A Vehicle Management End-to-End Testing and Analysis Platform for Validation of Mission and Fault Management Algorithms to Reduce Risk for NASA's Space Launch System

Luis Trevino, Ph.D.[1],
Jacobs ESSSA Group
NASA Marshall Space Flight Center
Huntsville, Alabama 35812

Stephen B. Johnson, Ph.D.[2],
Dependable System Technologies, LLC,
University of Colorado, Colorado Springs
Jacobs ESSSA Group
Colorado Springs, Colorado

Jonathan Patterson[3]
NASA Marshall Space Flight Center
Huntsville, Alabama 35812

David Teare[4]
NASA Marshall Space Flight Center
Huntsville, Alabama 35812

The development of the Space Launch System (SLS) launch vehicle requires cross discipline teams with extensive knowledge of launch vehicle subsystems, information theory, and autonomous algorithms dealing with all operations from pre-launch through on orbit operations. The characteristics of these systems must be matched with the autonomous algorithm monitoring and mitigation capabilities for accurate control and response to abnormal conditions throughout all vehicle mission flight phases, including precipitating safing actions and crew aborts. This presents a large complex systems engineering challenge being addressed in part by focusing on the specific subsystems handling of off-nominal mission and fault tolerance. Using traditional model based system and software engineering design principles from the Unified Modeling Language (UML), the Mission and Fault Management (M&FM) algorithms are crafted and vetted in specialized Integrated Development Teams composed of multiple development disciplines. NASA also has formed an M&FM team for addressing fault management early in the development lifecycle. This team has developed a dedicated Vehicle Management End-to-end Testbed (VMET) that integrates specific M&FM algorithms, specialized nominal and off-nominal test cases, and vendor-supplied physics-based launch vehicle subsystem models. The flexibility of VMET enables thorough testing of the M&FM algorithms by providing configurable suites of both nominal and off-nominal test cases to validate the algorithms utilizing actual subsystem models. The intent is to validate the algorithms and substantiate them with performance baselines for each of the vehicle subsystems in an independent platform exterior to flight software test processes.

In any software development process there is inherent risk in the interpretation and implementation of concepts into software through requirements and test processes. Risk reduction is addressed by working with other organizations such as S&MA, Structures and Environments, GNC, Orion, the Crew Office, Flight Operations, and Ground Operations by assessing performance of the M&FM algorithms in terms of their ability to reduce Loss of Mission and Loss of Crew probabilities. In addition, through state machine and diagnostic modeling, analysis efforts investigate a broader suite of failure effects and detection and responses that can be tested in VMET and confirm that responses do not create additional risks or cause undesired states through interactive dynamic effects with other

[1] Integrated Systems Health Management and Automation Branch (ISHM), Spacecraft and Vehicle Systems Department, EV43
[2] Analysis Lead, ISHM, Spacecraft and Vehicle Systems Department, EV43, Jacobs ESSSA Group
[3] M&FM Lead, ISHM, Spacecraft and Vehicle Systems Department, EV43
[4] M&FM VMET Lead, ISHM, Spacecraft and Vehicle Systems Department, EV43

algorithms and systems. VMET further contributes to risk reduction by prototyping and exercising the M&FM algorithms early in their implementation and without any inherent hindrances such as meeting FSW processor scheduling constraints due to their target platform - ARINC 653 partitioned OS, resource limitations, and other factors related to integration with other subsystems not directly involved with M&FM. The plan for VMET encompasses testing the original M&FM algorithms coded in the same C++ language and state machine architectural concepts as that used by Flight Software. This enables the development of performance standards and test cases to characterize the M&FM algorithms and sets a benchmark from which to measure the effectiveness of M&FM algorithms performance in the FSW development and test processes.

This paper is outlined in a systematic fashion analogous to a lifecycle process flow for engineering development of algorithms into software and testing. Section I describes the NASA SLS M&FM context, presenting the current infrastructure, leading principles, methods, and participants. Section II defines the testing philosophy of the M&FM algorithms as related to VMET followed by section III, which presents the modeling methods of the algorithms to be tested and validated in VMET. Its details are then further presented in section IV followed by Section V presenting integration, test status, and state analysis. Finally, section VI addresses the summary and forward directions followed by the appendices presenting relevant information on terminology and documentation.

I. The NASA SLS Mission and Fault Management Context

NASA has a traditional history of applying M&FM strategies on spacecraft and LV(S) and keeping pace with the technology trends over the decades [1]. With the plan for NASA to progress to deeper depths of human space exploration, the need for accommodating FM systems is ever-more warranted for next generation space transportation systems. Over time, NASA's applications have become increasingly capable and complex, which in turn will require more sophisticated FM systems to guarantee mission success without the expense of loss of life and resources. With LV(s) evolving to meet greater demands in launch and payload capabilities and maximizing mission success, M&FM principles have also progressed, such as reliable methods for incorporating LV situational awareness of its subsystems and handling of off-nominal mission and fault tolerance with fail-safe response management. Launch vehicles are inherently hazardous due to their highly dynamic components with thousands of gallons of combustible and cryogenic liquids. The science behind rocketry has improved the design, production, and operations with launch success well beyond that encountered during the fourth quarter of the last century, largely due to the technologies of sensing and engine advancements [1]. Situational awareness now includes improved caution and warning (C&W) indicators and related information processing for crew and ground systems displays [1].

The latest strategies for the SLS program (SLSP) are no exception and like its predecessor capabilities, the M&FM team at the Marshall Space Flight Center (MSFC) has become a core systems engineering beacon for ensuring all possible LV failures are quantified, identified, qualified, and classified with the most reliable or trusted detection and mitigation development and implementation strategies. For this, a full systems engineering analysis must be thoroughly performed in order to develop the testing infrastructure(s) to validate the M&FM methods. Since the Apollo era, NASA has nurtured a variety of institutions for a variety of testing, and verification and validation (V&V) for its mission critical flight systems. Many of these organizations focus on meeting mission-critical objectives. M&FM is no exception, as it is heavily focused on the analysis and development of M&FM algorithms and the V&V methods required for them. The VMET represents a focused systems engineering capability that helps to instill candidate M&FM principles early in the software lifecycle for the SLSP.

The M&FM philosophy for the SLSP is to implement a distributed detection concept in the FSW architecture for monitoring the health and status of the LV subsystems, with accompanying response methods commensurate with the level of severity of detected anomalous events. Such M&FM strategies embedded across the FSW subsystems are realized by the target platform which is the ARINC 653 partitioned operating system (OS) [2]. Conceptually this is represented by a subsystem manager (SSM) for each of the LV subsystems where each of the SSM monitoring and response algorithms are coded in their own respective OS partition, e.g., the MPS, TVC, and GNC. The ARINC 653 OS in itself adds a layer of protection against SSMs corrupting other SSMs due to any single event upset, undiscovered latent errors, or possibly any related hardware failure(s) in the computing platform or associated with a suspect SSM. Implementation details are presented in the FSW development plan, which is not available to the public and out of scope for this paper. The SSMs also include engine systems, boosters, avionics, and system management (SM), FM, electrical power systems (EPS), and sensor data qualification (SDQC). The M&FM algorithms address flight termination logic, event management, C&W, aborts processing, redundancy management (RM), and safing. Examples of safing responses include changing the state of the MPS valves for a

safe engine shutdown and preventing an uncontained engine explosion, initiating crew abort operations, or enabling or inhibiting commands from ground or the multi-purpose crew vehicle (MPCV).

Supporting the design and development of the M&FM algorithms is a wealth of analysis in order to adequately characterize the detection trigger thresholds for the SLSP-approved monitored conditions, their benefits and costs, categorizing C&W and aborts, and response analysis to detect early failure effects with adequate time to protect the crew and assets so as to avoid a catastrophic failure [3]. The M&FM analysis team was primarily responsible for this and helped define parameters used by the response algorithms, such as for redundancy and safing action algorithms for all flight modes including prelaunch. For SLS the analysis dictates that a probability threshold of 1 in 100,000 is adequate as a basis for judgment of the need for abort algorithms, but this parametric value could be altered based on a probabilistic risk assessment (PRA) as the SLSP further matures [4]. Central to this analysis is the assessment of the probability of false positives (FP) and false negatives (FN) for each SSM, respectively meaning a failure indication when there is no actual failure, and missing the detection of an actual failure [4]. Much of this early analysis is captured in the arsenal of M&FM documents covering all aspects required to justify the thresholds guiding the M&FM algorithms. A sampling of these documents are listed in Appendix A. These documents address a wide variety of SLSP topics such as program level vehicle management, FM plan, PRA, failure modes and effects analysis (FMEA), safety and hazard analyses, and design analysis, for example. The cross discipline teams working closely with the M&FM team represent the Integrated Design Team[5] (IDT) and includes representatives from Safety and Mission Assurance (S&MA), FSW, Ground Operations, crew office, Spacecraft and Payload Integration Office (SPIO), and the vehicle elements such as booster and engines [4], partially exemplified in Fig. 1. The next phase of algorithm design entails activities by the core modeling team (CMT) represented by members of the M&FM and FSW groups. Other mechanisms used by M&FM in its algorithm early analysis and planning is a suite of tools such as state analysis using Matlab Stateflow, a Goal Tree/Success Tree (GT/ST) developed using SysML, and an Integrated Vehicle Failure Model (IVFM) which provides the ability to trace to failure modes to specific sensors to detect and assess overall effectiveness for accurate detection and isolation of failures using the Testability Engineering And Maintenance System (TEAMS) tool, a PRA Fault Tree, and an Integrated Hazards Analysis [4, 5]. More details of M&FM analysis is summarized in Appendix A.

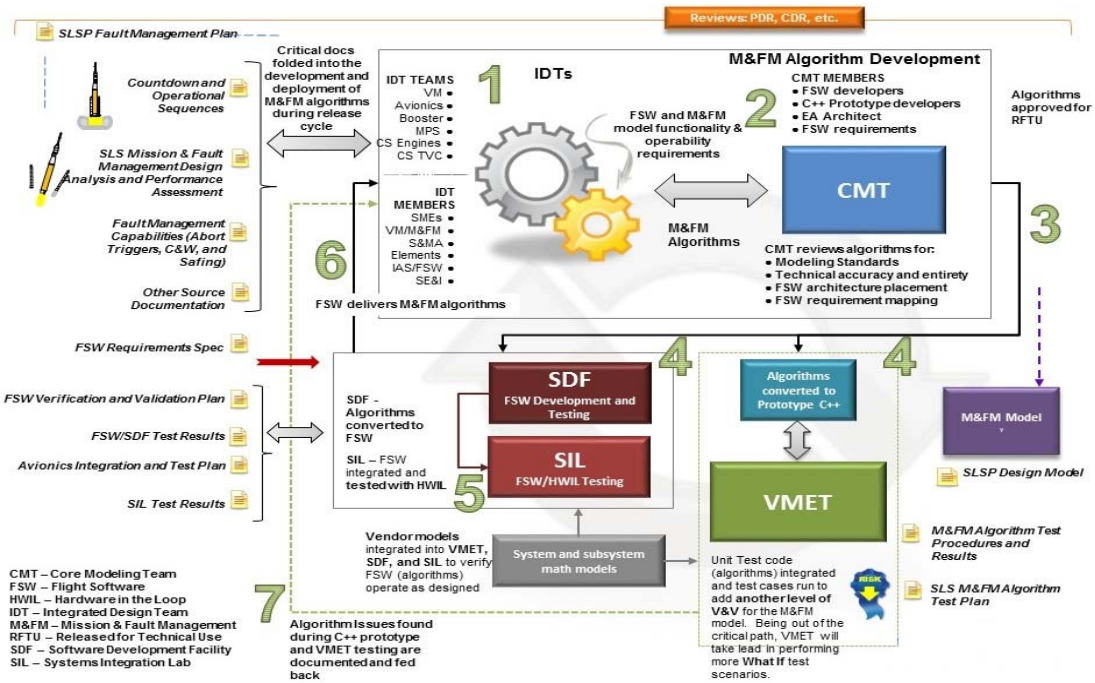


Figure 1. M&FM Algorithm Design, Development, and Testing Process [10]

[5] Created for Vehicle Management, Avionics, Booster, Liquid Engines, MPS, CS TVC, and Engine Green Run Testing

The M&FM process for algorithm development within the SLSP is depicted by Fig. 1 above and is indicative of efforts by numerous organizations across NASA leveraging from prior programs such as Shuttle and Ares, including concepts derived from health management efforts from industry and academia specific to subsystems such as engine health management initiatives including integrated systems health management (ISHM) concepts for LVs. The central theme from Fig. 1 is that there is a dedicated organization responsible for initiating and managing the M&FM concepts to be integrated early in the flight software design lifecycle and not distributed across multiple organizations. This minimizes the probabilities for gaps in human interpretation and implementation of early conceptual requirements which could get skewed or misinterpreted, causing costly remedies or failures later in the SLS development life cycle. Each specific LV SSM and its development is guided by the respective IDT which is led by an M&FM representative and a FSW co-lead. This in itself is a culture-changing initiative for the SLSP regarding M&FM which spans the spectrum of concurrent engineering across disciplines from early concept and analysis through implementation and certification testing. The M&FM team resides within the Spacecraft and Vehicles Systems Department where Vehicle Management (VM) is central to the overall design integrity of the SLS LV. This further contributes to a dedicated integrated team to help navigate the overall vehicle subsystem design and development. VM also encompasses the vital discipline of GNC working flight mechanics identifying, assessing, and designing many of the flight envelopes and capabilities that drive GNC-related M&FM abort and trigger thresholds (e.g., rate and attitude violations) [4]. Other groups from the Ames Research Center (ARC) and the Glenn Research Center (GRC) actively participate with the M&FM analysis team helping coordinate activates across the aerospace community working with the SLSP. Other groups working within the SLSP on M&FM-related activities include other NASA centers, most prominently the Johnson Space Center (JSC) and the Kennedy Space Center (KSC). From Fig. 1, VMET serves a crucial role in validating the M&FM algorithms.

II. Testing Philosophy of the M&FM Algorithms

The principal task of the VMET is to provide a platform for qualitative fidelity testing of the M&FM algorithms with goals to reduce risk of any latent problems in their integration for trusted implementation in the SLS FC. Fig. 1 illustrates the overall process depicting the flow of activities from conceptual design represented by the documents from generated analysis through activities of the IDT and CMT, through algorithm, prototype, and FSW development and all testing activities. Exterior to M&FM, algorithms are transformed into flight software and processed through formal SLSP testing via activities in the Software Development Facility (SDF) and the Systems Integration Lab (SIL) with hardware in the loop testing. M&FM is actively involved in supporting those exterior V&V processes for the M&FM-derived code. In each of those processes any latent complexities for each SSM is inherently exploited beginning with unit testing of the individual SSM software, both in the M&FM prototype code and FSW as embedded code for the target platform in the SDF. For M&FM unit testing, this entails verifying that code execution exhibits expected behavior as the algorithm developers intended, based on activities of the IDT and CMT. Once unit testing has progressed through all nominal and off nominal scenarios as guided by the M&FM Model (see below, Section IV), the coded algorithm representing a specific SSM then transitions into the VMET environment where it begins the integration process in preparation for exercising it with the VMET models and other LV SSMs. System complexity arises from the integration of all the SSMs with the physics-based vendor models integrated within VMET.

In the global scheme, each of the testing processes from M&FM and FSW-SDF unit testing to SIL testing represents the V&V process for the M&FM algorithms for the SLSP, including the early analysis processes. It is important to emphasize that the early analytical processes performed by the M&FM analysis team also establishes the foundational elements to evaluate the stability and performance of system functions, robustness to abnormal conditions, and reliability under software errors, SSM faults, hardware failures, and impacts to the LV assets and crew [6]. An important aspect of this activity entails system state analysis where a broader suite of failure effects, detection, and responses can be explored and compared to VMET testing where the goal is to solidify those early foundational design decisions of the M&FM algorithms. VMET's aims are to ensure that failures can reliably be detected and validate that the expected responses do not create additional risks or cause unwanted states through interactive dynamics with the other LV SSMs, collectively represented by the physics-based models and prototyped SSMs. Supporting this is the testability analysis performed by the analysis team where the IVFM is used to analyze abort conditions and triggers, C&W conditions, Redundancy Management (RM) conditions, and early assessment of Launch Commit Criteria (LCC). For each identified failure condition, the IVFM is used to perform a testability analysis. This includes a list of all failure modes detected by the identified failure conditions and any related detection metrics. The traceability of failure modes to abort triggers and abort conditions is documented in the

M&FM Monitored Condition Report (MCR) [3, 4]. The testability analysis verifies that failure modes are properly categorized (e.g., Crit 1, Crit 1R, Appendix A). Failure modes not detected by a particular abort trigger are also determined by the testability analysis. For conditions identified in the PRA and the System Safety (hazard) Cause Tree, the IVFM provides automatic generation of failure trees that are used to support the PRA and hazard trees to determine proper coverage and help identify any potential gaps and severity.

The risk in the interpretations and implementation of the M&FM concepts is unlike those in other software applications due to the nature of the application domain of providing FM for human-rated systems. The principal intent of VMET is to minimize this risk to the degree possible with the underlying goal that no latent errors in the M&FM algorithms will be manifested during the formal FSW test and certification phases. Any gaps in human reasoning and understanding of the M&FM algorithms need to be exposed in VMET to avoid the possibility of becoming latent SLSP problems in FSW and hardware-in-the-loop testing processes. Failures detected in later testing costs significantly more to fix and causes more significant schedule issues. In this context, system validation is a confirmation that the M&FM algorithms are performing their intended functions under all planned flight phases, expected off nominal LV states, and including ground operations and safing modes. Many of the focused objectives throughout testing include the effectiveness of the impact of false alarms (detection false positives), missed detections (detection false negatives), correct/incorrect identifications (fault isolation/identification false positives and false negatives), correct/incorrect decisions, failure/damage coverage and propagation effects, achievable dynamics under vehicle constraints and time delay effects [6]. Vehicle constraints may stem from degraded operational modes due to failures and time delay effects which may originate from reliable detection, isolation, identification, reporting, and mitigation response. Addressing these risks is the intent of the activities within the M&FM group where VMET will significantly contribute to its reduction.

III. Modeling

The task of interpreting M&FM concepts derived from the IDT and CMT activities is eased by the utility of the Unified Modeling Language (UML), a proven software design suite of modeling methods. UML has traditionally been used for software design but recently has been extended into systems engineering modeling through SysML, which derives from UML. The M&FM group has incorporated a hybrid modeling suite of SysML methods developed by the FSW group using the Sparx Systems Enterprise Architect (EA) product [7]. Using capabilities within EA, the FSW group has developed a modeling standard called the SLS Team Ontology Modeling Profile (STOMP) which defines a common set of concepts for modeling the characteristic behaviors and software structures for control of the SLS LV. The STOMP provides a set of elements, relationships, and diagrams for development of the M&FM and FSW models tailored for the SLSP. The STOMP methodology is based on the Modeling Driven Generation (MDG) Technologies capability within the EA tool. This modeling protocol is based on the SLSP Modeling and Simulation Standard (SLS-STD-038).

Figure 2 below exemplifies a modeling product using the EA and STOMP standard, which is a portion of the M&FM Model, which contains all M&FM-defined algorithms. Shown below is a UML activity diagram illustrating the fault monitoring logic for some generic off nominal pressure monitoring system for a LV subsystem such as MPS. Using simple descriptive language, the diagram is very similar to flow charts from the software engineering realm. The color coding scheme depicts a unique set of colors for SLS actions (depicted by <<sls_actions>>), SLS activities (depicted by <<sls_activity>>), and so forth for SLS events, data, and parametric data. Decision nodes are represented by a green diamond box and initial and termination nodes are represented by circular color coded symbols, (i.e., ActivityInitial, FlowFinal, and ActivityFinal). This example represents a

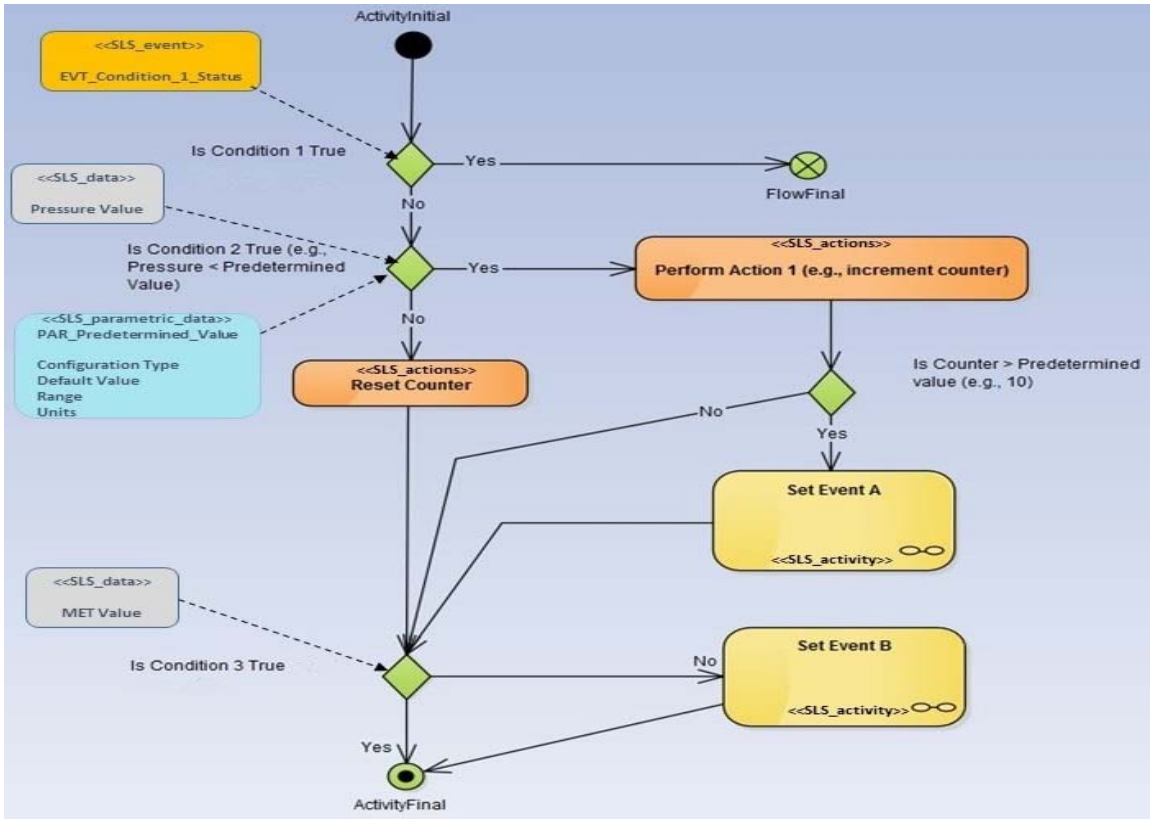


Figure 2 Sample UML Activity Diagram

graphical depiction of the sequence of subsystem checks to determine the state of the downstream pressure of a component such as a gaseous helium (GHe) valve with corresponding action if off nominal or less than a predetermined pressure limit. The top level green decision symbol determines the state of Condition_1 (e.g., LV not in flight mode meaning still in prelaunch or autonomous launch sequence operations) and if true, terminates executing the rest of the logic. If the LV is in flight mode the algorithm then checks if the downstream pressure is less than a hard predetermined value parameter, i.e., PAR_Predetermined_Value in the second green decision diamond from the top. If true or [Yes], the logic to the right of that decision diamond then uses a counter to accumulate limit violations, i.e., "Perform Action 1" <<SLS_actions>>. Then the mid-right green decision diamond (beneath that <<SLS_actions>> element) checks if the counter is greater than a "Predetermined value" such as computer processing cycles (meaning ten occurrences of the violation), the "Set Event A" activity is performed, i.e., an <<sls_activity>>. Such an event could be a posting of a caution and warning to the crew or used internally within the FC to trigger other logic in another subsystem(s) such as in the Fault Manager SSM to keep track of health and status of the critical valve downstream pressures. In this case the logic for setting such an event is depicted in another lower level activity diagram as depicted by the eyeglass or infinity symbol in the lower right corner of the yellow box for "Set Event A" which could be viewed as a function call in software code, for example. In similar fashion the lowest green decision diamond checks for Condition 3 such as if MET is less than a 100 (seconds). If true or "Yes" then no further action is taken and if false or "No" then another set of actions is engaged via the lower right yellow SLS activity box with the eyeglass symbol. Notice that there is no counter (<<sls_action>>) as there was in the upper decision diamond. This type of design detail is determined by the IDT and CMT working groups.

Although these UML-based models are based on extensive analysis and vetting in the IDT and CMT forums, it is empirically known they are always incomplete in that they have unknown failure modes, which are documented using traditional flight software metrics [8]. Furthermore, any component behavior that is inconsistent with all known nominal and failure modes is consistent with the unknown failure mode [9]. By modeling to the level of detail required to make relevant distinctions in detection and possible diagnosis of a fault, provides an avenue to discover unknown/unforeseen failure modes in extensive analysis and extensive off nominal testing in all feasible test domains, leading to the topic of the next section.

IV. Vehicle Management End-to-End Testbed - VMET

The M&FM team is composed of several sub-teams, with a mission to develop and validate methods to detect and respond to abnormal conditions on the SLS LV in order to protect its crew and environment. The principle end product of the M&FM team is the SLS M&FM Model, a portion of which is portrayed by the MPS SSM of Fig. 2. Although the M&FM products are part of the critical path where the FSW group is the customer, the process shown in Fig. 1 illustrates that the testing path of the M&FM algorithms within the VMET environment are not directly part of the critical path. However, they are indirectly critical, insofar as these internal M&FM algorithm tests discover any algorithm design flaws in VMET testing. Furthermore, critical path testing in FSW and the SIL may encounter M&FM algorithm-specific problems that may warrant VMET investigative test and analysis. VMET provides the capability to explore a deeper fidelity of nominal and off nominal testing scenarios. The process for transition of the M&FM algorithms to the VMET environment is depicted further in Fig. 3 below.

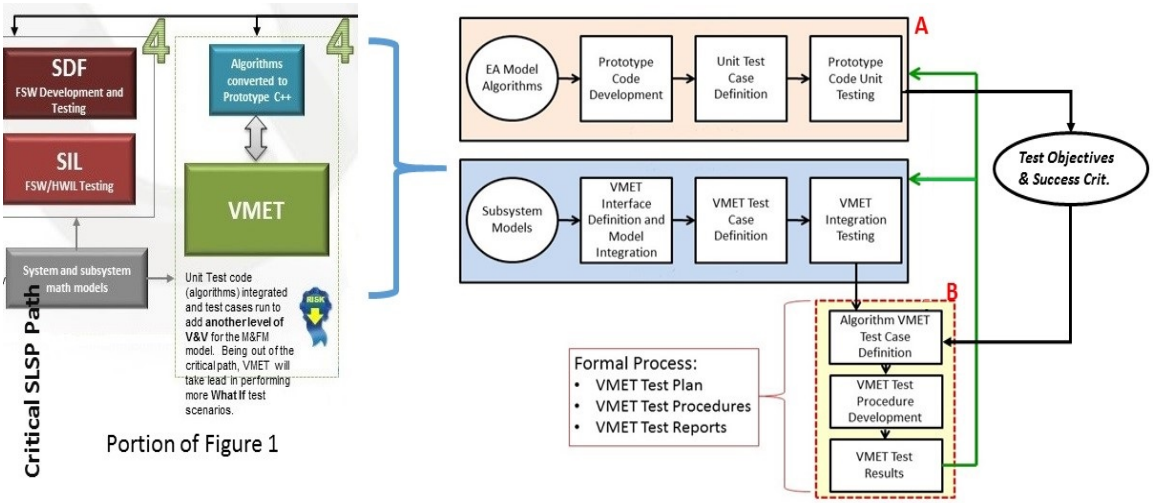


Figure 3. VMET Testing Process

The M&FM-developed prototype code implementing the UML-SysML based models is process-tested in two phases highlighted as A and B in Fig. 3 above. For Phase A, the prototype developers use the M&FM Model algorithms in EA with the developed prototype code to develop unit test cases and perform them exterior to the VMET environment. Once the prototype code is fully unit tested, the process continues into development of the Test Objectives and Success criteria for input to the VMET test team which is the entry point for Phase B. Using the MPS subsystem of Fig. 2 as a guide, a sample test objective and success criteria entails the following:

Sample Test Objective: Verify Down Stream Pressure of Ghe valve being less than Ghe regulated pressure for persistence less than 30 computing cycles does not set an event for any of the engines.

Sample Success Criteria: No events set for any engine.

In actuality this test objective would be more detailed for more test coverage of the code with more conditions to check in the success criteria (e.g., ensure no reporting that the floor pressure was breached). After the process of transitioning the Test Objectives and Success Criteria to the VMET test team, the VMET test procedures are generated and the process is begun of verifying that the prototype code can be successfully compiled and executed in the VMET environment before full integration with the overall VMET models and other SSM models residing within VMET. Initially, the unit testing performed by the prototype team is replicated by the VMET testers in the VMET environment using the FC model as a precursor validation step prior to full VMET testing as abstractly depicted in Fig. 3. In summary the prototype and VMET teams go through each of their respective processes prior to integration of the prototype code in the VMET environment to further ensure the M&FM algorithms go through their due process of unit test, test case generation, and verification. Depending on any discovered problems in the VMET Formal Process, they are reported back to the prototype or VMET developers for resolution. Note that this FC model is a subset of the Subsystem Models in Fig. 3. Details of the FC model is beyond the scope of this paper but it is important to note that it is modeled in similar fashion as that used in the FSW group.

The plan for phase B of the prototype testing then progresses into full VMET testing with all the required Subsystem models. The VMET team uses the Test Objectives and Success Criteria generated for each SSM to develop the test procedures specific to the VMET environment incorporating the relevant physics-based models for that specific SSM. The VMET test cases go into fuller detail describing "how" the test objectives shall be accomplished with specifics on timing and flight phases. It will also describe the associated commands and data being generated and which of the other subsystem models will be involved during all modes of the test from prelaunch through end of mission. The success criteria for each test case will describe in detail which data files needs to be reviewed, plotted, and analyzed. A good example of a VMET test case and analysis is shown in Appendix B. It's vital to note that the infrastructure for VMET is unlike that used by the FSW in the SDF and the SIL, whose details are beyond the scope of this paper. The VMET environment has implemented the necessary soft instrumentation and interfaces to be able to probe and validate the performance margins of the M&FM algorithms. It includes computing resources capable of simulating a distributed system with integrated full physics based models exhibiting the vehicle and subsystem dynamics. Although the FSW and M&FM VMET teams have their own approaches for implementing, processing, and testing the M&FM algorithms with specific SLSP objectives, they do work together through the IDT and CMT and share information such as testing status and especially any algorithm issues. Central to the VMET environment are the physics-based models provided by vendors and other participating organizations across NASA and industry. Furthermore, some of the resources utilized by the SIL are shared with the VMET team, notably the ARTEMIS (A Real-Time Environment for Modeling, Integration, and Simulation) and models developed within it such as the MPS and Core Stage Engine subsystems. This platform hosts a suite of models, simulations, and hardware interfaces used for simulating the SLS avionics hardware and software and is part of the SLS System integration Lab. Implementing these models within VMET is non-trivial due to the software interface constructs of ARTEMIS which needs to be manually removed or modified in the provided model code.

The vendor models, including the ARTEMIS models, are modified for usage in VMET, a non-trivial task with significant resources spent on adaptation, implementation, and testing [4]. Another important model implemented in VMET is the six degree of freedom (DOF) flight vehicle model[6] developed by the GNC group also within the Spacecraft and Vehicle Systems Department. As part of vendor model integration in VMET, Fig. 4 below depicts a sampling of the required understanding of the interfaces for these contractor-developed models, M&FM models, and those developed within the VMET team for methodical integration, depicted by the color coded elements in the Legend of Fig. 4. For this example the MPS is depicted with the subsystems of the PDCU and CCSE (Power Distribution Control Unit and Combined Control System Electronics) where the FC was presented earlier and VDM is the valve driver module. The specific details such as sub-address meanings is beyond scope and is proprietary to the vendors. The intent is to illustrate a sampling of the level of integration complexity undertaken by the VMET team for all the M&FM subsystem vendor models. All vendor models within the VMET infrastructure are hosted in the VMET Lab UNIX Servers within NASA secure firewalls.

[6] MAVERIC – Marshall Aerospace Vehicle Representation in C: 3 DOF & 6 DOF flight vehicle physics-based model

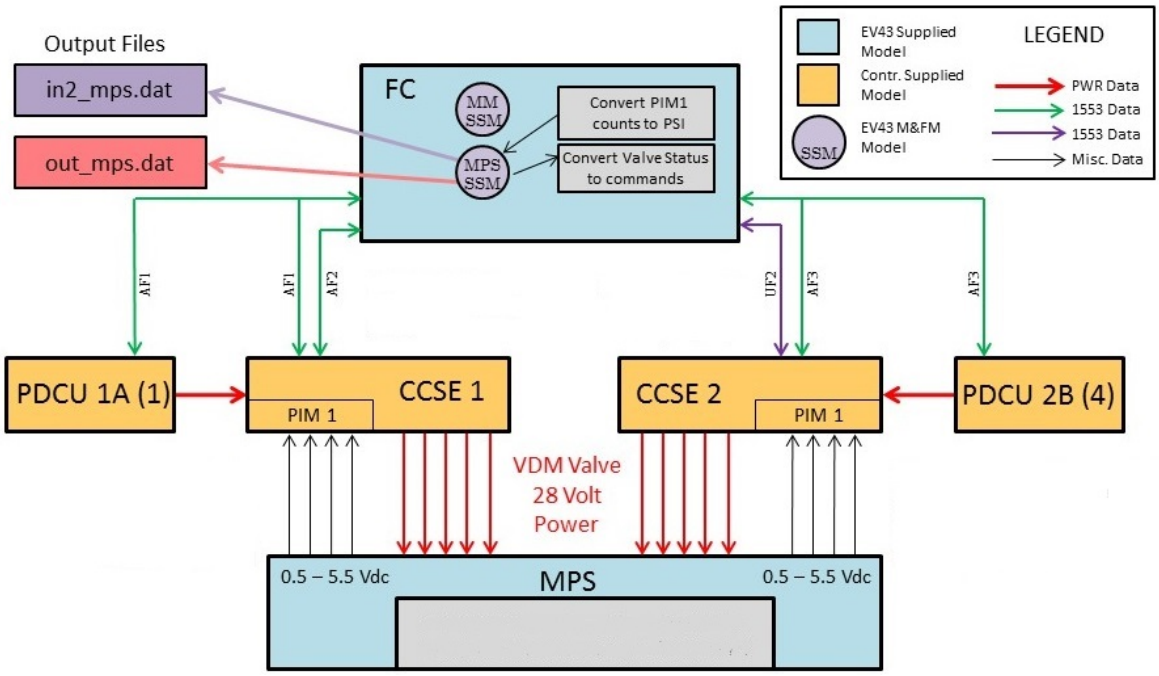


Figure 4. Sample View of Model Integration in VMET

To date there are approximately 408 M&FM algorithms. The integrated MFM Algorithms and vendor subsystem models communicate with an interface containing more than 10K variables/states. The current count of software lines of code (SLOC) within VMET is currently over 1 million, represented by Fig. 5 below. The number of test cases represented within the M&FM realm now stands at 668. These figures are preliminary and will increase as the SLSP progresses. As testing continues, the M&FM teams are discovering tools and methods for automation and simplicity, such as developing Python test scripts for each of the SSMs, are now becoming useful for regression testing and quick assessment of model changes and impacts to the M&FM prototype code.

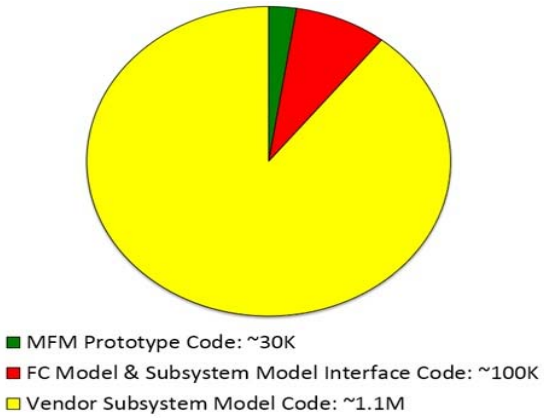


Figure 5. Software Lines of Code within the VMET Infrastructure [10]

V. Integration, Test Status, and State Analysis

The M&FM teams are continually maintaining updates to the M&FM algorithms based on recurring working meetings of the IDTs for each of the SSMs. To control this evolving process and manage each of the development phases, the M&FM and FSW teams have utilized a Release and Sprint Cycle as part of its scheduling process, each phase with its own unique sequential numbering system with a release and sprint cycle numeric indicator. At the time of the writing of this paper the results in Fig. 6 below are depicted by Release 10 Sprint 3. For Green Run Testing which is testing the Core Stage Engines (CSE) at the NASA Stennis Space Center with the M&FM algorithms residing in the FC which itself will reside in the SLS Vehicle on the test stand, the plan is to utilize Release 12 Sprint 1 (May 2015) for Green Run and Release 13 Sprint 1 (November 2015) for the first SLS flight. In Fig. 6 the status of each of the products and SSMs is represented by their respective column and row headings. The green cells indicate activity complete while the single orange cell indicates product activity for that SSM is in work. The single blue cell indicates forward work for off nominal testing, only nominal testing has been performed for that product activity. The non-colored cells indicate no activity yet performed. To date only the System Management and Electrical Power System M&FM models have been fully integrated and tested in VMET with supporting documentation. Sample test analysis documentation is shown in Appendix B.

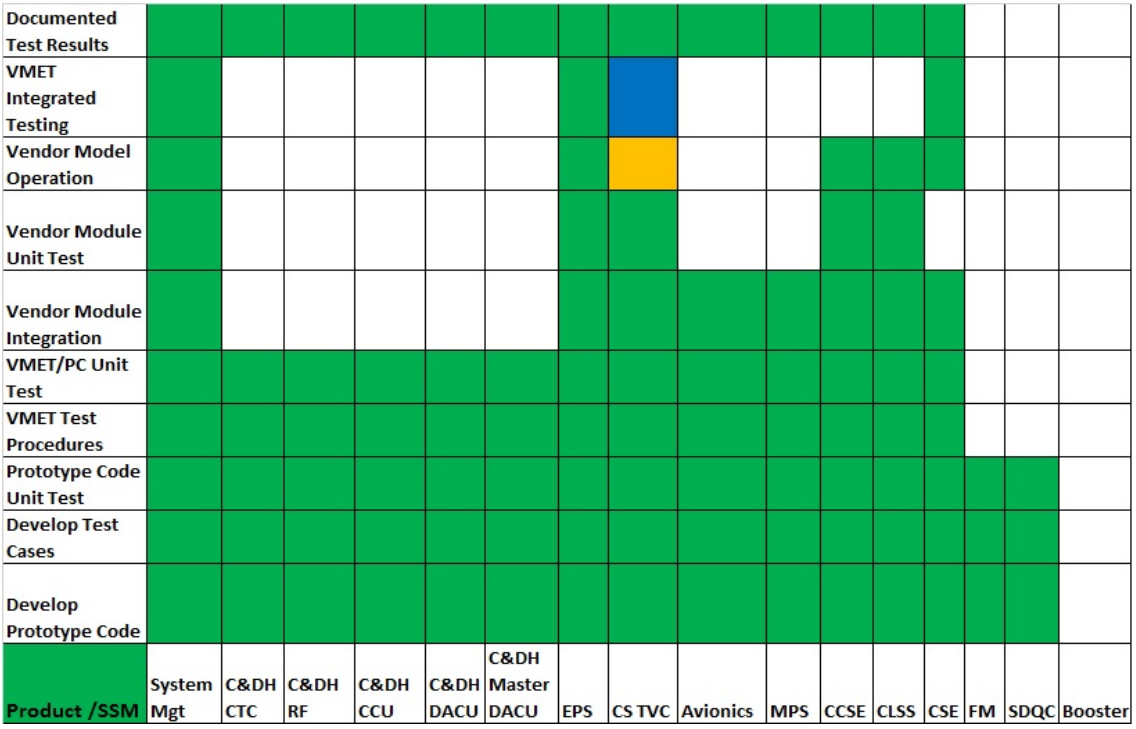


Figure 6. State of M&FM VMET Products and Testing, Release 10 Sprint 3 [10]

Much of the integration in VMET to date has been heavily focused on resolving basic technical problems in integration of the prototype code within the VMET infrastructure and interfaces. For example, initialization conditions and compile problems had to be resolved between the Prototype and VMET teams. Other instances include resolving timing and event reporting issues, and occasionally resolved with the assistance of the M&FM algorithm developers, i.e., the SSM subject matter experts. An actual example stems from integration of the MPS SSM and verifying the proper operation and timing of the propellant prevalve openings and closings during select flight modes, such as during nominal or off nominal engine shutdown of the four SLS LV engines, represented by the CSE models. Although the intent is to eventually test all the M&FM SSM models in the full integrated environment provided by VMET, such integration problems are being overcome in incremental fashion with goals leading to a stable robust test platform. The forward plan for integrated testing will first focus on nominal and then off nominal testing to ensure the M&FM algorithms respond as planned and potentially uncover any latent or VMET technical implementation issues. Current VMET test procedures are intended to guide this and will provide a

baseline from which to leverage forward testing options for unique extreme off nominal scenarios. Such examples include response due to loss of communications due to stale data on the AF, UF, or EF 1553 buses at different points in time throughout the mission flight phases (see Fig. 4) [5]. Other cases will focus on loss of power for certain flight components such as observing system behavior with loss of battery units, loss of CCSE functionality with RM response, valve response times in the presence of off nominal conditions, and CSE shutdown conditions, for example.

In support of VMET testing, extensive analysis is being performed by the VMET team such as that shown in Fig. B.1 (Appendix B) exhibiting prevalve command response. Analysis also includes the state analysis work being performed at the Ames Research Center (ARC) which is presented in the M&FM Design Analysis and Performance Assessment Document Volume 4, State Analysis [5]. In summary, this entails the concept of state machines which are mathematical models representing the behavior of a system at each instant of time. State machines graphically represent the states of the system under investigation and the transitional behaviors across operational phases [5]. The intent of this work is to smooth transitions between subsystem states indicating stable conditions while exposing any anomalous behavior of the interacting subsystems. The planned utility of state analysis is to fully analyze the interactions of the M&FM algorithms and expose any hidden integration or timing problems including any latent errors stemming from the SSM algorithms. As expected, the state analysis is finding such errors, and within the M&FM teams are investigating the preliminary results as reported in reference [5], cited above. This document focuses on the paths or conditions which lead to a hazardous state. A sample finding presents MPS state analysis and yields anomalies in performance of the MPS M&FM algorithm response due to CCSE valve driver module (VDM) failures. Current analysis at least within the algorithms and prototype code have been explored with no findings but cannot be fully explored until the VMET evolves to include integration of all the SLS SSMs and vendor models. These types of findings are preparing the M&FM teams for such expected conditions and others to be investigated further in forward work.

VI. Summary and Forward Directions

The M&FM philosophy as being worked within the SLSP has been presented. In section I, Fig. 1 portrays the NASA M&FM context and the flow of the paper progresses from the philosophy of testing, through the algorithms, design, development, test cases, and activities of the VMET. The culture-changing approach for implementing M&FM concepts early in the FSW development cycle supported by extensive analysis further ensures safety interests of the crew and protection of NASA assets. Section II presented the M&FM testing philosophy for the SLSP. Since the testing of the prototype code in VMET is not inherently part of the critical path compared to FSW testing, the VMET team is able to address a greater variety of nominal and off nominal testing scenarios. Lessons learned and algorithm findings discovered in VMET activities can be shared with the FSW and SIL personnel, supporting those exterior testing activities. From Fig. 1, recall the central purpose of VMET is risk reduction, which is also addressed by the M&FM analysis group working with other organizations such as S&MA, Structures and Environments, GNC, the crew office, and Ground Operations by assessing performance of the M&FM algorithms in terms of their ability to reduce LOM and LOC probabilities. Section III then presents the methods used to transform the M&FM concepts into simple to understand algorithmic flow chart procedures based on UML-SysML and STOMP tools of EA provided by the FSW group.

The VMET process is described in section IV with supporting images of testing the MPS SSM of Fig. 2. The FC model and its purpose in VMET is also presented with a simple description of the processing scheme for each of the M&FM SSMs. The Sensor Data Qualification (SDQC) and data quality indicator (DQI) system is part of the FSW implementation and is an example of an SSM currently planned to be part of the testing processes in VMET but is still in the planning phases. In the FSW realm, SDQC and DQI will sample redundant data from multiple buses and qualify select data from each bus and down select to one value for each sensor. It will then publish a consolidated value with a DQI for any SSM subscribing to that data. A schema for implementing this in VMET is still under review but will be analogous to that being planned for FSW. The sample view of model integration of Fig. 4 exemplifies the required understanding of the vendor model interfaces and needs for methodical adaptation in VMET. The presented metrics in this section are continually evolving as more models get integrated or updated as the SLSP progresses. Also, MAVERIC provides a proven flight vehicle suite of models for VMET and may need updating as the SLSP progresses in future missions beyond the first few SLS flights, particularly as developmental flight instrumentation provides data for flight analysis and flight vehicle characteristics which will be used to validate existing flight vehicle models, potentially impacting existing vendor and SSM models in VMET. Other

models that could be impacted include thermal, environment models, and the physics of failure models used in prior M&FM analysis.

The integration of the M&FM algorithms in VMET has progressed according to schedule and in the process overcame many technical integration problems as presented in Section V. With reference to Fig. 6, to date the VMET has successfully integrated eleven vendor models based on priorities of the SLSP focusing on Green Run Testing. The first SSM integrated was the System Management SSM followed by the Avionics SSM and those indicated in Fig. 6. This priority has also directed the unit testing for the vendor models. The testing of the M&FM SSMs with the vendor models is progressing and has successfully demonstrated initial integration of each of the SSM models with the FC model.

Forward work is progressing and leveraging from the state analysis work from ARC. Findings being investigated were presented in Section V. The state analysis uncovers algorithm and interactional problems, posing its findings to the M&FM teams to investigate these problems in detail as VMET progresses to incorporating all the SSM and vendor models with subsequent testing. The intent of state analysis is to fully support VMET testing and post analysis which include verifying the proper responses from each of the SSMs, such as correct caution and warning events and abort conditions. In the event of non-proper responses, the capabilities will be in place to help identify any gaps in diagnosis of actual execution problems and guide root cause analysis whether they exist in the M&FM algorithms, vendor models, or implementation of them and the related interfaces. The end product goal will yield a stable platform for VMET and will be further poised to support other test programs where the M&FM algorithms are also being tested in the SDF an SIL with hardware-in-the-loop integrated testing.

Final thoughts and future ambitions for VMET are that it will serve as a viable platform to provide M&FM support as the SLSP progresses and its future missions dictate M&FM algorithm updates and reliable cross platform V&V. Beyond SLSP other ambitions include being capable of serving as an M&FM platform and reconfigurable for new models and algorithms for other flight programs. This is already possible using MAVERIC, the GNC Flight Mechanics tool, which is configurable for different flight vehicles.[7] For deep-space human exploration requiring more autonomy, the M&FM algorithms will need to be more robust, reliable, and possibly able to accommodate predictive technologies [11]. The LV/spacecraft subsystem models (e.g., nuclear based) will exhibit more complexity with expected physics-based elements addressing off nominal conditions such as effects from environmental disturbances, vehicle system upsets, radiation and solar effects, including communication delay models [6, 11]. These types of models can be implemented in VMET. Furthermore, the supporting hardware and software platforms hosting the advanced algorithms, including any that are model based, will likely need to utilize advanced computing concepts such as those from the artificial intelligence realm (e.g., neural, fuzzy, or Bayesian methods) [11]. Advanced computing algorithmic concepts may also employ nonlinear mathematical constructs (e.g., inference engine and probabilistic methods), rapid detection systems using advanced fusion and reasoning algorithms for sensor data, information processing, and reliable decision theory [11]. Software related to these systems and their integration will require advanced testbeds with commensurate V&V methods particularly for certifying any adaptive diagnostic, prognostic, and control algorithms operating under off-nominal conditions. The viewpoint for the M&FM methods for such deep space LV/spacecraft are not unlike those for the SLS, but may be compounded with the need for more autonomy and less man-in-the-loop interactions. The ongoing work from Watson et al and others across NASA, academia, and industry are projecting these types of directions and the principal proposition is that VMET will be poised to provide the M&FM focus for such endeavors, especially with technology trending towards more integrated and so called intelligent systems [11].

[7] e.g., X-33, X-37, X-43C, OSP, Ares I, Ares V, Saturn V

References

[1] G. Herbella et al, "Evolution of Abort Management of Crewed Launch Vehicles from Mercury ASIS to Commercial Crew EDS,"

[2] SLS-PLAN-075 SLSP Flight Software Verification & Validation (V&V), Space Launch System (SLS) Program, NASA – Marshall Space Flight Center, 3/14/13

[3] SLS-RPT-087-01, M&FM Design Analysis & Performance Assessment Document Volume 1: Monitored Conditions Report (MCR)

[4] SLS-PLAN-085 SLSP Fault Management Plan, Version 1, Space Launch System (SLS) Program, NASA – Marshall Space Flight Center, 03/04/13

[5] SLS-RPT-087-04, M&FM Design Analysis & Performance Assessment Document Volume 4, State Analysis, NASA – Marshall Space Flight Center, 5/15/2014

[6] C. Belcastro, "Validation and Verification of Future Integrated Safety-Critical Systems Operating under Off-Nominal Condition," AIAA

[7] http://www.sparxsystems.com/uml-tutorial.html

[8] NASA Study on Flight Software Complexity, Final Report, Editor: Daniel L. Dvorak, Jet Propulsion Laboratory, March 2009

[9] K. Rajan et al, "Remote Agent: An Autonomous Control System for the New Millennium,"

[10] SLS-RPT-087-06, Space Launch System Program (SLSP) Mission and Fault Management (M&FM) Design Analysis & Performance Assessment Volume 6: M&FM Algorithm Test Procedures and Results, Draft, March 2015

[11] M.D. Watson et al, "Systems Engineering of Autonomous Space Vehicles," IEEE PHM 2014, June 22-25, Spokane, WA

Acknowledgments

This work was funded under JACOBS ESSSA Group for NASA under contract NNM12AA41C. The principal author thanks the fellow co-authors for their willingness and contributions of their combined knowledge of LV health management principles and the M&FM processes from analysis through testing which significantly contributed to the overall clarity of this paper. The authors thank the M&FM management team of Messrs. Joey Broome[8] and Dwight England[9] for their leadership and Mr. England's contributions to this paper. Special acknowledgement to Dr. Michael Watson[10] for his early involvement in the development of the M&FM team at MSFC and his continued inspirational NASA work on the investigation of the technological foresight for human space exploration. Further acknowledgement is also granted to the Flight Software Group and participating organizations[11] in all M&FM activities. In conclusion the authors especially acknowledge the overall M&FM team[12] for their friendly team spirit and cohesive efforts for addressing the M&FM needs for each of the SLS launch vehicle subsystems for the SLS Program.

[8] Former Chief, promoted to Vehicle Management Discipline Lead Engineer in April 2015
[9] Former Deputy Chief, promoted to Chief in May 2015
[10] Former Chief, now serving in the Chief Engineer's Office for Systems Engineering
[11] Such as Crew Office, Ground ops, SPIO, Avionics, GNC, KSC, JSC, GRC, ARC, Booster, Liquid Engines, and S&MA
[12] VMET, analysis, algorithm developers, schedule leads, IDT leads, prototype developers, and all administrative and project support personnel

Appendix A. M&FM Documents and Relevant M&FM Terminology

1. *Volume 1 – SLS Vehicle Abort Triggers Definition (ATD) (SLS-SPEC-197-01)* contains all abort triggers approved for monitoring and associated details, such as the detection measurements and sensors, thresholds, and applicable mission phases.
2. *Volume 2 – SLS Vehicle Caution and Warning (C&W) (SLS-SPEC-197-02***)** contains all Cautionary (Class 3) and Warning (Class 2) conditions approved for monitoring and associated details, such as the detection measurements and sensors, thresholds, and applicable mission phases.
3. *Volume 3 – SLS Vehicle Safing Conditions and Actions (SLS-SPEC-197-03* describes the safing actions performed upon detection of abort triggers defined in Volume 1, those actions performed upon receipt of an abort command from MPCV or ground during the various mission phases, as well as those actions performed during pre-launch upon receipt of a "Cutoff" command from ground or MPCV. It also defines approved failure conditions which, when detected by the vehicle, will precipitate vehicle autosafing Launch Halt during pre-launch and Automated Launch Sequence (ALS).
4. M&FM Design Analysis & Performance Assessment Document Volume 1: Monitored Conditions Report (MCR), SLS-RPT-087-01

Relevant M&FM Terminology

- *The Goal Tree/Success Tree* (GT/ST) is a graphical representation of the functions required for the SLS to perform its mission objectives. For SLS, that basic mission objective has two goals: the first is to ensure that the crew is safe and unharmed or the cargo is functioning, and the second is to place the MPCV or cargo payload to a specific target orbit or trajectory. The abort triggers are specifically targeted at addressing the goal of ensuring that the crew is safe and unharmed. The GT/ST is constructed by systematically decomposing the functions that enable SLS mission objectives to identify the supporting sub-functions necessary, while at each hierarchical level identifying the state variables that must be controlled for each function/sub-function in the decomposition. The GT/ST uses a "success space" approach, as this provides some useful advantages over existing S&MA fault tree approaches used in probabilistic risk assessment and in hazard analyses.
- *Crit 1 and 1R Failure Modes* are failure modes that Safety and Mission Assurance (S&MA) has determined may lead to a loss of crew. Criticalities are defined in the Space Launch System (SLS) Program Failure Modes Effects and Analysis/Critical Items List (FMEA/CIL) Requirements Document. Analysis is also performed to evaluate whether any Crit 3 failure modes can falsely activate any candidate abort triggers.
- *Failure Mode to Failure Effect Traces* using the Integrated Vehicle Failure Model (IVFM), supporting the calculation of: Abort Condition occurrence, LOM Scenario occurrence, Launch Commit Criteria assessment and resulting design, Line Replaceable Unit assessment and associated diagnostic procedure development.
- From operations, Fault Management (FM) uses the Integrated Mission Timeline to help define IVFM switch configurations achieve integrated, GT/ST phases, and abort analysis phases. FM also uses the operations Line Replaceable Unit (LRU) List in the IVFM. In return, FM supplies information on failure observability and LRU isolation capabilities to operations.
- *Abort Effectiveness Analysis*, using the Abort Analysis Matrix, which calculates the effectiveness of abort responses in Loss of Mission (LOM) Scenarios. This supports internal M&FM analysis of the effectiveness of Abort Triggers, and the PRA calculations of Loss of Mission (LOM) and the SLS contribution to the Loss of Crew (LOC).
- *Post-flight Analysis Observability Assessment* using the IVFM, which assesses the capability of the vehicle sensor suite to observe failure effects to the level necessary to support long-term SLS fleet operations.
- *Redundancy Management Effectiveness Assessment*, which assesses the performance effectiveness of SLS redundancy management (RM) algorithms, using formal equations described in Section 4.1.2 of the SLS Monitored Conditions Report (MCR) (SLS-RPT-087-01), supporting the PRA Loss of Mission model.
- *State Machine Analysis* using the SLS State Machine Analysis Model, which analyzes nominal and off-nominal behavioral interactions of SLS algorithms and components with each other and with external systems including MPCV and GSDOP. This includes assessment of interactions of abort and RM algorithms and responses. This is performed to assess potential interaction threats that can cause potentially catastrophic hazards, and to recommend design or operational changes or constraints to reduce these risks.

- *Caution and Warning "Message Storm" Analysis*, which assesses the number and content of C&W messages that will occur in credible LOM scenarios, using LOM scenario-based walkthroughs and the State Machine Analysis Model, to ensure that the C&W notification design does not overwhelm the astronauts in the MPCV. This will be performed with in-depth support of the MPCV and Crew Office.
- *Launch Commit Criteria (LCC)* - assessment of the ability to observe and isolate Line Replaceable Units for pre-launch operations, and assessments of pre-launch and post-flight failure mode observability.
- *The IDT* provides a forum for
  - Explanation of element and subsystem design and operation by Subject Matter Experts (SME)
  - Discussion and resolution of design issues as appropriate
  - Review and assessment of M&FM algorithms
  - Review and assessment of software requirements
  - Discussion of vehicle hazards and hazard controls
  - Coordination of integrated operations and interfaces between the vehicle and GSDO, MPCV, or MS.

Appendix B Sample VMET Test Objective and Results Analysis for MPS

This test verifies the functionality of specific portions of the Mission and Fault Management (M&FM) Main Propulsion System (MPS) Subsystem Manager (SSM) algorithm tested with the Vehicle Management End-to-end Testbed (VMET).

Objective: MPS-003 LO2 and LH2 Tank Pressurization algorithms – Verify the MPS Subsystem Manager algorithm responds to MPS supplied LO2 and LH2 tank pressures by energizing/de-energizing the necessary MPS valves such that the LO2 and LH2 tank pressures are maintained within a specified range starting at Autonomous Launch Sequence (ALS) and ending at Main Engine Cut-Off (MECO).

For this test the MPS SSM's tasks begin at T-30 (start of ALS). As a result, the VMET models will begin at T-40 seconds. This T-40 second start time allows time to start and initialize the FC, PDCU, MPS, and CCSE models prior to MPS SSM execution. Upon MPS SSM execution, the VMET models shall be in a nominal state for On Pad ops. The VMET models are configured to execute through MECO + minimum of 10.0 seconds and supply nominal data to test MPS-002, MPS-003, and MPS-007 throughout a nominal flight profile.

Note: The FC model is used to command the PDCU, CCSE, and MPS models into a nominal state for on pad operations prior to ALS. This task would nominally be performed via ground commands at a much earlier time.

Once the MPS SSM is executing, the FC (based upon MPS SSM input) issues CCSE VDM commands to the CCSE model which in turn energizes/de-energizes specific solenoid drive motors within the MPS model. Based upon the state of a subset of these solenoids within the MPS model, the LH2 and LO2 tank pressures increase or decrease based upon a first order algebraic expression. The MPS calculated tank pressures are returned to the CCSE as a voltage on one of the three CCSE's Pressure Interface Module (PIM) cards. For the LH2 and LO2 tank pressures this is PIM 1. The PIM1 pressure values are transmitted to the FC via 1553. The FC converts the 12 bit count values to floating point pressure values and passes these to the MPS SSM as inputs.

Upon test completion, data analysis is performed to verify the proper MPS VDM Valve positions are maintained as required for a nominal flight, the LO2 and LH2 tank pressures are maintained within their respective ranges, and the proper VDM valves are configured for a nominal MECO.

This test shall be performed once, and it covers all of the necessary states of the VDM valves and tank pressures required to meet the test objectives. (Note, the test could be performed a second time such that the LH2 and LO2 Ullage Valves are in the opposite state as the first test when MECO is achieved.)

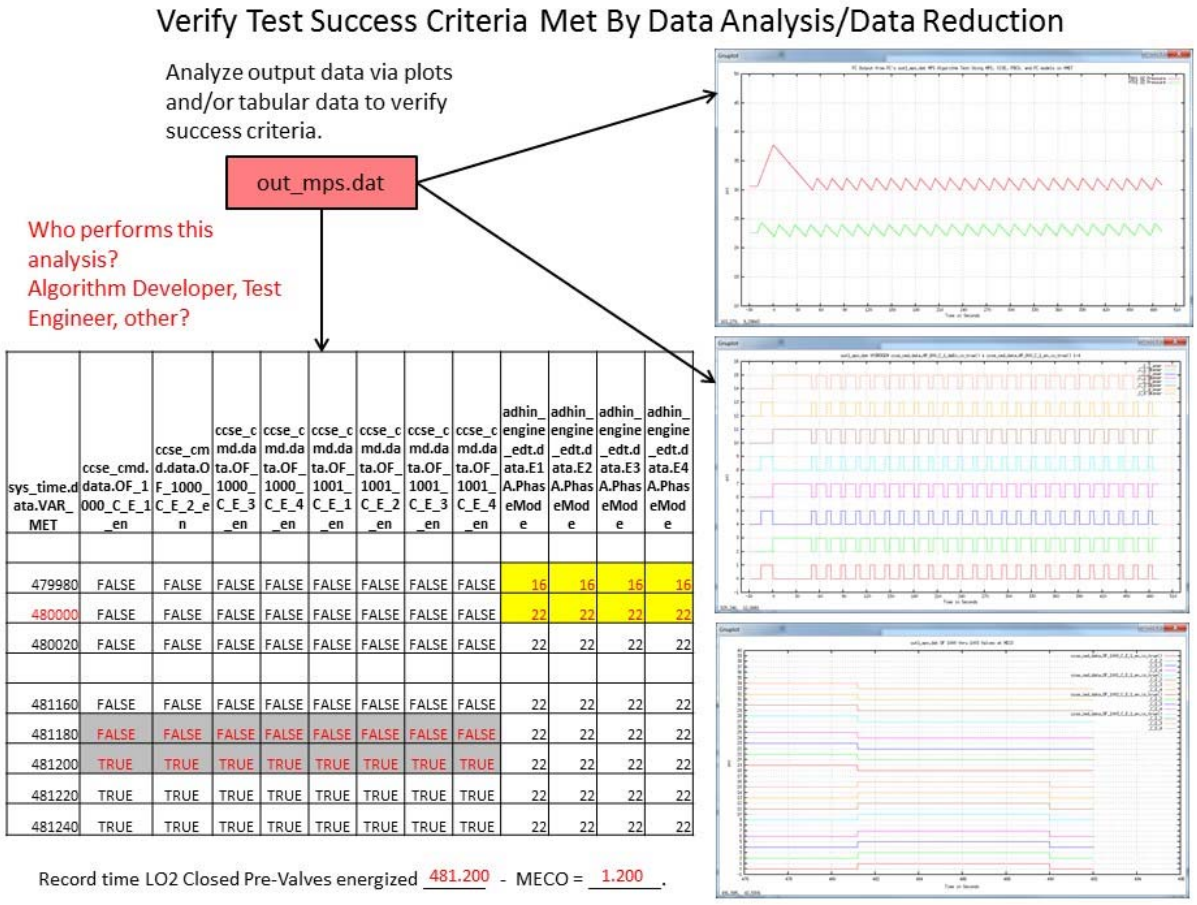
- ***Success Criteria***:
  Review out_mps.dat and verify that the four LH2 Ullage Valves listed below are energized and de-energized such that the average LH2 tank pressure is maintained at 31.0 psi (+/- 1.0 psi) from T-15.0 seconds through MECO + 5.0 seconds.

If LH2 Ullage Valves energized at MECO, record time LH2 Ullage Valves de-energized _____ - MECO = _____.

Review out_mps.dat and verify that the four LO2 Ullage Valves listed below are energized and de-energized such that the average LO2 tank pressure is maintained at 23.0 psi (+/- 1.0 psi) from T-15.0 seconds through MECO + 5.0 seconds.

If LO2 Ullage Valves energized at MECO, record time LO2 Ullage Valves de-energized _____ - MECO = _____.

Plot the average LH2 and LO2 Pressures for test duration to demonstrate the pressures are maintained within limits from T-15.0 seconds through MECO + 5.0 seconds.



sys_time.data.VAR_MET	ccse_cmd.data.OF_1000_C_E_1_en	ccse_cmd.data.OF_1000_C_E_2_en	ccse_cmd.data.OF_1000_C_E_3_en	ccse_cmd.data.OF_1000_C_E_4_en	ccse_cmd.data.OF_1001_C_E_1_en	ccse_cmd.data.OF_1001_C_E_2_en	ccse_cmd.data.OF_1001_C_E_3_en	ccse_cmd.data.OF_1001_C_E_4_en	adhin_engine_edt.data.E1A.PhaseMode	adhin_engine_edt.data.E2A.PhaseMode	adhin_engine_edt.data.E3A.PhaseMode	adhin_engine_edt.data.E4A.PhaseMode
479980	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	16	16	16	16
480000	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	22	22	22	22
480020	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	22	22	22	22
481160	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	22	22	22	22
481180	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	22	22	22	22
481200	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	22	22	22	22
481220	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	22	22	22	22
481240	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	22	22	22	22

Figure B. 1 Sample of Analysis Representation by the VMET Team