

SMA Support Office (SSO)

Presented by Kathy Malnick & Chad Schaeffer
September 10, 2014

Software Assurance Challenges for the Commercial Crew Program



- Commercial Crew Program (CCP) Overview
- SSO Support
- Software Assurance Challenges
- Questions



Program Overview

- Competitive program to transport crew to/from ISS using commercial services
- Managed by Kennedy Space Center
 - With support from around the Agency
- Highly visible program
 - Attention around the Agency and NASA Headquarters
 - Political/media attention and pressure
- Multiple program phases
 - Different “contract” vehicles (Space Act Agreements, formal contracts)
 - Providers may be down-selected at any of these phases
- Non-traditional Approach
 - Unique acquisition and partnering approach (fosters competition)
 - Reduced set of requirements that focus on what not how



Program Overview

- CCDev1 = Commercial Crew Development Round 1



Type: Space Act Agreement

Focus: Develop commercial crew transportation concepts and enabling capabilities

- CCDev2 = Commercial Crew Development Round 2



Type: Space Act Agreement

Focus: Design, development, test, review of systems



Program Overview

- CCIcap = Commercial Crew Integrated Capability



3 providers



Type: Space Act Agreement

Focus: Perform tests and mature integrated designs

- CPC = Certification Products Contract



3 providers
(same as CCIcap)



Type: Contract

Focus: 1) Develop products to implement NASA flight safety and performance requirements;
2) Develop certification plan to achieve safe, crewed missions to the space station



- CCtCap = Commercial Crew Transportation Capability

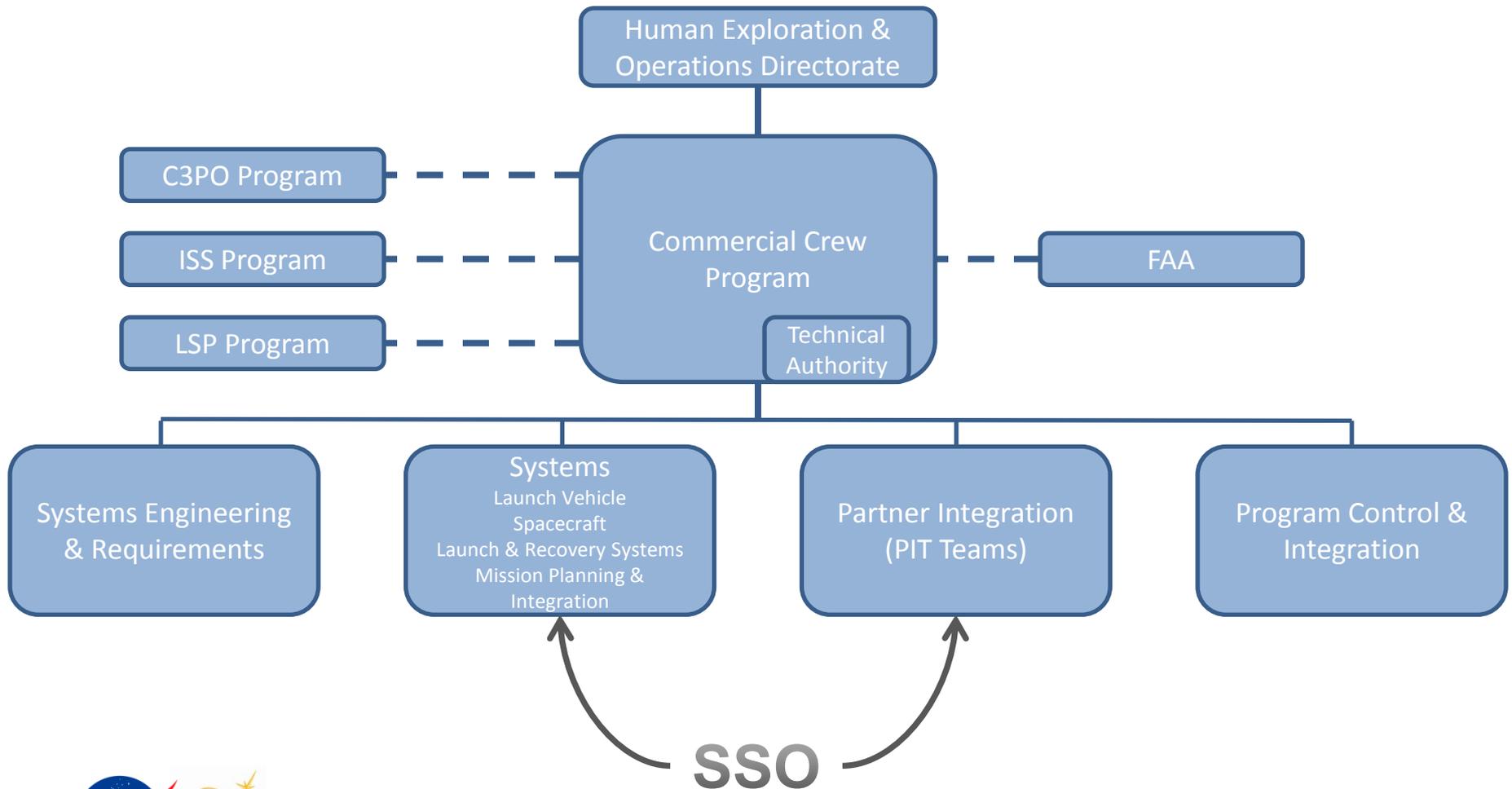


TBD providers
(dependent on funding)

Type: Contract

Focus: Final development, testing, verifications to allowed crewed demonstration flights to ISS

NASA CCP Organization Structure



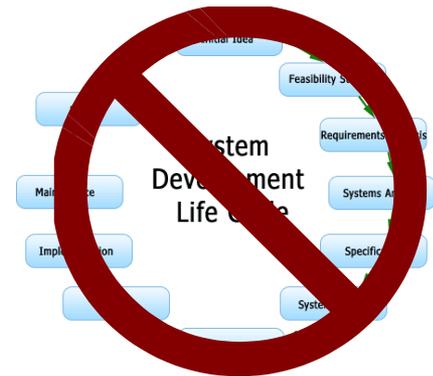
- CCP Safety & Mission Assurance (SMA) focused on crew safety
- SMA Support Office (SSO) is providing Software Assurance reach-back support for the CCP SMA team
 - Main support focused on assessing Alternate Standards and Hazard Reports
 - Also supported verification reviews, review boards, etc.
 - Provided support in CCiCap and CPC phases; support to continue through CCtCap phase
 - Generated approximately 700 comments with 99% acceptance rate



Software Assurance Challenges

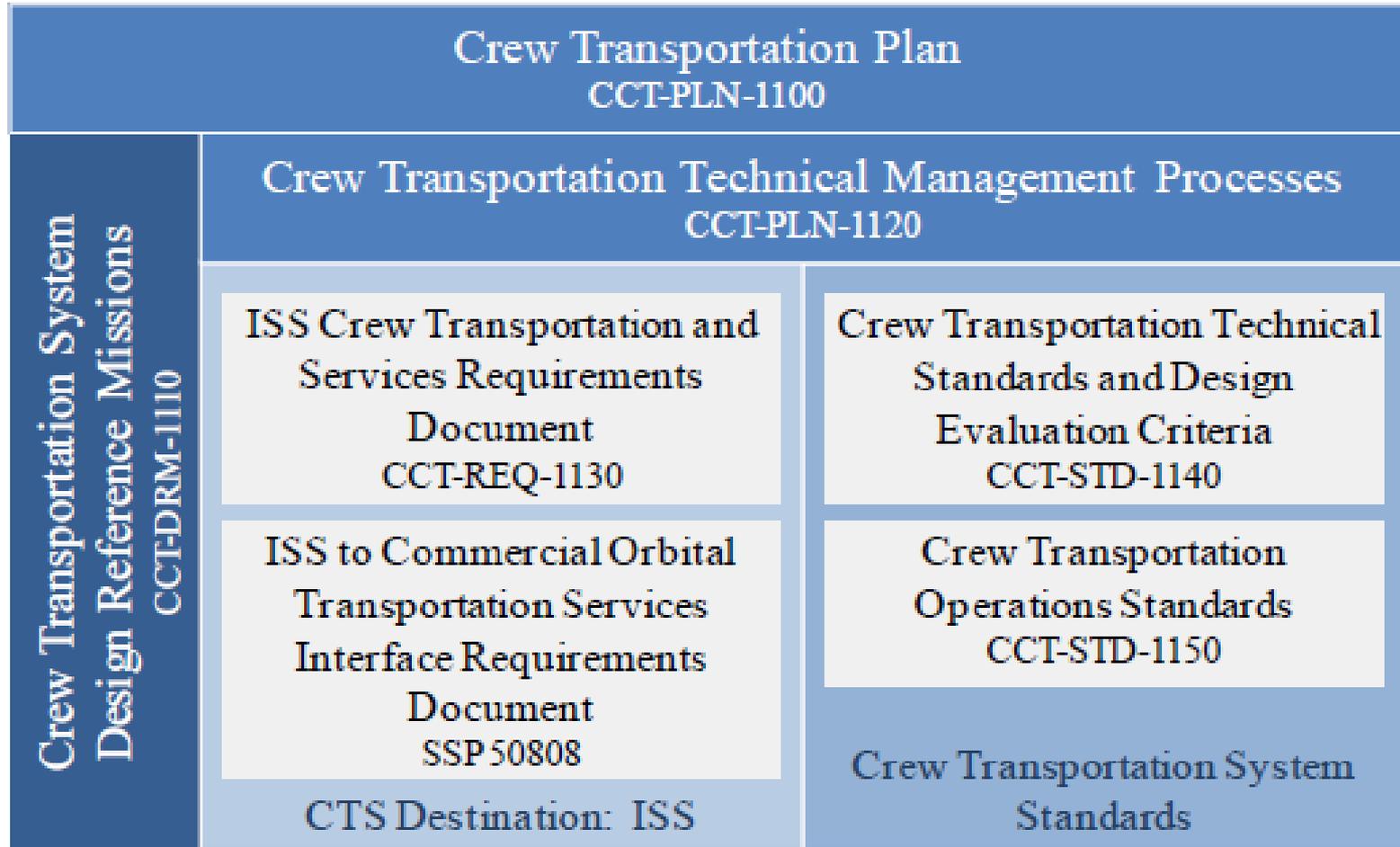


CCDEV1
CCiCap CCDEV2
CPC
CCTCap



- Challenge: Atypical approach
 - Unique requirements approach (“what” rather than “how”)
 - Allow alternates to NASA standards, including specific waivers
 - Unique provider methods, processes; varying levels of experience working with NASA
- Solution(s)
 - Map provider processes to NASA requirements = understand how NASA’s goals being met (“meet the intent”)
 - Requirement by requirement assessment across artifacts
 - Assess gaps to qualify and communicate risk
 - Be flexible; give providers as much freedom as possible without unnecessary risk to NASA





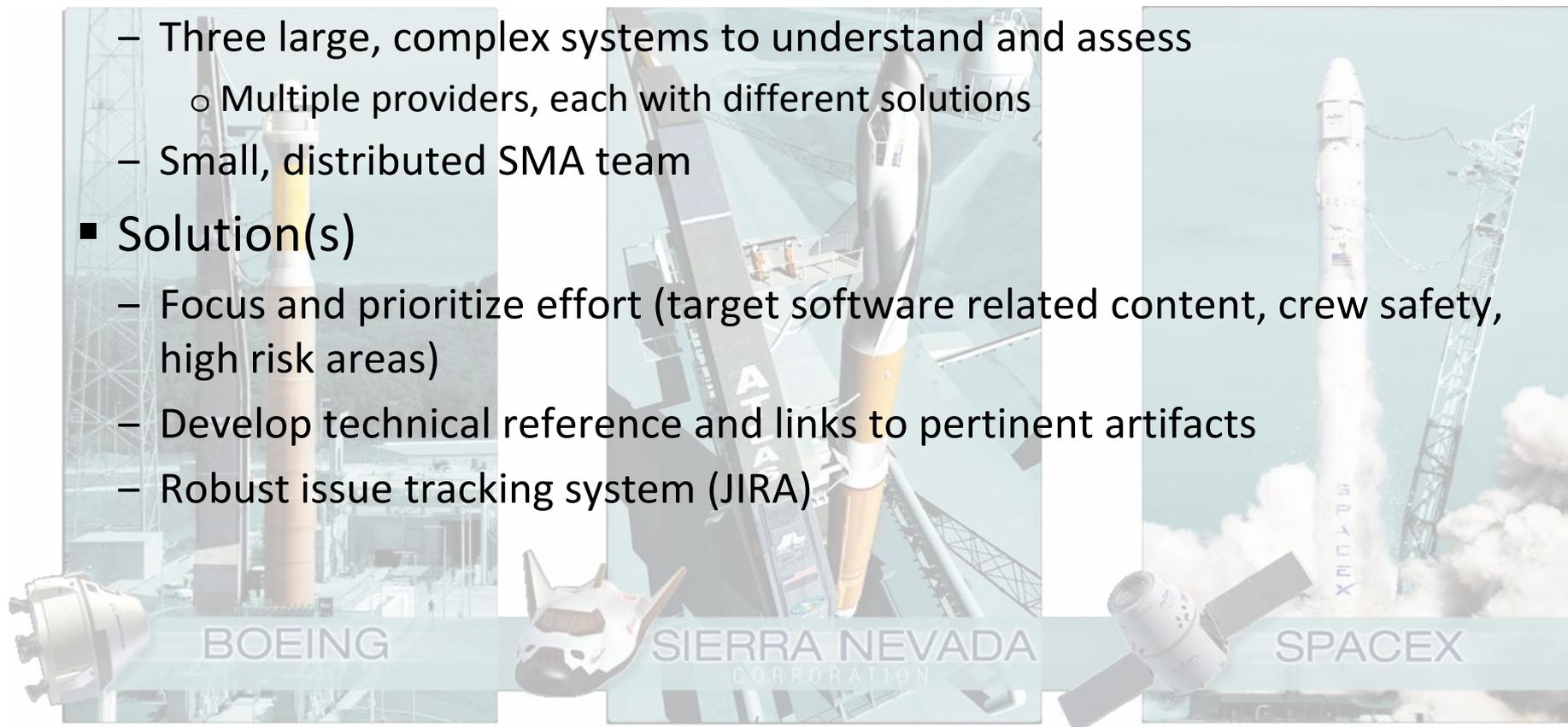
Large Program, Multiple Commercial Solutions

■ Challenge: Large amount of technical and process information

- Three large, complex systems to understand and assess
 - Multiple providers, each with different solutions
- Small, distributed SMA team

■ Solution(s)

- Focus and prioritize effort (target software related content, crew safety, high risk areas)
- Develop technical reference and links to pertinent artifacts
- Robust issue tracking system (JIRA)



Keeping Proprietary Data Separate

- Challenge: Protecting proprietary data
 - One team providing assurance to multiple providers
 - Cannot cross-pollinate information across providers
 - Core situations: performing analysis and during discussions such as teleconferences, review boards
- Solution(s)
 - Commercial Crew Program limited access to provider data
 - SSO used firewalls and processes to protect data
 - Point of contact (POC) assigned to each provider
 - Partner artifacts maintained on CCP repository (not stored locally)
 - Sensitive data stored in protected locations with restricted access
 - Separate analysis work products



Different Funding Vehicles

- Challenge: Different funding vehicles (rules of engagement)
 - CCP executing using combination of funding vehicles
 - Space Act Agreements, contracts each with different rules: improving product vs. grading; suggestions vs. direction
 - Blackout periods during contract selection
- Solution(s)
 - Rigorous peer review process (SSO and CCP)
 - Feedback provided to CCP SMA POC to share with provider at his discretion through available channels
 - Robust comment tracking system (JIRA)
 - Comments phrased as issues and recommendations to support both sets of commenting rules (when appropriate)
 - When in direct communication, ask questions to expose potential defects (rather than stating as issue)

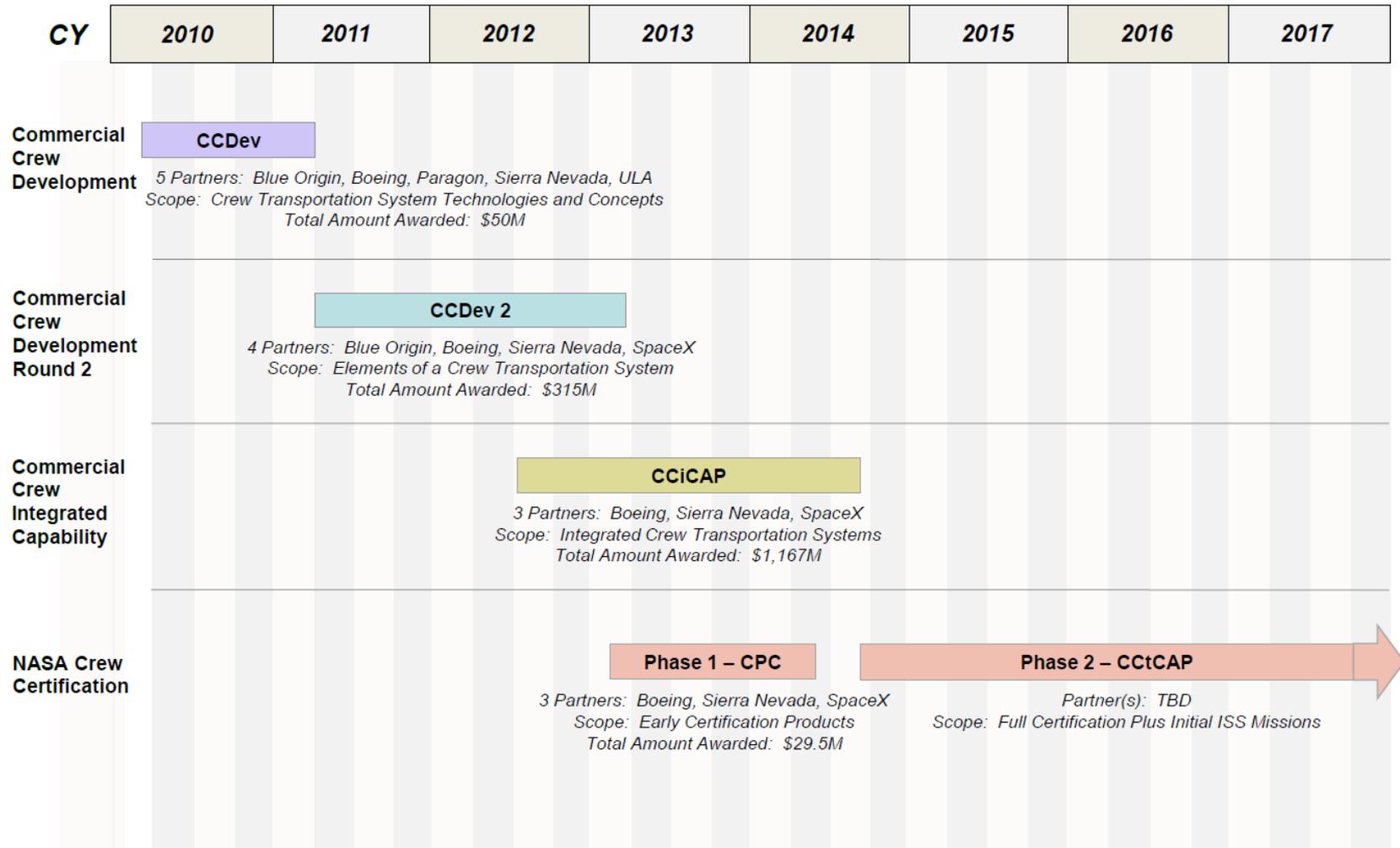


Concurrent Program Phases

- Challenge: Multiple phases executing concurrently
 - Concurrent phases with different rules
 - Artifacts delivered multiple times
- Solution(s)
 - Analysis work products persist across phases
 - Past comments are verified/updated
 - Assessment products capture history and current state of artifact
 - Provide evidence-based assurance (specific references into provider documents as basis for conclusions and findings)
 - Focus assessments on the changes (create compare reports using software tools, etc.)
 - Tailored deliveries (exports from JIRA) to CCP SMA POC based on “rules” for the specific phase



CCP Program Phases

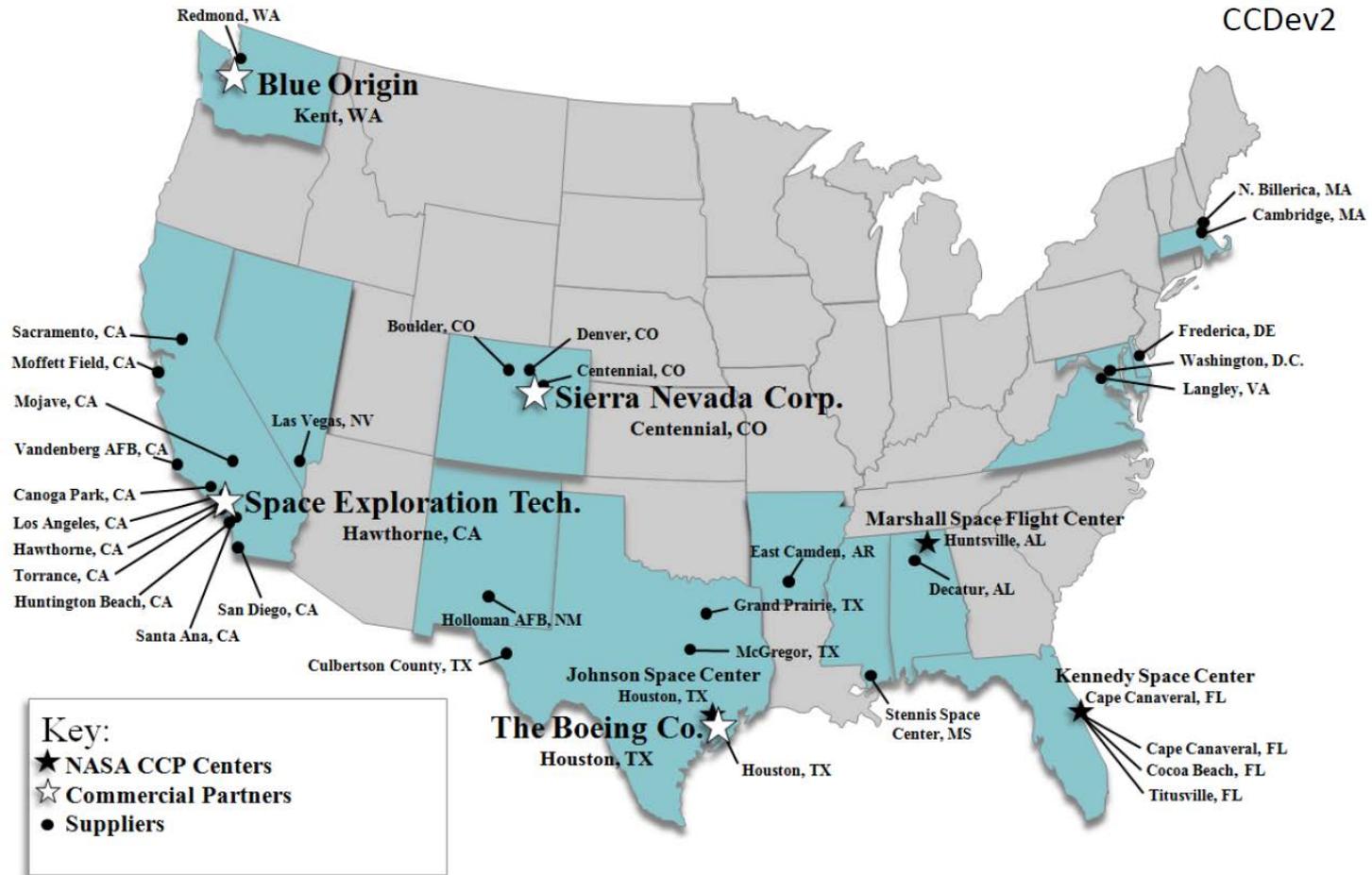


Multiple NASA Stakeholders, Projects

- Challenge: Multiple stakeholders
 - Distributed and diverse stakeholders
 - Other crewed programs have similar requirements/goals
 - Risk of providing inconsistent direction and interpretation
 - For example MPCV has similar requirements to CCP and may have interpreted them differently
 - Example: common mode software challenge
- Solution(s)
 - Large focus on establishing and maintaining communication (added onsite representative, face to face when possible)
 - Pro-actively identify and pursue potential areas of support
 - Document thought papers to facilitate communication
 - Use pre-determined criteria to keep assessment consistent



CCP Partners and Suppliers



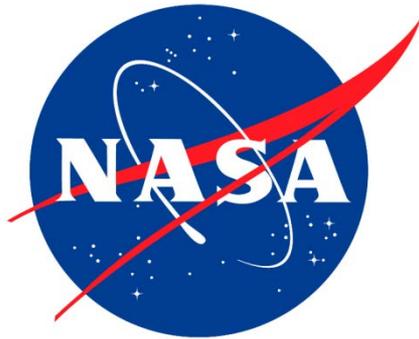
Other Challenges

- Reviews focused on delivered artifacts rather than program goals/standards
- Limited processes/templates to perform assessments
 - No definition for “meets the intent”
 - No process for how to assess hazard reports
- Shortened timeframes
 - Last-minute deliveries from providers
 - Late assignments by the Program



Questions?





TASC
INSIGHT APPLIED™

WVHTC
FOUNDATIONSM

Backup



- Partner Integration Teams (PITs)
 - Focal point to gain insight into provider design, practices
 - Utilize provider existing and planned activities and technical information to:
 - Gain knowledge, understanding of provider requirements, requirements flow-down, change management, design, processes
 - Identify, assess risks that could adversely affect performance milestones
 - Identify, assess risks that could adversely affect CTS certification
 - Assist provider with technical expertise, issue resolution
 - Integrated teams led by CCP representative
 - Engineering, Safety and Mission Assurance (S&MA), Crew Health and Medical (H&M), and Flight Crew and Operations representatives
 - ISS Program will participate to identify impacts to ISS controlled operations and hardware/software



- Partner Manager
- Deputy Partner Manager
- Technical Integration Lead
- Systems Lead (s)

*Dedicated Full Time
Members*

- Engineering
- Flight Crew Office
- Crew Health & Medical
- Operations
- Safety & Mission Assurance

*CCP Matrix Staff
Participation As
Needed*

➤ System & Discipline Specialists

*➤ Struc, Mech, Guid, Nav, Control, Prop, Pwr, Therm,
Comm, TPS, Aero, Crew Sys, ECLSS, etc.*

- NESC
- NSC

*External to CCP
Participation As
Needed*



Hazard Report Assessment Methodology



Hazard Report Assessment

- Hazard reports (HRs) are a contract deliverable for CPC and a required input to CCtCap contract milestones
- SSO has been providing reviews of hazard reports from a software assurance perspective (reach back support)
- SSO developed method to capture objective evidence (executed for all three partners' CPC initial deliveries)
 - Phase 1: Evaluate assigned HRs
 - *Phase 2: Assess hazard coverage
 - *Phase 3: Identify software content
 - *Phase 4: Evaluate additional HRs

*Stretch Goals



Phase 1: Evaluate Assigned HRs

■ Purpose

- Review CPC hazard reports that were assigned to SMA software assurance lead for software related defects
- Considered minimum success criteria

■ Method

- Defined evaluation criteria with rationale and guidance
 - Ensures all partners receive identical assessment
 - Documents evidence
- General comments (which apply to all HRs) were delivered separately to reduce perceived duplicate comments and documentation/tracking burden



Phase 2: Assess Hazard Coverage

- Purpose:
 - Identify catastrophic hazards that were not reported
- Method
 - Created a list of hazards from previous crewed missions (Constellation, Shuttle, etc.)
 - Leveraged IV&V Program's past experience
 - Assessed applicability for each partner (included all HRs, not just software influenced HRs)
 - Traced delivered hazard reports to expected hazards and identified gaps
- This approach was not intended to be a perfect solution and its limitations were well understood and documented
 - Independently performing a PHA was not feasible
 - One previously undocumented hazard that is accepted will add value in understanding the risk and more than cover expense of analysis



Phase 3: Identify Software Content

- Purpose
 - Identify additional hazard reports that should receive assessment by software assurance
- Method
 - Pre-defined where software causes and controls were expected for past hazard list (Yes/No/Maybe)
 - Documented where software is documented in each delivered hazard report (Yes/No)
 - Compared expectations with reality to find hazards where software was expected, but was missing
 - Additional prioritization schemes may be used in the future (e.g., severity, software impact)



Phase 4: Evaluate Additional HRs

- Purpose

- Review CPC hazard reports that were not assigned to SMA software assurance lead, but would benefit from such review

- Method

- Executed method described in Phase 1 for HRs identified in Phase 3



Metrics by Phase

HR Analysis Phase	# of Comments	POC Acceptance Rate
Phase 1	141	100%
Phase 2	3 (88 potentially missing hazards)	100%
Phase 3	N/A	N/A
Phase 4	40	97.5%

Phases 2-4 added significant value through generated comments, impressed CCP with rigor and methods, and improved SSO's understand of each provider's system and processes

*Only includes Significant and Noteworthy comments (excludes Editorial) from CPC initial delivery of hazard reports

**Acceptance Rate excludes comments with unknown acceptance (31 of 184 comments unknown at this time)



Large Program, Multiple Commercial Solutions

