Commercial Crew Program
Crew Safety Strategy

Nathan Vassberg
Chief Safety and Mission Assurance Officer
And
Billy Stover
Chief Kennedy Space Center CCP S&MA Office
04/20/2015
SpaceX:
Falcon with Dragon 2

Boeing:
Atlas V with CST-100
Agenda

- Commercial Crew Program Purpose
- Crew Safety Boundaries
- How we achieve Human Rating
- CoFR Strategy
- Shared Assurance Model
Purpose/Background

• **CCP Mission Statement:** The purpose of the CCP is to facilitate the development of a U.S. commercial crew space transportation capability with the goal of achieving safe, reliable, and cost effective access to and from low Earth orbit (LEO) and the International Space Station (ISS).

• **Background/Assumptions:**
  - CCP manages a human rated spaceflight services based contract
    - Commercial Provider owns the design (Not NASA)
    - NASA does not own the hardware, software, or systems used to fabricate, assemble, test, launch, or recover crew to and from ISS
  - Certification of the Commercial Transportation System (CTS) is the responsibility of the commercial partner
  - NASA Commercial Crew Program must provide a certification package (CoFR) to NASA Administrator indicating system is safe enough for NASA crew members to ride
  - NASA Technical Authorities must concur with Certification and Risk Acceptance
  - Resources to execute and manage CCP and meet agency expectations for Human Rated Program are limited therefore using Risk Based Approach to identify where, who, and how much so that crew safety is maintained
Definitions

Safety Critical Attribute: attributes that if violated that can credibly result in loss of human life. This includes witness or verification of hardware, manufacture, assembly, integration, test, maintenance, operation, or non-conformance resolution tasks which if, incorrectly accomplished could result in loss of life. (Reference NPR 8735.2)

Catastrophic Event: An event resulting in the death or permanent disability of a ground crewmember or flight crewmember, or an event resulting in the unplanned loss/destruction of a major element of the CTS or ISS during the mission that could potentially result in the death or permanent disability of a flight crewmember. (Reference CCT-PLN-1120 Appendix B: Definitions)

Shared Assurance: The use of NASA personnel assigned or supporting CCP that have the knowledge, skills, and experience to assure a partner’s activity is appropriate and meets the needs of NASA and CCP requirements for ensuring a “safe, reliable, and cost effective” delivery and execution of a certified CTS (Mission Success = Human safety/crew survivability + mission assurance).

CCP Safety Boundaries
(Catastrophic & Critical)

* - Exceptions to these boundaries will be identified during verification of CCT-REQ-1130 Sec:3.11.1

OR

Identified during HR and RBA reviews as control to a Catastrophic Event Cause (i.e. – manufacturing or Ops control)
Human Rating Requirements Flow down for CCP

Human-Rating Requirements for Space Systems NPR 8705.2B

Commercial Crew Transportation System Certification Requirements for NASA Low Earth Orbit Missions Certification Data Package HEOMD-CSD-10001 (formerly ESMD-CCTSC-12.10)

Allocated in full

NASA Certification Evidence & Endorsement

The CCTS Certification Requirements, based upon NPR 8705.2, provide a solid foundation for Contractor Assertion and NASA Endorsement of Certification

Allocated / Derived

NASA Insight

CCICap NASA Insight, Oversight and Independent Certification Activities

Allocated in full

CCT-PLN-1000

Commercial Crew Program Plan

CCT-PLN-1100

Crew Transportation Plan

CCT-PLN-1110

Crew Transportation System Design Reference Missions

CCT-PLN-1110

Crew Transportation System Technical Management Processes

CCT-PLN-1150

ISS Crew Transportation and Services Requirements Document

CCT-PLN-1130

Crew Transportation Standards and Processes Criteria

CCT-PLN-1140

ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document (IRD) SSP 50808

Allocated in full

Allocated in full

CCICap Contract Requirements J-01, Integrated Requirements J-02, Data Requirement Deliverables J-03, Performance Work Statement

Contractor Certification Data Package (DRD 112)

Allocated in full

Incremental Acceptance thru DRRs & Milestone Approval

CBS Data Package (DRD 102)

DCR Data Package (DRD 103)

FTRR Data Package (DRD 104)

ORR Data Package (DRD 105)

CR Data Package (DRD 106)

Certification Plan (DRD 107)

V&V Plan (DRD 108)

Flight Test Plan (DRD 109)

Hazard Reports (DRD 110)

VCNs (DRD 111)
NASA Process for Certification of Flight Readiness (CoFR)

CoFR

Certification + Accepted Risk

Surveillance

SMSR (Safety and Mission Success Review)

FRR (Flight Readiness Review)

Certification Surveillance + Accepted Risk CoFR
• While some areas of S&MA role have changed, S&MA has appropriate influence and authority
• S&MA TA is voting member of Safety Technical Review Board, Technical Review Board and Program Control Board
• CCP S&MA Office and TA have good working relationship with Program
• CCP S&MA Office works closely with S&MA TA
  • Alternate path through KSC S&MA director if needed
• S&MA TA has direct path to OSMA if concerns are not heeded

Certification Strategy Acceptable to S&MA
Assessment of Changes in Surveillance Scope and Roles

- No concerns about reduced surveillance if:
  - Maintain good communication between CCP offices
  - Setup and maintenance of Surveillance database
  - Adequate S&MA resources to support intra-program assurance role
- CCP S&MA Office and TA have good working relationship with Program
- CCP S&MA Office works closely with S&MA TA
  - Alternate path through KSC S&MA director if needed
- S&MA TA has direct path to OSMA if concerns are not heeded

Surveillance Strategy Acceptable to S&MA
Assessment of Accepted Risk Strategy

- Tracking and risk analysis modelled on LSP approach (Document KTI-3643)
  - Information gathered from insight efforts
  - Anomalies have progressive attention
    - Evaluation → Watch Item → Risk
- Issues will arise from both Certification and mission-to-mission phases
  - Design/mission/environment changes
  - Non-conformances in build process
  - Test failures from similar systems or other fleet vehicles
  - Acceptance test results
  - Use SMEs and VSEs to evaluate risk level
    - Can supplement with independent assessments, NESC, etc.
  - Increasing management notification as risk increases

Risk Acceptance Strategy Acceptable to S&MA
Shared Assurance: A process that uses risk based decision making to identify and allocate resources based on level of risk while minimizing or eliminating organizational overlap and redundancy

Key Concepts:
- Technical Breadth remains unchanged
- Technical depth changes
  - Level of penetration determined by Risk Assessment
  - NASA Insight is an essential to identify and develop understanding of risk
- Minimize Organizational Redundancy (limit multiple organizations overlap) – important to clearly define roles and responsibilities

- End goal is Certification of Flight Readiness (CoFR)
  - CoFR = Certification + Surveillance + Risk Acceptance
CCP Shared Assurance – What is Different?

Next: How to get from Traditional to Shared Assurance Model
CCP Shared Assurance - What are we giving up?

Giving Up: Depth of Coverage for Identified Low Risk Areas

Insight Baseline for CCP/Engineering/H&M/S&MA

Breadth of coverage by system not changed

Depth of coverage varies according to Risk Level

Traditional Cert LOE

CCP Baseline LOE

Sub systems and areas of Technical Risk

ECLSS  Structure  Power  TCS  Prop  C&T  GNC  IV&V  Non Conformances  CM

Note:
The profile is expected to be unique for each provider and changing over time

Changes in High Priority Areas?
### Safety and Hazard RBA/Shared Assurance Flow & Examples

#### Hazard Report Identifies Following Controls:

<table>
<thead>
<tr>
<th>Hazard Report</th>
<th>RBA Results</th>
<th>Surveillance Activities</th>
<th>Organization</th>
<th>Performance</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect for Sharp Edges and Burrs</td>
<td>Low Risk</td>
<td>None</td>
<td>N/A</td>
<td>Nominal Trending / Nonconformance Monitoring</td>
<td>Reports as required</td>
</tr>
<tr>
<td>Perform Integrated Hardware/Software Testing of GN&amp;C algorithm for docking with ISS</td>
<td>High Risk due to complexity and known sensitivity to algorithm tolerances</td>
<td>Witness and participation in testing. Perform Independent verification of algorithm(s)</td>
<td>Engineering: GN&amp;C and IV&amp;V</td>
<td>Performs on site visit to witness and participate in testing.</td>
<td>Activities documented in CCP Surveillance Database, summarized for CCTS CDP</td>
</tr>
<tr>
<td>Ensure proper quality assurance process implemented by component supplier</td>
<td>Moderate Risk that would makes NASA surveillance prudent</td>
<td>Process Audit</td>
<td>S&amp;MA: Quality Assurance</td>
<td>Performs a process audit to ensure proper flowdown of QA requirements to hardware supplier.</td>
<td>Activities documented in CCP Surveillance Database, summarized for CCTS CDP</td>
</tr>
</tbody>
</table>
Summary

- CCP is applying and verifying to Human Rating requirements
  - HEOMD-CSD-10001 Rev A

- CCP is using a Risk Based Assessment approach to identify the areas of high risk and focusing resources onto those areas
  - This is a living process and where risk arises adjustments will be made appropriately

- CCP is using a Shared Assurance model to adequately cover the identified areas with the right resources minimizing overlap and redundancy
  - S&MA will not review everything but everything will be reviewed by a US government employee with the right knowledge and skills

- CCP S&MA’s Prime Mission is Crew Safety

Purpose – “…with the goal of achieving safe, reliable, and cost effective access to and from low Earth orbit (LEO) and the International Space Station (ISS).”