NASA Space Flight Vehicle Fault Isolation Challenges

James R. Neeley[1],
Jacobs ESSSA Group, Huntsville, AL, 35806

James V. Jones[2],
Logistics Management Associates, Irvine, CA, 92620

Christopher J. Bramon[3], Sharon K. Inman[4],
NASA Marshall Space Flight Center, Huntsville, AL 35812

and

Loraine Tuttle[5]
NASA Kennedy Space Center, FL 32899

The Space Launch System (SLS) is the new NASA heavy lift launch vehicle and is scheduled for its first mission in 2018. The goal of the first mission, which will be uncrewed, is to demonstrate the integrated system performance of the SLS rocket and spacecraft before a crewed flight in 2021. SLS has many of the same logistics challenges as any other large scale program. Common logistics concerns for SLS include integration of discrete programs geographically separated, multiple prime contractors with distinct and different goals, schedule pressures and funding constraints. However, SLS also faces unique challenges. The new program is a confluence of new hardware and heritage, with heritage hardware constituting seventy-five percent of the program. This unique approach to design makes logistics concerns such as testability of the integrated flight vehicle especially problematic. The cost of fully automated diagnostics can be completely justified for a large fleet, but not so for a single flight vehicle. Fault detection is mandatory to assure the vehicle is capable of a safe launch, but fault isolation is another issue. SLS has considered various methods for fault isolation which can provide a reasonable balance between adequacy, timeliness and cost. This paper will address the analyses and decisions the NASA Logistics engineers are making to mitigate risk while providing a reasonable testability solution for fault isolation.

I. SLS Design Architecture

NASA's Space Launch System Program (SLSP) is the latest initiative in human space exploration and this ambitious program is challenged to meet significant innovative technical objectives in the midst of a national austere funding environment. The SLS vehicle concept utilizes an innovative "melding" of technologies, key concepts from the family of Saturn launch vehicles used during the Apollo Program, as well as designs and technologies from the more recent Space Shuttle and Constellation Programs. Figure 1 illustrates the SLS planned evolving architecture and Figure 2 shows the initial Block 1 configuration. While the SLSP design solution will evolve by incorporating the latest technology for propulsion, the first flights will make extensive use of heritage hardware to shorten development time and reduce the design cost. The SLS Elements consist of the Stages, Liquid Engines, Booster, Advanced Development, Spacecraft/Payload Integration and Evolution, and Ground Operations Liaison.

One of the key measures of success for the SLSP is remaining within the overall budget established by Congress while meeting the baselined launch date. NASA has long recognized that the concepts and processes of Integrated

[1] Supportability Engineering/ILS Lead, MSFC Mission Operations Laboratory, Operations Engineering/EO40.
[2] President, Logistics Management Associates, 19 Woodlawn, Irvine, CA, 92620.
[3] Operations Discipline Lead Engineer, MSFC Mission Operations Laboratory/EO01.
[4] Alternate Operations Discipline Lead Engineer, MSFC Mission Operations Laboratory/EO01.
[5] Logistics Technical Integration Manager, Logistics Development and Integration Branch/LXL00.

Logistics Support (ILS) and Logistics Support Analysis (LSA) provide a significant opportunity to minimize cost of ownership. NASA has established policy mandating program life-cycle logistics support through applicable phases and inclusion of supportability as part of the system's design characteristics to assist in ensuring system availability and affordability.[1]

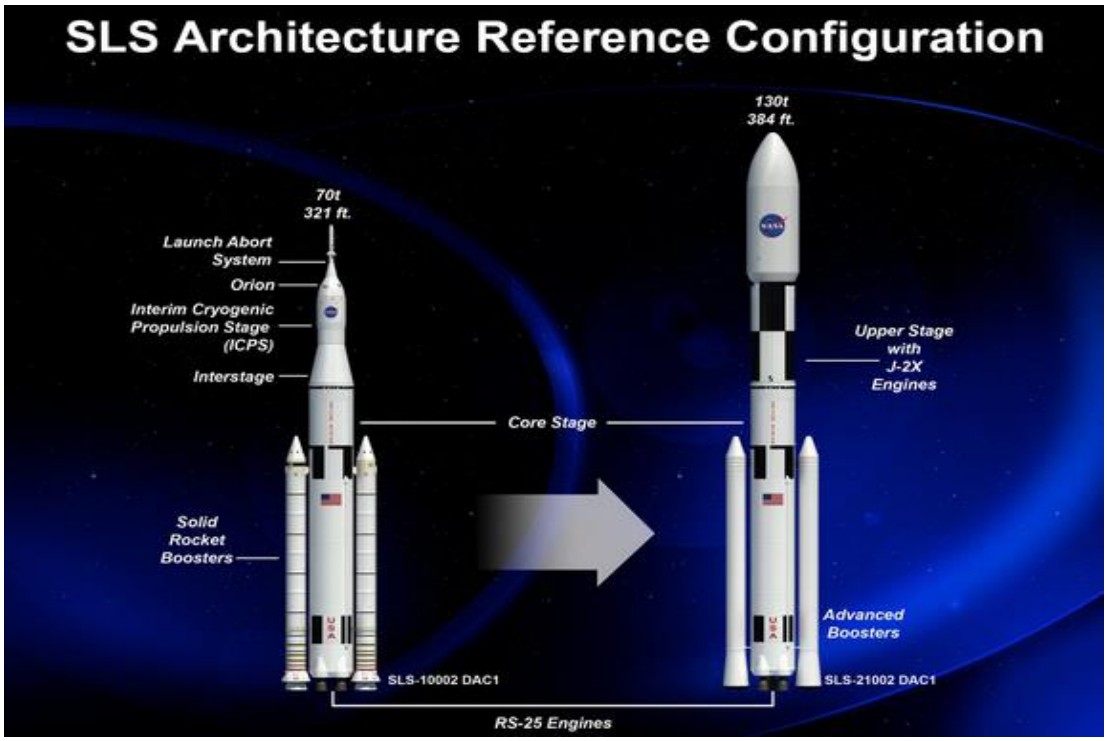

Figure 1. SLS Architecture Evolution.

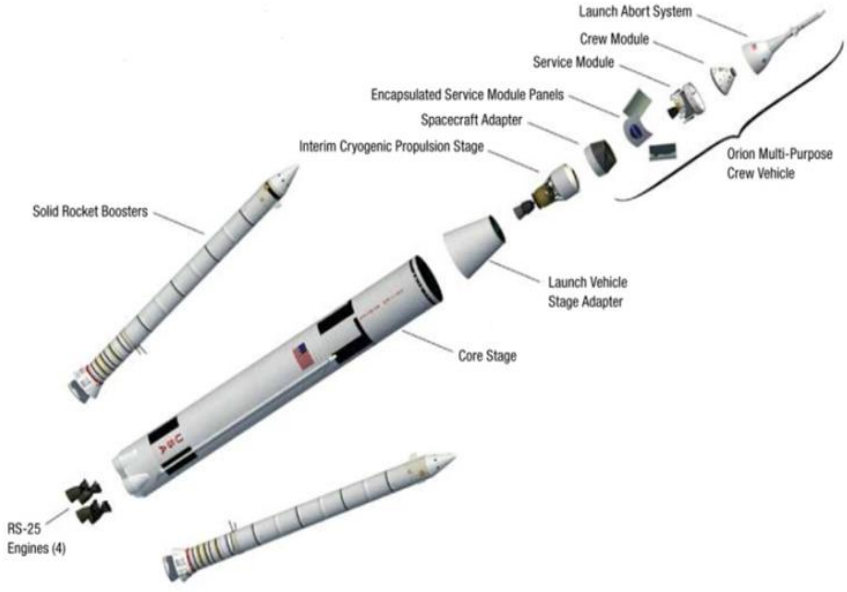

Figure 2. SLS 70 metric-ton Initial Block 1 Configuration, 321 feet tall.

II. Supportability in Traditional ILS Application

Traditional application of ILS during the design, development, test, and evaluation (DDT&E) of a system typically consists of two different but highly related processes, designing a supportable system and then developing a reasonable, responsive and cost effective support solution for the system.[2] This approach to ILS has been proven innumerable times by the US Department of Defense (DoD) as being effective and extremely beneficial through reduction of support infrastructures and increases in system operational availability.

Figure 3 illustrates how the expected application of ILS during system DDT&E consists of supportability engineering within the systems engineering process to assure that the system design defined for operation, when used within the mission profile and environmental limitations, will produce a design that requires the lowest possible in-service support solution. The maintenance task analysis (MTA) provides the foundation for development of the physical support resource package necessary to sustain the system over its possibly 30-50 year operational life. One of the basic premises of ILS is that a higher quality system will require far less support when in-service. Increasing system reliability, maintainability and testability, which can increase cost during development, can reasonably result in a much lower cost of ownership by reducing the logistics footprint, i.e. personnel, spares, facilities and other cost drivers, during in-service operation and support.

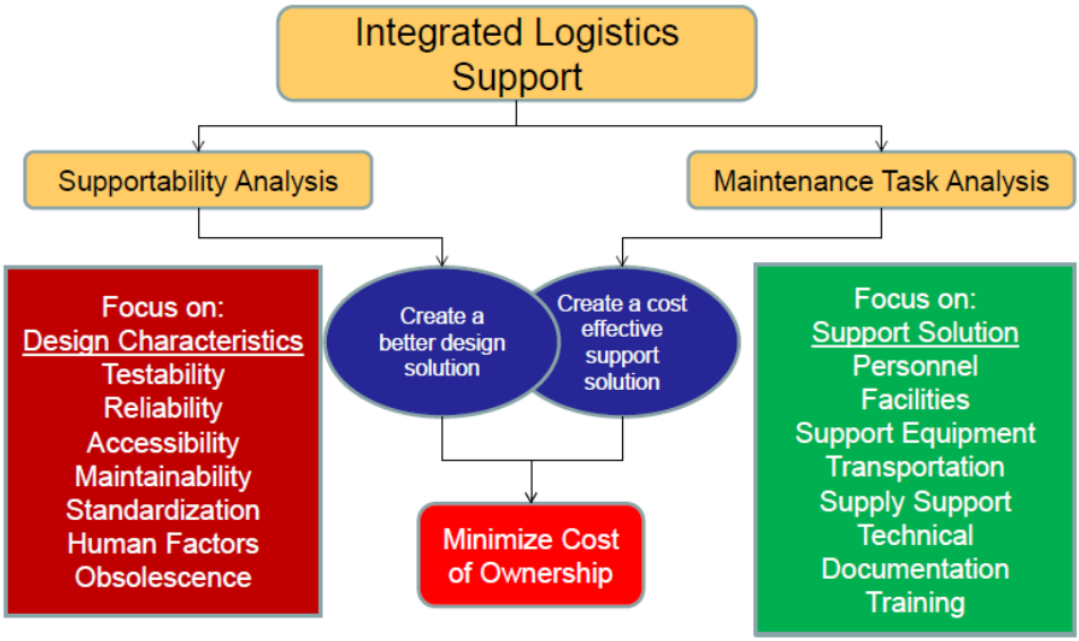

Figure 3. Integrated Logistics Support During System Development.

The specific application techniques and schemes for traditional ILS vary by technology, industry and organization; however, normally the supportability engineering process consists of LSA, human factors integration, reliability, and maintainability in a coordinated approach to design improvement. A simple comparison of traditional ILS concepts and processes with the unique circumstances of the SLSP indicates that application must be drastically different to be effective. The SLSP DDT&E phase will have one launch every three to four years, and each SLS vehicle will have significantly different technology baselines and physical hardware configurations for the first several flights. A large, costly logistics support infrastructure would be impractical and unaffordable. So, the SLSP application of ILS has been adapted to select and maximize those processes that will contribute to the program goals while at the same time taking a significantly different approach to meeting potential physical logistics support requirements. SLSP is performing a comprehensive, but non-traditional ILS program. A characteristic of supportability engineering impacted by SLSP unique circumstances is testability and particularly fault isolation.

III. Supportability and Fault Isolation Challenges

The universally accepted criteria for a supportability design are fairly simple in theory and in practice. The degree of supportability contained in a system design can be measured in the amount of time required to restore operability when a failure occurs. A supportable design has the following five attributes: [3]

1. *Fault Detection: The ability to detect any deviation from the expected normal performance parameters. A typical expectation is the ability to detect at least 99% of the failure modes identified through a Failure Modes Effects Analysis (FMEA).*
2. *Fault Isolation: The ability to isolate a detected fault to a single failed item using automated features at least 95% of the time, to one of two failed items at least 97% of the time and one of three or four items 99% of the time. Additionally, a false isolation not exceeding 1% of the fault indications used to assess fault isolation accuracy.*
3. *Access: The ability to gain unimpeded access to an item without moving other non-failed items or creating collateral damage.*
4. *Replacement: Rapid removal of the failed item by disconnecting lines, unplugging wires and removal of attaching hardware. Then this is followed by replacing with a fully functional item by reattaching hardware and reconnecting lines and wiring.*
5. *Confidence Test: The capability to test the system after replacement of the failed item to confirm restored operability and also confirm no other damage occurred or failure induced during the replacement process.*

Any item within the system architecture that meets these attributes is typically referred to as a line replaceable unit (LRU) indicating that the item can be replaced upon failure to restore system operability. Figure 2 shows the flow process for restoring operability for a space flight vehicle that incorporates a fault management (FM) and diagnostics capability. An ambiguity group is a collection of functions or failure modes for which diagnostics can detect a fault and can isolate the fault to that collection, yet cannot further isolate the fault to any subset of the collection. An optimal ambibuity group is estimated to be four to five LRUs.

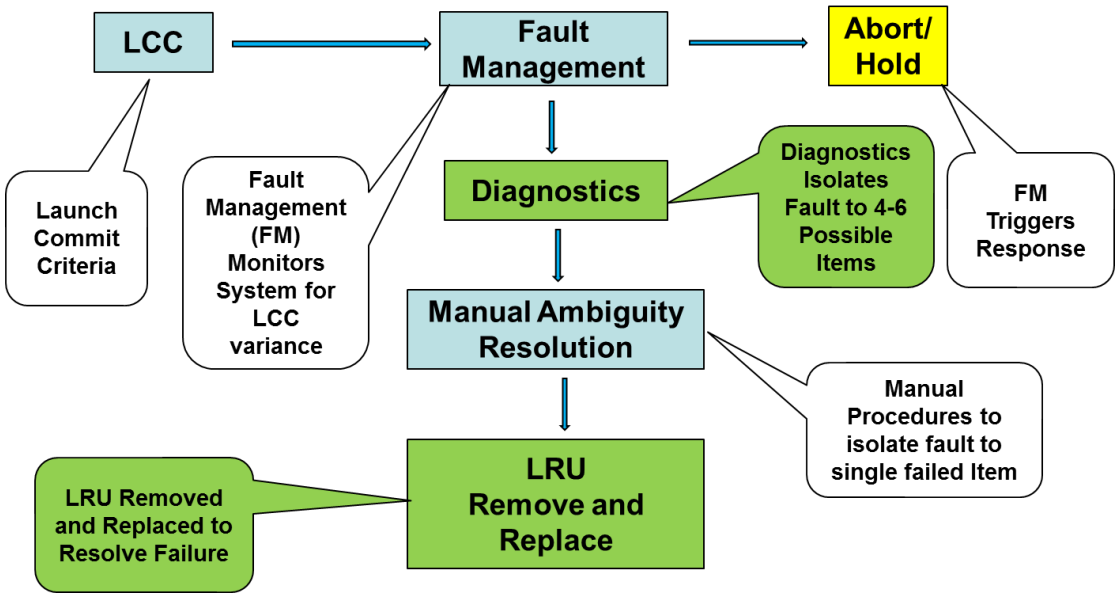

Figure 4. Flow Process for Fault Isolation and Failure Resolution

The time required to rectify failures is directly attributable to the attributes and characteristics of the design that allows rapid identification and response to non-conforming hardware or software. When the system design allows rapid fault isolation, access and replacement of the failed item, then the time penalty for the event is fairly short. However, in instances where the design does not allow rapid fault isolation, access and replacement of the failed item, the resulting time penalty can be severe which translates into a significant expenditure of resources (especially people) which increases cost. There is also the intangible, but very critical loss of reputation and credibility when successive launch attempts are unsuccessful. Table 1 shows the options for diagnostics and related challenges.

Table 1. Options for Diagnostics

Diagnostic Option	Challenge
No Diagnostics	Rollback from launch pad to Vehicle Assembly Building for likely vehicle disassembly and reassembly to resolve failure. Significant schedule delay.
Automated	Develop automated capability to extract fault data and input to a FM model to perform diagnostics. Increased cost for vehicle software design.
Manual	Develop manual capability to extract fault data from telemetry and manual input to FM model to perform diagnostics.
Ambiguity Resolution	Manual ambiguity resolution procedures will be required for any option to determine failed LRU.

IV. Relationship of Ground Systems Diagnostics

The ground launch management system at the launch site will determine which FM capabilities will be executed on the vehicle and which will be performed by the ground systems during pre-launch operations, as well as determining the proper response actions in the event of a detected failure. The Advanced Ground Systems Maintenance (AGSM) concept analyzes data and health status published by the Launch Control System (LCS) in order to provide advisory information related to fault isolation, projected component useful life, and anomalous conditions that users may evaluate using the LCS certified system data. This supports the building of prognostics and fault detection used by LCS operators during the launch cycle. A video of the AGSM concept is included with the presentation associated with this paper.[4]

V. SLS Methodology for Diagnostics and Fault Isolation

The SLS Operations team performed an assessment of supportability technical performance measures (TPMs), including launch availability and maintenance downtime, being applied during the DDT&E phase to assist with determining the best option for vehicle diagnostics capability. Progress toward the five basic supportability attributes as described above were considered, as well as the SLS unique circumstances of low quantity of launch vehicles, short service life, and the operations disposable nature of the flight hardware whereby no flight hardware returns for servicing. The assessment results led to the SLSP decision to develop a manual diagnostic capability that is non-intrusive and near real-time.

A task team that included the SLS design team and ground launch organizations was established to focus on implementing the basic fault isolation concept as shown in Figure 5 with the proposal to plan, develop, implement and manage a manual diagnostics capability to mitigate off-nominal conditions during preflight through failure isolation tools and procedures. The manual diagnostics capabilities will support quick response to LCC violations and support efficient troubleshooting of indicated failure conditions.

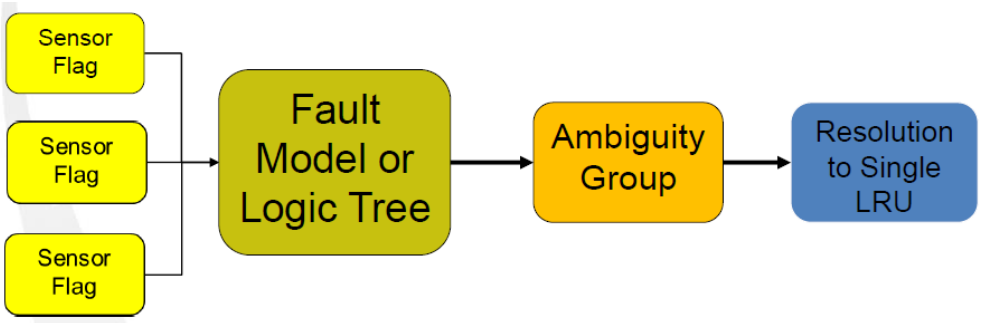

Figure 5. Fault isolation Concept

Where practical and feasible to do so, implementing certain Fault Detection, Isolation, and Recovery (FDIR) capabilities in the design of LRUs should be considered for the purpose of maximizing the affordability of troubleshooting and maintenance activities and the availability of the launch vehicle. This includes taking into account the launch pad accessibility of the LRU and determining if it is prudent to develop and utilize non-invasive, hands-off means of troubleshooting the failure in order to acquire as much knowledge about the failure as possible. Having such insight would be beneficial before deciding to roll back the vehicle to the Vehicle Assembly Building for removal and replacement (R&R) of the LRU or before continuing with launch. Moreover, such diagnostic functions for LRUs may also prove invaluable in test and checkout activities during vehicle integration and prior to launch.

The task team identified the following activities that would need to be accomplished.

1. *Assessment of number and coverage of sensors contained in SLS Element designs to assure adequate coverage of all failure modes on the SLS FEMA with linkage to LRUs.*
2. *Identification of all ambiguity resolution procedures necessary to complete fault isolation to a single failure SLS LRU. Ambiguity procedures, after identification, to be documented to allow development of off-nominal procedures.*
3. *Plan/prepare for use of Testability Engineering and Maintenance System (TEAMS) designer model for manual fault monitoring and isolation. Preparation should include assessment of telemetry data and appropriate method for extracting minimum data for TEAMS processing.*

The implementation process concept for a manual diagnostics capability is shown in Figure 6. This process would evolve from a shared responsibility between the designer and launch site responsibility after maturity of the SLS architecture design.

Figure 6. Manual Diganostics Implemention Process Concept

Conclusion

The SLSP has taken a measured approach in applying design considerations for vehicle diagnostics capabilities to aid in fault isolation of failed components during launch processing activities. Further work has been identified to develop a manual diagnotics capability with a focus on crewed missions, the first of which is scheduled to be Exploration Mission (EM)-2 currently planned for 2021.

References

[1] NASA Logistics Management Division, NASA Policy Directive (NPD) 7500.1D, "Program and Project Life-Cycle Logistics Support Policy", Washington, D.C., 2015, pp. 1.
[2] US Department of Defense, Assistant Secretary of Defense for Logistics and Material Readiness, "Product Support Manager Guidebook", Washington, D.C., 2011, pp. 10, 37-38.
[3] Jones, J.V., "Supportability Engineering Handbook", McGraw-Hill, New York, 2007, pp. 5.26-5.29, 6.2-6.6.
[4] NASA, "Advanced Ground Maintenance System", Kennedy Space Center (KSC), FL, The Institutional Multimedia Studio at KSC, 2013.