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


Process Flow Diagram is an example of visual modeling
Relationship between MBSE and traditional document-centric Systems Engineering

http://www.sysmlforum.com/
MBSE offers systems engineers the following advantages

<table>
<thead>
<tr>
<th>Technology Drivers</th>
<th>Technology Advantages</th>
<th>Business Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model = requirements</td>
<td>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).</td>
<td>Validate that you are “building the right system”...[Boehm 1984]</td>
</tr>
<tr>
<td>Model = analysis &amp; design</td>
<td>Provide a precise architectural blueprint organized by views that are meaningful to all system stakeholders</td>
<td>Verify that you are “building the system [the] right” way [Boehm 1984] Enable efficient system component building by 3rd parties/outsourcing</td>
</tr>
<tr>
<td>Model = simulation</td>
<td>Automate system validation and verification</td>
<td>Reduce errors and costs early in the lifecycle</td>
</tr>
<tr>
<td>Model = code</td>
<td>Automate generation of production quality code</td>
<td>Accelerate time to market</td>
</tr>
<tr>
<td>Model = test</td>
<td>Automate testing</td>
<td>Ensure system implementation is correct and reliable</td>
</tr>
</tbody>
</table>

http://www.sysmlforum.com/
Types of Models – Not Exclusive

User Needs
- Use Cases
- DRMs

Data
- Data Flow
- Data Structure

Behavior
- Functional Flow
- State Transition

Management
- WBS
- Gantt & PERT
- Budget models
- Risks
- Trades

Performance
- Power
- Thermal
- Consumables
- Mass

Form
- Physical architecture
- Product breakdown
- Packaging
- Classes

Data Exchange relationships

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

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 an 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
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
- VRL New avionics h/w & embedded s/w
- Software updated and consolidated
- GTP
- TM New Design
- Vent hole number and size
ISS SAFER System – Changes from USA SAFER

New Design

- New tower hinge, latch, HCM cover
- Add QDs, cover, and related plumbing
- New Avionics architecture

Modified Design

- Power
- Software
- FSE (Bags, Covers, etc.) [CMC]

Existing Design

- SAFER
- Test Module
- Structure & Mechanisms
- Propulsion
- Electrical
- FSE (Bags, etc.) [CMC]

ISS SAFER System

New avionics h/w & embedded s/w

GSE

- Ground Test Equipment
- Electronic Test Equipment
- Ground Test Processor
- Propulsion Test Equipment
- Ground Handling Equipment
- Handling Fixture
- Shipping Container

MSE

- Flight Simulation

VRL

- Crew Trainers
- NBL Trainer
- High Fidelity Trainers

Software updated and consolidated

Add QDs

15
ISS SAFER Requirements Included USA SAFER Plus
~600 New Space Station Certification Requirement

Will this requirements set will result in the desired capability?
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
Overview

- Introduction to MBSE
- ISS SAFER Project Overview
  - Replacement to USA SAFER
  - Challenge and Opportunity
- MBSE Examples
  - Requirements Validation
  - Test Planning
2nd Level SAFER (Segment) Level Physical Architecture Diagram
Before...
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.
# Hand Controller to Avionics Electrical Interface – Before and After

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

Avionics
- CEA
- VDA
- PSA
- HCEA
- IMU

Software
- Software Interfaces
  - Flight Control
  - Checkout
  - Fault Detection
  - Displays

Structure
- Main Unit
  - Tower Assemblies
    - Avionics Box
    - HCM Deployment Mechanism
    - Thermal Cover
  - Hand Controller Module
    - Hand Controller Unit
    - Display Controller Unit
    - HCEA

Propulsion
- Tank
  - Pressure Fill/Test Ports
    - Pyro Iso Valve
    - Manual Iso Valve
    - Regulator
    - Relief Valve
    - Thrusters
    - Filters
    - Instrumentation

Power Segment
- Housing
  - Cell Bundle
  - Gauge Board
Correlation of 2nd level SAFER Physical Architecture Diagram and Interface Requirements from End Item Specification
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

EDU Test Flow

SAFER End Item Test Flow
Table linking EDU Testing Events to Verification Activities to Specific Verifications Requirements for Each Resulting EDU Test Plan produced directly from Cradle, as will be future Qualification and Acceptance Test Plan.
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.