THE EVOLUTION OF THE NASA COMMERCIAL CREW PROGRAM MISSION ASSURANCE PROCESS

Amy Canfield

NASA, Kennedy Space Center, Florida, 32899, USA, amy.c.canfield@nasa.gov

ABSTRACT

In 2010, the National Aeronautics and Space Administration (NASA) established the Commercial Crew Program (CCP) in order to provide human access to the International Space Station and low Earth orbit via the commercial (non-governmental) sector. A particular challenge to NASA has been how to determine that the Commercial Provider's transportation system complies with programmatic safety requirements. The process used in this determination is the Safety Technical Review Board which reviews and approves provider submitted hazard reports. One significant product of the review is a set of hazard control verifications. In past NASA programs, 100% of these safety critical verifications were typically confirmed by NASA. The traditional Safety and Mission Assurance (S&MA) model does not support the nature of the CCP. To that end, NASA S&MA is implementing a Risk Based Assurance process to determine which hazard control verifications require NASA authentication. Additionally, a Shared Assurance Model is also being developed to efficiently use the available resources to execute the verifications.

1. HISTORY OF THE COMMERICAL CREW PROGRAM

The National Aeronautics and Space Administration (NASA) established the Commercial Crew Program (CCP) in March 2010 to facilitate the development of a United States commercial crew space transportation capability with the goal of achieving safe, reliable, and cost effective access to and from low Earth orbit and the International Space Station (ISS). The CCP has and continues to fulfill this objective through multiple procurements and acquisitions in which commercial companies develop elements, subsystems, and systems in support of an integrated commercial crew transportation system [1].

CCP is currently administrating and executing two Commercial Crew Transportation Capability (CCtCap) contracts awarded to The Boeing Company and Space Exploration Technologies Corporation or SpaceX. These contracts will grant NASA certification to each of the Commercial Provider's Crew Transportation System (CTS) when compliance to NASA requirements is demonstrated. It also grants each of the Commercial Provider post certification missions to bring NASA crew to the International Space Station (ISS). Independent from and supporting the CCP are the three NASA Technical Authorities (TA); Engineering, Health and Human Performance, and Safety and Mission Assurance. Each of the TAs are responsible for agency level requirements and are responsible for ensuring NASA Programs comply with the applicable requirements. In addition to the TAs, the ISS Program independently verifies the CCP Commercial Providers comply with the visiting vehicle requirements for the ISS.

The CCP has provided NASA the opportunity for a transformation in how to assure requirement compliance. The transformation started with the first phase, Space Act Agreements, which allowed NASA to provide feedback on each of the Commercial Providers' CTS designs while NASA was refining the CTS requirements. This included obtaining feedback from the Commercial Providers on the CTS requirements during development. Then, once the CTS requirements were baselined, the second phase of contracts allotted NASA the ability to provide feedback on the compliance to the NASA CTS requirements. The next section on the history of mission assurance continues to describe how NASA transformed its methods of compliance.

2. DEVELOPMENT OF PROGRAMMATIC MISSION ASSURANCE REQUIREMENTS HISTORY

NASA's mission assurance program developed throughout the human spaceflight programs, learning from past experiences. After the Apollo 1 accident, separate safety and reliability offices within NASA were formed and Congress formed an independent safety organization called the Aerospace Safety Advisory Panel (ASAP) tasked to provide an independent review of policies and procedures that contribute to risk in the areas of operations, management, and systems [2]. With the Rogers Commission's recommendations from the Challenger accident, NASA created the Office of Safety,

Reliability, and Quality Assurance responsible for safety-related policy; however, it was not until the Columbia Accident Investigation Board's recommendation that it became an independent technical authority [2].

In the development of the firm-fixed price CCtCap contract, the CCP was unwavering in discovering a new way of assuring contract compliance for the development work and services provided. The inspection clause, a deviation to the FAR Inspection of Services, allows inspection of both the services and the research and development work performed. In addition, this new direction also included a limited amount of data requirements deliverable (DRD) documents that necessitated the delivery to and approval by NASA. Therefore, to allow access to the data used in performance of the contract and to continue to cultivate the partnerships with the Commercial Providers, a special Government Insight clause was developed with a complementary DRD, *Insight Implementation Plan*. This Government Insight clause allows the Government to assure compliance to requirements through insight while the DRD allows the Commercial Provider to prescribe how NASA would have access to the data used in support of the CCtCap contract.

In addition, NASA contracts are required by the Federal Acquisition Regulation (FAR) Part 46, *Quality Assurance*¸ and NASA FAR Supplement (NFS) Part 1846, *Quality Assurance*, to ensure that the contractor conforms to the contract requirements. NASA Procedural Requirements (NPR) document 8735.2, *Management of Government Quality Assurance Functions for NASA Contracts*, was developed to implement quality assurance functions defined by these regulations. This document, depending on the criticality and complexity of the acquisition items, defines how NASA will determine its quality assurance functions, including product assurance actions (PAAs). These PAAs, or Government inspections, are selected based on risk factors that include criticality, complexity, maturity, supplier past performance, and personnel safety considerations. Also, PAAs were placed at the last opportunity for inspection in the assembly and integration of the space transportation system. These Government inspections are not a substitute for and do not relieve the Commercial Provider of its responsibility to perform quality inspections; these Government inspections are to ensure the final product is as promised by the Commercial Provider. Programs are required to assign a PAA for every product, processing, and/or performance attribute where a noncompliance could result in loss of human life; these are considered safety-critical [3].

During the Space Shuttle Program, NASA had PAAs, also called Government Mandatory Inspection Points (GMIPs), based on the failure modes and effects analyses and critical items lists for each of the shuttle system elements. Post-Challenger, there were approximately 44,000 GMIPs per flow at Kennedy Space Center [4], which were reduced to approximately 10,000 GMIPs by the end of the Space Shuttle Program. The performance of these GMIPs required the contractor to stop, inform, and wait for NASA quality assurance personnel to witness or verify the compliance to the requirements, which increased the ground processing timeline of the Space Shuttle elements. With the Space Shuttle GMIPs, the quality assurance program was performed mostly through direct oversight of the contractor.

With the move to the commercial environment, the CCP had to find a way of ensuring compliance without performing 100% inspection into the Commercial Providers' organizations, while still complying with NPR 8735.2 requirements. In 2013, the NPR was revised by the Office of Safety and Mission Assurance, permitting programs new ways of determining PAAs, including allowing an exemption of safety-critical PAAs based on either statistical process controls or a formally documented risk analysis [3]. The second exemption, a formally documented risk analysis, is how the CCP determined to proceed. The exemption allows the CCP to use a documented technical risk analysis based on many factors including hazard analysis controls/mitigations to determine and assign PAAs. The Government Insight clause is how NASA prescribed the use of a RBA for determining the PAAs. The following section describes the CCP RBA Process.

3. RISK BASED ANALYSIS (RBA) PROCESS OVERVIEW

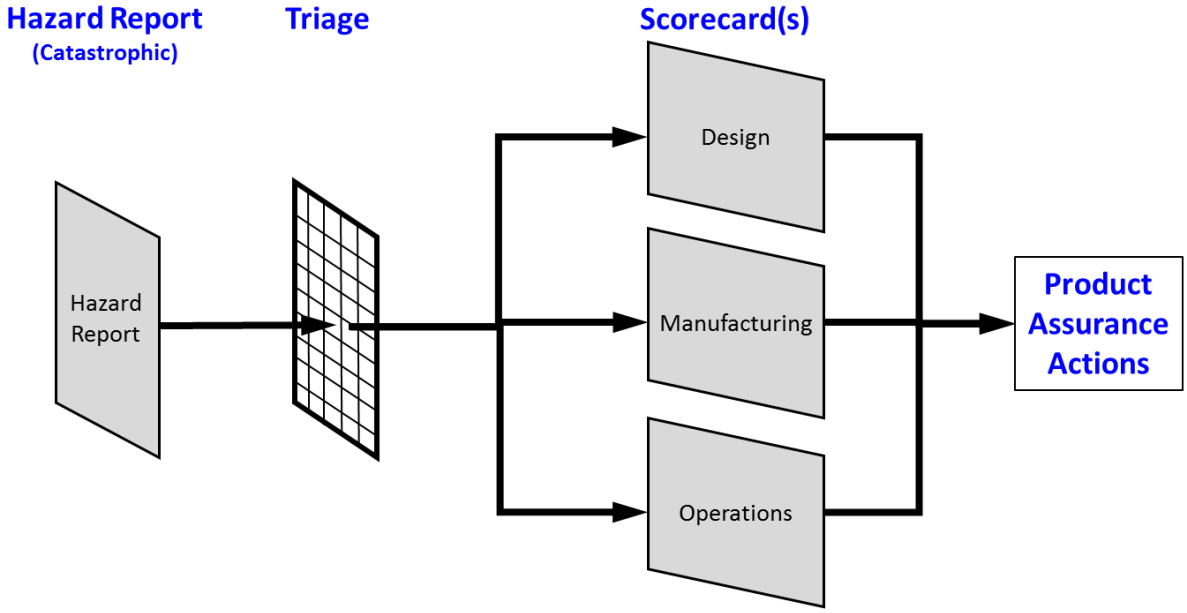

Figure 1. Commercial Crew Program Risk Based Analysis Process

The Safety and Mission Assurance Office supporting the CCP developed the CCP RBA process in ***Figure 1*** by using Safety Technical Review Board (STRB) approved catastrophic hazard reports. The STRB process is described in the previously mentioned paper, "The Evolution of the NASA Commercial Crew Program (CCP) Safety Process [1]." It was determined that catastrophic hazard reports would be beneficial in the process of identifying safety-critical attributes as they address hazards that, if not mitigated, results in loss of human life. The RBA team includes Engineering, program representatives, safety, and quality personnel, most of whom supported the STRB process. The RBA team reviews each catastrophic cause/control/verification set within the hazard report to determine the risk posed if it is not properly implemented. After the RBA team determines the risk of each cause/control/verification set, than based on the risk posed, it is determined whether a PAA(s) is assigned. Unlike the Space Shuttle Product Assurance Actions, the Commercial Provider does not have to wait on the Government to perform its inspection; however, the Commercial Provider is required to provide the Government with enough notice that the activity affected by the PAA is going to take place within a period of time. The RBA process consists of three phases: Triage, Scorecard(s), and Product Assurance. However, the most important part of the RBA process is that it is an iterative process. Once a risk profile is determined, it is re-evaluated after a time to determine if the risk has been abated, stayed constant, or has increased. If the risk has been abated, the PAA will be retired. If the risk is constant or increased, the PAA(s) may be changed. Each of these phases is defined further in the following sections.

3.1 Triage Phase

Upon receipt of the approved catastrophic hazard report, it goes through a Triage. This is a quick sorting of the control/verification sets associated with each catastrophic cause within the Commercial Provider's hazard report. The first two criteria the RBA team takes into account for each cause is an associated Program Risk and an associated risk identified by the Probabilistic Safety Assessment (PSA). The PSA informs CCP of potential risks to loss of crew and loss of mission. These two criteria and evaluation at the cause level allows the RBA team to understand where the CCP has identified potential risks. Next, each control/verification set is evaluated against four criteria and the likelihood of (or risk to) it not being properly implemented. The RBA team gives each of these four criteria a quick "yes" or "no." These four criteria are:

> **Complexity**: whether the design and/or process described within the control/verification set is multifaceted, intricate, complicated, and/or difficult to perform;

Maturity in Aerospace Industry: whether the design and/or process is new or relatively new to industry;

Past Performance: whether the Commercial Provider or sub-tier supplier lacks experience in successfully implementing the control and/or verification; and

Subject Matter Expert and/or Quality Engineer's opinion: is there a high risk to correctly implementing the control/verification set.

If the RBA team answers "no" to all six criteria, then the risk is determined to be low and no PAA is assigned. If there is a single "yes" to any of the six criteria, the RBA team may provide rationale for not sending the cause/control/verification set into the Scorecard(s) phase. However, if the RBA team answers "yes" to more than one of the six criteria, the cause/control/verification set is brought forward to the Scorecard(s) Phase.

3.2 Scorecard(S) Phase

The Scorecard(s) phase is used to further evaluate the risk of the cause/control/verification set against criteria and to calculate a total risk score. A cause/control/verification set can be sent to one or more scorecards, depending on what is described within the control/verification set. The scorecards are: Design, Manufacturing, and Operations.

Design: evaluates the control/verification set with a focus on design, including processes and tools. The criteria include configuration management, design maturity, design complexity, Commercial Provider's past performance in controlling the design.

Manufacturing: evaluates the control/verification set with a focus on manufacturing, including fabrication, assembly, and the associated processes. The criteria include: maturity, complexity, personnel competency, degree of difficulty in the implementation of the verification, and Commercial Provider's past performance or similar experience in manufacturing, processing, materials, and tooling.

Operations: evaluates the control/verification set with a focus on operations, including integration, final assembly, and the associated processes. The criteria include: maturity, complexity, personnel competency, degree of difficulty in the implementation of the verification, and Commercial Provider's past performance or similar experience in operations or processing, materials, and tooling.

The RBA team determines the risk associated with each of the scorecard's criteria and a total risk score is calculated. For the above described criteria, the RBA team defines the risk based on a scale of one to three; with one being low and three being high. In addition, each scorecard includes the hazard cause likelihood from the hazard report and the overall subject matter's and/or quality engineer's opinion of the likelihood of the control/verification set being properly implemented as criteria. For the latter criteria, the RBA team defines the risk based on a scale of one to five; with one being low and five being high. The likelihood is as stated in the hazard report. The total calculated risk score will be between zero and 100. If the risk score is 60 or above, the cause/control/verification set is identified for Government surveillance. If the risk score is below 60, the RBA team may still determine to assign Government surveillance; if not, rationale is provided to support no Government surveillance. The RBA team may also provide to the Quality Engineering team what activity or action the Government surveillance might resemble for the Product Assurance Phase.

3.3 Product Assurance Phase

After the RBA is completed on the hazard report and determined that Government surveillance is necessary for assuring implementation, the Quality Engineering team considers the risk score results and determines the appropriate PAA for each of the cause/control/verification sets identified. These PAAs become the mandatory Government surveillances on the safety-critical attributes of the Commercial Provider's CTS. A cause/control/verification set that is identified for Government surveillance will be assigned a single or multiple PAA(s) that are developed from the descriptions within the hazard report. Quality Engineering may choose from four types of PAAs:

Record Review - A review and verification that recorded data properly evidences conformance to contract requirements (e.g., invoked drawings, specifications). Recorded data, including contractually required data deliverables, may document work performance, product attributes, product configuration, product performance, or quality assurance actions performed by each Commercial Provider. This also includes an assessment of document(s) to verify the planned work conforms to contract requirements [3];

Process Witness - A physical observation of each Commercial Provider's work processes or demonstrations (including tests) to ensure compliance with documented procedure(s) and contract requirements. This includes processes related to manufacturing, fabrication, assembly, integration, repair, maintenance, refurbishment, test, and inspection [3];

Product Examination - A physical inspection, measurement, or test to ensure product conformity to prescribed technical and contract requirements. This method may also include Engineering's independent Verification and Validation of an analysis, model, simulation, or test results 3]; and

Process Audit - Provides assurance of general process health, confirmed by assessing factors such as, process yield, nonconformance(s), and/or repeatability; meaning that the process is clearly-defined and shows consistent adherence to requirements or the manufacturing of the product is stable (e.g., low nonconformance rate). Product/Process audits ultimately confirm that the process is capable of achieving the safety critical attribute(s). Process audits should also confirm that process drift has not occurred since baseline, that process changes are being adequately identified and assessed, and, where applicable, that control plans are adequately defined and implemented [5].

In the development of the PAAs, Quality Engineering assigns the most suitable function for performing the PAA and a CCP System Office the responsibility to ensure its execution. Quality Engineering will also assign a frequency for the performance of the PAAs and also indicates when a re-assessment of the risk profile determined by the cause/control/verification set is performed. The draft PAAs are then sent to the CCP System Office for the assignment of a point of contact (POC). Based on the description of the PAA the POC may be from the Program, Engineering, or Safety and Mission Assurance, allowing for shared assurance. This allows the most suitable personnel be assigned to execute the PAA.

As previously stated, the iterative nature of the CCP RBA process is important. The S&MA Office supporting CCP is responsible for ensuring that the RBA process continues to identify those areas requiring PAAs by understanding the risk profile of the executed PAAs and determining any risk profile changes from other sources, including nonconformance trends and audit findings. The CCP is still in the process of approving Phase II hazard reports, but there has been a large reduction in Government surveillance on safety-critical attributes through this documented risk based analysis.

In the long term, the S&MA Office is investigating a way to allow the RBA process to become a part of the STRB process, eliminating the duplication of meetings for the same resources to discuss the risk profiles of hazard reports. This combining of the STRB and RBA process will allow for a more streamlined approach where the triage and scorecards are combined, enabling a documented risk score for all control/verification sets that includes a weighting for Program risks and Probabilistic Safety Assessment impacts.

4. SHARED ASSURANCE MODEL

The key to making the PAAs for CCP even more powerful is a shared assurance model. The Shared Assurance model is where the most suitable person is allocated based on the skill and expertise which minimizes or eliminates organizational overlap and redundancy [1]. In Shared Assurance, S&MA relies on other organizations to provide some of the assurance functions that were traditionally performed by S&MA.

Traditionally, NASA accepted and owned the hardware/software. The Commercial Provider was responsible for ensuring compliance to NASA levied requirements of the hardware/software; however, NASA programs and TAs had a substantial role, not only in certification, but also in the assurance of flight safety [1].

In the CCP business model, NASA is purchasing a service. The Commercial Providers retain ownership of the hardware/software and are required to certify their CTS to NASA CTS requirements. As NASA is purchasing a service, its traditional role is reduced; however there still exists a responsibility to assure crew safety. As described in the previous sections, the PAAs developed from the risks identified from catastrophic hazard reports during the CCP RBA will be executed by the most suitable personnel; for example, a design-type PAA, like a stress analysis, engineering would be the most suitable. In addition, the CCP is sharing the resources and data from the ISS Program and the Launch Services Program. The key aspects of Shared Assurance are using the most suitable persons to perform the PAA, allowing the elimination of overlap among the NASA Program and TAs without losing the ability to assure the safety of NASA's crew.

5. SUMMARY

The Risk Based Assurance process that enables the CCP to use a technical analysis of risk to determine which hazard cause/control/verification sets require NASA surveillance has greatly reduced the number of mandatory Government surveillance points. Initial runs of the RBA process confirm that this is indeed the case. The RBA process in conjunction with shared assurance, is allowing the CCP to efficiently use available resources to execute the mandatory Government verifications and provide sufficient surveillance to ensure each of the Commercial Providers are providing the Government a safe crew transportation system to the ISS.

REFERENCES

1. Kirkpatrick, P., and N. Vassberg. *The Evolution of the NASA Commercial Crew Program (CCP) Safety Process*. Proc. of 7th IAASS Conference "Space Safety Is No Accident", Friedrichshafen, Germany: October 2014. Print.
2. Columbia Accident Investigation Board. *Columbia Accident Investigation Board Report*. By Harold W. Gehman. Vol. I. Arlington, VA: Columbia Accident Investigation Board, August 2003. Print. 178 to 193.
3. United States. National Aeronautics and Space Administration. Office of Safety and Mission Assurance. *NASA Procedural Requirements (NPR) 8735.2B, Management of Government Quality Assurance Functions for NASA Contracts. NODIS Library*. NASA Safety and Mission Assurance, 12 August 2013. Web. 8 April 2016.
4. United States. Government Mandatory Inspection Point Independent Assessment Team. *Government Mandatory Inspection Point (GMIP): Independent Assessment Final Report*. Washington, D.C.: National Aeronautics and Space Administration, January 2004. Print.
5. United States. National Aeronautics and Space Administration. Commercial Crew Program. *Commercial Crew Program Surveillance Plan*. Kennedy Space Center: CCP Program Control and Integration, December 2015. Print.