Opportunities for Launch Site Integrated System Health Engineering and Management

Authors: Robert D. Waterman, Patricia E. Langwost,
Susan J. Waterman, Alan Zide – NASA Kennedy Space Center

Abstract: The launch site processing flow involves operations such as functional verification, preflight servicing and launch. These operations often include hazards that must be controlled to protect human life and critical space hardware assets. Existing command and control capabilities are limited to simple limit checking during automated monitoring. Contingency actions are highly dependent on human recognition, decision making, and execution. Many opportunities for Integrated System Health Engineering and Management (ISHEM) exist throughout the processing flow. This paper will present the current human-centered approach to health management as performed today for the shuttle, Expendable Launch Vehicles (ELV), and space station programs. In addition, it will address some of the more critical ISHEM needs, and provide recommendations for future implementation of ISHEM at the launch site.

Introduction to Launch Site Operations

Launch site operations begin with the arrival of flight hardware, which can range from an individual component shipped from a vendor to a fully assembled vehicle that has returned from a recent space mission. Upon arrival, acceptance tests and inspections are performed to assess the hardware's health. Hardware that arrives from a vendor is usually subjected to a complete end-to-end test of its electrical systems, including copper path (continuity) checks, stray voltage (isolation) checks and channelization (interface) tests. Hardware that is reusable and has proven system functionality during flight is generally not subjected to the same rigorous test protocols that are required for new hardware. Copper path testing is performed to verify signal continuity following connector de-mates. These de-mates are often the result of intrusive redundancy test procedures.

Prior to flight, functional testing is performed to certify hardware capabilities such as system functionality and redundancy paths. Hardware capabilities are often tested in a non-integrated environment such as the Orbiter Processing Facility (OPF), which is used to test only an orbiter and not a fully assembled shuttle. These functional tests are frequently re-performed at the Launch Pad after the orbiter has been stacked with its Solid Rocket Boosters (SRB) and External Tank (ET) into an integrated shuttle system and moved into launch position. Some functional tests are performed each time power is applied regardless of where the orbiter is in its processing flow.

Human-Centered Health Engineering and Management

In today's launch site test environment, system health engineering and management is typically human-centered. Tests are performed by engineers who determine when non-conformances occur and initiate the proper paperwork to document the anomaly. In some cases, software is used to automate data collection or summarize results; however, it is ultimately the responsibility of the engineer to evaluate the data to determine if an anomalous condition exists.

Today's Human-Centered Health Engineering and Management (HCHEM) approach to launch site test and evaluation is costly, inefficient and dependent on the available engineering expertise. The goal of an ISHEM approach is to improve the ability to accurately detect anomalies in a more timely and consistent manner than HCHEM techniques can provide.

The following sections will discuss current launch site health engineering and management problems and will suggest areas where replacing HCHEM with ISHEM will benefit launch site operations.

Space Shuttle Turnaround Operations

Most of the time required to turnaround space shuttle hardware is spent determining hardware condition following the previous flight. (McClesky 2005, 1-15) The majority of this time is spent performing structural and thermal protection system inspections; and verifying the integrity of the various fluid systems. A significant amount of additional time is spent performing unplanned work associated with troubleshooting anomalies, replacing failed components (including removal of system components to gain access) and performing retest. Finally, system functional testing is performed to assess the hardware's readiness to support the next phase of the processing flow.

Inspections are typically labor-intensive operations where an experienced engineer uses techniques such as: dye penetrant inspections to detect the depth of dings and scratches; eddy current measurements to assess structural health; other non-destructive evaluation approaches that have become available throughout the years. These techniques provide the engineer with information that can be used to determine if an anomalous condition exists and rely on the engineer's knowledge of system specifications and previous test results. In the case of dye penetrant inspections, acceptable dings and scratches are entered into a "Ding Log" that is used to document and track known conditions. These logs require manual entries that cite the position, shape and depth of the anomaly.

Fluid systems are revalidated after every flight because all fluid systems leak. Many of the fluids, such as oxygen and hypergols, are corrosive and will damage system seals and components over time which will lead to leaks. Some leaks that are deemed acceptable following an inspection may become unacceptable at a later point in time. One area of particular concern is the ability to accurately characterize the current state of a fluid system. This characterization is impeded by two problems. The first problem is that many fluid system areas are not instrumented, so the ability to directly sense the current state is not available and must be inferred. The second problem is that many shuttle sensors are not regularly calibrated and can therefore provide inaccurate information. To compensate, engineers maintain manual "cheat sheets" that adjust for errors based on sensor readings that are obtained under known conditions such as the value of ambient pressure a pressure sensor should read at sea level. The engineer must calculate the actual pressure value based on the returned sensor reading and the known error obtained from the "cheat sheet." For example, a pressure sensor should read ambient pressure at sea level as 14.7 psia; however some shuttle pressure sensors may read this value within a range of -2.0 to 45 psia. A pressure sensor whose "cheat sheet" value indicates that it reads ambient pressure as 5 psia is offset by 9.7 psia. So when the sensor indicates that the system is at a pressure of 15 psia, the engineer must actually add the offset value to determine that the actual pressure is 24.7 psia. This scenario occurred in 1995 in the orbiter's Orbital Maneuvering System (OMS). A test engineer inadvertently failed to compare the value returned by a pressure sensor against the "cheat sheet" offset and believed that the OMS system was at ambient pressure. When a technician opened the joint instrumented by this sensor, fluid escaped and started a fire in the OPF around the orbiter Discovery. (NASA 1995, p1-2)

Unplanned work is the result of an HCHEM system that reacts to component failures as opposed to an ISHEM system that detects component degradation before failure limits have been exceeded. In other words, current launch site monitoring capability is designed to react based on pass/fail criteria as opposed to determining the component health and annunciating degraded conditions. (Maclise 2004, p1-4) In the case of a valve with open and closed positions, indicators provide insight into when an open or closed command is sent to the valve and whether or not the valve responded properly. While these indications generally provide enough information to declare the valve either functional or non-functional, they provide little insight into its health. An experienced engineer may be able to infer some health information from the indicator readings; however, the scope of what can be inferred is limited by the type of information being sensed.

For example, timing data is collected when Main Propulsion System (MPS) propellant valves are cycled open or closed. In this case, the propellant valve has two indicators, one located at the open position and the other at the closed position. When the valve is commanded open, the closed indicator will change state first. The open indicator will then change state once the valve has traveled to the fully open position. An experienced engineer uses this data to infer whether or not the valve has become sluggish when starting to move or slow to cycle from one position to another. This inferred health detection is accomplished by: comparing the time the command is sent to when the first indicator changes state (detects sluggish valve); and comparing the time the first indicator changes state to when the second indicator changes state (detects slow to cycle).

System functional testing includes redundancy verification including: power, command paths and data paths. While avionics systems have more redundant paths than electro-mechanical systems, testing is generally more automated and therefore less time-consuming.

International Space Station (ISS) Element Integrated Testing

The Kennedy Space Station Payload Processing Directorate tests all of the payload items that will go into the Shuttle Bay. This includes the elements of the International Space Station (ISS), the Multi-Purpose Logistics Modules (MPLM), and experiments that will fly onboard the ISS or Shuttle. This testing is done in the Space Station Processing Facility (SSPF) and is the final functional testing performed before launch.

ISS Test and Verification

Multi-Element Integrated Testing (MEIT) is the testing of system functionality and interface compatibility between International Space Station elements. A standalone test is the testing of a single element to ensure functionality after shipment to KSC and prior to interfacing with the ISS. It can also satisfy requirements that have not been met through previous testing at a different site. A MEIT or standalone takes several years to develop and execute. Agreements are made during Phase A (source gathering), such as concepts, testing ground rules, and test plan responsibility matrix need to be made between International Partners, participants, and the ISS Program. Detailed Test Objectives (DTO) need to be developed, evaluated and approved during Phase B (definition). This includes identifying support equipment and software, testing timeline, interdependent subsystems and their associated activities. Phase C (design) involves requirements development for functional testing, support equipment and software. For Space Station Processing requirements are known as "Assembly, Checkout, Operations and Maintenance Configuration" (ACOMC) or Operational Maintenance Requirements and Specifications (OMRS). During Phase D (development) test schedules are baselined, integrated test procedures and test support products are developed, team members are identified and a console team is formed, test site preparations are completed, and off-site risk reduction activities are performed at the ISS Software Integration Lab. All pre-test (constraints review, readiness review, and pre-test briefing) and test activities are performed during Phase E (Operations). Phase F is the closure phase. The post-test debriefings are conducted, all paper is dispositioned and closed, and lessons learned are gathered.

MEIT 1 included 3A (Z1 Truss/Pressurized Module Adaptor #3), 4A (Integrated Electronics Assembly/P6 Long Spacer), 5A (US Lab), 5A.1 (Racks), 6A (Space Station Robotic Manipulator System), Flight Emulator (Node), and CITE (Cargo Integration Test Equipment). There were six configuration changes in MEIT1. MEIT 2 included 8A (S0 Truss/Mobile Transporter/Mobile Base System), 9A (S1 Truss), 11A (P1 Truss), 12A (P3/P4 Trusses), Flight Emulator (Node and US Lab). MEIT had five different configurations. MEIT 3 included 10A (Node 2), 1J (Japanese Experiment Module – Pressurized Module), and the Flight Emulator. Each of these includes regression testing for requirements that were not met due to time constraints or technical issues and needed to be re-tested.

ISS Utilization/Research

Payloads/experiments can be accommodated in Facility Racks, EXPRESS Rack/Pallet, Mid-decks, and as Attached Payloads which connects them to the United States International Standard Payload Rack Checkout Unit (USICU) in the SSPF Intermediate Bay. The USICU emulates the ISS. The verification and acceptance testing that is performed is the final payload-to-ISS functional interface testing and EXPRESS experiment-to-EXPRESS Rack functional interface testing. The USICU connects to the Payload Test and Checkout System (PTCS), which emulates the ground systems. PTCS includes an Enhanced Huntsville Operations Support Center (HOSC), which acts like the MSFC Payload Operations Integration Center (POIC).

ISS Re-supply and Return

The purpose of Re-supply and Return missions is to transfer racks, cargo, and Orbital Replacement Units to and from the ISS in order to keep the ISS operational and to maintain a capability for the ISS to conduct scientific research. Typical material transferred to and from the ISS includes: Science Payloads/Experiments; Flight Crew Items (food, clothing, personal hygiene, etc.); Logistics Items (tools, replacement parts, ORU, etc.). All of the items are transferred in a Multi-Purpose Logistics Module (MPLM).

MPLM Processing Flow

The first step in the MPLM processing flow is performing system tests and configuring the module to support its next flight. Mission specific experiment racks and stowage racks are then installed and verified to be functional. Integrated system checks, closeout activities and leak checks are performed. The MPLM, fully loaded with supplies, is then installed into the payload carrier, rotated to the vertical position and transported to the launch pad for integration with the Space Shuttle payload bay. Once the Space Shuttle is docked to the ISS, the MPLM is lifted out of the payload bay and berthed to Node 1 on the ISS. The hatch is opened and the logistics are transferred. Returning experiments and trash are then stowed in the MPLM. Once back on Earth, time critical removals are destowed. The MPLM is then removed from the Space Shuttle and returned to the processing facility to be deconfigured, after which the processing cycle starts over again (NASA, 2004).

The Test Control Monitor System (TCMS) is utilized for all of the testing described above. TCMS consists of integrated networks of computers, software, data communications devices, displays, and controls required to control and monitor flight systems Ground Support Equipment (GSE) in direct support of International Space Station (ISS) ground operations at KSC. TCMS emulates Mission Control Center - Houston (MCC-H) during local test operations and is a sub-set of S-band downlink telemetry.

Launch Pad Operations

Launch Pad operations involve performing activities that must be accomplished prior to Launch Countdown. These activities include: loading hazardous storable propellants, installing ordinance, performing unplanned maintenance activities and checkout of the integrated shuttle system. Prior to loading hazardous storable propellants, ground personnel suited in special protective gear service ground support equipment and perform facility-to-vehicle connections. Loading can only occur after these preparations have been completed. During loading operations, automated ground software cycles valves as needed to maintain a strict pressure and temperature profile. Since the amount of propellant transferred to the orbiter’s tanks cannot be directly measured, ground software performs complex calculations using pressure, flow rate and time to determine the actual density and amount of propellant loaded.

Final checkout of the integrated shuttle system includes performance of leak checks, hydraulic system conditioning, Inertial Measurement System calibrations, and payload end-to-end testing. Performing leak checks and isolating leaks to specific components is a particularly difficult task.

The lack of sensing capability makes it difficult to directionally isolate the leak and determine its leak rate.

Ordnance loading requires the shuttle to be powered down and the launch pad to be cleared of non-essential personnel.

Launch Countdown

Launch countdown involves powering up systems, configuring them for liftoff and performing final verification that that they are ready to support the launch and the mission.

One of the most hazardous launch tasks involves loading cryogenic hydrogen and oxygen into the external tank. Strict temperature control is maintained during cryogenic operations, and is particularly critical during oxygen loading. Excess heat buildup in the oxygen system can lead to bubble formation which will travel up the feed line on the outside of the External Tank (ET). A "water hammer effect" will occur as the bubbles burst at the orbiter/ET interface where the plumbing makes a 90 turn. A "water hammer effect" can be of sufficient magnitude to cause the line to rupture with catastrophic consequences.

The dynamic nature of cryogenic propellant loading requires continuous evaluation of system health to identify anomalous conditions. This evaluation is performed by comparing current data to data obtained during previous loading activities performed on the given shuttle. The harsh environment created by cryogenic activities usually causes multiple hardware failures during each propellant loading. These hardware failures must be identified, assessed, and remediated. The types of hardware failures most often observed are: leaks, loss of electrical continuity due to pin contraction, and sensor errors caused by impedance or resistance changes.

Expendable Launch Vehicle Processing

The Lockheed Martin Atlas V Evolved Expendable Launch Vehicle (EELV) team successfully completed its inaugural flight of the Atlas launch vehicle on August 21, 2002. The first Boeing Delta IV EELV lifted off on November 20, 2002. These first flights culminated the five year development of new expendable launch systems, and mark a major milestone in the modernization and improvement in Integrated System Health Engineering Management (ISHEM) performance, reliability, efficiency, and cost effectiveness of the U.S. space launch fleet.

A key philosophy of the EELV program is to utilize ISHEM techniques instead of just Integrated Vehicle Health Management (IVHM). The ISHEM includes Integrated Health Management (IHM) in the Launch Site Testing Systems, Integrated Work Control Systems and on the vehicle

The EELV System Integration Laboratory (SIL) contains a complete set hardware and software for airborne and ground systems that is linked to the launch vehicle integration facilities for health management testing including anomaly resolution. A key difference between a re-usable launch system and an EELV is that components and boxes are only flown one time. There are no re-use or lifecycle requirements for the EELVs. Anomalies from a wear and tear standpoint do not typically exist for EELVs. However, it still makes sense to capture vehicle performance data in a Systems Engineering Database (SEDB) for comparison to similar components from the same development lot. The SEDB is closely tied to the electronic requirements database for each mission and can create a snapshot system engineering configuration for anomaly resolution. Many times during anomaly resolution, the problem may present itself in multiple systems and is difficult to troubleshoot down to an individual component. The integrated data systems allow the troubleshooting team to review a slice of time to quickly understand the exact configuration of the vehicle at the time the anomaly occurred. This capability is only possible through the use of the ISHEM.

ISHEM can only be effective if it receives a comprehensive set of data from testing and flight. This requires that test data and flight performance data be saved in a format that a common automated data mining tool can recognize. EELV testing at the launch site is performed using an electronic (paperless) procedure system. During each test step, test data is automatically captured, formatted and saved in the events database so that it can be easily retrieved for automated health management troubleshooting. It is possible to take snapshots of the same event from testing or flight performance and overlay the period of performance to look for the differences. The electronic procedures include embedded metrics that can enhance problem understanding.

The EELV program recognizes the value of ISHEM and has attempted to integrate this philosophy into the Launch Site, launch vehicle, testbeds, procedure systems and data management. Through the first 10 flights of the EELVs, ISHEM has helped identify processing efficiencies thus leading to large reductions in program costs.

Integrated System Health Engineering and Management

Integrated System Health Engineering and Management will greatly improve safety, mission effectiveness and supportability over current launch site HCHEM techniques when applied to future launch systems. ISHEM will tackle the problem space with an integrated scope, instead of focusing on one problem domain area. It will also provide an engineering approach to determining system health and will incorporate specific requirements and design solution space to adequately cover the integrated scope. Finally, it will provide a management function that will do more than just annunciate problems; it will work with the system's control authority to initiate remedial actions. Some specific areas that need to be addressed for future or derived launch systems are discussed below.

Sensing

Advances in sensing capability are needed to provide detection and isolation of defects such as cracks, weaknesses, and scratches in sealing surfaces. These advances must be accomplished without adding weight to the spacecraft or increasing power usage. Advances are needed in how failure mechanisms are directly sensed. For example, how do you sense the physics of a given failure as opposed to just monitoring the effect of the failure in the component? To illustrate this point, sensing technologies are needed that can detect when the tolerance between a valve piston and cylinder have changed or the spring constant has become degraded instead of just monitoring valve functions such as open and close indications.

The change in valve piston-to-cylinder tolerance and degraded spring constant will ultimately lead to valve failure; however, they are extremely difficult to detect using current sensing technology.

Integrated Data Environment

Adequate monitoring and health determination require both current and historical data. An integrated capability is needed to easily access real-time and historical data based on a given part number and serial number or based on a given event. The current approach indexes data based on its vehicle location. For example, a measurement identification might be V51P0088C1. "V51" indicates that this measurement belongs to the orbiter Landing and Deceleration System. "P" is a pressure designator. "0088" is its Landing and Deceleration System measurement location and "C1" is the data path the measurement takes to get to the ground. This measurement identification is not easily correlated to a component after it is removed and placed in another location. This approach is not only inflexible; it is incapable of correlating data with a specific component. In an integrated data environment, the measurement would include metadata that would provide access to relevant data for any given component regardless of where it is located.

Configuration Data Automation

An ISHEM Configuration Data Automation capability would integrate measurement data, metadata and logistical data. The ability to track pertinent component configuration data is required to automate health assessment and improve situational awareness. For example, configuration data can be used to automatically track component power-on time. If the component fails after a given number of power-on hours, then all components with the same part number and comparable power-on hours must be evaluated. This would also aid in tracking hardware designated as Limited Operating Life Items (LOLI). This analysis today requires manual integration of data derived from multiple resources. Some of these resources currently provide limited data collection tools. Another candidate for improving configuration management can be found in the ISS Electronic Connect/Disconnect Log (ECDL). Currently ECDL data is manually entered in a database after a connection is mated or de-mated. Correlating a connector entered in the ECDL to a drawing can be a time consuming and labor-intensive operation. Integrating the vehicle drawings with ECDL information would provide significant time savings by automating the process of linking connector mates and demates to a vehicle drawing. A final example where configuration management can be enhanced is by providing an automated process for updating drawings and procedures whenever the contents of Re-supply Stowage Platforms (RSP), Re-supply Stowage Racks (RSR), or drawers are changed. Currently drawings and procedures must be manually updated, and weight and center of gravity measurements recalculated anytime something is removed or added. Linking these items would significantly improve configuration management.

An ISHEM Configuration Data Automation capability is needed that will integrate all sources of configuration data with other relevant data. For example, integrating component configuration data with its historical data would improve the ability to make detailed and refined health assessments.

Launch Site Abort and Emergency Egress

The goal of Launch Site(LS) and Launch Vehicle(LV) ISHEM systems are to increase survivability and significantly reduce the probability of Loss of Crew (LOC) by providing an advanced warning of incipient failure. The crew is defined as both the ground personnel who support launch operations and the astronauts.

ISHEM must have access to the appropriate level of LS and LV data to detect a failure or failure trending. The data provides the Spacecraft ISHEM with situational awareness of trends toward failure and provide an abort recommendation if a failure occurs that can have catastrophic consequences. The spacecraft can use this data to make a final abort initiation decision on the pad. In order to detect a failure or degradation of the LS or LV system, the following determinations must be made:

- What failures could occur along with their probabilities of occurrence
- What effects the failures will have on the system
- What concurrent failures can be detected
- What failures can not be detected and what needs to change in order to detect them.

A unique opportunity exists to truly integrate ISHEM into the LS and LV systems. During the initial system engineering requirements development phases of a program, analyses will need to be performed. The analyses include Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL), Hazard Analysis, Probability Risk Assessments, Fault Trees, and Fishbone (cause and effect) diagrams.

The FMEA/CIL utilizes a bottom-up approach to analyzing the effect of failures on a system and, when included as part of a reliability assessment, the probability of occurrence. The FMEA categorizes the LS and LV systems based on their criticality. The CIL documents components that are defined as criticality 1 or 2 and includes a list of single point failures. The CIL requires the development of retention rationale for listed components. Information in the FMEA/CIL aides in identifying system components that require health monitoring.

All of these analysis products serve as inputs to a Fault Coverage Analysis (FCA). The goal of the FCA is to:

- Map failure modes to existing detection mechanisms
- Identify gaps in which potential failures would not be detected
- Identify the fault tolerance of the detection methods being used (single string or no fault tolerance, single redundant, dual redundant, dissimilar redundancy, etc.)
- Identify ways to corroborate failures (e.g. through redundant sensors; by using disparate detection methods through independent systems).

The results of the FCA are vital to the successful design of an ISHEM system. These results can be used to:

- Determine existing sensors that LS and LV should monitor
- Determine if and where sensors should be added to detect unmitigated failure modes
- Determine if corroborating sensors should be added to increase measurement reliability and prevent false indications.

The FCA as well as the products feeding into the FCA must be updated throughout the program lifecycle. It is critical for a feedback mechanism to exist that provides the means to update the FMEA/CIL/FCA to reflect any system changes that occur as the ISHEM evolves, Analyses of these changes may drive updates to the hardware or software. The development of supporting analysis products should be undertaken prior to preliminary ISHEM design.

In conclusion, the primary task of the LS and LV ISHEM is to provide a message to the spacecraft and to the ground control system so that the integrated system can implement an abort or emergency egress in sufficient time to prevent a Loss of Crew. Since the LV and LS ISHEM are only one link in this chain, a “time budget” should be established for abort and emergency egress messages. This time budget must be critical to the ISHEM design and the overall success of the emergency escape system.

Summary

Many ISHEM opportunities exist for future or derived vehicles that will be processed and launched at the launch site. This paper has merely scratched the surface by providing some of the higher priority ISHEM needs. Additional information on launch site health management needs can be found in the following documents: the Advanced Spaceport Technology Working Group (ASTWG) baseline report (Guidi 2003, p1-80) and the Advanced Range Technology Working Group (ARTWG) report. (Skelly 2004, p1-80) These reports were generated by national working groups composed of leaders in industry, academia, and government.

Past health management focus has been concentrated on the vehicle side such as Integrated Vehicle Health Management, Integrated Intelligent Vehicle Health Management; however, many opportunities exist for ground and launch site health management. The Evolved Expendable Launch Vehicle program has made many advancements over the legacy Space Shuttle and International Space Station programs. Future development activities to derive new launch vehicles must expand the ISHEM envelope. A truly Integrated System Health Engineering and Management system can only be developed and successfully implemented when both the ground and vehicle requirements are jointly considered during the design process.

McCleskey, Carey, 2005, *Space Shuttle Operations and Infrastructure – A Systems Analysis of Design Root Causes and Effects*, NASA/TP-2005-211519

NASA, 1995, *Interim Problem Report 069V-0037 “1995 OMS Fire during fuel feed line disconnect from thruster RIA”*

NASA, 2004, *Kennedy Space Center ISS/Payload Processing Directorate Overview*

Maclise, Dougal, Wilson, Scott, 2004, *Orbital Space Plane Integrated Health Management Summit Results, Recommendations and Lessons Learned*

Guidi, Cris, 2003, *Advanced Spaceport Technologies Working Group Baseline Report*

Skelly, Darin 2004, *Advanced Range Technologies Working Group*