that a design meets requirements
2) validity of the processes that create the design definition
3) validity of the processes that produce the system
4) validity of the tools that verify the design
5) control of the design definition
6) control of product manufacturing, assembly, inspection and testing
7) verification of the CTS operational capability

2.1 The Design Element

The design element of Certification is a broad term to encompass many design activities and processes that allow NASA to approve the use of a system. Certification can only occur after establishment of a design baseline post-CDR, and after all analysis and qualification testing have been completed, including all modifications needed for qualification-caused corrective actions. An item built to the design definition and intended for testing to verify a requirement is often called a qualification article. Similarly, a test performed on a qualification article is often called a qualification test.

2.1.1 Verification that a Design Meets Requirements

Verification methods include test, analysis, inspection, demonstration or combinations of these methods. To establish that a design meets requirements, verification methods are determined, planned and conducted, and results are assessed. A system is characterized by a product breakdown structure (PBS), with example PBS levels being "system-element-modules-subsystem-units-component." Verification is conducted at the levels of the PBS necessary to satisfy the applicable requirements. A set of requirements contain individual requirements written at different levels of the PBS, such as system requirements for integrated performance and subsystem requirements for specific functional performance of a subsystem. Requirements are allocated down by the providing organization to the lowest level necessary in the PBS to accomplish a function or meet an objective. Requirements derived from hazard analyses as hazard controls are considered program level derived requirements and are expected to be treated like program level specified requirements within the Provider's Certification. These controls are implemented in design, production, and operations. Verifications are performed at the allocated level and as necessary at the next higher assembly level. The verifications at the higher assembly level may be analysis of the integrated performance at that level based on the results of verification at the level below. Verification of the allocated requirement is rolled up to prove that the system meets the requirement. To support the roll up of verifications at the top level of the PBS, data products at the lowest level of allocated performance are identified and are available to support Certification.

Verification that a design meets requirements includes any necessary functionality and performance during exposure to environmental conditions (e.g., vibration, temperature, pressure) that the item will be subject to during all phases of the service life. The service life extends from the completion of fabrication to final disposal of the item and includes all acceptance test

environments, handling, transportation, storage, ground operations, flight, and recovery. Qualification testing is generally conducted with margin beyond the design specification required conditions with respect to amplitudes, cycles, or duration of exposure. This type of testing is done to account for unit-to-unit variability in the flight production hardware, to justify allowable test tolerances, and to demonstrate an overall robustness of the design to withstand the environmental conditions expected throughout the service life. The item is qualified with margin beyond the specification required conditions in order to certify the design to the specification required conditions.

In order for verification to be valid, it must be conducted on an article or model representative of the design to be certified. To verify a requirement by test, the test must be conducted on an item that has been produced in accordance with the design definition for those attributes where test results would be used as verification evidence. In addition, the test equipment or facility must be shown to be capable of conducting a test that exposes the item under test to the conditions necessary to simulate the environment and measure the results. To verify a requirement by analysis, the analysis must be conducted on an item that represents the design attributes being analyzed and with valid results.

2.1.2 Validity of the Processes that Create the Design Definition

The design definition includes extensive information produced to document the design, such as drawings, manufacturing models, analysis models, interface models, assembly procedures, special process instructions, specification sheets for parts or materials, and sampling procedures. The processes used to create these individual information products must be credible and repeatable.

In addition to the tools that produce the design definition, the establishment of consistent use of source data and use of that source data within different design definition articles must be understood. CAD and mathematical models used to define, produce and analyze the design must be consistent with the design source data. If the material property is changed in the CAD model or production plan, the analysis must be changed to account for the different material property and re-run to determine that the design still meets the requirements.

2.1.3 Validity of the Processes that Produce the System

When the processes used to produce the end item do not maintain the production process in accordance with the intent of the design definition, the product may not represent the design. Processes that produce the system may impart unintended stresses or flaws in the product that will not be detected by inspection and test. Understanding the capability, repeatability and weaknesses in the processes that produce the end item allows the design, manufacturing and test organization to establish the test, inspection and sampling requirements that have the best opportunity to identify and prevent flaws. The processes that produce the system must be capable of producing products that meet the tolerances and critical attributes in the design definition and must account for additional factors such as material selection and control; mechanical and electrical parts management processes; metrology and tool calibration; limited life identification and tracking; separation of flight and non-flight stock; control of flight hardware from unauthorized and un-recorded activities that could damage or remove cycle life.

When a system contains items that are re-used or refurbished, additional processes are necessary. In addition to the processes that produced the system, additional processes are established to ensure that the item is capable of performing an additional mission.

2.1.4 Validity of the Tools that Verify the Design

To verify a requirement by test, the test must be conducted on an item that has been produced in accordance with the design definition for those attributes where test results would be used as verification evidence. Flight and ground test, with appropriate instrumentation, are typically needed to validate environments, functionality, system performance, and margins.

2.1.5 Control of the Design Definition

Management systems that define and control implementation processes are necessary to certify that produced products are understood, and are representative of the design. They describe the organizational structure, along with roles, responsibilities and relationships for managing systems engineering processes and tools. Relevant sub-tier plans address processes control of critical functions including quality management, procurement quality, configuration management, material control, requirements management, risk management.

Configuration control is key to defining hardware and software configuration from baselining of all products at initial release of the Product Breakdown Structure (PBS) to completion of final Certification. Configuration control is key to ensuring that the correct system is built, and that improper substitutions are not made. Configuration control of training and operational products used to operate the hardware and software is also necessary to ensure that the system is not operated out of its certified design range.

The design definition must be controlled to understand changes that are made and the impact to the certification. Design drawings must be controlled so that a change to a drawing that affects the form, fit, or function of that item or its production process is given a

different designation (such as a different dash number or configuration item identifier) from the original drawing (part) number. Any change to the material property in any of the design definition must be controlled so that the change is properly accounted for in all design definition and the impact of change is understood and agreeable by the affected functional disciplines.

2.2 The Production Element

Production certification is the confirmation that a Provider's production process will result in properly integrated "as-built" elements of the system that match the overall physical CTS design or "print." This confirmation assures the elements will meet the performance, safety, reliability, and quality requirements established and verified at the functional level. The scope of this element of the CTS Certification applies to the hardware and software associated with production tooling, test equipment, qualification article(s), flight test articles, and all production articles. Certification of personnel and processes used to create the production articles are also included in the scope. Since the production processes derived for the qualification and first flight articles apply to all articles produced with the scope of this element of Certification.

The Provider's production certification emphasis will be on production and assembly processes that implement critical attributes; failure tolerance, redundancy and hazard controls; and the tests, analyses, demonstrations, and/or inspections supporting the verification of the as-built CTS.

Certification of the system and ability to endorse flight readiness relies on knowing that the products produced and identified by that certified configuration are controlled. The basis of why certification was granted can be affected by manufacturing and special process changes; changes to assembly procedures, which include critical processes; and inspection and testing, which have been identified as part of the design certification. Lessons learned from past programs have highlighted areas where deficiencies in control and screening of hardware resulted in erosion of design margins to the point of failure.

Production critical planning, processes, and inspections, utilized to manufacture flight articles or maintain reusable elements must be compatible with the Provider's hardware and software design and producibility definition. The production system will include a quality management system that meets the intent of AS9100. During manufacturing, despite best efforts in production Certification and process control, there will inevitably be unplanned deltas between the "as-designed" and "as-built" hardware or software elements. These departures will need to be eliminated through rework or ultimately deemed acceptable. Dispositions to non-conformances typically involve either rework intended to return hardware to print, and/or accepting changes to the "as-designed" configuration of the hardware, following review and evaluation. These resolutions often involve exceptions to approved designs or production processes, which are documented through a Provider approved Material Review Board (MRB) and/or waiver/deviation process. Furthermore, non-conformance resolutions must continue to comply with management process requirements for maintaining accurate records of the "as-built" CTS configuration, and for maintaining appropriate levels of production traceability.

A key component of production control is product acceptance by the Provider. Product acceptance is the verification activity that demonstrates that each flight-item produced performs in accordance with requirements and has been fabricated with acceptable quality and workmanship. Formal acceptance test begins at the unit level of assembly and progresses through higher levels of assembly as appropriate up to the final highest level of integrated assembly.

2.3 The Operational Element

CTS Certification includes the confirmation that operational plans, processes, procedures, and operational support systems are consistent with the design of the flight elements and will result in operations which meet mission requirements, while remaining within the constraints established by the verified and validated capabilities of hardware, software, and humans involved. Processes defined for operational authority, such as risk acceptance, material reviews, deviations and waivers, etc. should be included in operational Certification.

Early in the design phase, operational concepts are developed by the Provider which influences the design of flight systems and ground architecture. As these design elements mature, so do the operational concepts. NASA expects the Provider to document these maturing operational concepts and architectures in periodically updated operations concepts documents and in baseline operations plans, which describe the operational support facilities, personnel performing operations in those facilities, and mechanisms to define and control operational processes.

Operations facilities are reviewed to assure that mission critical infrastructure can support the missions and interface with external operational facilities such as the ISS mission control center, Eastern Range, STRATCOM, etc.

3. NASA ROLE IN CTS CERTIFICATION

Traditionally, the NASA approach to certify and accept human spaceflight systems was to provide sufficient resources to engage in complete oversight of the requirements, Design, Development, Testing, and Evaluation (DDT&E) phases. This included full

participation and oversight in the development and operations of the system. The Government employed an integral process review that enabled direct participation and direction by NASA of the design along with its trades and analyses used to drive the design configuration and verification program. Independent assessments, modeling and testing rounded out this resource intensive model of engagement in the design certification of the hardware and software. This ensured the Government had detailed knowledge of the design and the design performance, and provided direction to resolving issues identified during this phase. Established resident office personnel augmented the knowledge gathering of the manufacturing and production phases. Full accountability of ownership of the design and the system were vested in the Government at acceptance and transfer of accountability of the system. Additionally, the Government was responsible for system operation.

With the acquisition strategy implemented by CCP, the Government will neither own the CTS design nor the CTS hardware/software, nor assume operation of the system. CCP will rely more on the Provider to perform the detailed tasks of Certification. The level of knowledge of the CTS required by CCP is modified from the traditional approach, enabling efficiencies to be realized in development and certification phases. CCP will implement a risk-based engagement approach with reduced NASA involvement to substantiate the Provider assertion of Certification.

Factors used to focus this engagement are dominated by two arenas—those that are unique to the Provider and those that are driven by vehicle architecture. Unique characteristics of the Provider are reflected in its program management plans; maturity and control of standards and processes; resources available for peer review and checks and balances; and depth of experience and skill in critical functional areas. Factors driven by vehicle architecture are reflected in functionally critical systems, high-energy or high-risk systems, maturity technology readiness levels (TRL), complexity and robustness of design and hazard controls driven by safety.

3.1 Certification, Verification And Validation Plan Review Task

NASA will review the certification plan to assure it captures the processes to be used and activities to demonstrate the CTS can be certified. In order for this plan to be accepted it must contain:

1) A summary level of CTS configuration with its PBS planned for certification, and a description of each reference mission for which it is being certified.
2) Schedule of certification activities, including critical path, certification milestones, and events within the schedule.
3) Strategy for certifying flight hardware, flight and ground hardware/software including qualification of design, acceptance of flight systems, and mission operations capabilities.
4) Identification of physical resources (facilities, software, and simulators/mock ups, and personnel for human-system performance testing) required to perform the verification and validation activities.
5) Descriptions of the contents of hardware and software qualification reports, hardware and software acceptance reports, verification and validation reports.
6) Description of the products that provide evidence for NASA confirmation of manufacturing, operations, hardware and software qualification and acceptance test programs, environmental testing, and for validation of models and simulations used throughout the life cycle for making critical decisions that may impact human safety.
7) List of content to be delivered in the Certification Data Packages.
8) Understand and accept residual risk due to hazards, waivers, non-compliances, etc.

NASA will review the Verfication and Validation (V&V) Plan, its activities, methods, products, and processes that develop the evidence that all requirements are met:

1) Detailed description of the verification and validation activities to be performed.
2) Descriptions of the documentation and products to be delivered to support verification compliance report closures.
3) Manufacturing and operations verification and validation plans that include hazard controls implemented.

Once these plans are accepted, compliance will be monitored and surveyed throughout the design and development phases using NASA Engineering and Quality insight, with emphasis on potential high risk areas.

3.2 Approval of Alternate Standards

NASA has identified a set of standards for design, production, and operations that represent proven techniques for achieving safe, reliable spaceflight. Alternate standards will be evaluated by the responsible technical authority for its ability to meet or exceed the intent of the NASA designated standard. A formal approval process will be used to determine the suitability of these alternate standards to show they meet the acceptance criteria. When approved by NASA, these standards become the standards by which design, production, and operations products are measured and assessed by NASA.

3.3 Assessment of Management and Process Control

CCP will review Provider's plans to assess capabilities to manage requirements; perform peer reviews; enable robust checks and balances; manage change and process

control; implement quality systems in procurement and production; control non-conforming hardware; and manage elements of risk. Initial assessments and acceptance will be reviewed during major milestone reviews with monitoring for compliance performed throughout the life cycle.

3.4 Assessment of Hazard Reports

NASA will review the Provider's hazard analysis results to assure all potential hazards and hazard causes associated with the CTS have been identified, adequately assessed (qualitatively and quantitatively), and that sufficient controls have been implemented to mitigate each hazard cause. Expectations regarding the Provider's hazard analyses include the following:

1) A description of the hazard analysis methodology used by the Provider and how hazard analysis results are used to influence the integrated CTS design, production, and operations.
2) Hazard analysis results including a description of all potential hazards, hazard causes, controls and crew survival capabilities, and a risk assessment of each hazard cause (consequence and likelihood).
3) A closed loop system for tracking implementation and verification of each hazard control and crew survival capability identified in the hazard analysis.
4) A process for evaluating CTS performance/anomalies, design and operational changes for impacts to hazard controls and associated risks.

The NASA Technical Authorities will review results of the Provider's hazard analyses for completeness and acceptability of residual risks, and make an acceptance recommendation to the CCP program manager. NASA will be responsible for formal approval of the Provider hazard analyses, and acceptance of the identified residual risk.

3.5 Operational Plans

NASA will review the operational plans to assure it captures the processes to be used and activities to demonstrate the CTS can be certified. In order for this plan to be accepted it must contain:

1) What plans and products are required from all CTS elements to prepare or certify readiness for the mission.
2) Plans for implementing the entire operations sequence, including production, processing, scheduling, assembly/integration/test, launch preparation, launch countdown and ascent, on-orbit mission execution, and reentry and recovery.
3) Evidence that integrated space vehicle and facilities are operated within design limits.
4) Include personnel training plans, personnel workload plans, a ground processing plan for launch preparation, a flight plan for launch countdown and mission execution, and abort plans for all mission phases.

3.7 Monitoring of Elements of Design, Development, Testing and Evaluation (DDT&E)

NASA will use a proactive approach to assess critical elements of the DDT&E phases by maintaining a continuous vigilance of the Provider activities to mature the system. Provider planned periodic exchanges of information with the design teams enable NASA's timely recognition of issues involving safety features and reliability concerns that warrant changes while minimizing costly modifications later in the process. NASA will participate in testing activities (test plans, test procedures, test readiness reviews, and the test) for high risk items.

3.8 Substantiation of CTS Certification

CCP's substantiation process includes all of the above tasks performed over the duration of the DDT&E phases of the program. Some of these tasks are two stages (e.g. an approval of a Provider's plan followed by a verification of compliance with that plan). Others are a less formal activity such as monitoring the process for decisions that define the design, production and operations. These less formal processes allow for early detection of problems and to elevate these residual risks for technical or management resolution. Success is measured against the criteria documented in the CCP requirements and plans.

4. NASA ENGAGEMENT IN ASSESSMENT OF PROVIDER CERTIFICATION

CCP implementation of the certification strategy outlined in this section is a proactive approach employing a risk-based method to allocating technical resources and engaging with industry in performing NASA Certification compliance assessments. The implementation of this certification strategy defines the approach to technical evaluation of development and verification activities to obtain confidence that NASA Certification requirements are being adequately implemented and verified. The primary responsibility within CCP for this assurance is delegated to the program Systems Engineering & Integration (SE&I) and systems offices. The Office of Primary Responsibility (OPR) and Subject Matter Expert, in coordination with the Certification Deputy Manager and Partner Manager, define the depth and level of this penetration within the Partner Integration Team (PIT). The SE&I and systems offices, consistent with their OPR assignments, are responsible for assessing compliance to the program requirements. The PIT is responsible for executing the processes outlined within this section in close coordination with the industry partner.

Initially, the PIT will determine the allocation of resources and insight assessment priorities at the outset of each phase of the program using the guidelines described in this section. The SE&I and systems offices are responsible for ensuring that the resources across

the PIT are balanced and commensurate with the assessed risk. The insight assessment will be a continuous activity throughout each phase of the program and will be adjusted as necessary to fit the observations of the PIT assigned to each partner. As technical issues and challenges arise, the adjustments will be accomplished through collaboration between the appropriate representatives on the PIT.

Certification compliance assessments will be documented and maintained through the life of the program by the Certification Deputy Manager. These assessments will reflect the level and depth of penetration achieved through the process outlined above. The two components of NASA endorsement to Certification are completion of the risk-based Certification approach described herein and the closure or acceptance of risks.

4.1 Provider Factors Driving NASA Engagement Strategy

Factors that influence the Provider's ability to provide a robust transportation service include: management and control processes; skill set and experience level in critical functional disciplines; depth in staffing to provide adequate peer review; a strong in-house process of checks and balances across the DDT&E phases; and an effective independent assessment support function. CCP PITs for each Provider will develop knowledge of the capabilities, processes, and risks to align insight resources for optimum support to the Provider as well as knowledge capture relative to the NASA Certification.

How well a Provider implements these features in their organizational structure must be a critical factor in determining NASA resource engagements. Active participation by the NASA team adds value through early identification of risks and enables opportunities for more cost effective mitigations.

The PIT role is critical in understanding and assessing the Provider's CTS and its Certification. Insight acquired by the PIT is the mechanism by which CCP collects data to support substantiation of the Provider's assertion of Certification.

PIT members and their supporting technical discipline leads are assumed to have access to Provider's supporting information. Whenever feasible, they will also be included in the Provider's coordination and/or, planning forums, readiness reviews, design reviews, engineering boards, simulation reviews and briefings, test reviews and briefings, and hardware or operational demonstrations to gain proper insight penetration. The PIT's focus is on activities and practices that support CTS Certification.

Examples of material that PIT members will have access to as part of insight:

1) Products demonstrating closure of NASA verification requirements.
2) Provider standards for design, development, production, manufacturing, operations, training, and other relevant standards.
3) Testing and analyses supporting development, qualification, and acceptance of vehicle hardware/software.
4) Modeling and test article fabrication.
5) Hazard analysis and reports with mitigation plans, requirements, controls, and results.
6) Processes for communication and management of flight safety risk.
7) Products associated with Provider identified risks and mitigation plans, requirements, controls, and results.
8) Products associated with internal and independent verification and validation.
9) Project manufacturing and development.
10) Waivers and deviations.

4.4 Oversight in Certification

Oversight in the CCP context means the acceptance of the Certification information provided by the Providers as evidence of compliance to the requirements. System office personnel are embedded in the PITs to facilitate successful certification and simultaneously review formally submitted documentation for approval. NASA will execute this acceptance through the approval of specific information outlined in the approved certification plans for each Provider.

CCP approval is under the authority of the Program Control Board (PCB) as delegated from the agency. The PCB has delegated limited authority for the approval of technical products to the Technical Review Board (TRB). Certification plans and delivered certification products will be approved by the designated boards after review by program, technical authorities, and flight crew office. In addition, the completion of specified milestones will be approved by the program boards by reviewing a summary of the evidence provided against the entrance and exit criteria established in the contracted Certification plan.

The compliance with safety requirements is formally executed as a subset of CTS Certification. NASA accomplishes this primarily though insight into the decisions affecting safety and engagement of the technical community in decisions affecting risk, and through delivered hazard reports. Safety risks, documented on hazard reports, will be approved by NASA in the program boards as the hazard mitigation process is performed. NASA approval means that NASA understands and accepts the risk documented on the report.

5. GRANTING CERTIFICATION

Certification will be granted when the Provider has shown that they have completed the Certification Plan

and NASA substantiates the Provider's assertion of certification. Recommendations for certification will be reviewed through the CCP PCB, the Joint (CCP and ISS Program) Program Requirements Control Board (JPRCB), and finally through NASA/HQ to the NASA AA. It is anticipated that the recommendation for certification to the NASA AA will be done upon completion of activities associated with the DCR milestone prior to launch. The Provider will perform and show verification satisfaction for requirements. The Provider will also show the agreed-to standards and an established set of project processes have been followed. NASA will perform independent verification and/or validation in some critical areas and of critical models to gain confidence in the Provider. Validation testing agreed to by both NASA and the Provider will be completed to buy down risk. As evidence for review by the NASA AA, CCP will develop a set of recommendations (see CCT-PLN-2000) that will show the certification elements have been met. For missions to ISS, the ISS Program will provide a recommendation to the NASA AA on the completion of the ISS Integration Process. Certification of the CTS for use in transporting NASA crew in accordance with the ISS DRM is granted by the NASA AA.

6. CERTIFICATION MAINTENANCE

After NASA has granted Certification of the CTS for the first crewed flight to LEO, NASA will continue monitoring the Provider's execution of processes described by this paper with the focus shifting to evaluation of changes to the design, production, and operational baseline established in the original certification. In addition, continued operation of the system may expose unforeseen risks through post-flight reconstruction, production failures, obsolescence, or in-flight anomalies. NASA will not assume the responsibility for baseline maintenance of the certification but will be involved through insight in the assessment of changes. When changes are deemed to affect the baseline established at certification, NASA will assess and potentially re-grant certification of affected systems. Key tenets of insight focus on the following areas:

1) All design modifications will be assessed for compliance with Certification requirements.
2) Expansion of operating limits previously certified for the system.
3) Non-conformance/anomaly reviews during production and operations.
4) In-flight anomalies.
5) Pre-flight assessments.
6) Post-flight reconstruction.
7) Audits will be conducted in key areas such as:
    a. Adherence to design and construction standards.
    b. Adherence to operational requirements.
    c. CM and quality audits of production operations.
8) Close-calls and mishaps program will be maintained.

Certification maintenance is the responsibility of the Provider. Significant deficiencies or changes identified through insight or formal audit activities could result in the revocation of the Provider's certification if not addressed by the Provider; therefore, it is in the best interest of the Provider to establish and execute repeatable and reliable processes throughout the life of the system.

7. CONCLUSION

The CCP approach to assuring crew and personnel safety is a combination of CTS Certification to an established set of safety requirements and incremental acceptance of risk by the Provider, NASA, and ultimately the user. Risk is identified, managed, and controlled through defined safety analyses. The residual risk of the CTS is initially accepted through the certification and is managed through proactive maintenance of this certification. CTS Certification consists of three elements: design, production, and operations Certification. Certification of each of these elements is described as a three step process comprised of the Provider developing a CTS that they assert will meet NASA's safety and technical requirements, NASA substantiation of the Provider assertion, and NASA granting Certification. The paper describes the elements that comprise certification and focuses on what must be done by the Provider to achieve certification and by NASA to grant Certification. The traditional NASA approach to certify and accept human spaceflight systems was to provide sufficient resources to engage in complete oversight of the DDT&E phases. With the acquisition strategy implemented by CCP, the Government will neither own the CTS design nor the CTS hardware/software, nor assume operation of the system. As described, CCP will implement a risk-based engagement approach with reduced NASA involvement to substantiate the Provider assertion of certification. Factors used to focus this engagement are dominated by two arenas—those that are unique to the Provider and those that are driven by vehicle architecture