



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



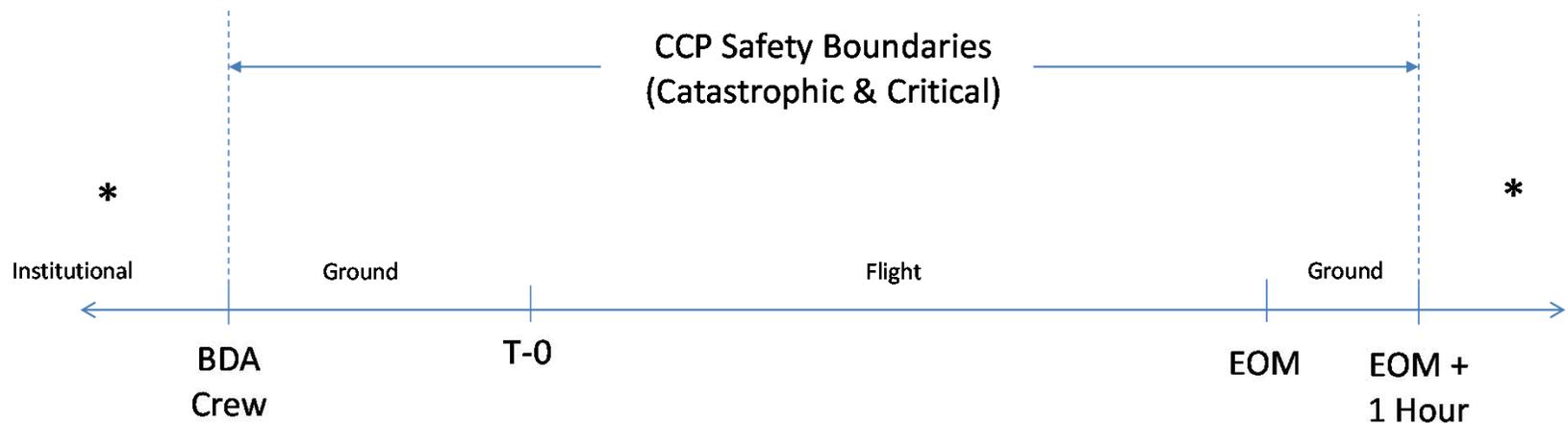
Crew Safety – CCP Scope and Boundaries

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 closeout 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).



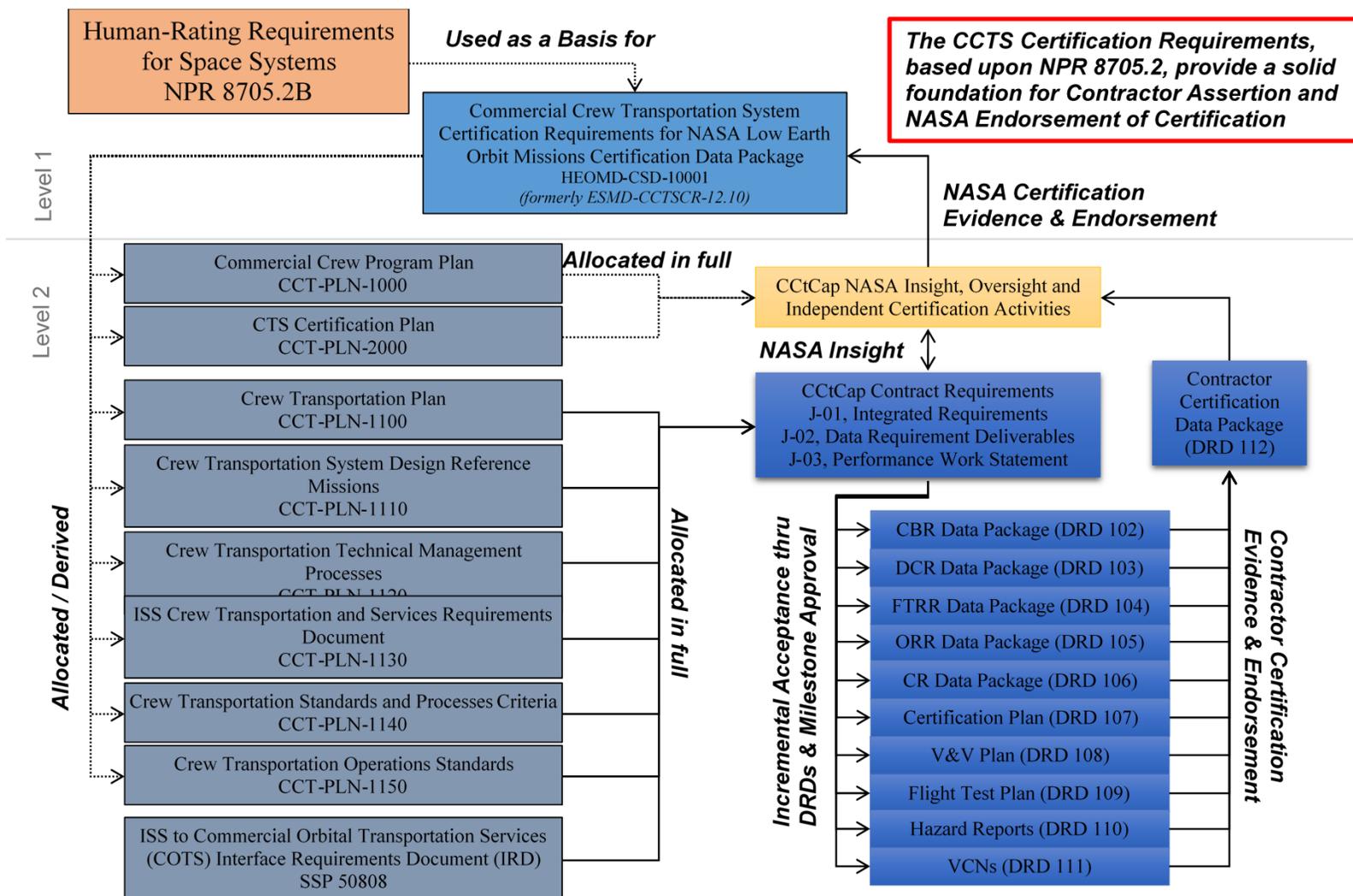
* - Exceptions to these boundaries will be identified during verification of CCT-REQ-1130 Sec:3.11.1

OR

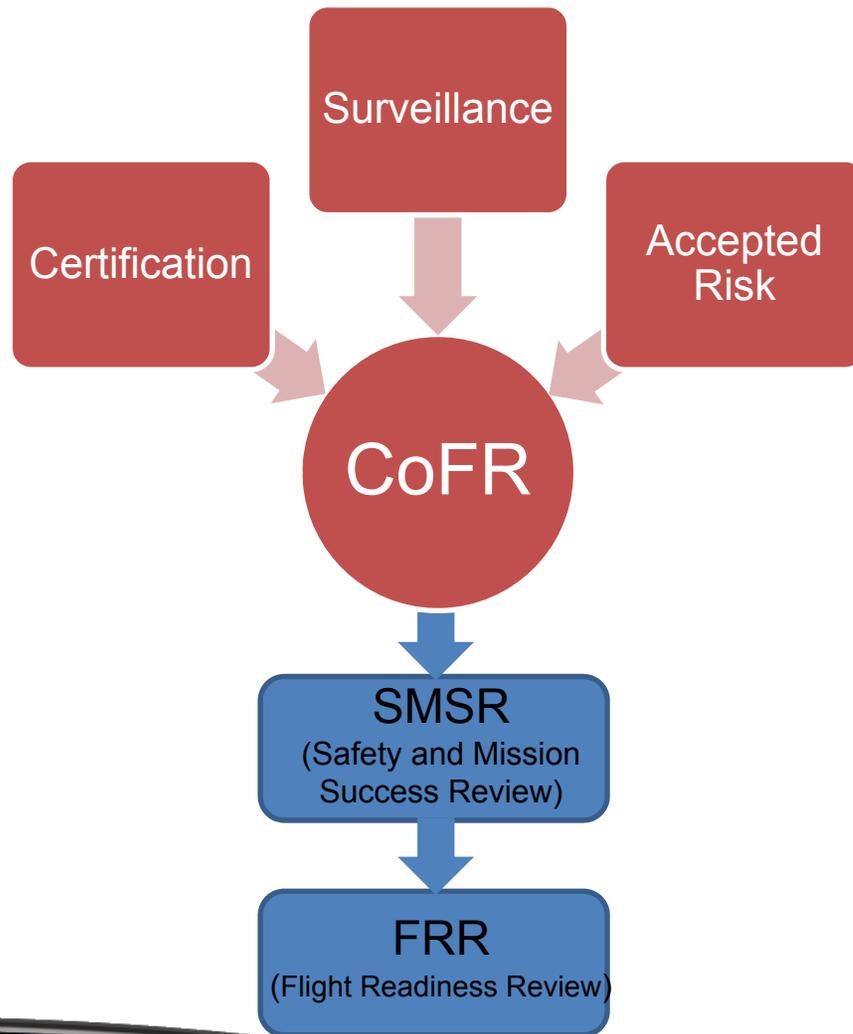
Identified during HR and RBA reviews as control to a Catastrophic Event Cause (i.e. – manufacturing or Ops control)



Human Rating Requirements Flow down for CCP

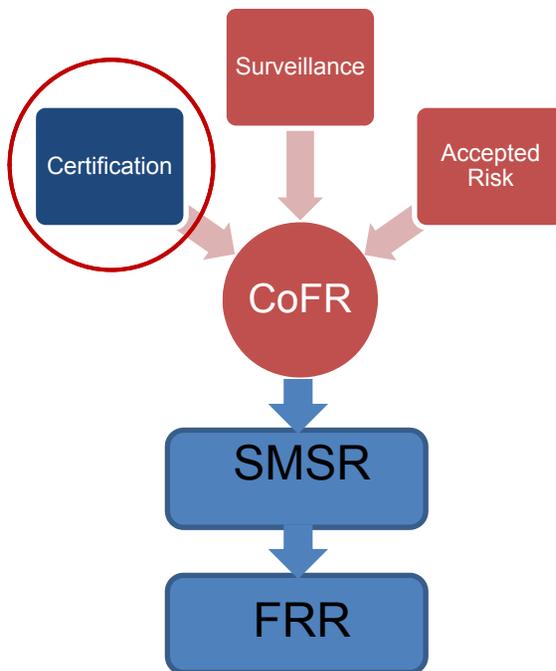


NASA Process for Certification of Flight Readiness (CoFR)



$$\frac{\text{Certification} + \text{Surveillance} + \text{Accepted Risk}}{\text{CoFR}}$$

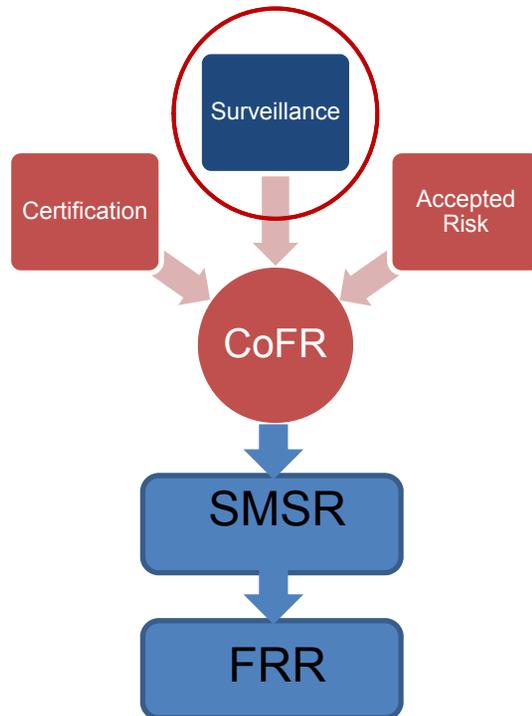
Assessment of Changes in Certification Endorsement Role



- 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

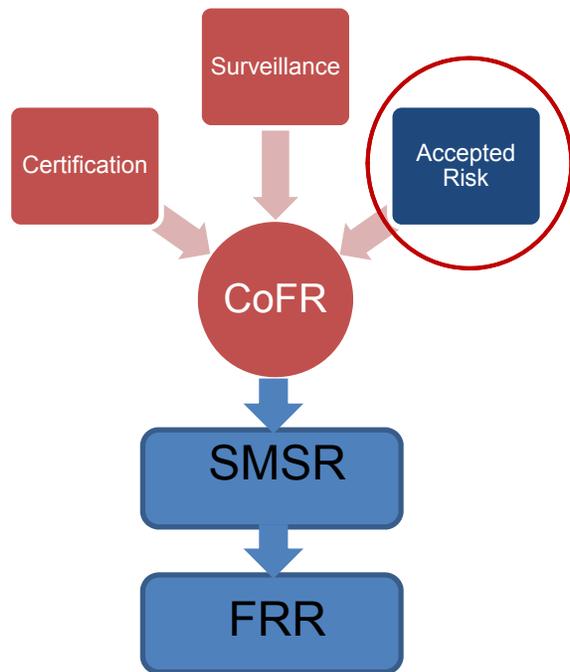


- No concerns about reduced surveillance if:
 - Maintain good communication between CCP offices
 - Setup and maintenance of Surveillance database
 - Adequate S&MA resources to support intra-program assurance role
- CCP S&MA Office and TA have good working relationship with Program
- CCP S&MA Office works 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, NESCA, etc.
 - Increasing management notification as risk increases

Risk Acceptance Strategy Acceptable to S&MA



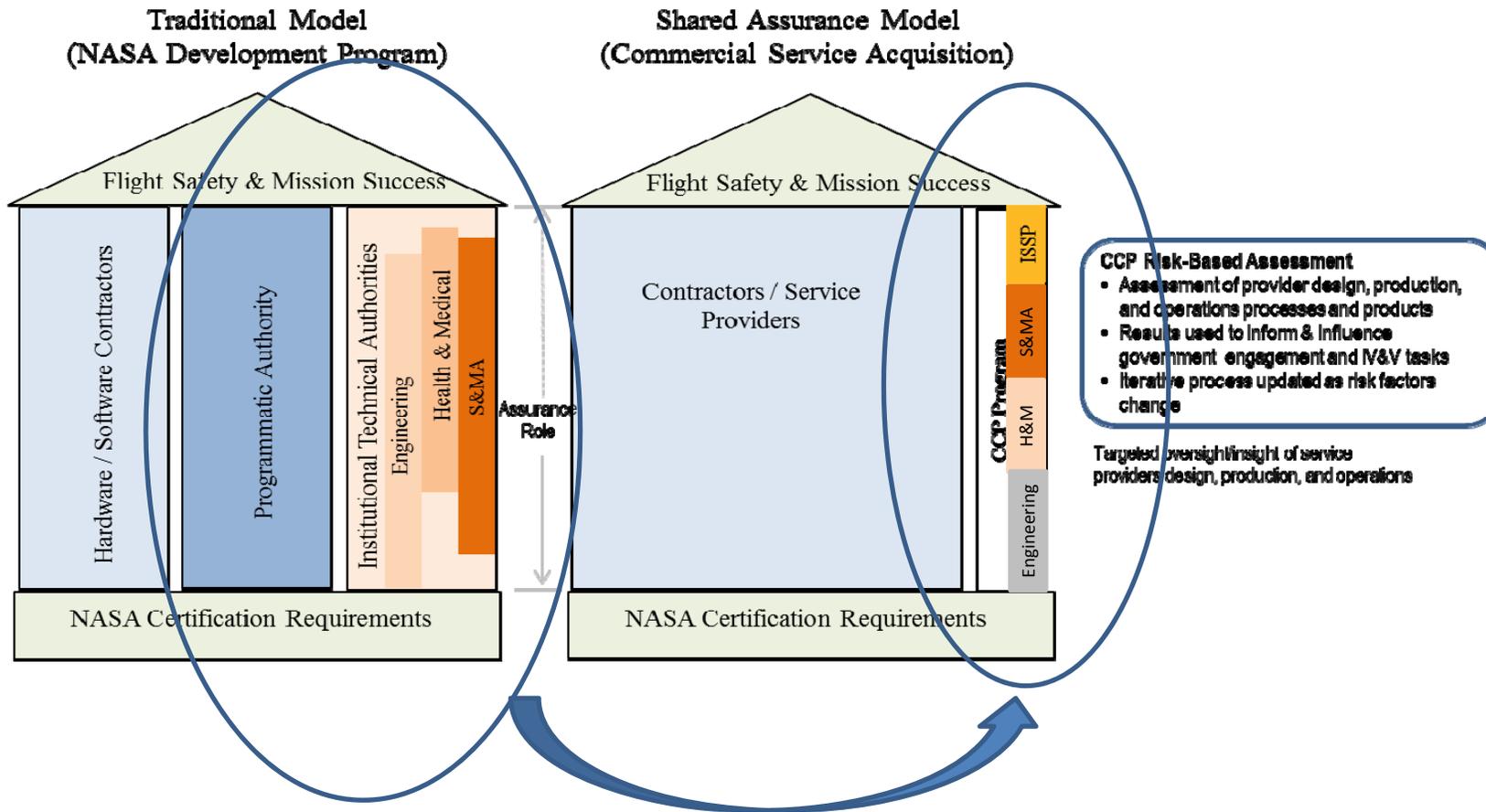
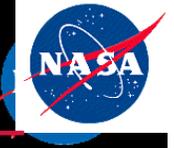
Shared Assurance

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:

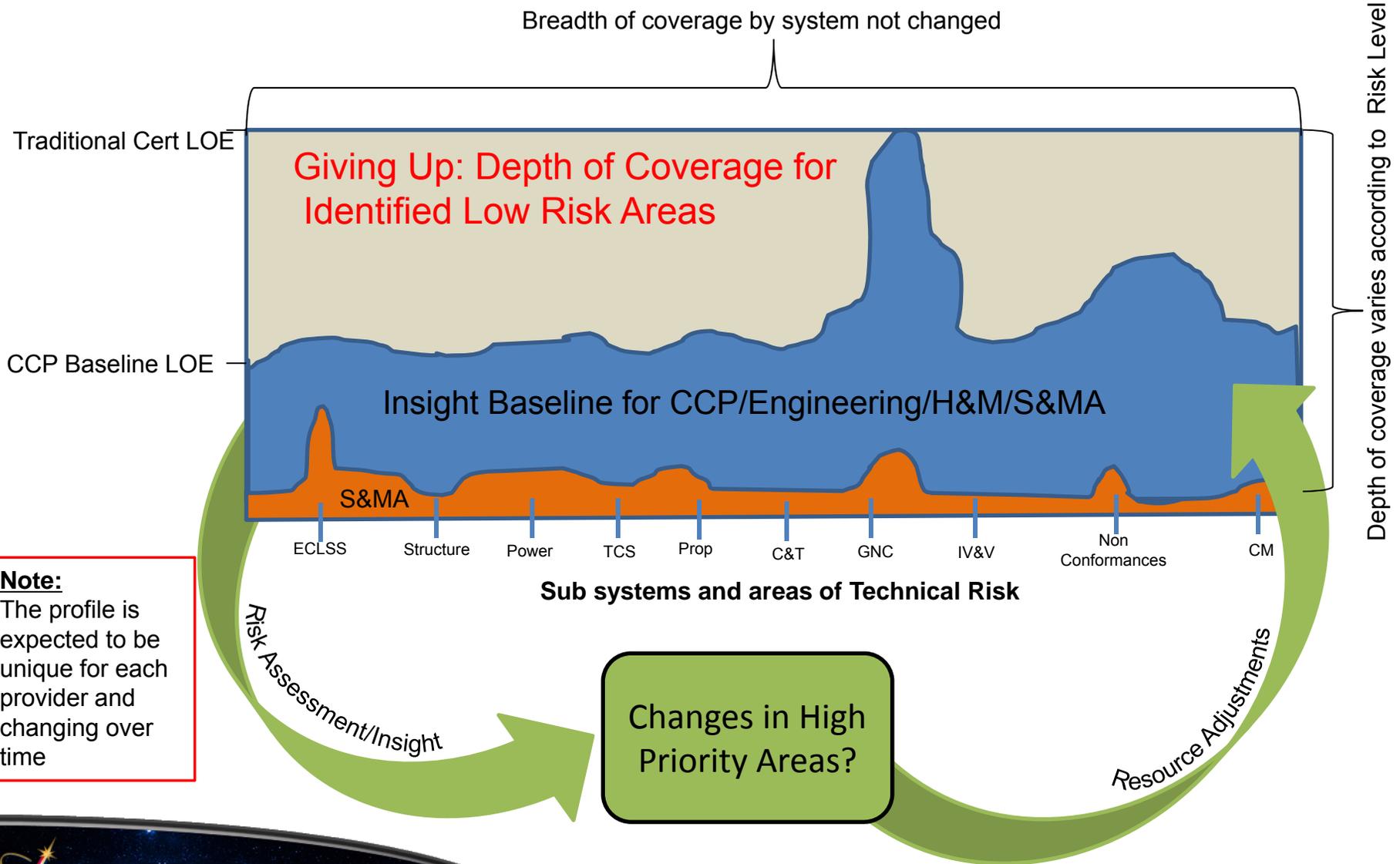
- Technical Breadth remains unchanged
- Technical depth changes
 - Level of penetration determined by Risk Assessment
 - NASA Insight is an essential to identify and develop understanding of risk
- Minimize Organizational Redundancy (limit multiple organizations overlap) – important to clearly define roles and responsibilities
- End goal is Certification of Flight Readiness (CoFR)
 - CoFR = Certification + Surveillance + Risk Acceptance

CCP Shared Assurance – What is Different?

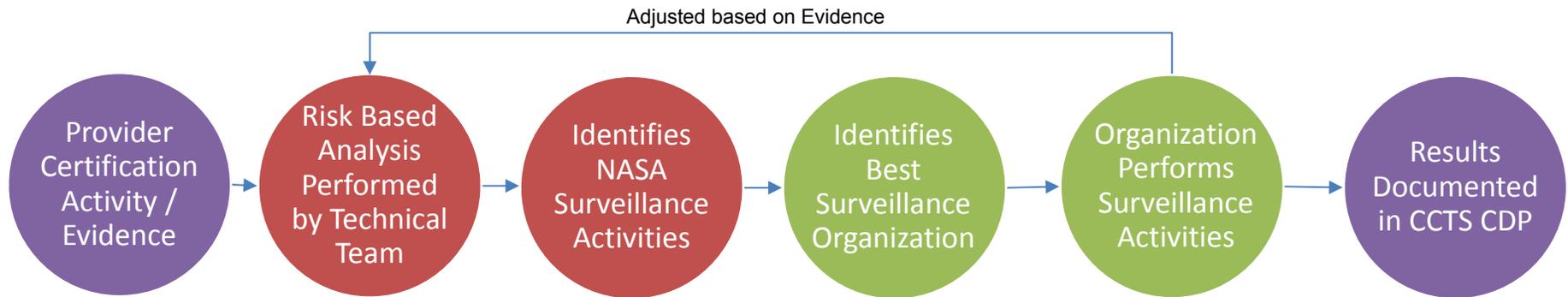


Next: How to get from Traditional to Shared Assurance Model

CCP Shared Assurance - What are we giving up?



Safety and Hazard RBA/Shared Assurance Flow & Examples



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

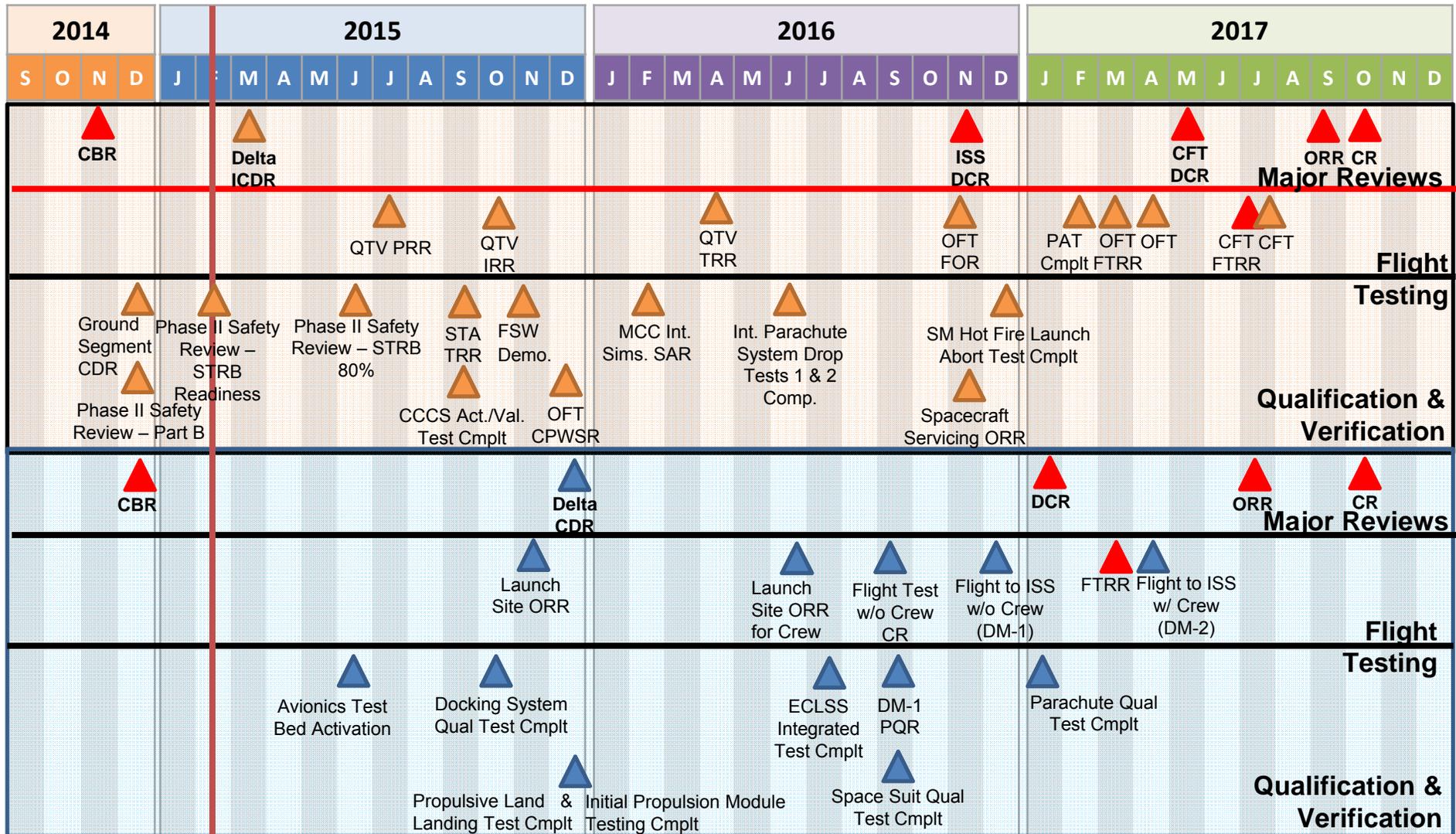


Summary

- 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).”

CCTCap Combined Milestone Summary



CCTCap CMS-Official February 2, 2015
 Data Source: Boeing FY15Q1 / SpaceX
 FY15Q1
 POC: Debbie Cole 321-867-0834

- Required Milestone
- Boeing Milestone
- SpaceX Milestone.