Modeling in the State Flow Environment to Support Launch Vehicle Verification Testing For Mission and Fault Management Algorithms in the NASA Space Launch System[1]

Luis Trevino, Ph.D.[2],
Jacobs Technology
NASA Marshall Space Flight Center
Huntsville, Alabama 35812

Peter Berg[3]
NASA Ames Research Center
Moffett Field, CA 94035

Dwight England[4]
NASA Marshall Space Flight Center
Huntsville, Alabama 35812

Stephen B. Johnson, Ph.D.[5],
Dependable System Technologies, LLC, and
University of Colorado, Colorado Springs
Colorado Springs, Colorado

Analysis methods and testing processes are essential activities in the engineering development and verification of the National Aeronautics and Space Administration's (NASA) new Space Launch System (SLS). Central to mission success is reliable verification of the Mission and Fault Management (M&FM) algorithms for the SLS launch vehicle (LV) flight software. This is particularly difficult because M&FM algorithms integrate and operate LV subsystems, which consist of diverse forms of hardware and software themselves, with equally diverse integration from the engineering disciplines of LV subsystems. M&FM operation of SLS requires a changing mix of LV automation. During pre-launch the LV is primarily operated by the Kennedy Space Center (KSC) Ground Systems Development and Operations (GSDO) organization with some LV automation of time-critical functions, and much more autonomous LV operations during ascent that have crucial interactions with the Orion crew capsule, its astronauts, and with mission controllers at the Johnson Space Center. M&FM algorithms must perform all nominal mission commanding via the flight computer to control LV states from pre-launch through disposal and also address failure conditions by initiating autonomous or commanded aborts (crew capsule escape from the failing LV), redundancy management of failing subsystems and components, and safing actions to reduce or prevent threats to ground systems and crew. To address the criticality of the verification testing of these algorithms, the NASA M&FM team has utilized the State Flow environment[6] (SFE) with its existing Vehicle Management End-to-End Testbed (VMET) platform which also hosts vendor–supplied physics-based LV subsystem models. The human-derived M&FM algorithms are designed and vetted in Integrated Development Teams composed of design and development disciplines such as Systems Engineering, Flight Software (FSW), Safety and Mission Assurance (S&MA) and major subsystems and vehicle elements such as Main Propulsion Systems (MPS), boosters, avionics, Guidance, Navigation, and Control (GN&C), Thrust Vector Control (TVC), liquid engines, and the astronaut crew office. Since the algorithms are realized using model-based engineering (MBE) methods from a hybrid of the Unified Modeling Language (UML) and Systems Modeling Language (SysML), SFE methods are a natural fit to provide an in depth analysis of the interactive behavior of these algorithms with the SLS LV subsystem models. For this, the M&FM algorithms and the SLS LV subsystem models are modeled using constructs provided by Matlab which also enables modeling of the accompanying

---

[1] SPACE 2016, AIAA Space and Astronautics Forum

[2] Integrated Systems Health Management and Automation Branch (ISHM), Spacecraft and Vehicle Systems Department, EV43

[3] M&FM State Analysis Lead, Stinger Ghaffarian Technologies

[4] Chief, ISHM, Spacecraft and Vehicle Systems Department, EV43

[5] Analysis Lead, ISHM, Spacecraft and Vehicle Systems Department, EV43

[6] Part of the suite of tools with Simulink by the MathWorks Inc., an American corporation specializing in mathematical computing software

interfaces providing greater flexibility for integrated testing and analysis, which helps forecast expected behavior in forward VMET integrated testing activities.

In VMET, the M&FM algorithms are prototyped and implemented using the same C^{++} programming language and similar state machine architectural concepts used by the FSW group. Due to the interactive complexity of the algorithms, VMET testing thus far has verified all the individual M&FM subsystem algorithms with select subsystem vendor models but is steadily progressing to assessing the interactive behavior of these algorithms with LV subsystems, as represented by subsystem models. The novel SFE applications has proven to be useful for quick look analysis into early integrated system behavior and assessment of the M&FM algorithms with the modeled LV subsystems. This early MBE analysis generates vital insight into the integrated system behaviors, algorithm sensitivities, design issues, and has aided in the debugging of the M&FM algorithms well before full testing can begin in more expensive, higher fidelity but more arduous environments such as VMET, FSW testing, and the Systems Integration Lab[7] (SIL). SFE has exhibited both expected and unexpected behaviors in nominal and off nominal test cases prior to full VMET testing. In many findings, these behavioral characteristics were used to correct the M&FM algorithms, enable better test coverage, and develop more effective test cases for each of the LV subsystems. This has improved the fidelity of testing and planning for the next generation of M&FM algorithms as the SLS program evolves from non-crewed to crewed flight, impacting subsystem configurations and the M&FM algorithms that control them. SFE analysis has improved robustness and reliability of the M&FM algorithms by revealing implementation errors and documentation inconsistencies. It is also improving planning efficiency for future VMET testing of the M&FM algorithms hosted in the LV flight computers, further reducing risk for the SLS launch infrastructure, the SLS LV, and most importantly the crew.

[7] Hardware in the loop facility hosting FSW and M&FM algorithms