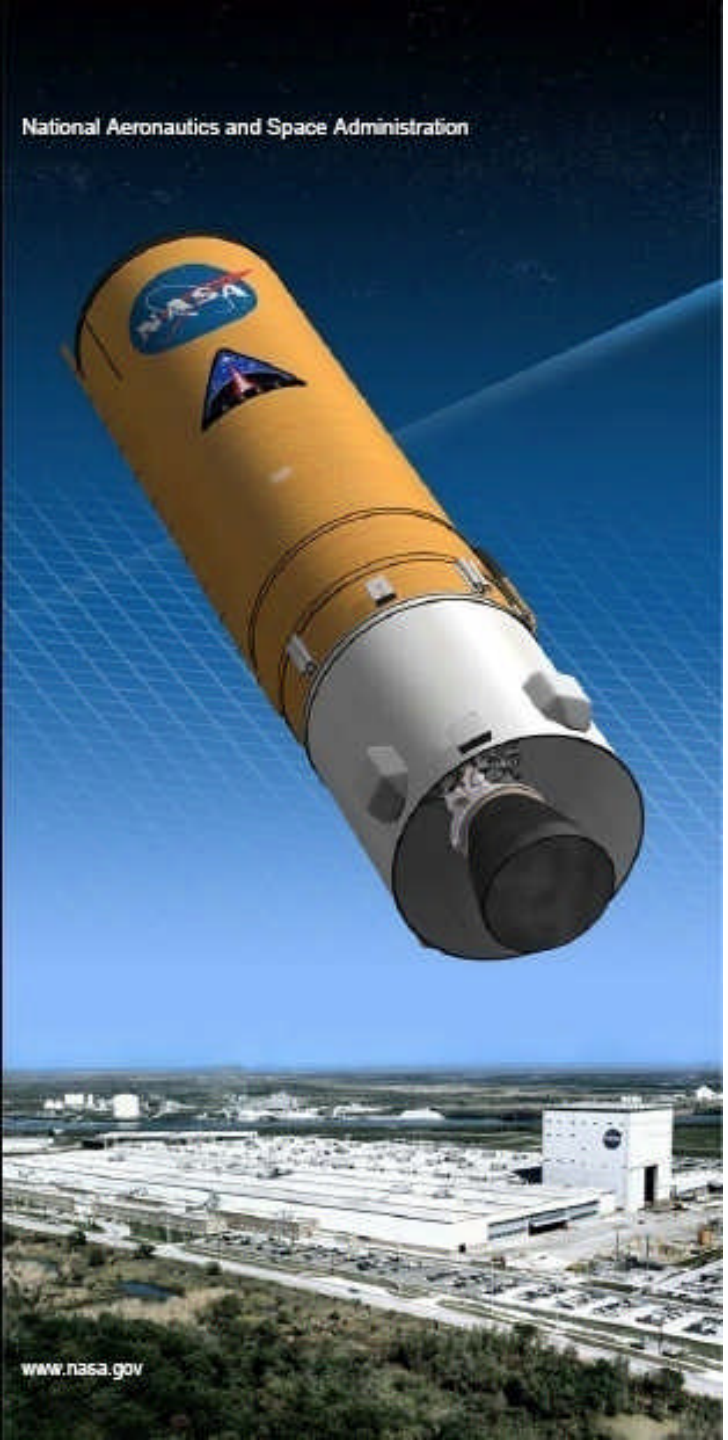


Safety and Mission Assurance for In-House Design

Lessons Learned from Ares I Upper Stage

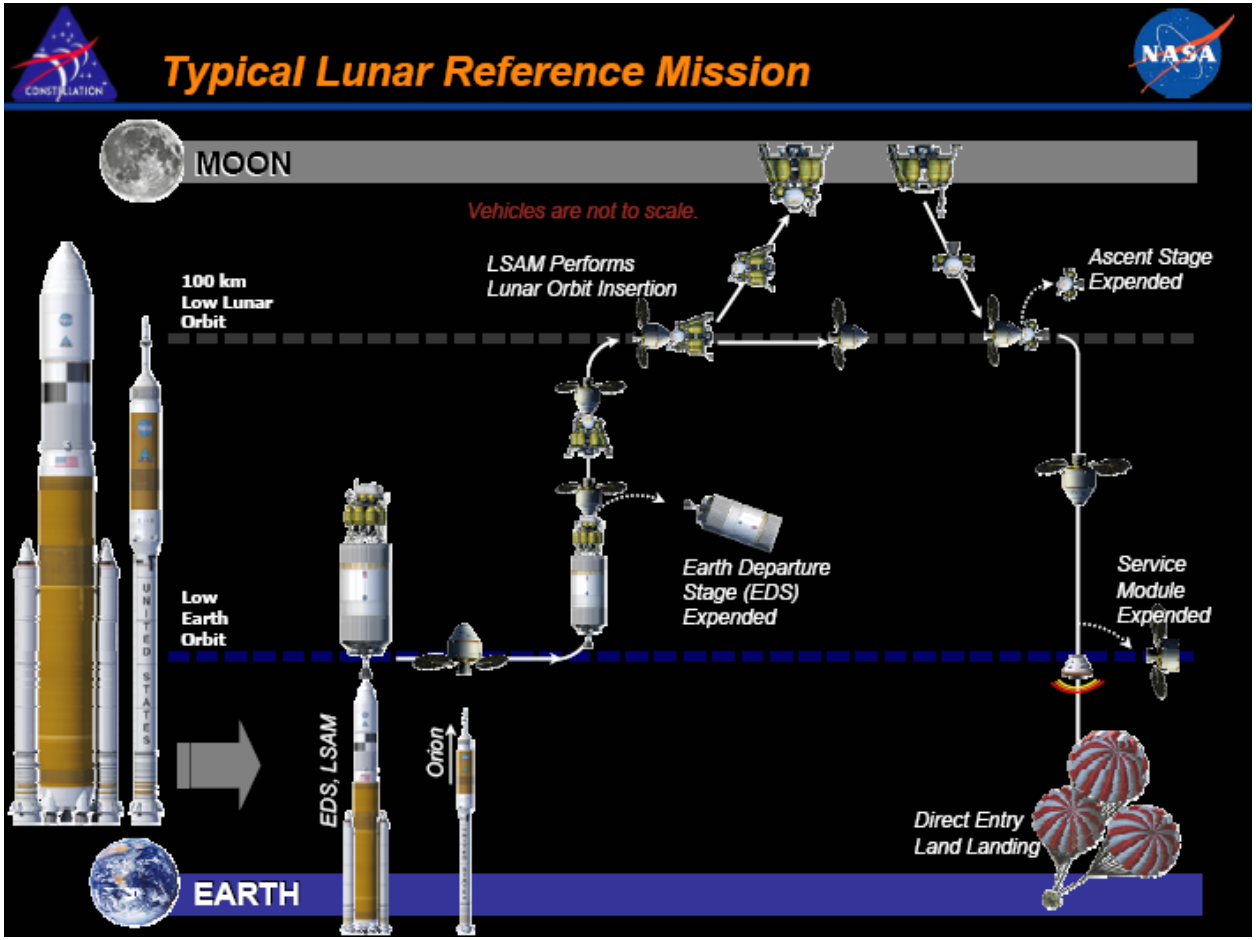
Joel M. Anderson

MSFC/QD33

Upper Stage/External Tank Branch Chief

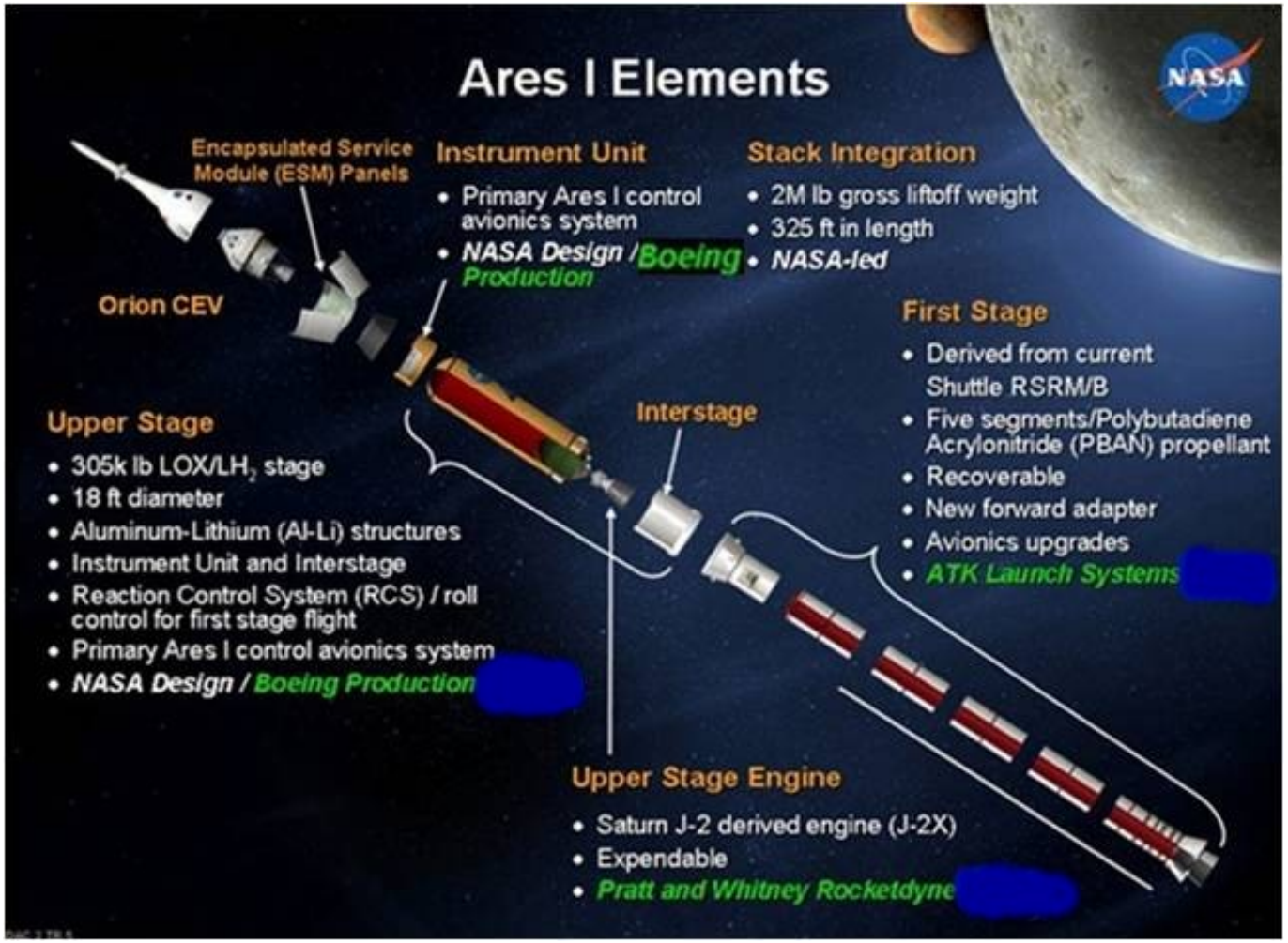
Introduction

- The Ares I Launch Vehicle was part of the Constellation Program, initially intended to provide transportation to orbit for crew en route to the ISS and later to be part of the "launch and a half" solution for follow-on missions to the moon.

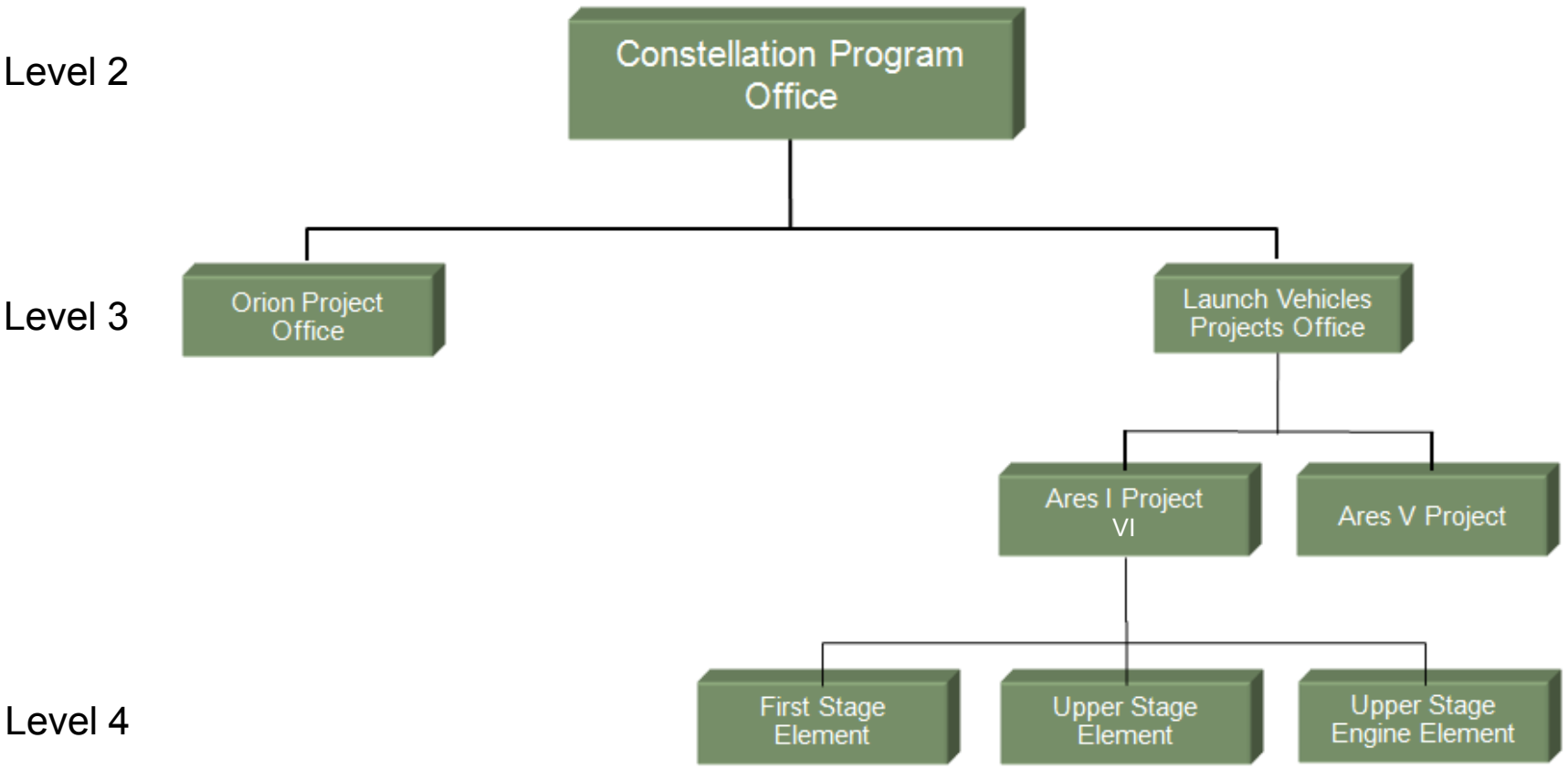


Introduction

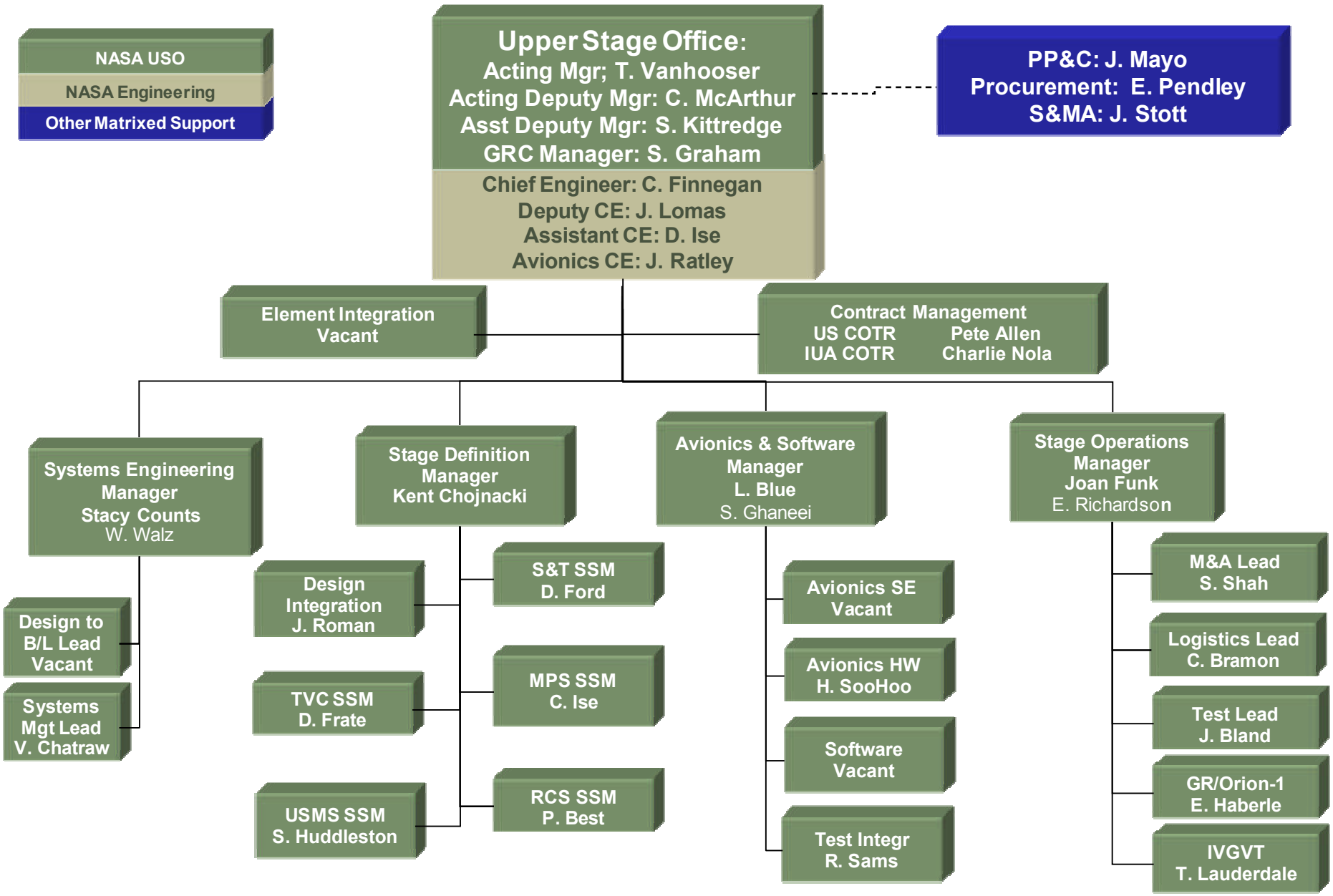
- The Constellation Program office was established at the Johnson Space Center in Houston
- The Orion Project Office was also established at JSC
- The Ares I Launch Vehicle Project was established within the Launch Vehicles Projects Office at the Marshall Space Flight Center---3 primary elements managed out of Element Offices at the center



Constellation Organization



Upper Stage Organization



Presentation Structure

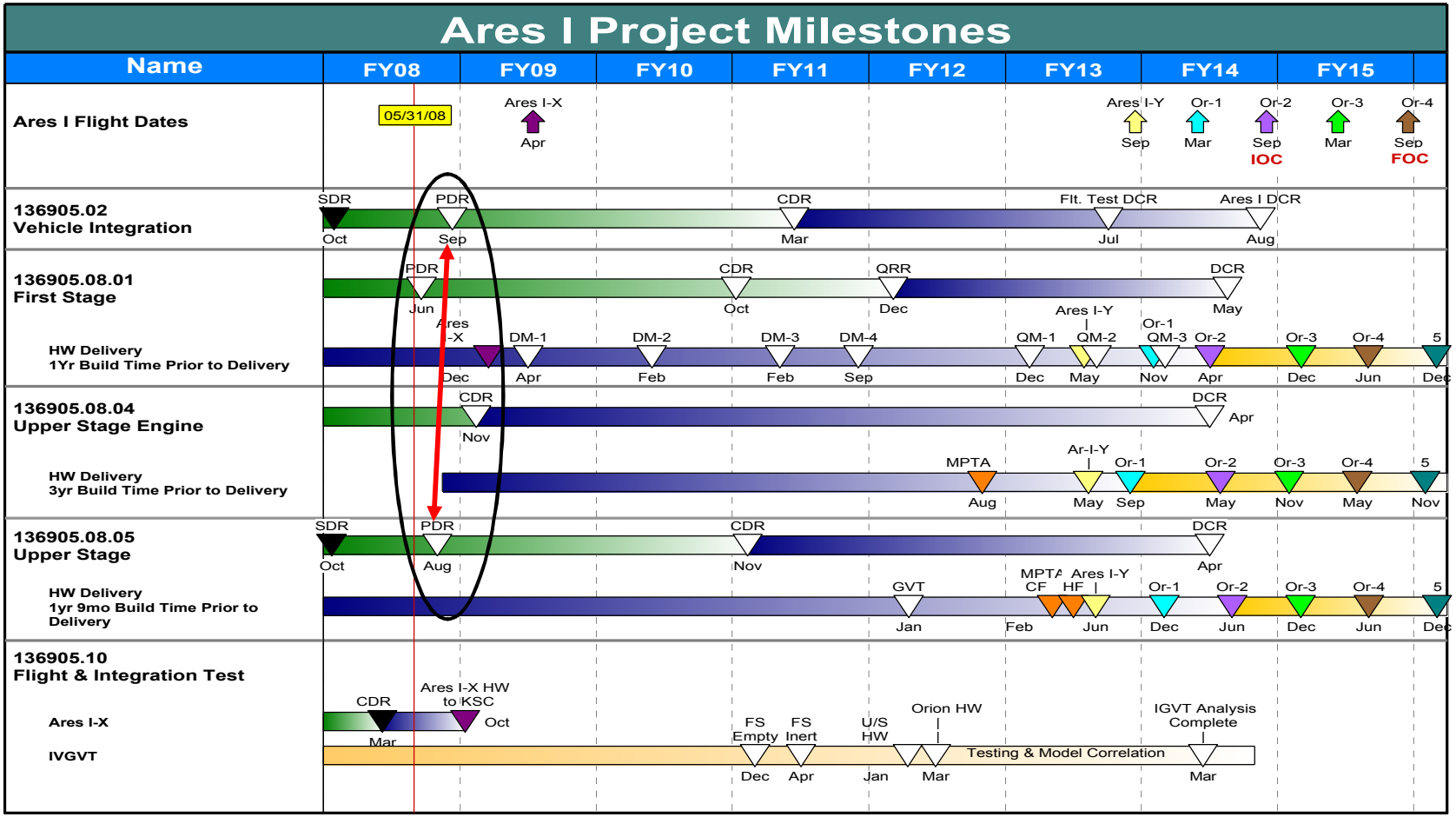
- **This presentation is structured to identify a lesson encountered in the course of the Upper Stage Element design and development effort**
  - First chart will identify the lesson and some observations from the project
  - Second chart identifies a recommendation to address the lesson
- **Note that some of the lessons identified are not unique to an in-house project such as the US and may have been encountered by contractor organizations as well**

Lesson-Importance of Systems Engineering/Integration

- **Level 3 (Ares I, Orion) and Level 4 (Elements, including Upper Stage) efforts were initiated before Level 2 (Constellation Program) was fully up and running**
  - Resulted in contracts and in-house effort that was not fully compliant with eventual Level 2 programmatic requirements
  - Required additional effort to demonstrate compliance or equivalence when Level 2 requirements ultimately approved
  - Early start of lower level projects was schedule driven
    - Elements/Orion had to move out if schedule was to be met

Lesson-Importance of Systems Engineering

- **Schedule of milestone reviews did not allow complete flowdown of requirements (at SRR) or integration of analyses (PDR)**
  - Resulted in significant rework and delta reviews



Note: All Design Review dates are Board dates

CxP 72130

Lesson-Importance of Systems Engineering

- **Recommendation(s)**
  - Assure that high level requirements are identified to the maximum extent possible to assure appropriate flow down to lower level elements/projects
  - Assure milestone schedule allows for integration at the next higher level
    - If schedule is not available, assure lower level analyses are provided “for information” to allow early integration efforts

Lesson-Importance of Early S&MA Involvement

- **S&MA involvement at the earliest stages of the project allows early identification of potential safety issues (starting at concept phase)**
  - S&MA was involved in the Constellation Program from the beginning of the Exploration Systems Architecture Study through program cancellation
- **In addition to safety issues, comparative assessment of reliability can be performed**
  - **Note**: the tendency to focus on absolute numbers in early reliability assessments must be avoided. Early numbers have wide uncertainty and are often based on similarity analyses. The significance is found in relative reliability of design options
- **Trade studies must adequately weigh safety and reliability along with other figures of merit**
- **Early involvement allows S&MA to identify risks and support development of mitigation if performance issues drive selection of "less safe" options**
  - Allows appropriate planning for risk reduction

Lesson-Importance of Early S&MA Involvement

- **Recommendation(s)**
  - Assure the Safety and Mission Assurance is involved at the earliest phase of project life cycle
    - Safety and Reliability issues need to be identified early and resolutions coordinated
    - Early involvement helps to minimize issues at later phases of the project where “fixes” are likely to be more expensive both in cost and schedule
    - Assure Safety and Reliability assessments are included, and properly weighted, in figures of merit supporting trade studies and design decisions

Lesson-Importance of Appropriate Staffing Levels

- **This is a difficult issue to address with fixed funding creating a zero sum game**
  - What one organization “wins”, another must “lose”
  - S&MA support is not independently funded
    - S&MA workforce and other funding must be negotiated with the project or element management team
- **As the responsible in-line engineering organization for S&MA deliverables, failure to obtain appropriate funding for in-house effort results in incomplete, late or inadequate analyses**
  - This is a different issue than reducing insight into development of the products by a prime contractor
  - Insufficient funding means the work does not get done within planned schedule
- **Intent is to be proactive in implementing S&MA requirements in the design.**
- **Inconsistent approach to managing S&MA resources at multiple centers created funding issues**
  - GRC S&MA funding approach changed during project execution

Lesson-Importance of Appropriate Staffing Levels

- **Recommendation(s)**
  - S&MA must be adequately funded to proactively support design and development
    - Note: Documentation of the S&MA analyses is less important than application of the tools/analyses to impact the design of the system
  - Lead Project S&MA organization must account for and manage resource requirements to support the project across all involved centers

Lesson-Importance S&MA Team Deployment

- **The US Element was organized into numerous Integrated Product Teams (IPT)**
  - IPTs included design responsibility for US Systems (e.g. Main Propulsion System, Thrust Vector Control, Small Solids), Manufacturing and Assembly, Test, Logistics
    - Ideally, most design IPTs would have dedicated Safety, Reliability & Maintainability and Quality Engineers assigned
    - Software design and development IPTs would have assigned SW Assurance personnel in Safety, Quality and Reliability (if required)
  - M&A and Test IPTs are supported by Quality Engineering/Assurance and Industrial Safety
  - Logistics IPT was supported by Reliability and Maintainability
  - This deployment allows for immediate input from the S&MA community on trade studies and design decisions
- **The US S&MA team was assigned such that these disciplines were available to each of the subsystem IPTs**
  - Insufficient personnel were funded to assign dedicated support
- **S&MA Involvement in the design process made a positive impact on by identifying potential issues early**

Lesson-Importance S&MA Team Deployment

- **Recommendation(s)**
  - Assure deployment of S&MA workforce to allow real time support to integrated product teams
    - Assure assignment of Safety, R&M, Quality Engineering to subsystem design IPTs
    - For Software development IPT, assure assignment of Software Quality, Software Safety and, if required, Software Reliability
    - Assure assignment of Quality Engineering/Assurance and Industrial Safety Support to Manufacturing & Assembly and Test IPTs
      - Some System Safety support for analysis of test articles in support of Test
      - Potential for R&M Support to M&A for Process Failure Modes and Effects Analysis and Design of Experiments (less frequent)

Lesson-Understanding of S&MA In-Line Engineering versus Assurance

- **The implementation of S&MA support to Upper Stage for an in-house design and development effort placed the S&MA team in a position of in-line engineering**
  - This would have been the case until late in the development cycle when sustaining engineering was to be transferred to Boeing
  - NASA/Support Contractor team performed in direct support of the design effort rather than in an oversight/insight role
  - Raises the question…if the NASA S&MA team is doing an in-line engineering function, who is performing the assurance function?
    - Independent S&MA personnel not supporting the project
    - “Gray beard” organizations

Lesson-Understanding of S&MA In-Line Engineering versus Assurance

- **Recommendation(s)**
  - Both in-line and assurance functions are required elements of the S&MA effort for in-house projects
    - Resource planning must include performing both functions

Lesson-Importance of Close Coordination between Supportability and Reliability/Maintainability

- **Reliability and Maintainability engineering are closely tied to Logistics (Supportability)**
  - These specialty engineering functions are often placed in the same organization
- **MSFC places R&M in the S&MA organization and Logistics (Supportability) in the Engineering organization**
  - This does not create insurmountable issues but does make appropriate communication, coordination and data exchange very important
- **Need to avoid "trap" of considering Logistics and Operations to be one and the same**
  - Operations are only a portion of Logistics

Lesson-Importance of Close Coordination between Supportability and Reliability/Maintainability

- **Recommendation(s)**
  - Assure appropriate coordination between R&M and Supportability
  - Identify data exchange needs as early as possible in the project
  - Assure that R&M is appropriately represented on the Logistics IPT and Logistics Control Boards

Lesson-Importance of Engineering Data Systems

- **Numerous engineering data systems were created to use as data repositories and data exchange sites**
  - Windchill
  - DDMS
- **Benefits**
  - Secure data transfer for Sensitive But Unclassified (SBU) information
    - Note: Be aware of “overclassification”
- **Issues**
  - Data Access
    - Difficult to find through search utility
    - Data difficult to find through manual search
    - Link required to be sent to minimize effort to locate desired information
  - Multiple data systems used by different segments of the program resulted in the need for multiple access/passwords
  - Data systems were changing during the course of the project

Lesson-Importance of Engineering Data Systems

- **Recommendation(s)**
  - Assure data systems are developed and available for use at the beginning of the project
  - Assure data systems are accessible to individuals with need to know
  - Design data/folder structure to allow efficient location and access to data
  - Minimize data systems in use across the program

Lesson-Importance of Early Development of Supporting Databases

- **The Constellation Program developed numerous databases to be used for Hazard Analysis (HA), Failure Modes and Effects Analysis (FMEA) and Problem Reporting and Corrective Action (PRACA)**
- **Database development lagged the initiation of the analyses for HA and FMEA resulting in "extra" effort to transfer initial offline analysis data into the databases**
- **Databases did not appropriately consider export for document development**
- **PRACA was developed sufficiently early but needed to consider how it would interact with existing contractor failure reporting systems**
  - CxPRACA not fully implemented due to program cancellation
  - Constellation appeared to address (or attempt to address) most of the issues that have limited the value of previous PRACA systems (such as inconsistent failure descriptions)
    - Would have allowed better use for failure trending data

Lesson-Importance of Early Development of Supporting Databases

- **Recommendation(s)**
  - Develop databases as early as possible and with consideration of data import from existing government and contractor systems
  - Need to assure databases allow efficient outputs for document publishing
    - Editable
  - Do not “overreach” and mandate database usage for activities more efficiently accomplished by other means
    - Initial efforts defined PRACA as including all Material Review Board activities

Lesson-Importance of Coordination with Safety Assessment/Review Panels

- **Upper Stage conducted numerous reviews with the Constellation Safety and Engineering Review Panel**
  - This allowed for early identification of potential issues and appropriate coordination of responses
- **Reviews were well supported by US Element Management, US Chief Engineer, and US Engineering in addition to the US Safety Team**
  - CSERP travelled to MSFC which resulted in minimum impact to ongoing work allowing design engineering to participate fully
- **The CSO for the element under review served as the S&MA Technical Authority on the CSERP**
  - This created a potential for insufficient independence given the CSO role in developing and reviewing the analysis prior to the CSERP review
- **Software Safety was addressed in much greater detail than prior reviews and guidance from the panel was not thorough and consistent**

Lesson-Importance of Coordination with Safety Assessment/Review Panels

- **Recommendation(s)**
  - Define expectations for hazard analysis content and approach, including Software, in program methodology documents
  - Consider appropriate independence of Safety Review Panel (CSO for project/element under review may not be appropriate)
  - Continue Safety Panel approach of travelling to design and development center to allow appropriate technical experts from the project to support

Lesson-Implementation of Software Reliability

- **Software Reliability is a relatively new discipline within the agency**
  - SW Reliability was implemented on Upper Stage
  - Products developed included Software Failure Modes and Effects Analysis, Reliability Predictions
- **SW Reliability is not yet well established or understood**
  - Software has long been “disregarded” in Reliability because “software doesn’t fail”
  - While it is true that software does not fail in the traditional sense, it remains a significant source of system failure risk due to many potential sources of incorrect software functionality
    - “Bad” requirements
    - Incorrect coding
    - Insufficient testing
- **Benefits may include**
  - Analysis of software design to establish functional criticality
  - Definition of minimum testing required to achieve Reliability target
  - Reviews Software development processes and products for error prevention

Lesson-Implementation of Software Reliability

- **Recommendation(s)**
  - Develop consistent methodology and implementation of software reliability
    - Identify minimum content of software reliability analysis and support based on software classification
  - Assure impact of software on system risk is included in analyses

Lesson-Implementation of S&MA Technical Authority/Chief S&MA Officer

- **The position of Chief S&MA Officer was recently established as the mechanism for implementing S&MA technical authority**
  - Position is analogous to a Chief Engineer for S&MA
- **Relationship between technical authority of Chief Engineer and Chief S&MA Officer is important and must be understood by all parties**

Lesson-Implementation of S&MA Technical Authority/Chief S&MA Officer

- **Recommendation(s)**
  - Define and implement the roles and responsibilities of the Chief Engineer and CSO in the technical authority chain in support of the project
  - Note: implementation of the Medical Technical Authority is under development for project support

Lesson-Importance of S&MA Evaluation of Project Risks

- **Risk Management for Constellation was set up to have S&MA assess project risks for Safety impact and document the assessment in the Constellation Integrated Risk Management Application (CxIRMA)**
  - Element Management/Chief Engineer/Engineering assessed most risks as “No Safety impact” based on the presumption that we would “not fly like that”
    - Based on that approach, risks would never have Safety impact
  - S&MA assessed many risks as having a safety impact
    - By definition, risks with a safety impact were assigned a consequence score of 5 because the Ares I vehicle had only catastrophic hazards
- **After consultation between the Engineering Technical Authority and the S&MA Technical Authority, agreement was reached to have independent scoring of Safety risk by S&MA and Risk Owner**

Lesson-Importance of S&MA Evaluation of Project Risks

- **Recommendation(s)**
  - Assure assessment of risks based on likelihood and consequence **before** any mitigation actions are implemented
  - S&MA should consider whether an approach to Safety risk scoring exists which would allow more discrimination between risks
    - By definition, a Safety risk is catastrophic in the launch vehicle world (all safety risks were severity 5)
    - Since Safety and Reliability Analyses are “worst case”, the consequence does not change. Only likelihood is impacted by mitigation

Lesson-Implementation of Critical Items List and Government Mandatory Inspections

- **CIL inspections and Government Mandatory Inspection Points are targeted as causes of high operations costs**
  - Move initiated to eliminate or reduce such inspections to save money
- **Constellation Program offered approach by which assessment of the probability of failure in the Failure Modes and Effects Analysis and inspection results in operation would be used to justify elimination of inspections**
  - Assessment of individual failure rates by failure mode is very expensive
  - Some disagreement within R&M community of the value of the early assessed probability to the decision to eliminate a CIL inspection
- **Some value may be gained by assuring a single inspection at the latest point in the flow**
  - This approach may increase cost and/or schedule risk if issues are discovered late in the flow
- **An approach has been proposed in which government inspectors are available for the duration of a process rather than stopping the process to await an inspector in order to improve efficiency**

Lesson-Implementation of Critical Items List Mandatory Inspections

- **Recommendation(s)**
  - Avoid duplication of CIL inspections
    - Inspect at the latest point in the flow where characteristic can be inspected
      - Requires acceptance of cost and schedule risk associated with late discovery of issues
      - This is mitigated by contractor inspections
  - Provide inspectors dedicated to process where government mandatory inspection is required to reduce manufacturing and assembly wait/down time

Lesson-Implementation of Test Article Safety Analysis

- **Industrial Safety and System Safety should work together to analyze the entire set-up and conduct of test activities**
  - Industrial safety analysis often treats the test article as a “black box” in conducting hazard analysis
  - System Safety is normally focused on the safety of flight hardware but should support integrated test safety assessment

Lesson-Implementation of Test Article Safety Analysis

- **Recommendation(s)**
  - Test safety analysis should assess the integrated test set-up, including facility and test article safety
  - Assure analysis is done sufficiently early to impact hazard control design and implementation

Lesson-Importance of Procurement Quality

- **Many procurements take the path of least resistance and end up bypassing quality**
  - Credit cards
  - Procurement through support contractors
- **As a result, hardware sometimes is delivered to receiving with no requirements identified for acceptance**
- **“Fixing” issues with receiving inspection of procured hardware can be more costly and time-consuming than up front coordination**

Lesson-Importance of Procurement Quality

- **Recommendation(s)**
  - All procurements must be coordinated with Quality Engineering for assignment of “quality sensitive” designation and identification of procurement quality and receiving requirements
  - Consideration should be given to creating and staffing Procurement Quality organization to assure consistency in the identification of “quality sensitive” hardware and application of quality requirements

Summary

- **Early S&MA involvement is critical to efficient integration of safety, reliability and quality into design and development efforts**
  - Both in-line and assurance must be considered
  - Personnel must deployed to provide real time support to design and development teams
- **Project Management focus must be to create the safest and most reliable operational system satisfying allocated technical, cost and schedule requirements**
  - While S&MA does not specifically focus on performance, impacts to performance should be identified and understood
  - Where “less safe” options are desirable for performance reasons, early identification allows risk mitigation to be identified and implemented to make the design acceptable from an S&MA perspective
- **Support systems and databases must be available early and provide support to the design, development and analysis documentation effort rather than being overly burdensome**
- **In-house systems to support manufacturing and test are needed**

The primary goal of S&MA support to design and development projects should be to impact design decisions rather than to document the impact of design decisions

Contributors

- **Numerous members of the Upper Stage Safety and Mission Assurance Team contributed to the content of this presentation and are recognized here**
  - Dr. Jim Stott — Reliability and Maintainability Lead/Acting CSO
  - Mike Giuntini — Senior Quality Engineer
  - Carolyn Goodloe — Senior Safety Engineer
  - Brian Brown — Safety Engineer
  - Steve Broussard — Reliability and Maintainability/Logistics Engineer

Questions