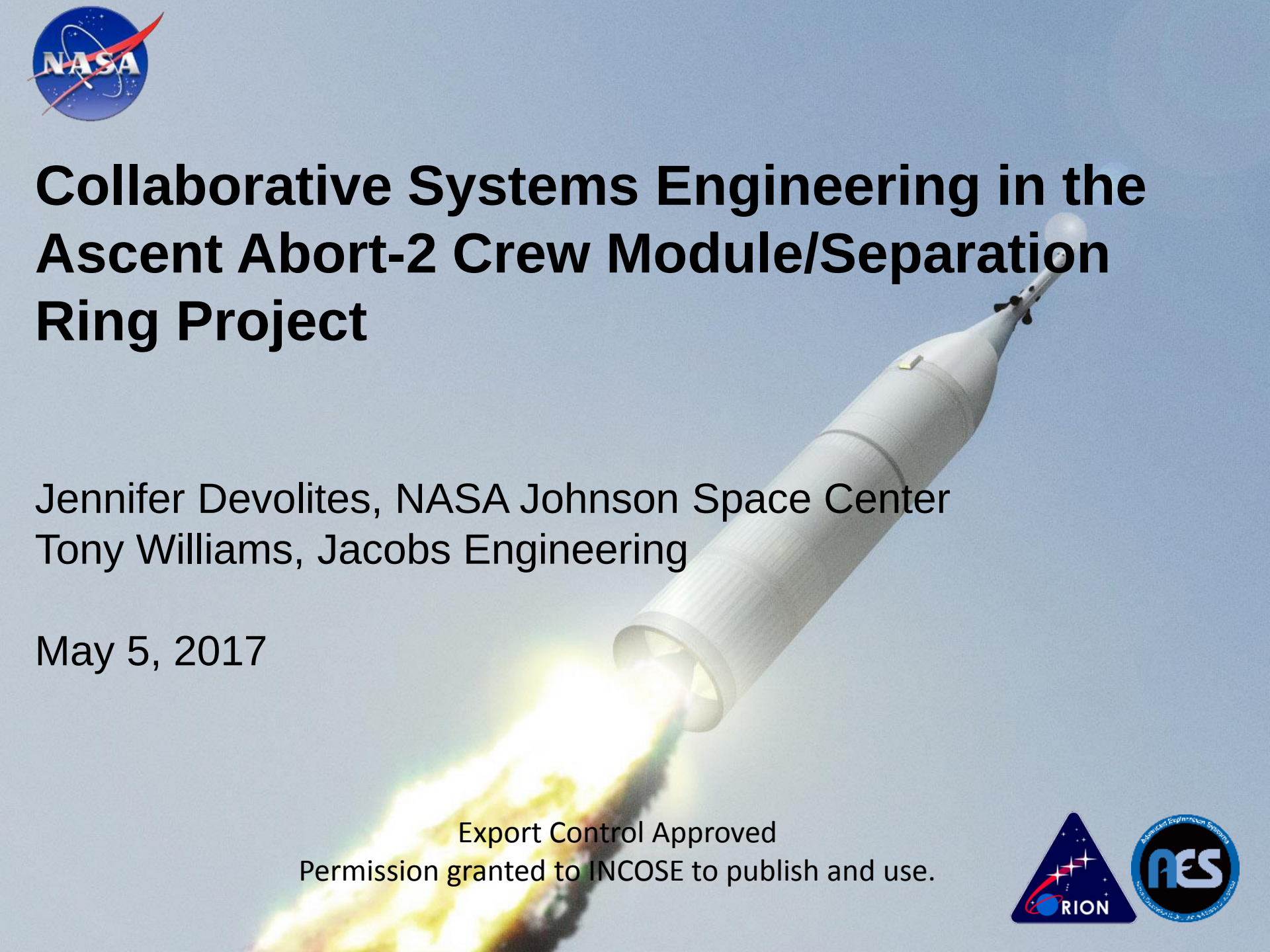


Collaborative Systems Engineering in the Ascent Abort-2 Crew Module/Separation Ring Project

Jennifer Devolites, NASA Johnson Space Center
Tony Williams, Jacobs Engineering

May 5, 2017

Topics

- Systems Engineering Value Proposition
- Ascent Abort 2 Overview
- AA2 Systems Engineering Approach and Environment
- Conclusions

Why Systems Engineering?

- Oil and Gas community has proven track record developing, operating, maintaining highly complex systems in harsh and remote environments
- Systems Engineering offers promise of improved cost and schedule efficiency and reduced defects

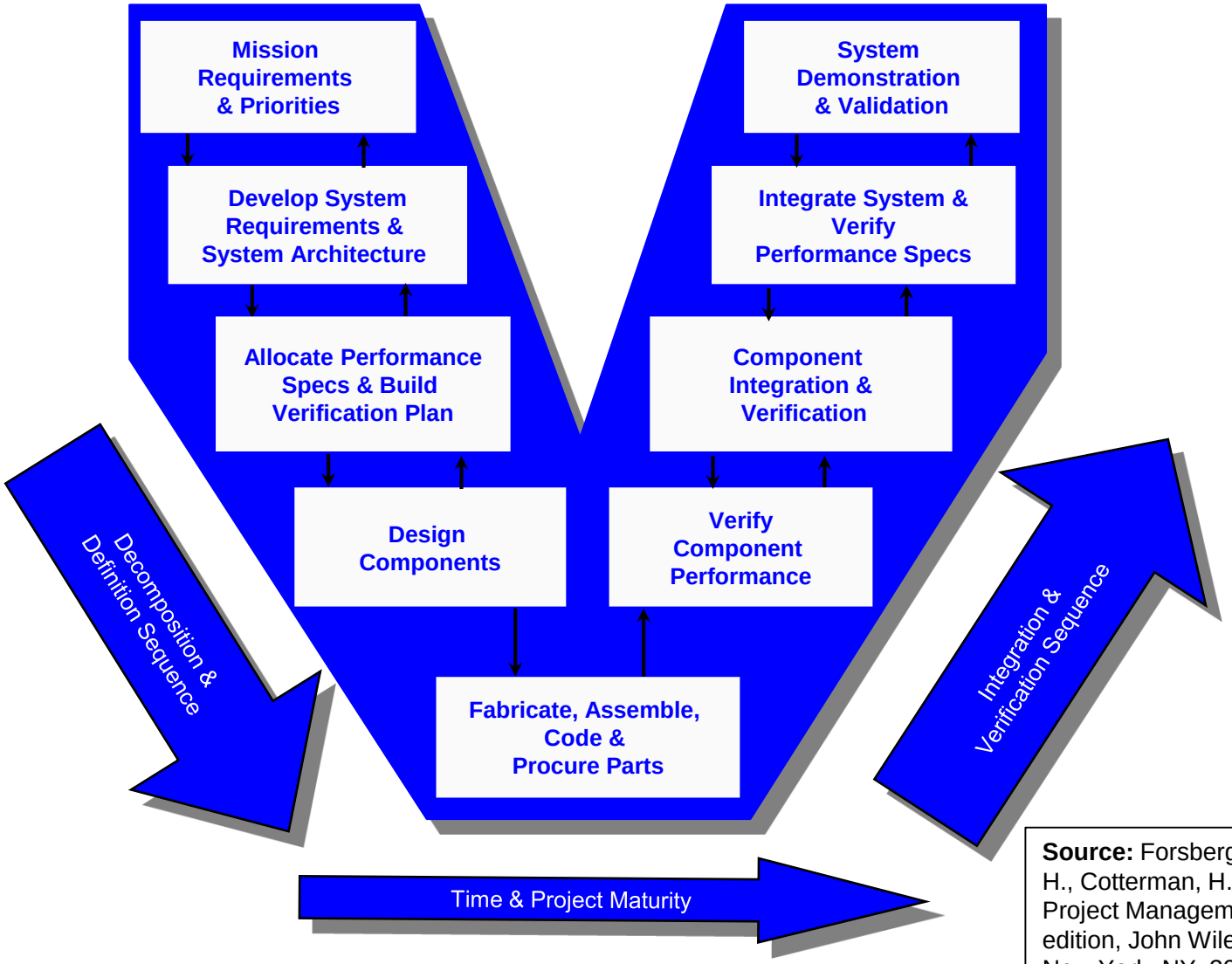
Findings and Conclusions from Lit Rev

- 67 case studies justified by claiming benefits of:
  - Completeness, consistency, and improved communications
  - Or highlighted contributions to test and evaluation, V&V, concept exploration, design reuse and systems margin analyses
- 21 case studies justified with quantified results of:
  - Cost and schedule improvement
  - Finding defects and preventing rework
- Case studies were from:
  - (67) 8 countries, 10 defense, 33 space, 5 non-defense, 6 commercial
  - (21) 4 countries, 12 defense, 5 space, 4 commercial, 6 used MBSE to develop complex weapon systems

15

"Systematic Literature Review: How is Model-based Systems Engineering Justified?", Ed Carroll, November 9, 2016, SAND2016-11485 PE, Sandia National Laboratories

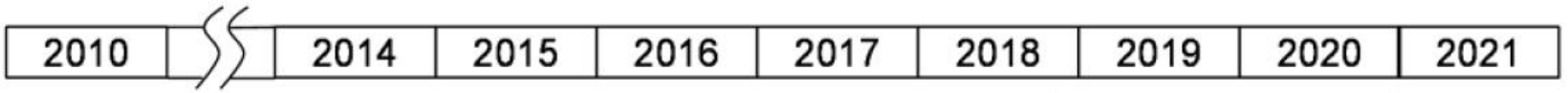
The Systems Engineering 'Vee' Model



Source: Forsberg, K., Mooz, H., Cotterman, H. Visualizing Project Management, 3rd edition, John Wiley and Sons, New York, NY, 2005.

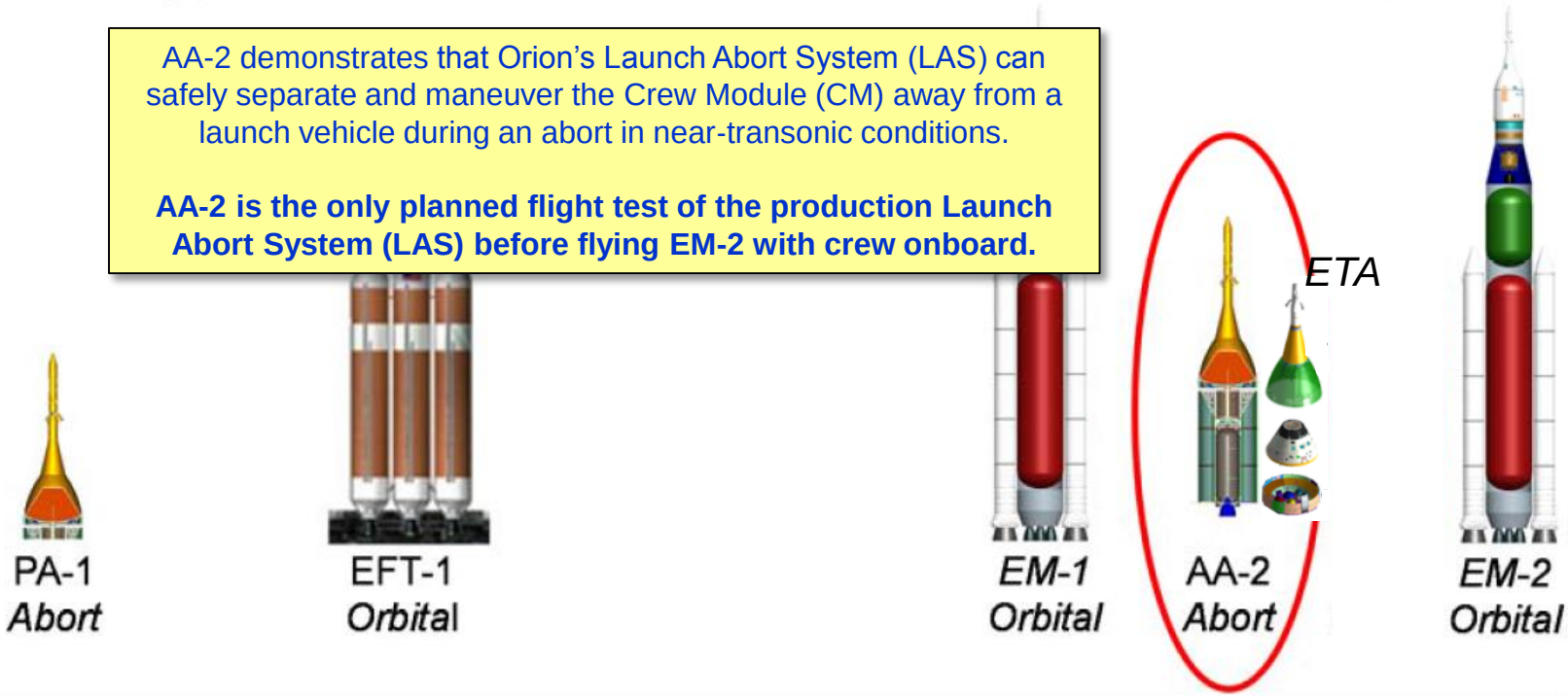
AA-2 Overview

Background: Orion's Ascent Abort 2 Flight Test



AA-2 demonstrates that Orion's Launch Abort System (LAS) can safely separate and maneuver the Crew Module (CM) away from a launch vehicle during an abort in near-transonic conditions.

AA-2 is the only planned flight test of the production Launch Abort System (LAS) before flying EM-2 with crew onboard.



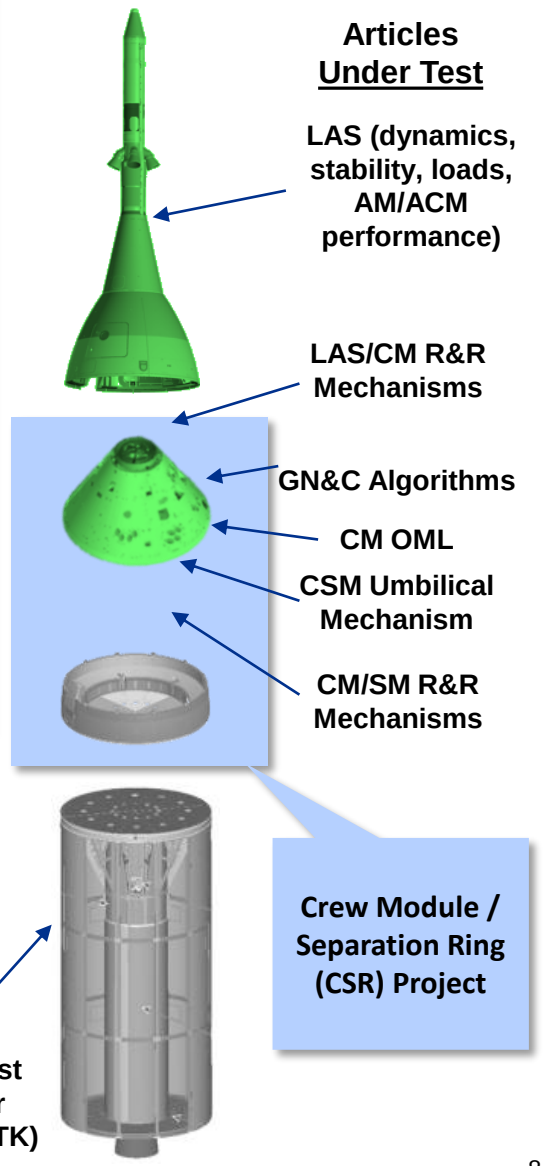
PA-1	Pad Abort 1	Abort from Launch Pad	Occurred May 6, 2010
EFT-1	Exploration Flight Test 1	Un-crewed high speed entry flight	Occurred December 5, 2014
EM-1	Exploration Mission 1	Un-crewed circumlunar flight	September 2018
AA-2	Ascent Abort 2	Un-crewed Ascent Abort	December 2019
ETA	Environmental Test Article	Ground Test	February 2020
EM-2	Exploration Mission 2	Crewed high lunar orbit flight	August 2021

AA-2 Mission Profile

AA-2 Flight Test Objectives

Top test objectives:

1. Demonstrate abort capability at the defined test condition (between 30,000 and 40,000 feet)
2. Determine the stability characteristics and reorientation dynamics
3. Obtain structural loads data
4. Determine performance of the abort motor and attitude control motor
5. Demonstrate and gather data from the separation mechanisms
6. Collect instrumentation data on the external environment – acoustic, aerodynamic, thermal, acceleration, etc.



CREW MODULE - SAME AS MAINLINE ORION

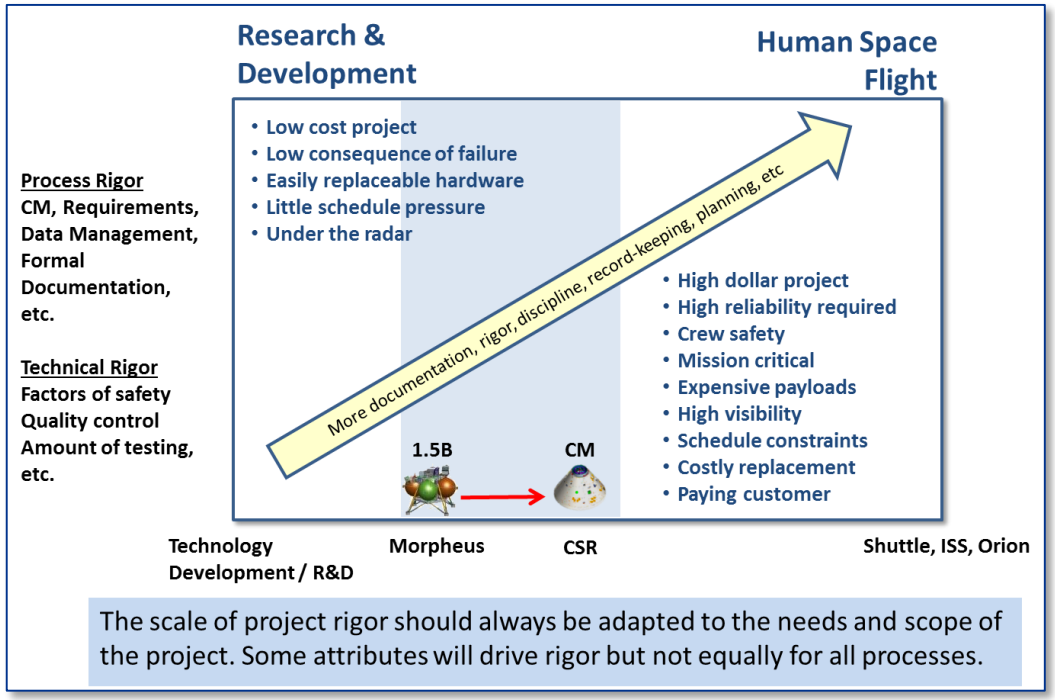
- Shape
- Center of gravity
- Separation mechanisms and pyrotechnics
- Abort sequence of events
- Guidance, navigation and control software (controlling re-orientation)

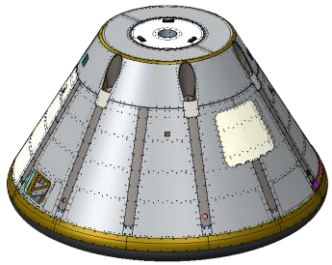
CREW MODULE - DIFFERENCES

- Built as NASA as Government-Furnished Equipment (GFE) instead of by the Lockheed Martin prime Contractor for Orion
- No thermal protection system, no attitude control propulsion, no windows, no hatch mechanism, no crew systems
- Primary structure materials and configuration
- Different flight computers, software, power, communications, instrumentation
- No parachutes
- Terrestrial only, not designed for space

AA-2 CSR Project Execution

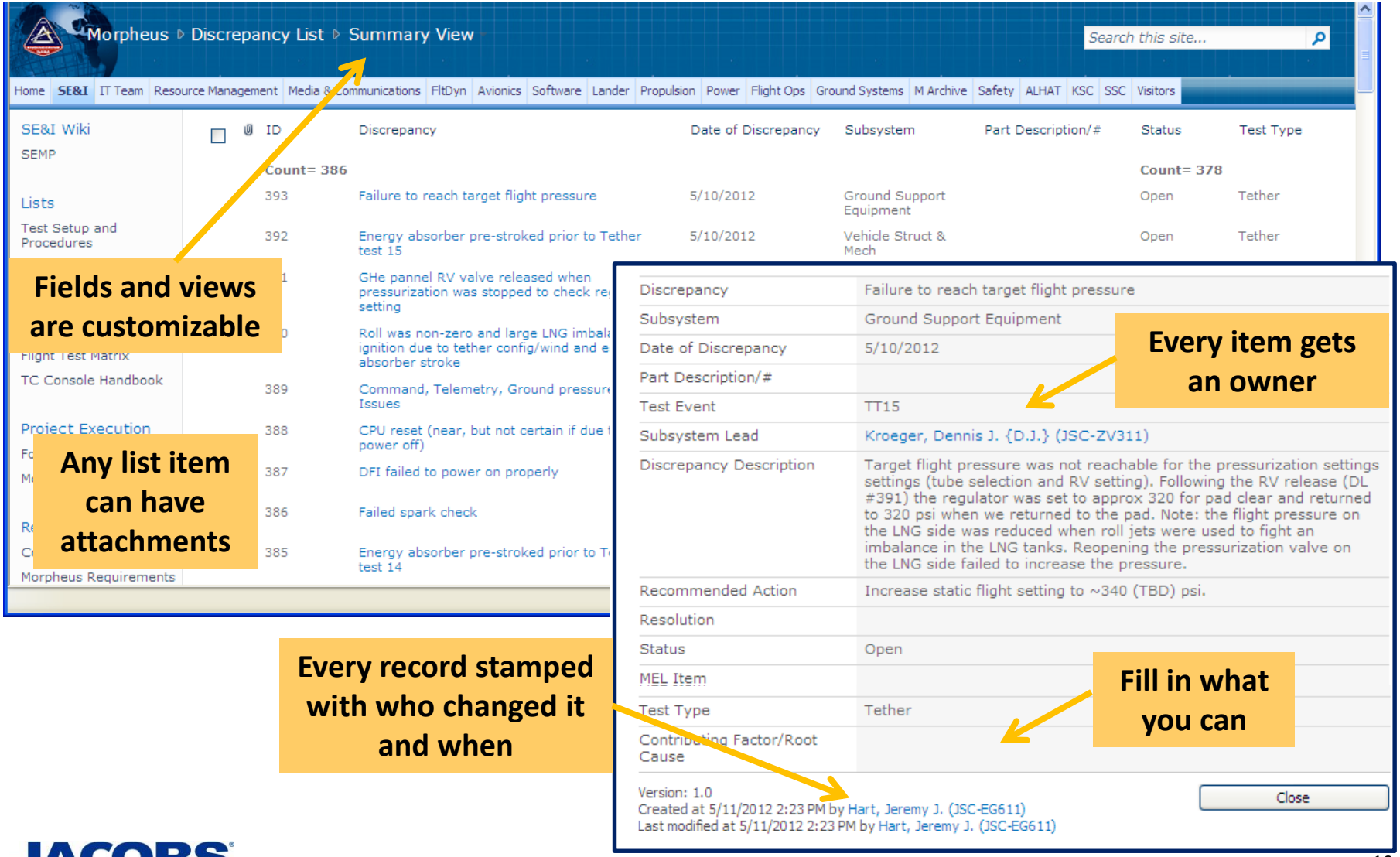
- Advanced Exploration System (AES) has a goal of pursuing lean development practices
- Many innovations were established on the Morpheus Lander Project from 2010-2014
- AA-2 CSR on the scale of rigor →
  - Rigor and risk posture consistent with flight test
  - CSR hardware is handled as either flight or non-flight (classification)
  - CSR flight software is Class B, safety critical, and leverages Goddard's core flight software
- PM/SEI
  - Leverages PM/SE&I approach developed for the Morpheus lander
  - Project executed in collaborative environment
  - Integrated and project-level content maintained online (no stack of documents for review)
  - Distributed authority and responsibility
  - Prototype development key to mitigating risk (hardware/software integration)





SharePoint List Example

SharePoint Lists are a cross between Excel and an online database, with some features of each.



Balancing Power and Accessibility

Accessibility

Standard Office Applications

Dedicated SE Environments

Cradle
CORE™
magicdraw
Architecture Made Simple
Rational. software
Innoslate

Power

AA-2 CSR Major Tasks/Products in SharePoint Collaborative Environment

AA2 Crew Module/Sep Ring IPT

Requirements and Plans	Design and Analysis	Development	Assembly and Integration	T&V	Flight Operations
Tech and Mgmt Plans	Design	Software End Items (Flt and Ground)	AI&T Plan	T&V Plan	Flight Test Procedures
Technical Performance Measures	Design Analysis Cycles	Hardware End Items (Flt and Ground)	Procedures	Verification Requirements	CSR LCCs and Flight Rules
Level 3 Req (incl. I/F)	Design Reviews		Records	TRRs	Displays
Level 4 Req. (incl. I/F)	RIDs			Test Proc.	Ops Consoles
Requirements Reviews	Analysis Reports			Acceptance Records	
RIDs	FMEA/CILs and Single Point Failures			Reports	
	Integrated Products				

KEY: Managed in SP for CSR; SP Option

Facility Requirements

Hardware Test Preparation Sheets

Discrepancy Tracking

Hazards and Hazard Controls

Configuration Management / Master Product Library

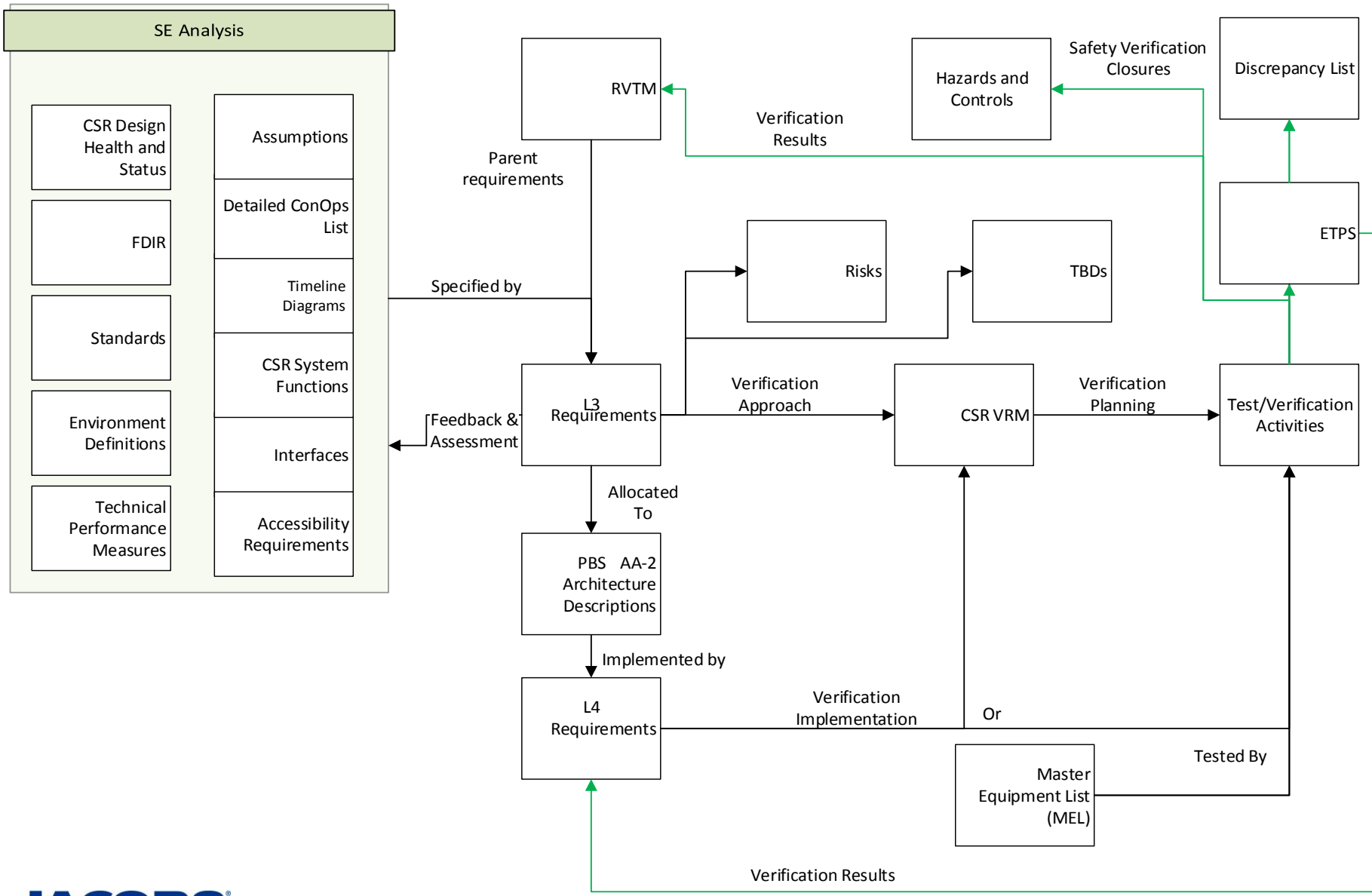
Master Equipment List

Data over whole life cycle (not tied to phase): Actions; Calendar; Meetings; Schedule; Risks; Decisions; Issues; Cost

Note: this is just a partial list of project tasks and products.

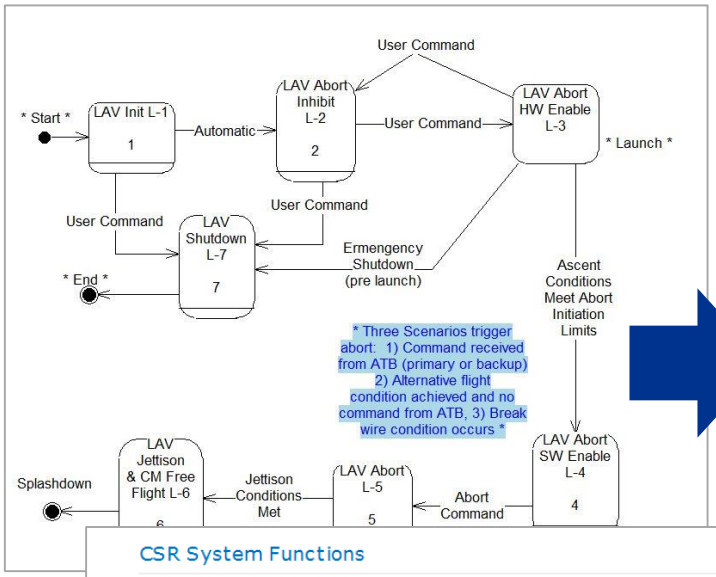
JACOBS

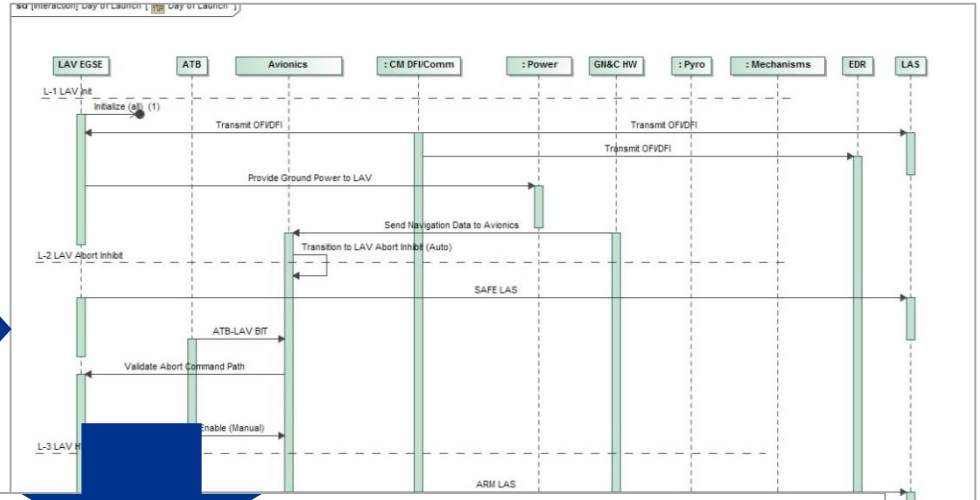
AA-2 CSR Collaborative Environment – Data and Linkages (Requirements Centric Perspective)



Example Thread – Functional Requirements

Functional Analysis using Cradle and MagicDraw Models Resulted in List of Functions in Sharepoint





CSR System Functions

ID	Title	Description	Elements	Allowable LAV State
1	Initialize	EGSE initalizes the CSR from an power-off to power-on. Initialization checks are run and responses provided to EGSE.	CM, EGSE	LAV Init L-1
2	Transition to Abort Inhibit	After Initialization, and status checks confirming all systems are green, system automatically goes into LAV Abort Inhibit Mode. Additionally, users can manually move back into Abort Inhibit from LAV Abort HW Enable- Pre-Launch - L-3-1.	CM	LAV Init L-1, LAV Abort HW Enable - Pre Launch L-3-1
3	Transition to Shutdown	EGSE transitions CM to Shutdown State	CM, EGSE	LAV Init L-1, LAV Abort Inhibit L-2
5	Transition to LAV Abort HW Enable - Pre Launch	EGSE initiates transition to LAV Abort HW Enable - Pre-Launch.	CM, EGSE	LAV Abort Inhibit L-2
8	Transition to Abort Enable (SW)	When ascent conditions meet abort initiation limits, transition to LAV Abort SW Enable mode.	CM	LAV Abort HW Enable - Post Launch L-3-2
10	Transition to Abort Mode	Transition to abort mode when one of the following occurs: (1) Abort signal received from ATB (e.g., 2 of 4 discrete indications that abort condition has been achieved (TBR))., (2) Break-wire signals meet abort	CM	LAV Abort SW Enable L-4

Example Thread – Functional Requirements

Functions List Drives Requirements, which are traced to Parent and also generate TBDs

Document	SRD
Document Section	3.1.2.1 FTV Functional (F) Mode Transition Requirements
Reqt. No.	FTV-F-01
Shall Statement	The FTV shall transition from unpowered to the following modes upon receipt of user command: a) LAV [L-1] b) [L-1]
Rationale	

Function List

Reqt Number	Title	Shall Statement	Rationale	Subsystem Allocation	TBD ID	L2/2.5 Parents	Functional Parent	Verification Method
Applicable LAV/ATB Mode : L-1 LAV Init (4)								
CSR.CM.0387	Power up to Safe State	The CM shall power up, boot, and initialize in a known, safe configuration with at least two inhibits in place to prevent catastrophic failure.	The CM needs to be nominally safe after power up. Safe state is normally taken to mean that two or more inhibits are in place to prevent catastophic failure, such as accidental pyro firing or SRM ignition (i.e. no transient commands possible to PIC cards, power relays, etc).	Flight Software W/GN&C, Avionics, EDR, Power, Mechanisms, GN&C HW		2.5-N/A; FTV-F-01	Initialize	Analysis
3690	Initialize CM	The CM shall transition from unpowered to LAV Init (L-1) upon application of power.	User command includes turning power on. LAV Init [L-1] - LAV subsystems are commanded by the user to power on and complete start-up tests. Subsystems are powered up, init tests are running.	Flight Software W/GN&C		2.5-N/A; FTV-F-01	Initialize	Test
CSR.CM.0356	Provide CM Status	The Crew Module shall provide the status for each active subsystem after start-up via the OFI data stream.	Initialization checks are needed to verify software and system are operating properly.	Flight Software W/GN&C, Avionics, EDR, Power, Mechanisms, GN&C HW, CM DFI	TBD-CM-01	FTV-OP-04; 2.5-N/A	Initialize	Test
CSR.CM.0357	Automatic Transition to LAV Abort	The CM shall automatically transition from LAV Init (L-1) to LAV Abort Inhibit	Per ADD (FTMO-100 automatically enters when initialization is	light Software W/GN&C		FTV-F-02; 2.5-N/A	Transition to Abort Inhibit	Test

TBD ID	TBD-CM-01
OldTitle	Self-Test Content
Description	What level of self testing is needed and planned for each subsystem
Assigned Team	CSR SE&I
Closure Milestone	CDR
Burn-down Plan	1) Each subsystem present self-test approach at (SEIWG/APS). 2) Review/adjust to get consensus, 3) capture in L4 requirements

Example Thread – Functional Requirements

Requirements are satisfied by Verification Requirements which are implemented by Test/Verification Activities

Requirements List

Review Status	Req(s) Verified	Req Shall Statement	VR ID	Title	Success Criteria	Verif. Method	Resp. Org (WBS)
⊞ General Verification Activity Title : (21)							
⊟ General Verification Activity Title : CM Antenna Functional Test (1)							
⊟ Verif. Method : Test (1)							
Consensus Approach	CSR.CM.0571; CSR.CM.0574	CSR.CM.0571 - The CM shall transmit LAV DFI/OFI via the LAS RF from TBD (pre-launch) until LAS Jettison Command. CSR.CM.0574 - The CM shall transmit LAV DFI/OFI through CM antennas after abort initiation.	V.CSR.CM.0571	Transmit OFI/DFI via RF	A functional test of the Integrated CM shows it successfully sends LAV OFI & DFI RF telemetry to RF receiver system during a simulated mission from 30 sec pre-launch until initiation of LAS Jettison. (Note - test durations will be short for safety reasons)	Test	SE&I

Actions

Title	CM Full Functional- Comm Check
Method	Test
Test Objective	Verify Functional Requirements associated with communications
Description	Using EGSE, and break-wire emulators as needed, verify that commuications is received by EGSE and CM and that antenna switch occurs per nominal mission sequence.
POC	WILLIAMS
Test Owner	SEIT

Example Thread – Functional Requirements

Test/Verification Activities are implemented by Electronic Task Production Sheets. Completed ETPS become evidence of requirement satisfaction

Requirements List

TPS Header

Document No	TPS-00029 (Revision 0)
Status	Created as of 3/22/2017
Short Title	Test - Hani
Created By	Obafunwa, Christiana (JSC-EA511)[Jacobs Technology, Inc.] on 3/22/2017 4:02 PM

Submit for Approval | Copy

Details | References | Steps | Parts | Tools | Attachments | Signatures/Approvals | Comments | History

Add Step | Renumber Steps

Steps

Action	Line	Step	Additional Data	Update Status
	1.00	Step 1.00	MIPS, GMIPS, Parts, Tools, Attachments	3/22/2017 4:12 PM by: Obafunwa, Christiana (JSC-EA511)[Jacobs Technology, Inc.]

Add Step | Renumber Steps

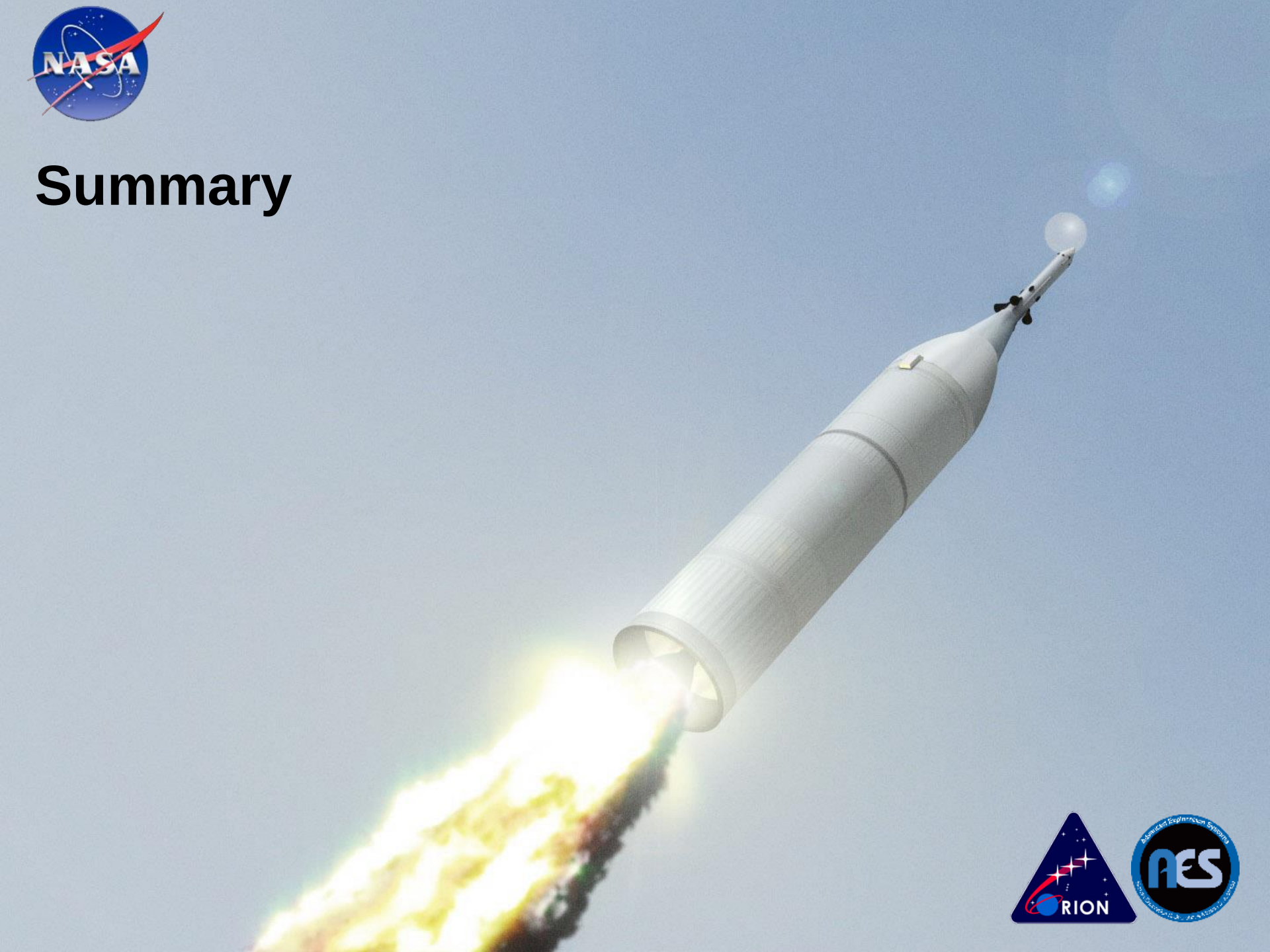
Manage | Actions

Document	SRD
Document Section	3.1.1.1 FTV EGSE Interface (I) Requirements
Reqt. No.	FTV-I-01
Shall Statement	The FTV shall send the following signals to the LAV EGSE per items 1 & 5 in table 1: a) LAV Abort (Abort Motor (AM) / Attitude Control Motor (ACM)) and Jettison Motor (JM) [S0] Safe & Arm Status b) LAV Ground Command status [S1A] c) LAV OFI/DFI [S1B]
Rationale	To monitor the LAV and associated DFI prior to launch.
Assumptions / Remarks	• LAV EGSE ICD is the overarching document and will include the signal definition. Intermediate interface requirement documents will reference the LAV EGSE ICD for signal definition. • Supports testing during AI&T and ground operations (includes control room). • Abort (AM / ACM) and Jettison Motor (JM) Safe & Arm Status [S0] – 2 safe & arm (1-ACM/AM, 1-JM) Defined in LM IDD. Originates from LAV EGSE & passes thru ATB, SR, CM to the LAS. • LAV Gnd Cmd Status [S1A] – To LAV EGSE through harness in ATB/SR. Required up to launch. CM-SepRing ICD defines the pass-thru interface details. • LAV OFI/DFI [S1B] – To LAV EGSE through harness in ATB/SR. Required up to launch for ground monitoring. LAV EGSE will send IRIG-B time to DFI system. CM-SepRing ICD defines the pass-thru interface details. • Signals will be sent from the FTV to LAV EGSE across the Network

	NRD 0.5c-1111
Children Requirements - CSR	CSR.CM.0584; CSR.CM.0592; CSR.CM.0543; CSR.EGSE.0537; CSR.EGSE.0699; CSR.EGSE.0701
Children Requirements - All Others	(LAS)
Children Requirements - Notes	waiting on LAS spec release in December
Tracing Complete	No
Parent Source Document(s)	
Parent Requirements - RVTM	
Verification Objective	
Verification Success Criteria	
Verification Events/Activities	
Closure Statement	
Closure Summary	
Links to Closure Evidence	
CE/ITA Signature	
SE Lead Signature	
Verification Owner Signature	
S&MA Lead Signature	

Created at 8/25/2016 2:43 PM by Dean, Hani K. (JSC-EA511)[Jacobs Technology, Inc.]
Last modified at 1/9/2017 11:26 AM by Aubuchon, Vanessa V. (LARC-D317) Close

Summary



Conclusions

- SP environment selection based on need for collaboration across a larger team, with geographic and organizational diversity
  - Lean development, team integration, high level of collaboration, and still have SE discipline
- SP strengths have paid off – demonstrated by our requirements products, on-line milestone reviews, extensively linked data, and nearly full engagement by 100 person team
  - Recommend that this collaborative environment be considered along with other commercial tools
- Challenges:
  - Lack of true ‘relational database’ is a challenge that continues to be worked – requires continued assessment and some ‘back-office’ development