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

Herbert A. Anderson[1]
Johnson Space Center, National Aeronautics and Space Administration, Houston, TX 77058

Antony Williams[2]
Jacobs Engineering, Houston Texas, 77058

Gregory Pierce[3]
Jacobs Engineering, Houston Texas, 77058

Abstract

The International Space Station (ISS) Simplified Aid for Extra Vehicular Activity (EVA) Rescue (SAFER) is the spacewalking astronaut's final safety measure against separating from the ISS and being unable to return safely. Since the late 1990s, the SAFER has been a standard element of the spacewalking astronaut's equipment. The ISS SAFER project was chartered to develop a new block of SAFER units using a highly similar design to the legacy SAFER (known as the USA SAFER). An on-orbit test module was also included in the project to enable periodic maintenance/propulsion system checkout on the ISS SAFER.

On the ISS SAFER project, model-based systems engineering (MBSE) was not the initial systems engineering (SE) approach, given the volume of heritage systems engineering and integration (SE&I) products. The initial emphasis was ensuring traceability to ISS program standards as well as to legacy USA SAFER requirements. The requirements management capabilities of the Cradle systems engineering tool were to be utilized to that end. During development, however, MBSE approaches were applied selectively to address specific challenges in requirements validation and test and verification (T&V) planning, which provided measurable efficiencies to the project. From an MBSE perspective, ISS SAFER development presented a challenge and an opportunity.

Addressing the challenge first, the project was tasked to use the original USA SAFER operational and design requirements baseline, with a number of additional ISS program requirements to address evolving certification expectations for systems operating on the ISS. Additionally, a need to redesign the ISS SAFER avionics architecture resulted in a set of changes to the design requirements baseline. Finally, the project added an entirely new functionality for on-orbit maintenance. After initial requirements integration, the system requirements count was approaching 1000, which represented a growth of 4x over the original USA SAFER system. This presented the challenge - How to confirm that this new set of requirements set would result in the creation of the desired capability.

---

[1] Project Manager, Simplified Aid For EVA Rescue, Dynamic Systems Test Branch
[2] Chief Engineer, SE&I, Engineering Department
[3] Senior Systems Engineer, Engineering Department

To address this challenge, the development team used a very limited MBSE implementation. By modeling the systems architecture, interfaces, and functions, the team was able to provide a highly efficient assessment of the requirements deployment against these system elements, resulting in identification and correction of dozens of requirements disconnects.

The SE team also identified an opportunity – using MBSE to model the system verification and validation activities, and manage requirements complexity by linking requirements, verification requirements, and verification activities directly to the engineering unit certification, and acceptance phase test activities. This provided extra benefits since end item specifications were still in development during Engineering Design Unit (EDU) testing. Modeling these activities resulted in a number of efficiencies, including automated generation of plans for analyses, and engineering and verification tests. This also set the framework to rapidly generate verification and certification documentation.

Overall, MBSE provided a tailored solution to the 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 an opportunistically applied tool, provided the ability to solve challenges without imposing the MBSE approach on the entire project. This efficiency was enabled by a trained SE team and inherent capabilities in the Cradle systems engineering environment that was leveraged. Further, this prototype application paved the way for larger applications in future projects.

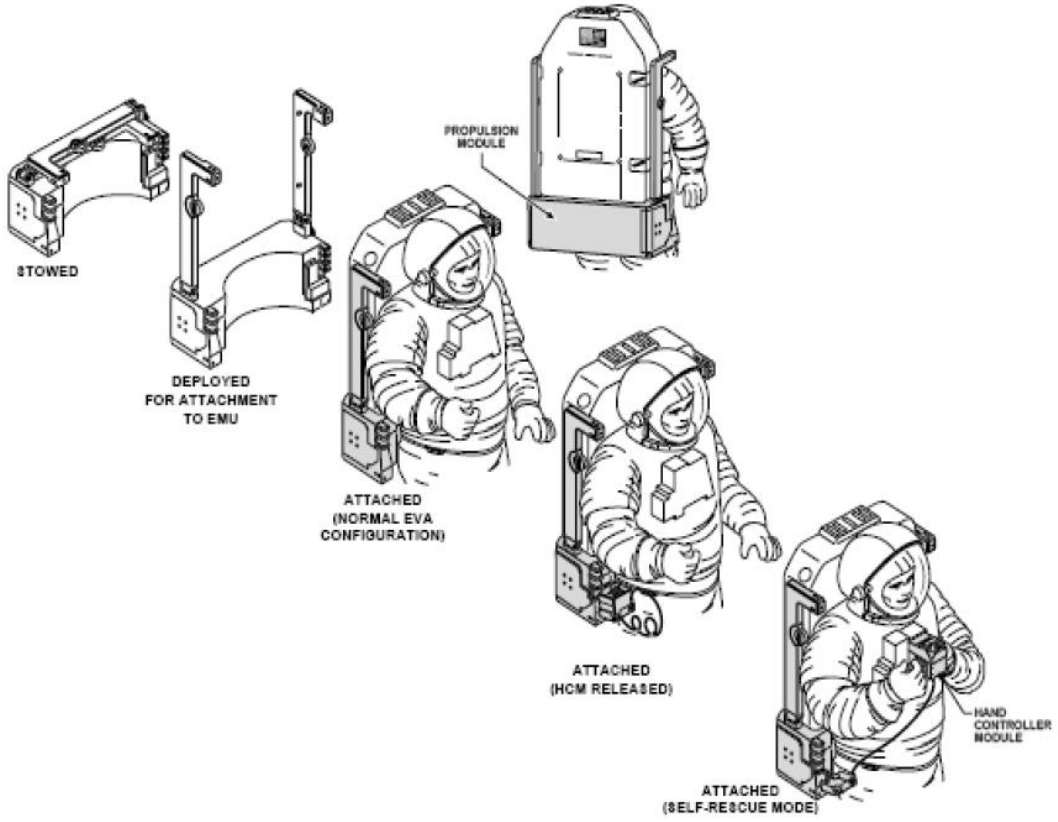
This paper will provide a walkthrough of the system problem domain, the need for the ISS SAFER, the architecture and methodology used to model the system and verification process, and draw conclusions on efficiency and lessons learned for subsequent projects. In summary, opportunities exist for selectively leveraging MBSE methods and tools to create a win-win scenario that meets project needs optimally.

Introduction -

ISS SAFER Project

The SAFER unit is a small, self-contained, free-flyer providing an EVA crewmember with adequate propellant and control capability for self-rescue maneuvering in the vicinity of the International Space Station structure. It fits around the Extravehicular Mobility Unit (EMU) life support system as shown in Figure 1 without limiting spacesuit mobility. It provides six degrees-of-freedom control through a single hand controller that can be held by the crewmember or attached with Velcro to the EMU Display and Control Module (DCM) cover. The total delta velocity capability will be the same as provided by the original USA SAFER units. The unit folds as shown in Figure 1 for storage during launch and landing and when not in use on orbit. The ISS SAFER and Test Module units will be stowed in foam-lined stowage bags located in a pressurized compartment during launch and landing. The ISS SAFER provides self-rescue capability, which can be used to provide the fault tolerance to inadvertent crew separation required by SSP 41000BU, Paragraph 3.3.6.1.1.1, catastrophic hazard: “The on-orbit Space Station shall be designed such that no two failures, or two operator errors, or one of each can result in a disabling or fatal personnel injury, or loss of one of the following: Orbiter or ISS,” and SSP 50021, Paragraph 3.2.1.3, Failure Tolerance: “The International Space Station shall be one fault tolerant to prevent loss of an EVA

crewmember due to inadvertent separation from the International Space Station.” History - USA SAFER overview



- ISS SAFER changes and goals

The International Space Station Simplified Aid for EVA Rescue (ISS SAFER) System is intended to replace the existing USA SAFER. Per JSC-37967, Project Management Plan for Simplified Aid For EVA Rescue (SAFER) and ISS SAFER Production Project, the ISS SAFER replacement is intended to leverage the existing USA SAFER design to the maximum extent possible while also providing a means to extend the on-orbit usable lifetime (which is limited to two years for the USA SAFER). This will be accomplished by providing an on-orbit test module to verify the ISS SAFER propulsion system at periodic intervals. Other changes to the ISS SAFER design will be limited to those driven by parts availability (including redesign of avionics and software and a redesigned tower hinge) and complying with ISS program compliance requirements. Specifically, JSC-37967 imposes the following program requirements on the ISS SAFER:

- SSP 50835, ISS Common Interface Requirements Document
- JSC-26626, Extravehicular Activity Generic Design Requirements Document (GDRD) (ISS SAFER only, as Test Module is an Intravehicular Activity (IVA) end item only)
- SSP 50021, ISS Safety Requirements, Appendix J
- JPR 8080.5, JSC Design and Procedural Standards

The ISS SAFER provides the means for a crewmember to return to the ISS in the event he/she becomes untethered during EVA operations. The system includes the capability of performing IVA on-obit maintenance and checkouts of the hardware, ground checks, and

ground maintenance. The system also includes upgrades of the Virtual Reality Lab (VRL) hardware and software which supports training crewmembers on the ground in preparation for flight.

- The ISS SAFER System consists of the ISS SAFER, Test Module, GSE, and MSE required to support crewmember on-orbit functions and ground maintenance and training (see Figure 3.1-1 ISS SAFER System Product Breakdown Structure).
- Initial SE Approach

2. MBSE implementation challenge – system level buy-in

1. The Challenge – Requirements Validation
    a. Problem statement – confluence of inputs creating a questionable requirements set
        i. SRR material
    b. Solution elements
        i. From first presentation, add process to the figures
2. The Opportunity – Model-Based verification planning and execution
    a. Initially used for engineering unit test planning
        i. From first presentation
    b. Generated AVP & QATP
        i.
3. Lessons Learned
    a. Stealth MBSE