JACOBS

Integrating MBSE Into Ongoing Projects: Requirements Validation and Test Planning for ISS SAFER

Tony Williams, ESEP

Jacobs Engineering

Chief Engineer, SE&I - Engineering Department

Director, INCOSE Americas Sector @incose_americas

Co-Authors:
Gregory Pierce, Jacobs Engineering
Herbert A. Anderson, NASA JSC

Overview

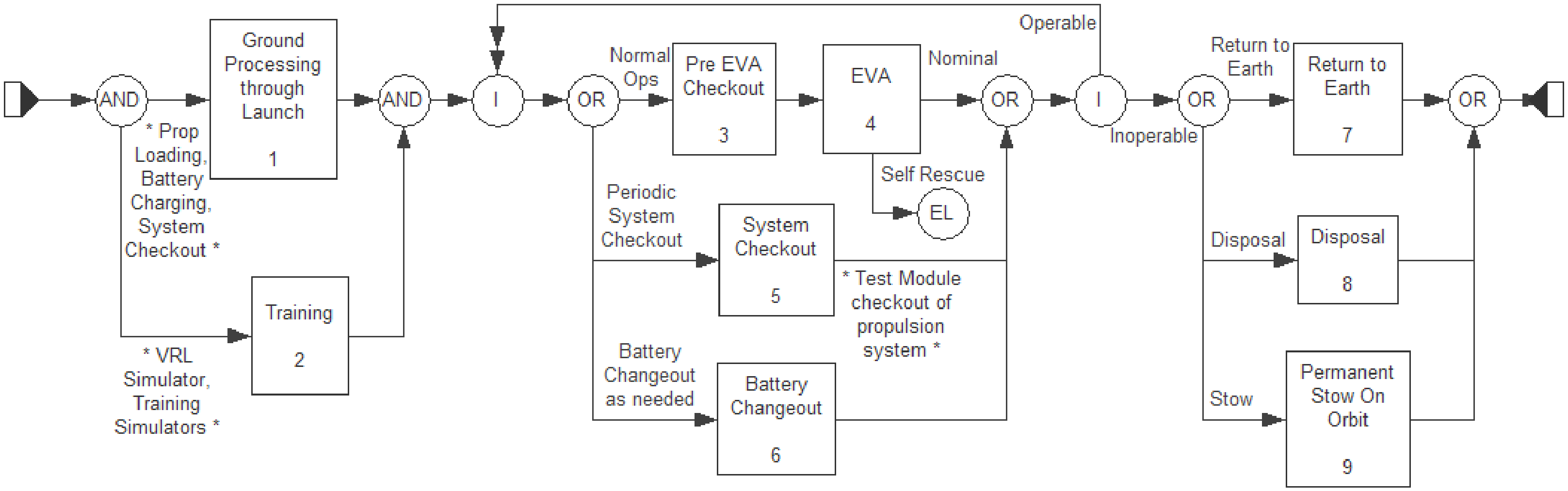
- Introduction to MBSE
- ISS SAFER Project Overview
  - Replacement to USA SAFER
  - Challenge and Opportunity
- MBSE Examples
  - Requirements Validation
  - Test Planning

What is Model-Based Systems Engineering (MBSE)?

- Model-Based Systems Engineering (MBSE) is an umbrella term that describes an approach to Systems Engineering that: emphasizes a **system architecture model** as the primary work artifact throughout the System Development Life Cycle
- Combines traditional systems engineering best practices with rigorous visual modeling techniques

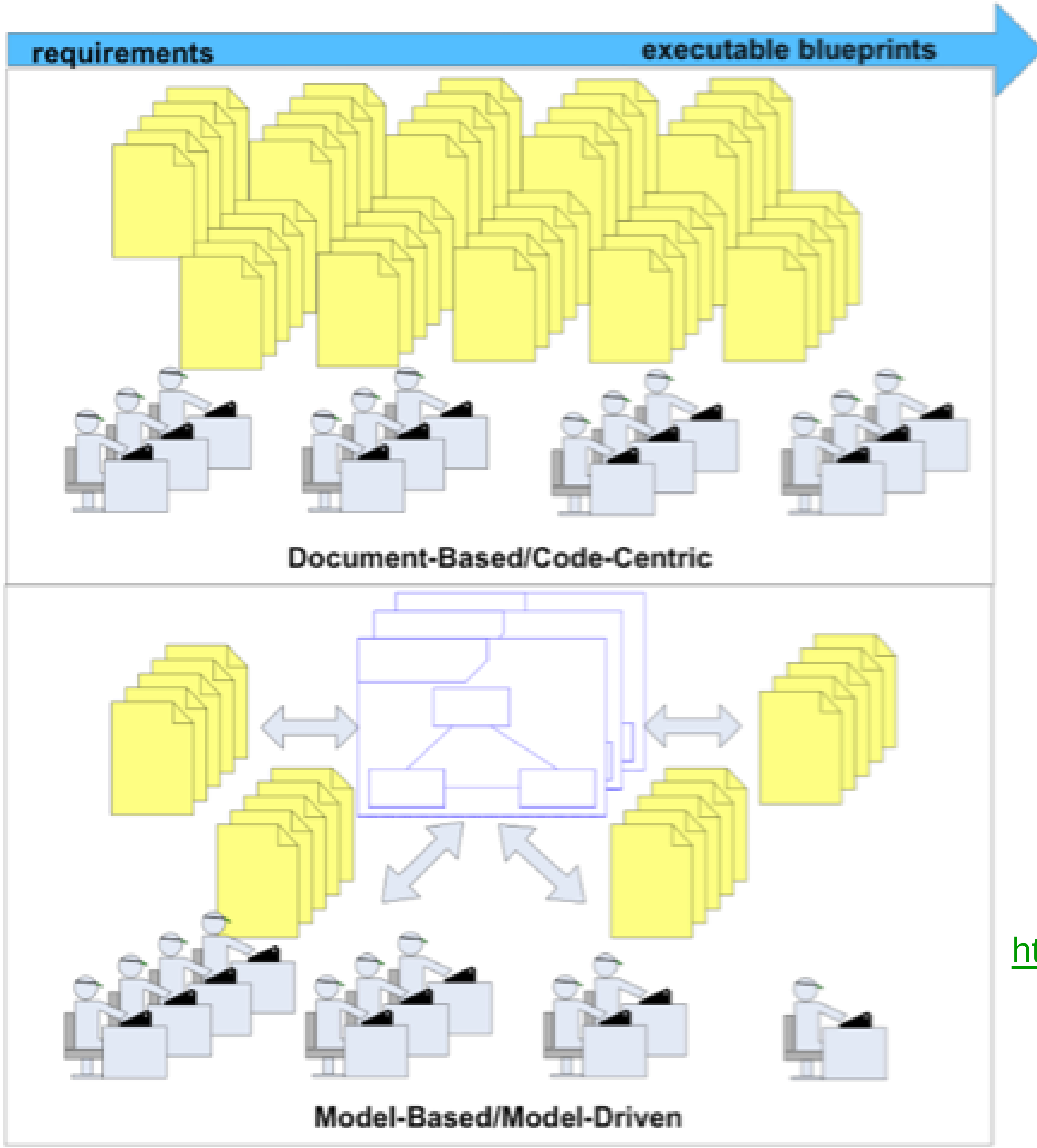
Source: http://www.sysmlforum.com/

MBSE Wiki Link
http://www.omgwiki.org/MBSE/doku.php



Process Flow Diagram is an example of visual modeling

Relationship between MBSE and traditional document-centric Systems Engineering



http://www.sysmlforum.com/

JACOBS

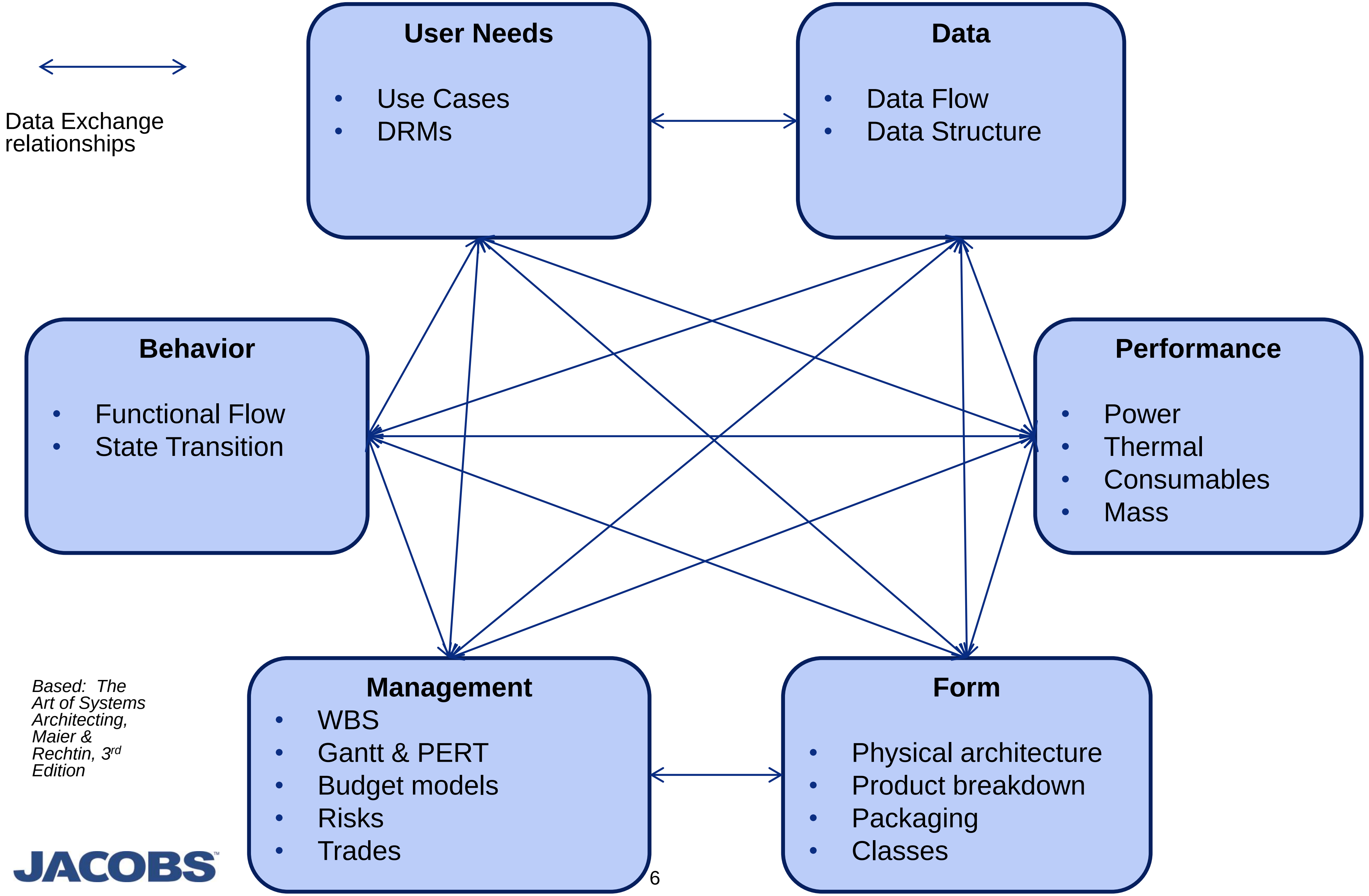
Advantages

- MBSE offers systems engineers the following advantages

Technology Drivers	Technology Advantages	Business Advantages
Model = requirements	Ensure that requirements are an integral part of model and all other parts of the model can be traced back to requirements (cf. requirement driven).	Validate that you are "building the right system"…[Boehm 1984]
Model = analysis & design	Provide a precise architectural blueprint organized by views that are meaningful to all system stakeholders	Verify that you are "building the system [the] right" way [Boehm 1984] Enable efficient system component building by 3rd parties/outsourcing
Model = simulation	Automate system validation and verification	Reduce errors and costs early in the lifecycle
Model = code	Automate generation of production quality code	Accelerate time to market
Model = test	Automate testing	Ensure system implementation is correct and reliable

http://www.sysmlforum.com/

Types of Models – Not Exclusive



Based: The Art of Systems Architecting, Maier & Rechtin, 3rd Edition

JACOBS

MBSE – Potential Opportunities in System Development

- Reduces project risk by linking requirements to Conops steps, systems functions, interfaces, or design elements
  - Reduces likelihood of unnecessary requirements
  - Improves coverage – reduces likelihood of under- or over- specification
  - Identifies and corrects gaps in coverage
  - Enhances traceability, since many types of system elements can be linked
    - Stakeholder & Design Requirements, Functions, constraints, interfaces, design elements, risks, ….
  - Errors can be caught earlier, reducing rework
- Schedule and corresponding cost savings – project team and stakeholders are able to share system models views, facilitating concurrent engineering
- Improved communications among stakeholders - picture is worth 1000 words
- Benefits in managing system complexity by enabling a single system model to be viewed from multiple perspectives (known as views)
  - Facilitates ability to analyze the impact of change
- Improved product quality by providing an unambiguous and precise model of the system that can be evaluated for consistency, correctness, and completeness.

JACOBS

System Life Cycle Costs Are Set Early In Development

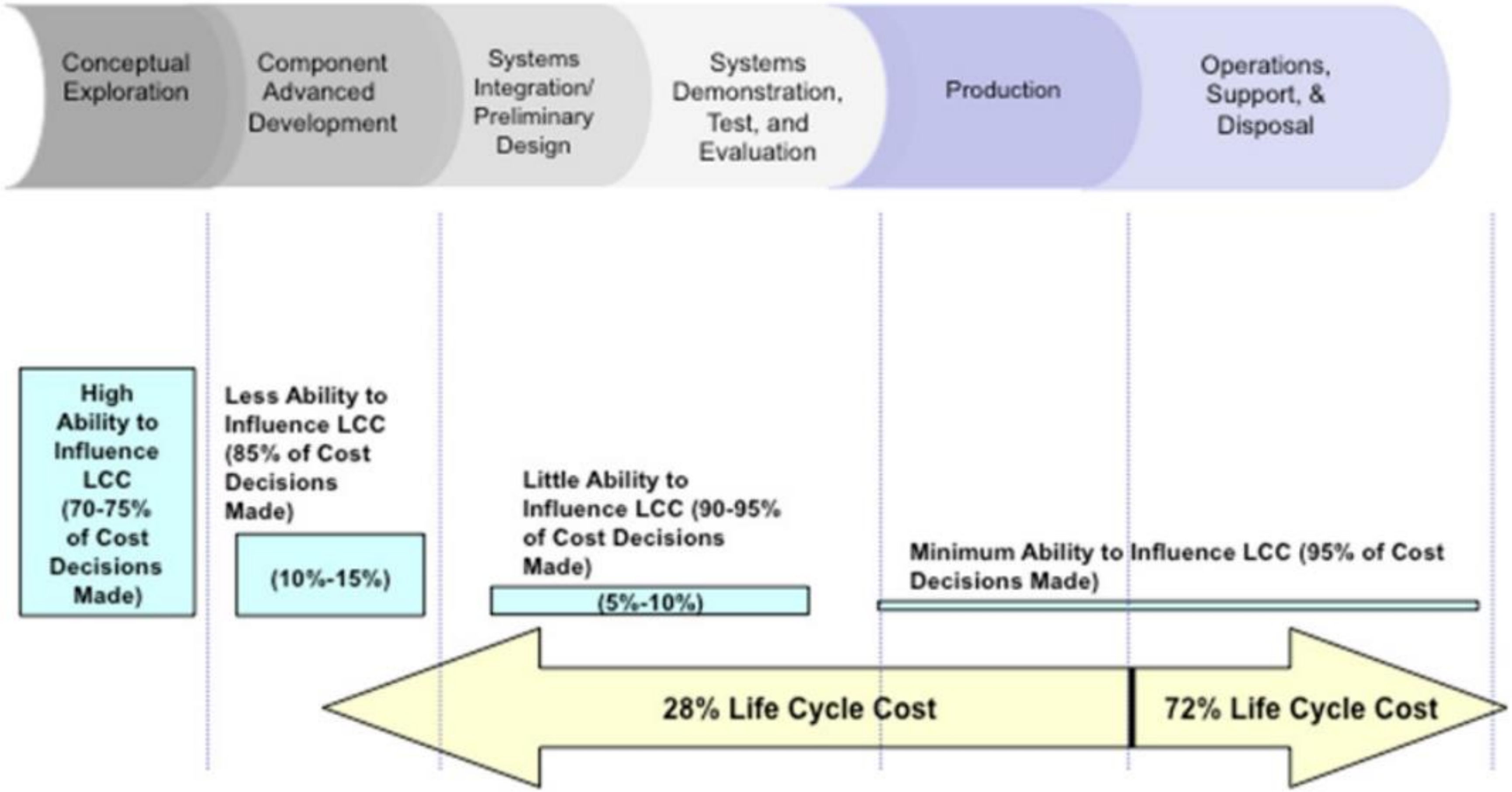


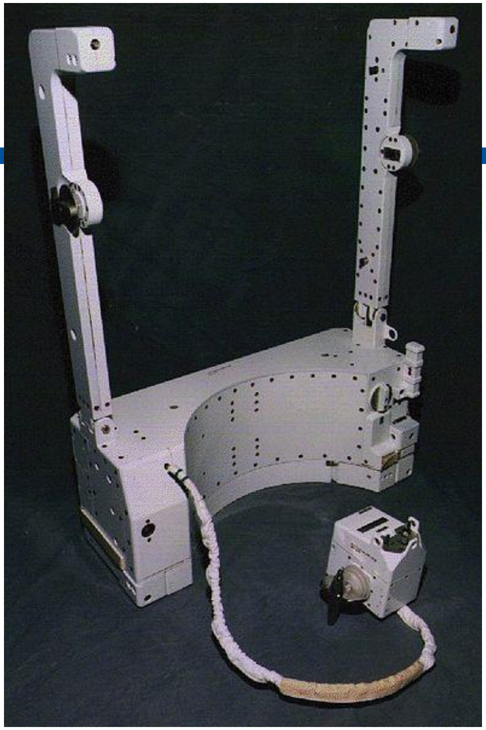
Fig. 3. Costs incurred and committed during our systems life cycle acquisition process (modified from Andrews, 2003)

Source: Life Cycle Costs Considerations for Complex Systems, John V. Farr, March 2012

Overview

- Introduction to MBSE
- ISS SAFER Project Overview
  - Replacement to USA SAFER
  - Challenge and Opportunity
- MBSE Examples
  - Requirements Validation
  - Test Planning

Simplified Aid for EVA Rescue (SAFER)



- A small, self-contained, propulsive backpack system used to provide free-flying mobility for a International Space Station (ISS) crewmember during extravehicular activity (EVA)
- SAFER is a small, simplified version of the Manned Maneuvering Unit (MMU) intended for contingency use during spacewalks.
- SAFER is designed to be used as a self-rescue device for a separated EVA crewmember in situations when no vehicles can provide rescue capability
  - SAFER can provide a total change in velocity (delta-v) of at least 10 ft/s

JACOBS

SAFER Applications

- SAFER is worn by ISS crewmembers using an Extravehicular Mobility Unit.
- Developed by the Software, Robotics, and Simulation Division of NASA at the Johnson Space Center
- SAFER was the design solution to the Shuttle Program's requirement to provide a means of self rescue should an EVA crewmember become untethered during an EVA

On-Orbit Testing

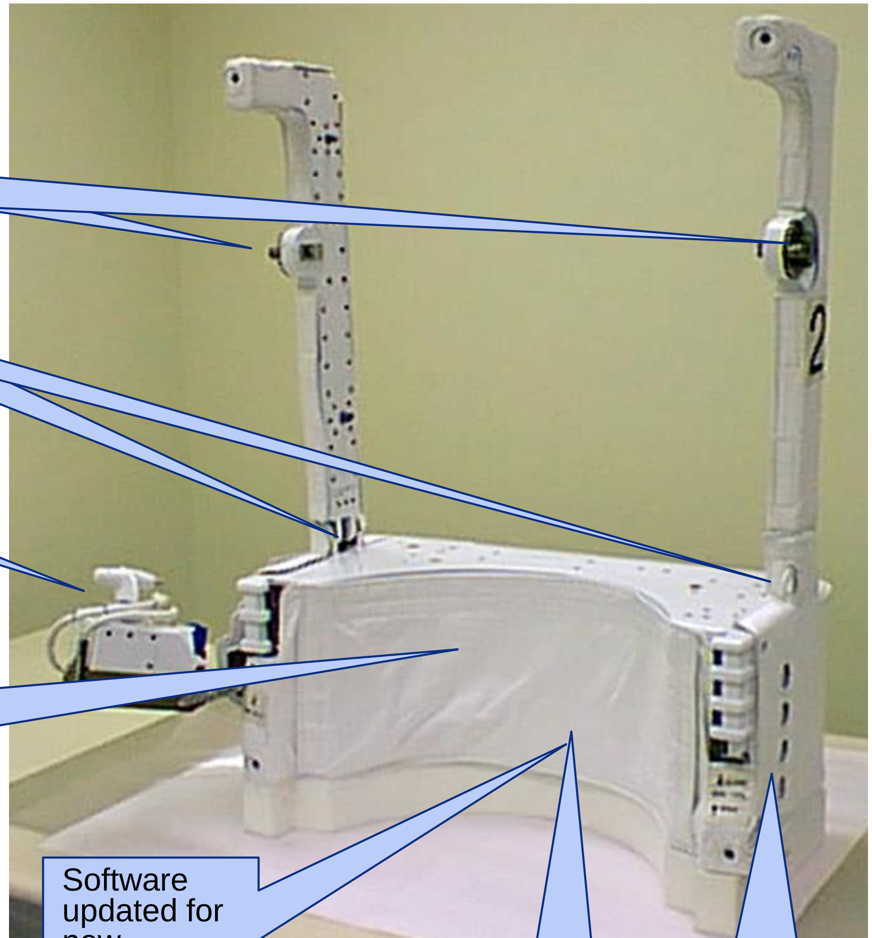
- First flown on STS-64 (9/9/1994)
  - Untethered flight test was performed first by astronauts Mark Lee and Carl Meade
  - Astronauts flew SAFER up and around the Shuttle's Robotic Arm along with a demonstration test of the SAFER's automatic attitude hold feature.
    - Arrests uncontrolled rotation of a detached crewmember expected in an accidental separation

STS-64, Astronaut Marc Lee tests the (SAFER) Simplified Aid for EVA Rescue system 130 nautical miles above earth.

ISS SAFER Project Overview

- Objective – Build replacement SAFERs for Space Station to provide EVA self-rescue capability from 2014 – 2020, with extension capability to 2028
  - Life expires on current fleet of 5 SAFERs between 2012 – 2014
  - Replicas with only some required minimal design changes
- Replacement fleet will include 3 flight ISS SAFERs + 3 ground spares
  - On-orbit life to be 7-8 years – an extension from current 2 year duration
- Extension requires test of prop system components that contain soft seals, requiring development of a new on-orbit Test Module
  - Crew use Test Module to exercise each SAFER prop system
  - Avoids the ~2-year ground maintenance cycle required of USA SAFER
- ISS SAFERs and Test Module to launch to ISS on alternate vehicles

ISS SAFER System – Changes from USA SAFER



New latch housing

New Hinges

Modified HCM cover

Add QDs, modify cover and plumbing

Software updated for new Avionics

New Avionics architecture

Vent hole number and size

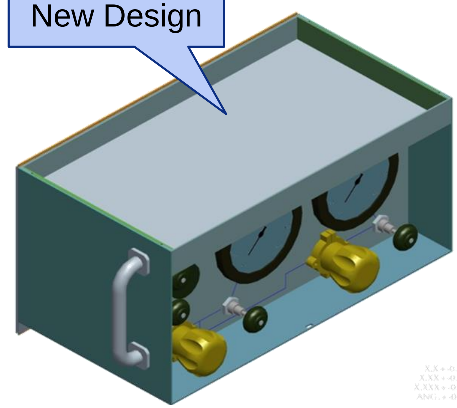
Software updated and consolidated

GTP

VRL

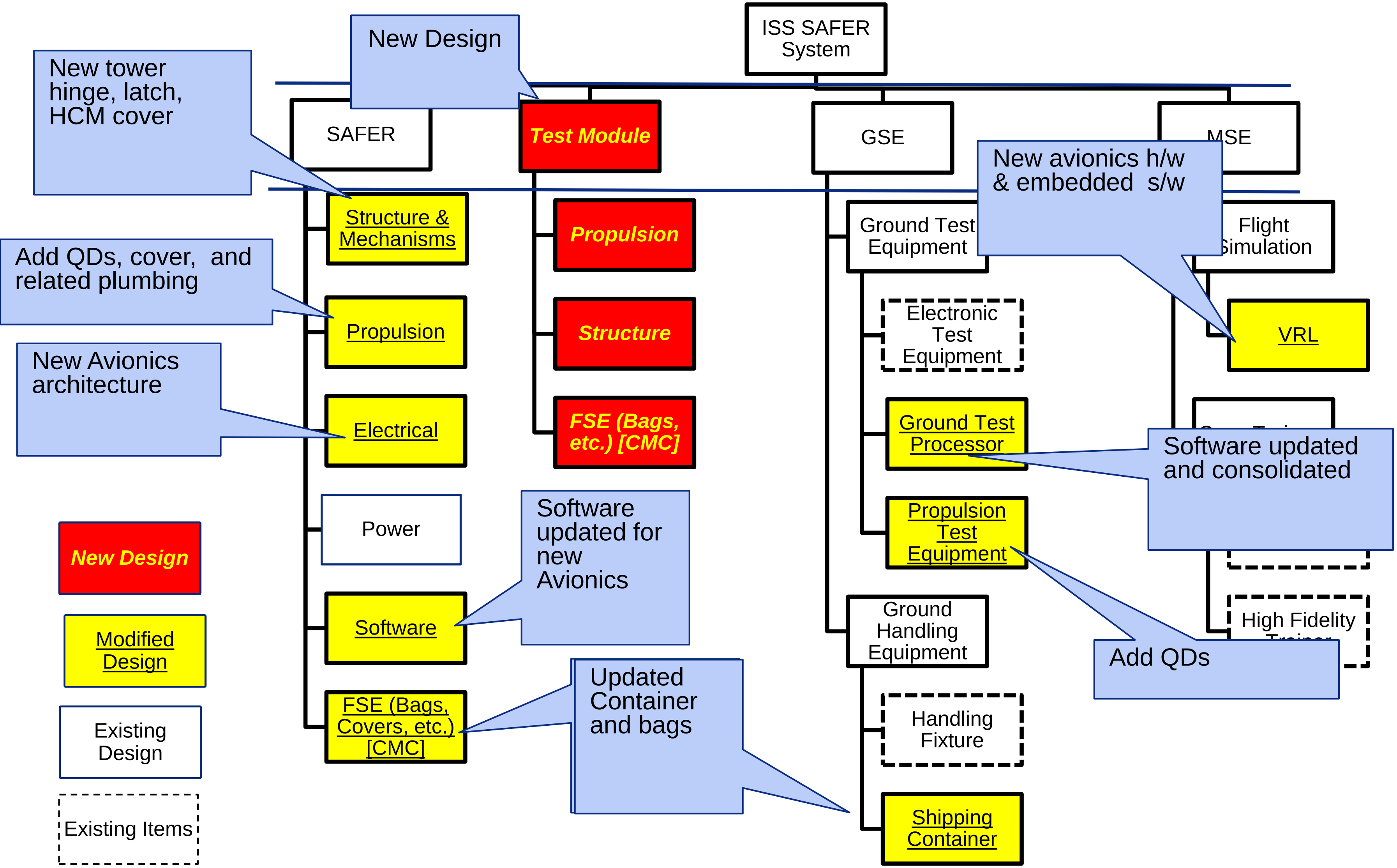
New avionics h/w & embedded s/w

TM New Design

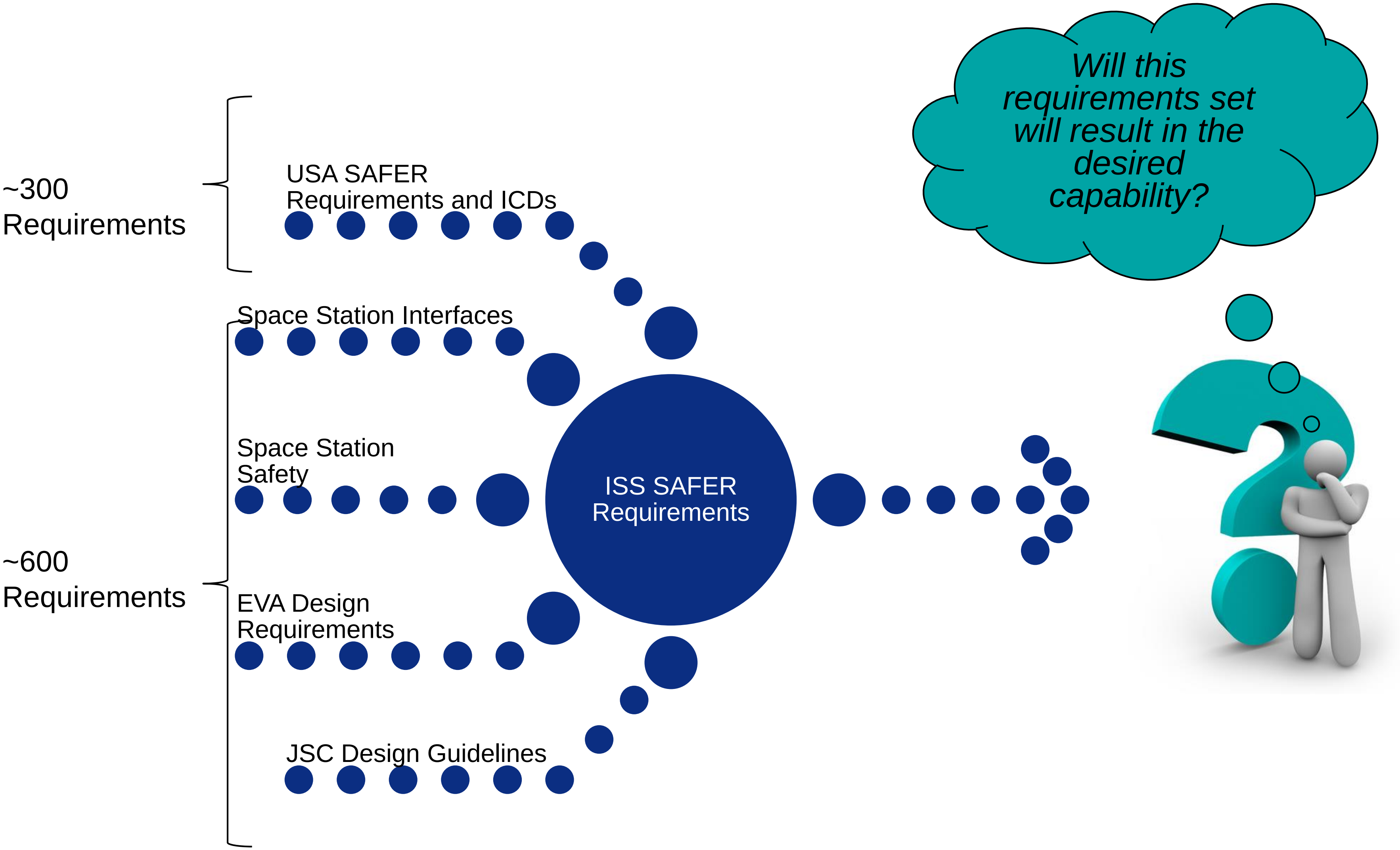


JACOBS

ISS SAFER System – Changes from USA SAFER



ISS SAFER Requirements Included USA SAFER Plus ~600 New Space Station Certification Requirement



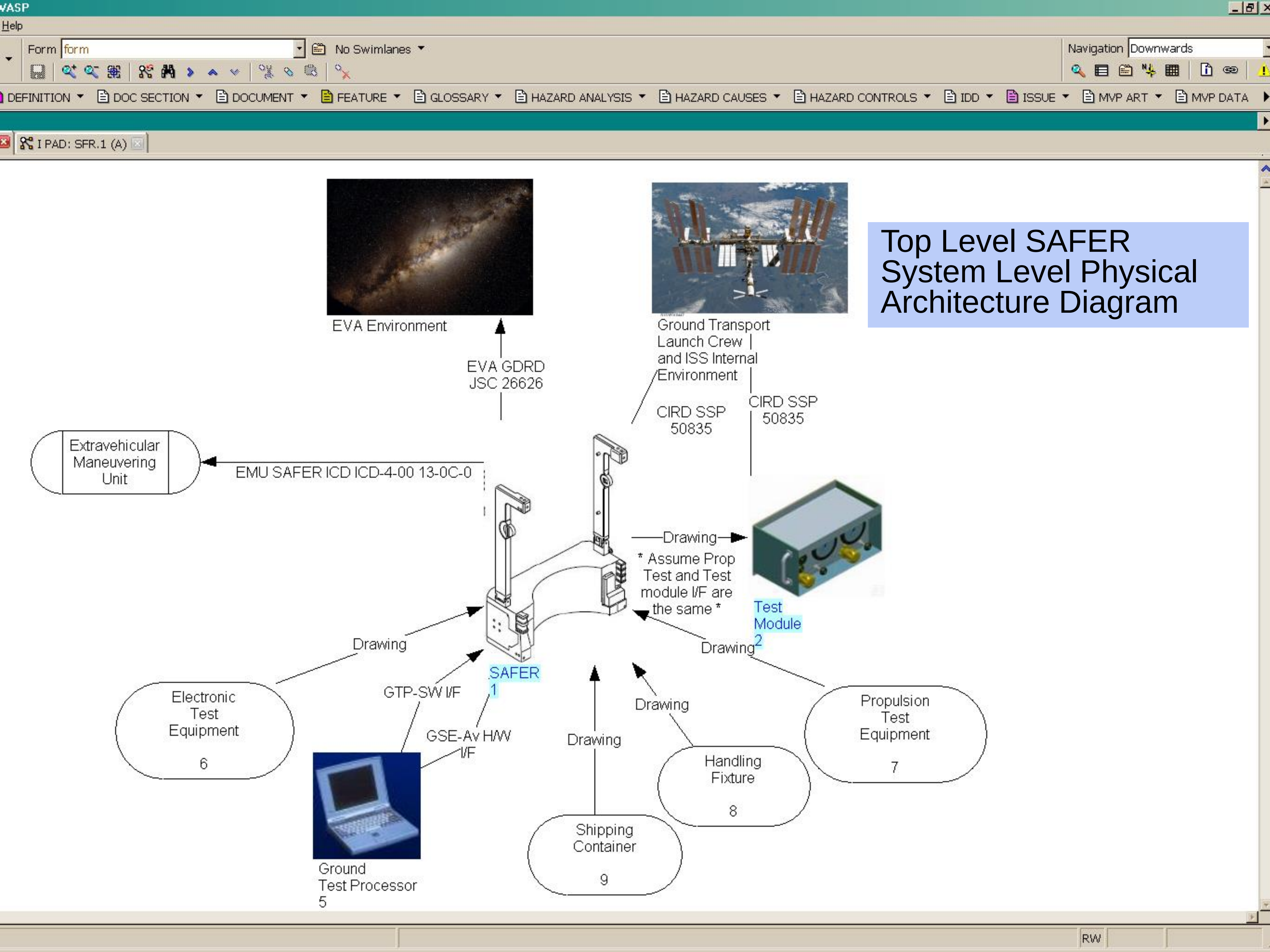
Challenges/Opportunity for ISS SAFER Leading to Use of MBSE

- Challenge –
  - Original operational and design requirements baseline had many modifications –
    - Addition of Common IRD, Space Station Safety, ISS Computer Based Control System, and more rigorous application of EVA requirements
    - Substantial modification of Avionics architecture and resulting design requirements changes
    - Addition of new functionality – Test Module and on-orbit maintenance
  - Challenge – How to confirm that resulting requirements set will result in the desired capability – the ISS SAFER
  - Solution - Requirements Validation of Specifications – Modeling to ensure all interfaces, system elements, and functions are appropriately addressed by specifications:
- Opportunity –
  - Engineering development unit (EDU) testing intended to rehearse certification test program
  - Opportunity existed to model engineering unit and certification test activities and manage requirements complexity by linking requirements, verification requirements, and verification activities directly to engineering unit and certification phase test activities
    - Provided extra benefits since end item specifications are still in development during EDU testing

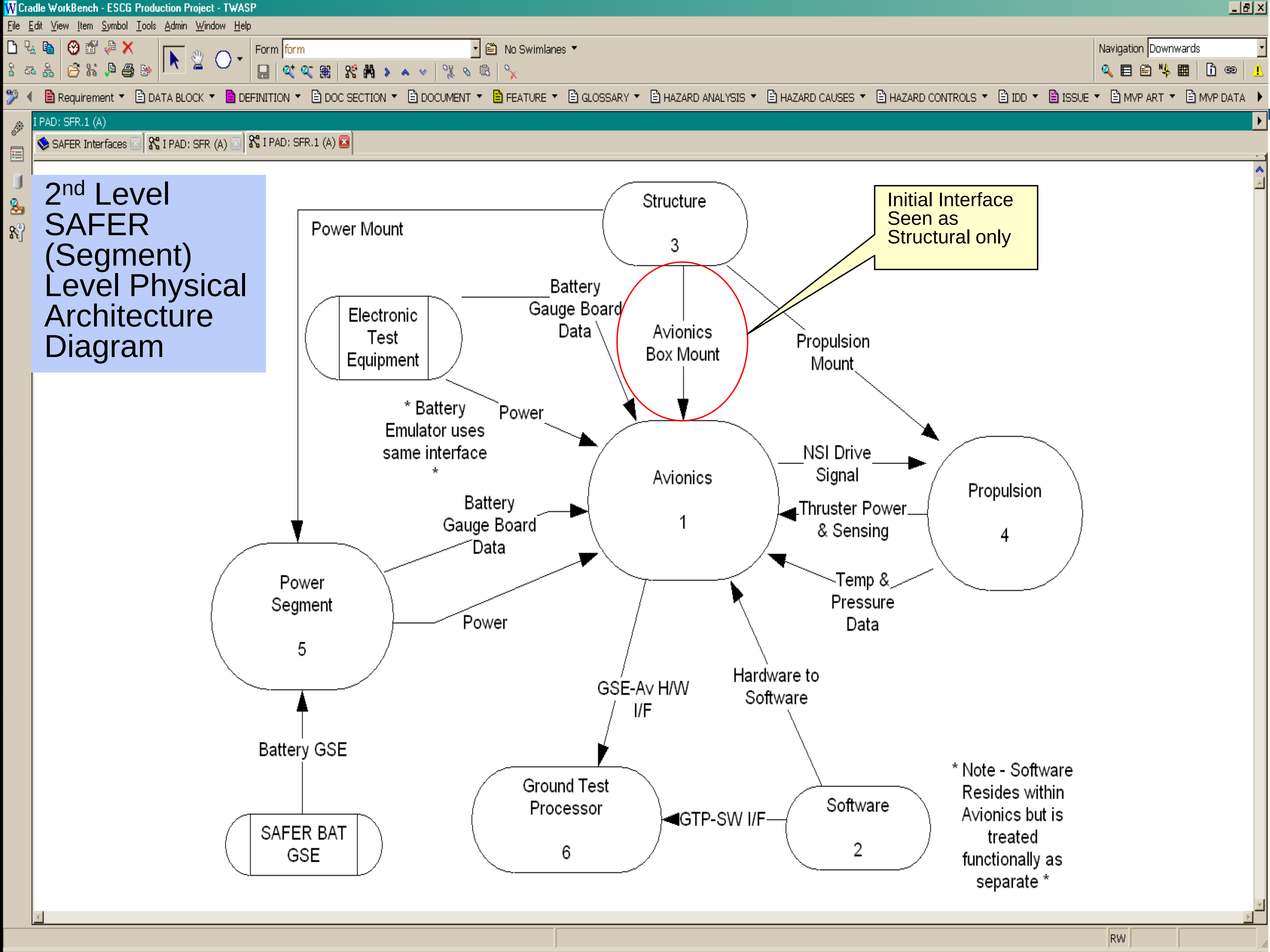
JACOBS

Overview

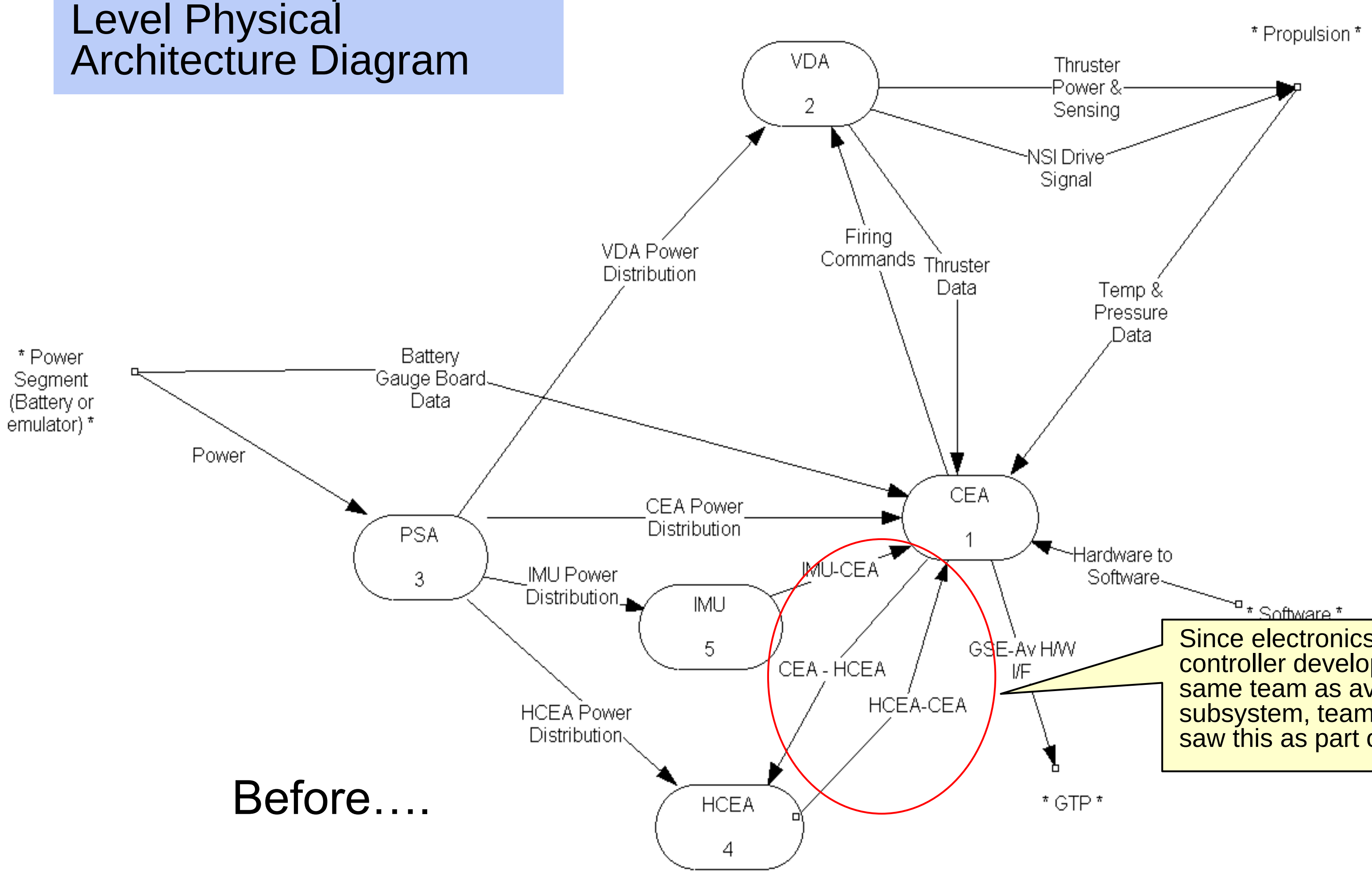
- Introduction to MBSE
- ISS SAFER Project Overview
  - Replacement to USA SAFER
  - Challenge and Opportunity
- MBSE Examples
  - Requirements Validation
  - Test Planning



VASP
Help
Form form
No Swimlanes
Navigation Downwards
DEFINITION
DOC SECTION
DOCUMENT
FEATURE
GLOSSARY
HAZARD ANALYSIS
HAZARD CAUSES
HAZARD CONTROLS
IDD
ISSUE
MVP ART
MVP DATA
I PAD: SFR.1 (A)
Top Level SAFER System Level Physical Architecture Diagram
EVA Environment
EVA GDRD JSC 26626
Ground Transport Launch Crew and ISS Internal Environment
CIRD SSP 50835
CIRD SSP 50835
Extravehicular Maneuvering Unit
EMU SAFER ICD ICD-4-00 13-0C-0
Drawing
* Assume Prop Test and Test module I/F are the same *
Test Module 2
Drawing
SAFER 1
Drawing
Electronic Test Equipment 6
GTP-SW I/F
GSE-Av H/W I/F
Drawing
Drawing
Propulsion Test Equipment 7
Handling Fixture 8
Shipping Container 9
Ground Test Processor 5
RW


Cradle WorkBench - ESCG Production Project - TWASP
File Edit View Item Symbol Tools Admin Window Help
Form form
No Swimlanes
Navigation Downwards
Requirement
DATA BLOCK
DEFINITION
DOC SECTION
DOCUMENT
FEATURE
GLOSSARY
HAZARD ANALYSIS
HAZARD CAUSES
HAZARD CONTROLS
IDD
ISSUE
MVP ART
MVP DATA
I PAD: SFR.1 (A)
SAFER Interfaces
I PAD: SFR (A)
I PAD: SFR.1 (A)
2nd Level SAFER (Segment) Level Physical Architecture Diagram
Initial Interface Seen as Structural only
Structure 3
Power Mount
Electronic Test Equipment
Battery Gauge Board Data
Avionics Box Mount
Propulsion Mount
* Battery Emulator uses same interface *
Power
Avionics 1
NSI Drive Signal
Propulsion 4
Thruster Power & Sensing
Battery Gauge Board Data
Power Segment 5
Power
Temp & Pressure Data
GSE-Av H/W I/F
Hardware to Software
Battery GSE
SAFER BAT GSE
Ground Test Processor 6
GTP-SW I/F
Software 2
* Note - Software Resides within Avionics but is treated functionally as separate *
RW

3nd Level SAFER Avionics Component Level Physical Architecture Diagram

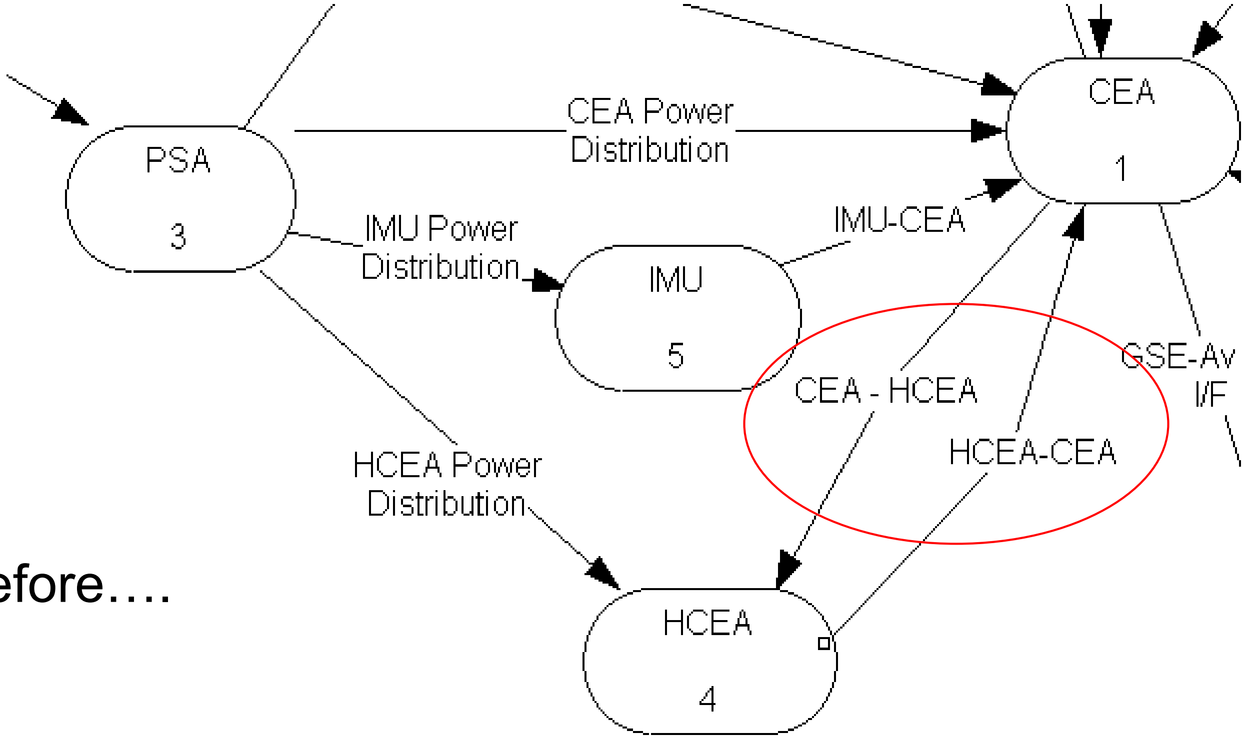


Since electronics in hand controller developed by same team as avionics subsystem, team initially saw this as part of avionics

Before….

Initial Findings - Example

- Modeling interfaces and project system structure between Hand Controller's electronics and Avionics electronics identified several different view points – Hand controller electronics assembly (HCEA) as part of Avionics, HCEA as part of Hand controller module (HCM) or both – with corresponding duplication, overlap, and conflict, of requirements.



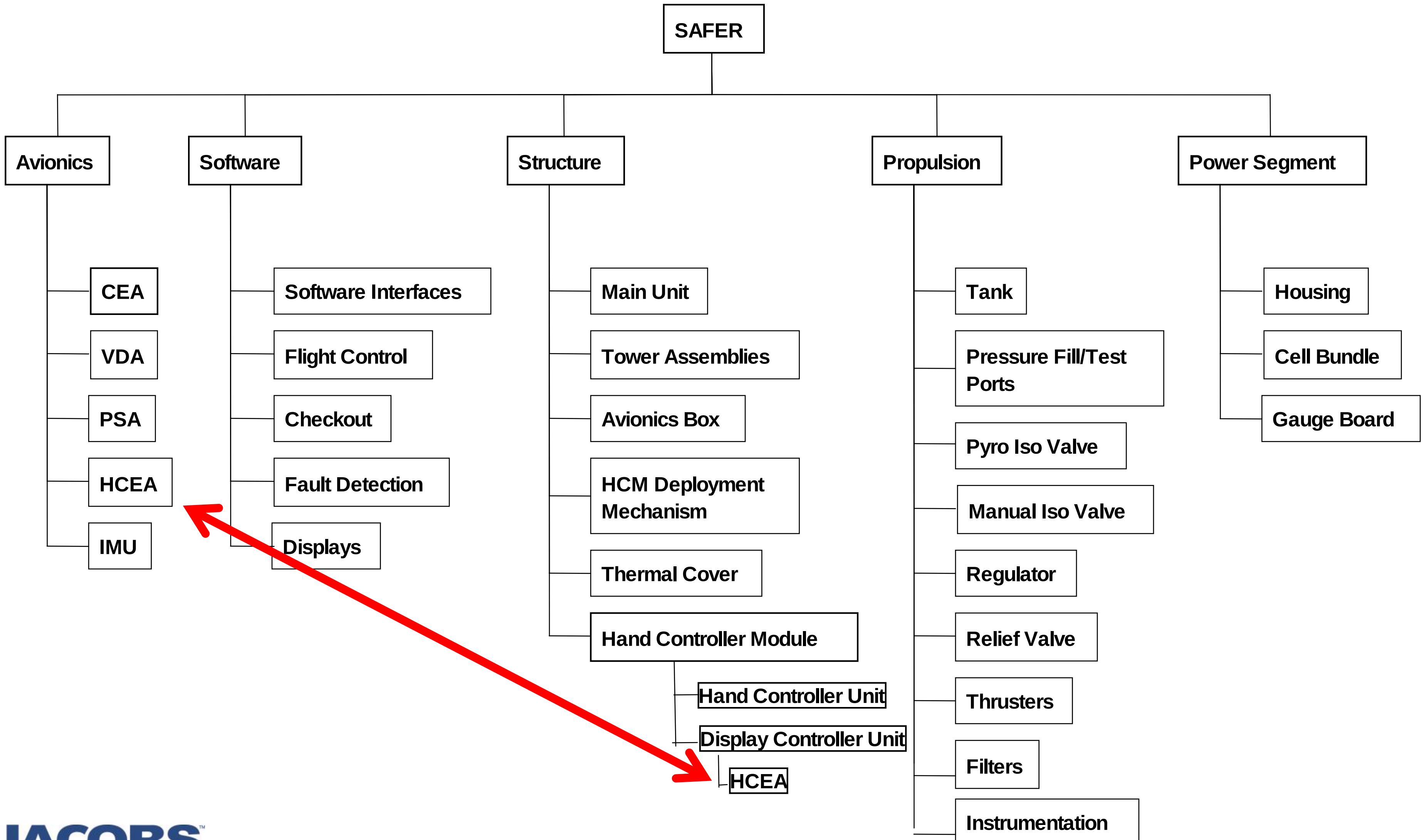
Before….

Hand Controller to Avionics Electrical Interface – Before and After

Identity	Name	Before	Name	After
R.SFR.SA.205	HCEA to CEA Interface	The HCEA (within the Hand Controller Module) shall communicate with the CEA (within the Avionics Subsystem) through a serial port.	HCEA to CEA Interface	Delete
R.SFR.SA.221	HCEA Data Signal Type	The ISS SAFER CEA shall communicate with the HCEA (physically within the HCM) via an RS422 serial interface.	HCEA Data Signal Type	Delete
R.SFR.SA.233	HCEA Data Rate	The HCEA data rate shall be 115200bps. Note: Refresh rate is aperiodic and based on state changes. Note: HCEA physically resides with HCM.	HCEA Data Rate	Delete
R.SFR.SA.235	HCEA Data Protocol	The communication between the CEA and the HCEA (within the HCM) shall be per RS-422 protocol.	HCEA Data Protocol	Delete
R.SFR.SA.236	HCEA Data Protocol	The HCEA transmit and receive data format shall be RS-422, 8 data bits, 1 stop bit, no parity, at 115200 bps.	HCM Data Protocol	The HCM transmit and receive data format shall be RS-422, 8 data bits, 1 stop bit, no parity, at 115200 bps. Note: Refresh rate is aperiodic and based on state changes.

Considering just the data format between the avionics subsystem and HCM identified significant duplication and overlap

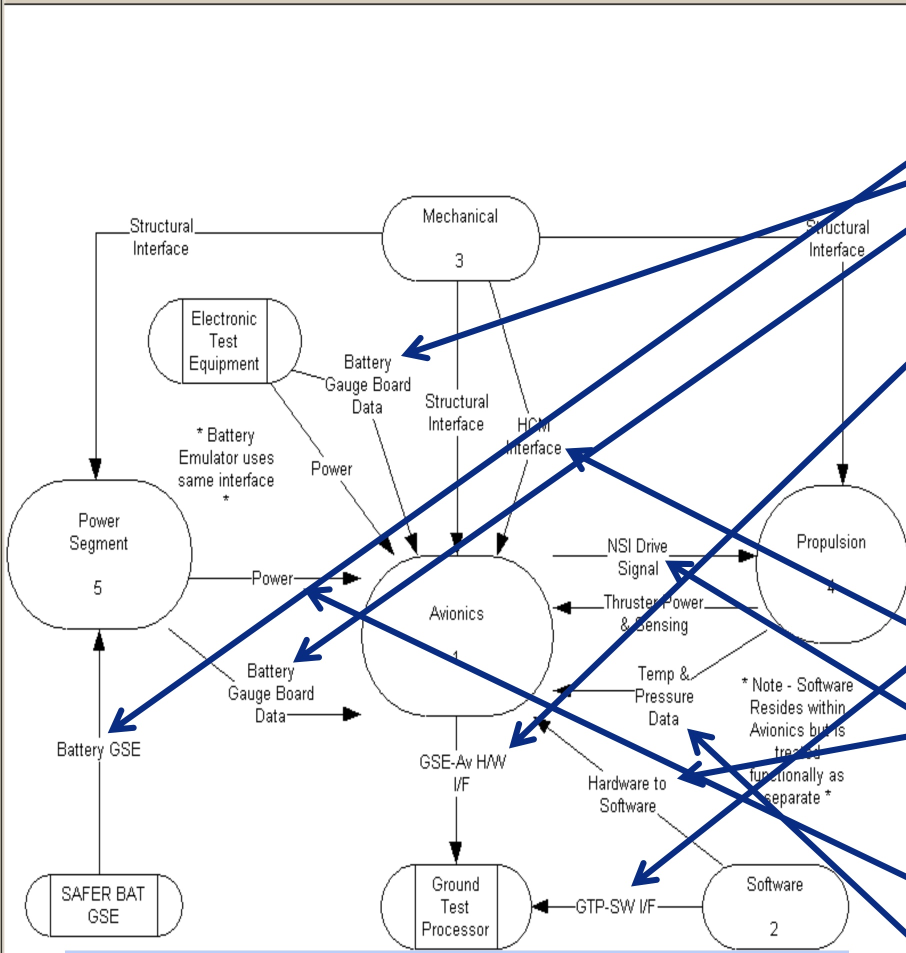
Project Breakdown Structure Modeling Identified Differing Viewpoints



JACOBS

Cradle WorkBench - ESCG Production Project - TWASP

I PAD: SFR.1 (A)

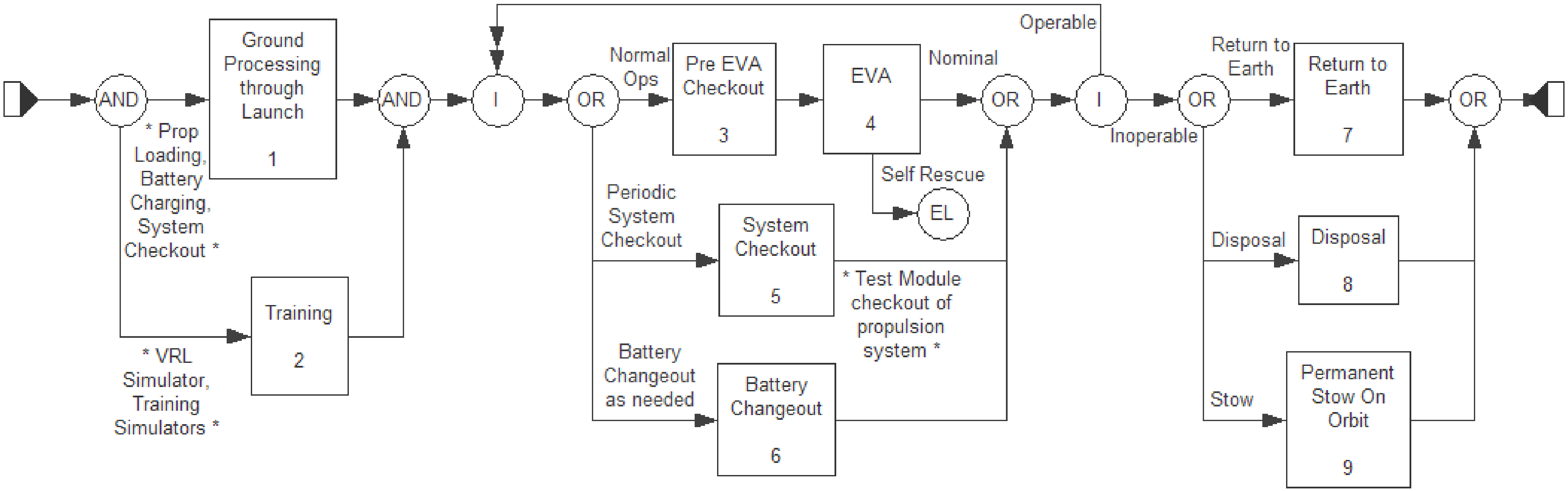


Query: SAFER Interfaces

#	Identity	Linked Items Identity	Name	Text
	Previous...			
1	Battery GSE	R.SFR.SA.199	Battery - GSE Interface Parameters	The ISS SAFER Power sub-system battery capacity gauge circuit shall provide all
2	Battery Gauge Board Data	R.SFR.SA.148	Battery Capacity Gauge Circuit - CEA	The ISS SAFER Battery capacity gauge circuit shall transmit data to the Avionics CEA as
		R.SFR.SA.215	IO Memory - Battery Data	The CEA shall read remaining capacity, voltage, temperature parameters from battery
3	GSE-Av H/W I/F	R.SFR.SA.075	Avionics Serial Input/Output	The Avionics Subsystem shall provide a serial interface through a connector located on the
		R.SFR.SA.076	CEA - GTP Interface Data Content	The CEA shall exchange data parameters with the GTP as defined in SRSD-12-004, ISS
		R.SFR.SA.222	GTP to Avionics Interface Connector	The GTP shall interface to the ISS SAFER using a USB connector for ground support
		R.SFR.SA.223	GTP Communication Protocol	The GTP communication shall use a USB 2.0 interface. (note - there is a dongle that
		R.SFR.SA.239	SAFER to GTP Interface Data Protocol	The Avionics Subsystem serial (GSE) port transmit and receive data format shall be
		R.SFR.SA.241	CEA to GSE Data Packet Rate	The ISS SAFER CEA shall transmit data packets at a rate of 4ms and receive data
		R.SFR.SA.272	GTP Dongle	There shall be a GSE dongle that connects to the GTP USB port and presents an RS-232
4	GTP to Av S/W ICD	R.SFR.SA.267	GTP Software to Avionics Software Interface	The GTP Software and Avionics Software shall interface as specified in SRSD-12-004, ISS
5	HCM Interface	R.SFR.SA.236	HCM Data Protocol	HCM Data Protocol The HCM transmit and receive data format shall be RS-422, 8 data
6	Hardware to Software	R.SFR.SA.266	Avionics Hardware-Software Interface	The Avionics Hardware and Avionics Software shall interface as specified in SRSD-12-003,
7	NSI Drive Signal	R.SFR.SA.064	Firing Commands - Drive Signals	Upon receipt of thruster and NSI firing commands from the CEA, the VDA shall apply
		R.SFR.SA.067	Output Drive Signal - NSI	The VDA shall generate an output drive signal that provides energy necessary to "fire" the
		R.SFR.SA.070	Current Flow Through NSI	The VDA shall be able to sense a small current flow through the NSI circuit during
8	Power	R.SFR.SA.246	Battery Power	The ISS SAFER Battery shall supply power to the ISS SAFER Avionics Subsystem as follows:
9	Structural Interface	R.SFR.SA.106	Main Unit Contents	The Main Unit structure shall consist of a frame for mounting ISS SAFER components
10	Temp & Pressure Data	R.SFR.SA.227	Propulsion Data - Temperature Signal	The ISS SAFER CEA shall receive one analog temperature signal from an RTD located on
		R.SFR.SA.248	CEA Receive Analog Pressure Signal	The CEA shall receive one analog pressure sensor signal from the Propulsion Module GN2
		R.SFR.SA.249	Propulsion Data - Pressure Sensor	The Propulsion pressure sensor signal shall be differential with full scale output amplitude of

Correlation of 2nd level SAFER Physical Architecture Diagram and Interface Requirements from End Item Specification

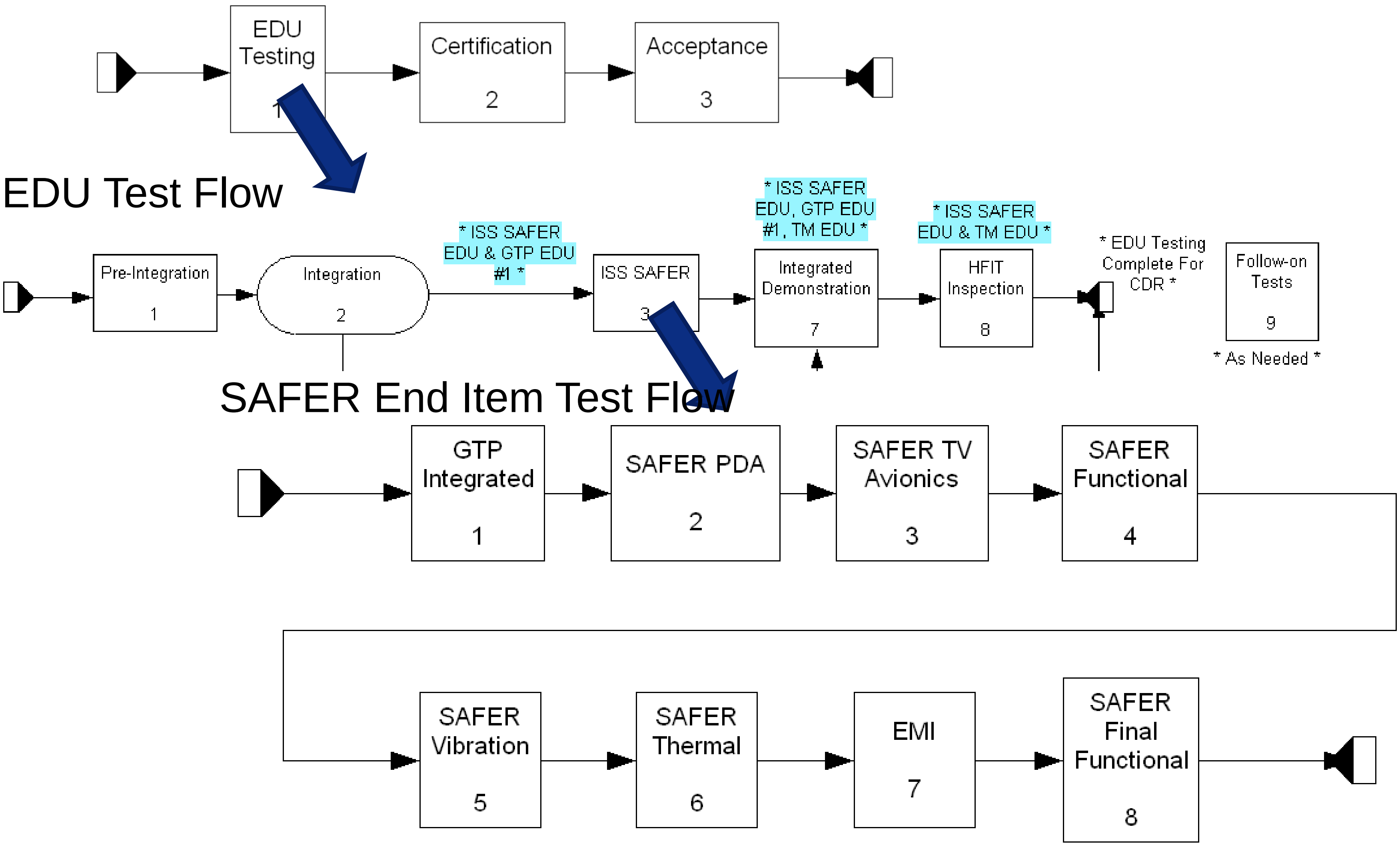
Top-level Process Flow – ISS SAFER System



As in the case of the interfaces, the structure and functions of the SAFER were mapped to requirements to ensure full coverage, lack of conflicts and appropriate level

EDU Test Plan Development

Overall Test Flow



Cradle WorkBench - ESCG Production Project - TWASP

File Edit View Item Query Tools Admin Window Help

View: VV Activity - VA - VR | Navigation: Bidirectional

Requirement | DATA BLOCK | DEFINITION | DOC SECTION | DOCUMENT | FEATURE | GLOSSARY | HAZARD ANALYSIS | HAZARD CAUSES | HAZARD CONTROLS | IDD | ISSUE | MVP ART | MVP DATA

Query: SAFER PFDs - VV Operations

I BD: FF.SFR.001 (A) | I BD: FF.SFR.001.3 (A) | I BD: FF.SFR.001.3.2 (A) | I BD: FF.SFR.001.2 (A) | I PFD: P.VV (A) | I PFD: P.VV.1 (A) | I PFD: P.VV.1.3 (A) | SAFER PFDs - VV Operations

Table linking EDU Testing Events to Verification Activities to Specific Verifications Requirements for Each

	Identity	Name	Linked Items					
						Identity	Name	Text
4	P.VV.1.3.3	SAFER TV Avionics	VA.SFR.E75	Thermal Vacuum Test - SAFER	Test	The purpose of Thermal Vacuum (TV) testing for the ISS SAFER EDU is: 1) Update thermal model for new avionics and provide improved inputs		
						V.SFR.016b	Displays - Qualification Thermal Vacuum	A qualification ... functions in the ... roller display
						V.SFR.047b	Unique EVA Thermal Environment - Qualification	A qualification ... the EVA thermal environment. The test must use the test conditions determined by the associated thermal analysis.
						V.SFR.410a	EVA Pressure Environment - Qualification Thermal Vacuum	A qualification thermal vacuum test must show the ISS SAFER meets performance requirements when exposed to overall steady state pressure extremes of 1x10-12 psia.
5	P.VV.1.3.4	SAFER Functional	VA.SFR.E00-1	ISS SAFER Functional Testing	Test	The purpose of this test is to reconfirm ISS SAFER performance folloiwng environmental testing and/or reassembly. The USA SAFER FTP procedure TBD will be performed, and captured in the ISS SAFER FTP via redlines.		
6	P.VV.1.3.5	SAFER Vibration	VA.SFR.E77	ISS SAFER Random Vibration Testing	Test	Vibration testing serves two purposes (1) confirming that the system, as designed and built, will function after exposure to the launch environment and other vibration environments and (2) confirm that the workmanship for the system is satisfactory and that it was assembled properly.		
						V.SFR.605-1	Shock Pulse - SAFER	Shock testing must show that the ISS SAFER meets functional and performance requirements while experiencing a 20-g 11-millisecond terminal-peak sawtooth pulse per MIL-STD-810, Method 516.4, Procedure I while being operated in its intended functional mode without
						V.SFR.SA.154	Random Vibration	A test shall be performed to show that the ISS SAFER meets the specified performance requirements after exposure to the design random vibration environment for launch.
						V.SFR.SA.171b	Acceleration - Launch and Landing - Test	A test must be performed on the ISS SAFER to demonstrate compatibility with the launch vehicle environments for launch and landing.
						V.SFR.SA.257	Workmanship Vibration	An Acceptance Random Vibration test must show that the ISS SAFER can withstand the defined environments in SSP 41172, Section 5.1.4.
7	P.VV.1.3.6	SAFER Thermal	VA.SFR.E73	Thermal Cycling - SAFER	Test	Since the ISS SAFER elements will see different temperature ranges, ther... (TBD) based on the thermal ranges expected +/- 20 deg F (per SSP 4117... ...and Towers		
						V.SFR.016c	Displays - Qualification Thermal Cycling	A qualification t... functions in the ... ller display
						V.SFR.046d	Don/Doff - Thermal Cycling	A thermal cyclin... exposure to the ... ring
						V.SFR.047c	Unique EVA Thermal Environment - Qualification	A qualification thermal cycling test, performed in accordance with SSP 41172, section 4.2.3, must show the ISS SAFER can operate in the EVA thermal environment. The test must use the test conditions determined by the associated thermal analysis.
						V.SFR.404-1c	IVA Operating Temperature - SAFER Qualification Thermal	A qualification thermal cycling test, performed in accordance with SSP 41172, section 4.2.3, must show the ISS SAFER meets performance requirements when exposed to temperatures ranging from 41 to 113 ºF.
						V.SFR.SA.175	Pre-Launch Ground Handling Temperature	A thermal test must be performed in accordance with the guidelines in SSP 41172 to show that the ISS SAFER meets all safety and performance requirements after being exposed to temperatures ranging from -18ºC to +50ºC (0ºF to 122ºF).
						V.SFR.SA.259	Thermal Cycling	A Thermal Cycling test must show that the ISS SAFER can withstand the defined environments in SSP 41172, Section 5.1.3.
8	P.VV.1.3.7	EMI	VA.SFR.E71	EMI Test	Test	(not yet reviewed)		

Resulting EDU Test Plan produced directly from Cradle, as will be future Qualification and Acceptance Test Plan

Identity: Ascending - Case sensitive | 9 items

Conclusions

- MBSE provided tailored solution to challenge of requirements validation for ISS SAFER design specifications and provided benefits in managing simultaneously changing test plans and design requirements data sets
- MBSE as opportunistically applied tool provided ability to solve challenges without need to impose MBSE approach on entire project
  - Enabled by trained SE team and inherent capabilities in Cradle
- Produced direct savings to project (~2.3 person years)
  - Reduced RIDs, rework, errors, and unnecessary verifications
  - More efficient verification planning
- Paves the way for larger applications in future projects