Commercial Crew Launch Emergency Detection System The Key Technology for Human Rating EELV

Michael Holguin, Gary Herbella, and Rick Mingee
United Launch Alliance (ULA)
9100 E. Mineral Avenue
Centennial, CO 80112

Abstract

In February of 1962, John Glenn was the first American to reach earth orbit, lifted into space aboard an Atlas rocket. The most significant change to human rate the early Atlas launch vehicle (LV) was the addition of an Emergency Detection System (EDS) known as the Abort Sensing and Implementation System (ASIS). ASIS monitored 13 basic LV health measurements and could send a signal to the Mercury capsule to escape if an emergency arose. Now, in partnership with the NASA Commercial Crew and Cargo Program Office, ULA is re-creating that capability. Moreover, United Launch Alliance is flying even more reliable and fault tolerant LVs than John Glenn flew.

In 2010, ULA was awarded a Commercial Crew Development (CCDev) contract to develop a high-fidelity EDS testbed and demonstrate that system in the Atlas V LV systems integration laboratory (SIL). Over the past several years, ULA has expended significant efforts to ensure that the EELV fleet is compliant with human spaceflight requirements. Atlas V and Delta IV are well suited to support crew abort scenarios since they are both liquid propellant engine systems that can be shut down in a catastrophic event EDS is the critical technology and key enabler to safe commercial human spaceflight using the mature, reliable EELV transportation system to Low Earth Orbit. In the unlikely event of a LV failure, the EDS provides the crewed spacecraft sufficient advance warning to safely abort, as well as safing the LV by shutting down the liquid rocket engines to terminate thrust and minimize danger to the crew during the abort maneuver. This development effort is a required step along the way to a fully human-rated EELV system, and it is part of an overall Atlas and Delta LV evolution plan that builds on today's success to provide a safer and more capable crewed launch solution. ULA is working in partnership with NASA and several other CCDev partners to ensure that EDS capability on the flight-proven EELV fleet can support its unique crewed spacecraft designs.

I. Introduction

In March 2010, ULA began work on a prototype Emergency Detection System (EDS) demonstration effort under a Space act Agreement that we were awarded as part of the Commercial Crew Development (CCDev) effort. Detection of an impending catastrophic situation and warning the crew are not new concepts in human spaceflight rocket systems. Nor is it a new technology or capability in aerospace or other applications. In fact, EDSs are used in everyday life, from accelerometers in cars that sense a crash and deploy airbags, to airplane collision warning systems and smoke detectors in our homes. Each emergency detection system is designed to notify and/or protect the occupants from hazards in a timely manner, "safing" the system and/or enabling the occupants to get away from the hazard, guarding against loss of life or limb. In a crewed launch vehicle (LV), the detection of an impeding catastrophic failure is extremely time critical, measured in fractions of a second for the worst case to many minutes in others, and the results of a failure can be dangerous to crew safety. This paper discusses three main topics: (1) the overall approach to an EDS implementation for the existing flight proven EELV fleet of LVs, (2) the approach to developing a comprehensive fault coverage analysis identifying and determining timing and effects of potential failure modes that are hazardous to the crew, and (3) an overview of the proposed EDS architecture for EELV.

II. Emergency Detection Approach to Crew Safety

The fundamental tenets of the President's proposed commercial crew program using existing LVs are embodied in two statements the current NASA administrator made during the proposed FY2011 NASA budget rollout. Excerpts from that speech are quoted below:

…"what the President has provided is a fundamental reinvigoration of our nation's exploration effort. If we are going to have the technology and capabilities needed for tomorrow, we have to invest in them today. We must harness the nation's entrepreneurial energies to fulfill our needs for access to low Earth orbit and reap the benefits of enabling those new businesses."

"Commercial launch vehicles have for years carried all U.S. military and commercial – and most NASA – satellites to orbit. Now, as 50 years ago when we upgraded existing rockets for the Gemini program, NASA will set standards and processes to ensure that these commercially built and operated crew vehicles are safe." Charlie Bolden, NASA Administrator, February 1, 2010

In fact, this is not the first time that we will use the expendable LV fleet as safe, reliable, and affordable crew transportation. The progenitors of these rockets once safely carried astronauts like John Glenn to orbit. ULA is working with NASA as a Space Act Agreement Partner in the CCDev EDS Demonstration & Development effort to ensure the development is consistent with Human Spaceflight approach. EDS is the key technology that remains to be implemented that will enable the existing flight proven EELV fleet to fly crew, in addition to certifying the LV for human rating under the Commercial Human Rating Plan. The Atlas V and Delta IV Fleet have proven themselves in over 29 successful flights since the launch of the first EELV. EELV has its heritage in over 50 years worth of processes maturation, years of evolution of systems and subsystems that increased performance and incorporated fault tolerance, reliability improvements, and the latest technology. Adding EDS to this flight proven system along with an intact abort capability minimizes risk to crew safety to the maximum extent possible. Figure 1 illustrates the main characteristics of a System-Level Crew Safety approach using the existing EELV fleet.

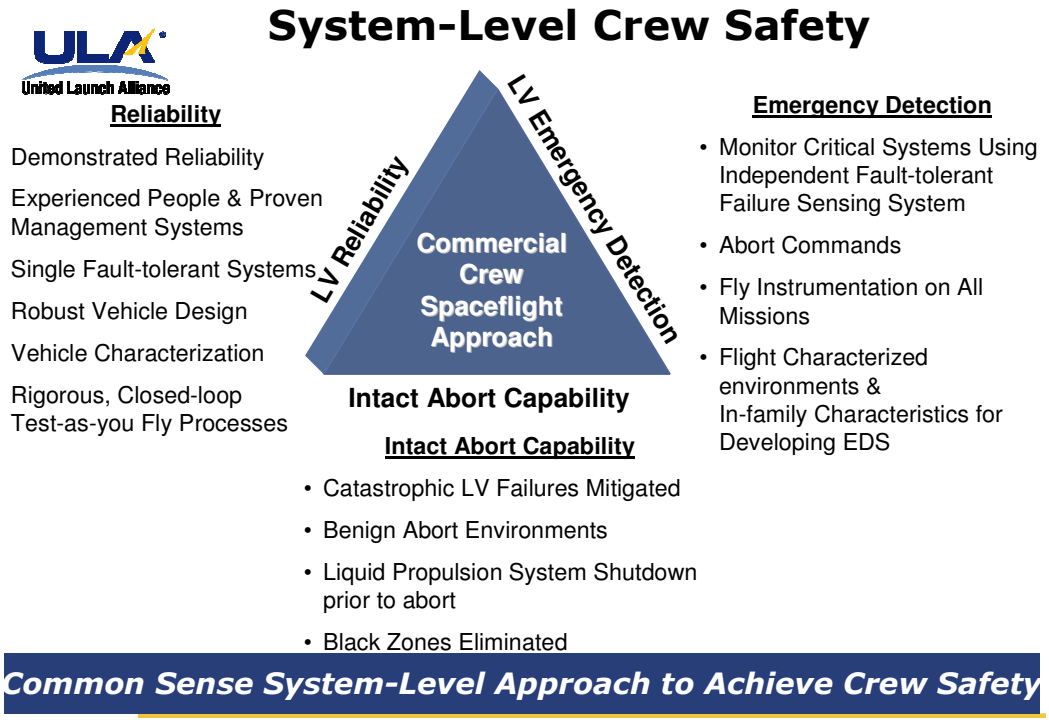

Figure 1. Main characteristics of a system-level crew safety approach using the existing EELV fleet.

III. EDS Operational Overview

EDS augments a single fault tolerant EELV launch system. Its job is to monitor the LV, detect anomalous conditions that will result in a crew safety critical situation, and, based on a predetermined set of thoroughly investigated failure modes and the associated criticality of the event, send a signal to the crewed spacecraft in sufficient time for the spacecraft to abort and get safely away. EDS monitors only those potential LV events that are Criticality 1 crew safety hazards. LV Emergency Detection is not intended to provide any maintenance-related LV prognostication or redundancy management in the form of LV reconfiguration. The existing LV design integrates redundancy management and reconfiguration functions within the current system and subsystem architecture. The EDS design takes advantage of the fault tolerant technology that exists within the current LV and experience in

evolving multiple generations of Atlas and Delta LV configurations, combining that with upgraded sensors and technology as appropriate.

The key function of the EDS is to notify the crew of an impending or occurring degrading condition as soon as detected and issue an abort signal to the spacecraft when the situation becomes critical. At the same time, the EDS initiates LV engine shutdown prior to spacecraft separation. In addition, if a failure has occurred but the situation is not immediately safety critical, the EDS will issue a caution including an estimated time to abort based on the failure mode itself. This information will be augmented with other "actionable" situational awareness information that the flight and ground crew can use to determine next actions: (1) inhibit a potential abort (if the situation will not manifest itself prior to reaching orbit or other safe state (e.g., staging of malfunctioning system); (2) immediately abort due to other information (e.g. spacecraft condition, phase of flight, etc.) ; and 3) monitor the situation prior to further action from the ground or flight crews. However, if no crew input is received, the EDS is intended to function entirely without human interaction, making abort recommendations to the spacecraft to initiate the separation and abort sequence if the crew is incapacitated or when no time for reaction is possible. The system also allows the crew to initiate an abort on the spacecraft side of the interface, which will also safe the LV (engine shutdown). It also allows them to inhibit an abort if the situation warrants it.

On the flip side, the EDS must also be able to discern false indications of a degrading system – hence the need for a corroborating set of measurements that validate the any indication of failure or degradation of any one system. It's critically important to protect lives, and also important to protect mission success. It's a bad day to have to abort due to a systems failure, but also a bad day to abort off of a perfectly good rocket for a false abort indication. A redundant systems architecture helps guard against both situations.

Because the operational concept relies on the spacecraft to perform separation from the LV and maneuver to a safe distance, and each spacecraft abort system has unique characteristics, these must be considered in the design of the overall system. ULA has been working with NASA and several of the commercial crew partners to understand the characteristics of proposed crewed spacecraft to ensure compatibility with their systems.

To support the spacecraft Mission Control Center in assessing LV performance and making timely flight critical decisions, ULA will have engineering teams with experts in each system monitoring the LV performance in flight from down linked telemetry. These teams will be located in the launch control facilities at Cape Canaveral, augmented by engineers in the Denver launch control support center. LV performance will be communicated to the NASA and spacecraft teams at their launch control facilities. Figure 2 shows that this is consistent with the EELV operational construct today.

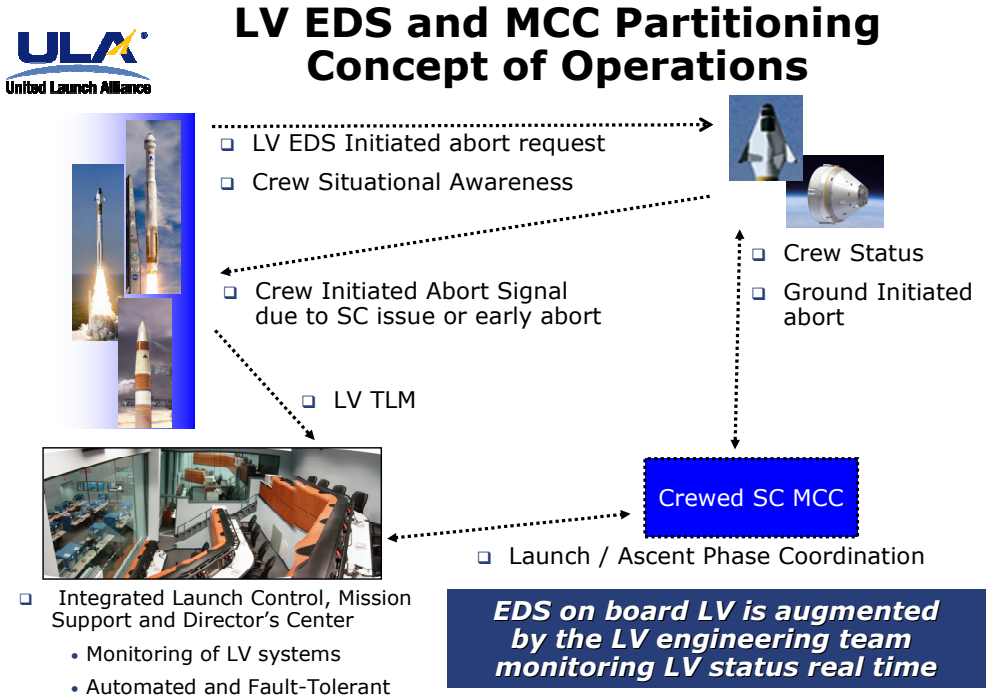

Figure 2. LV EDS Concept of Operations

One key benefit of using the existing EELV system is that the operation of EDS can be validated over many flights if it is flown in passive mode, piggybacking on non-crewed EELV flights. The risk to existing missions flying this in piggyback mode is made inconsequential by integrating the EDS into the existing architecture with minimal intrusions, not disturbing the function of the current vehicle.

Other aspects that enable the EDS in the current EELV fleet include the fault coverage analysis that determines failure modes critical to be monitored and associated timing and failure characteristics, and the common architecture that can be integrated into the Atlas and Delta system architectures to maintain the integrity and flight-demonstrated reliability.

IV. Approach to Developing a Comprehensive Fault Coverage Analysis

Determination by an Emergency Detection System that an emergency condition has arisen within a highly energetic and dynamic LV first requires a full understanding of the failure mechanisms inherent in the LV design and the hazards to the crew for of any of those failures. A comprehensive assessment of these characteristics can be used to determine which measurements can provide the timeliest evidence of these faults. These can then be prioritized to obtain the optimum fault coverage for the EDS to act on.

ULA has an extensive set of analytical and empirical data regarding potential failure modes and system reliability. Those data were analyzed in previous activities to provide system confidence assessments for high value (and/or loss critical) missions such as the Pluto New Horizons spacecraft, which contained nuclear material for its power supply. These were bottom-up approaches, starting with specific failure modes and ending with system-level impacts, as shown in Figure 3. The resulting Probabilistic Risk Assessment (PRA) includes a Master Logic Diagram, which documents system-level failure events as a function of subsystem and component level faults.

The fault-coverage assessment process in the CCDev EDS project expands on failure mode and fault coverage work performed over many years and focuses on system reliability.

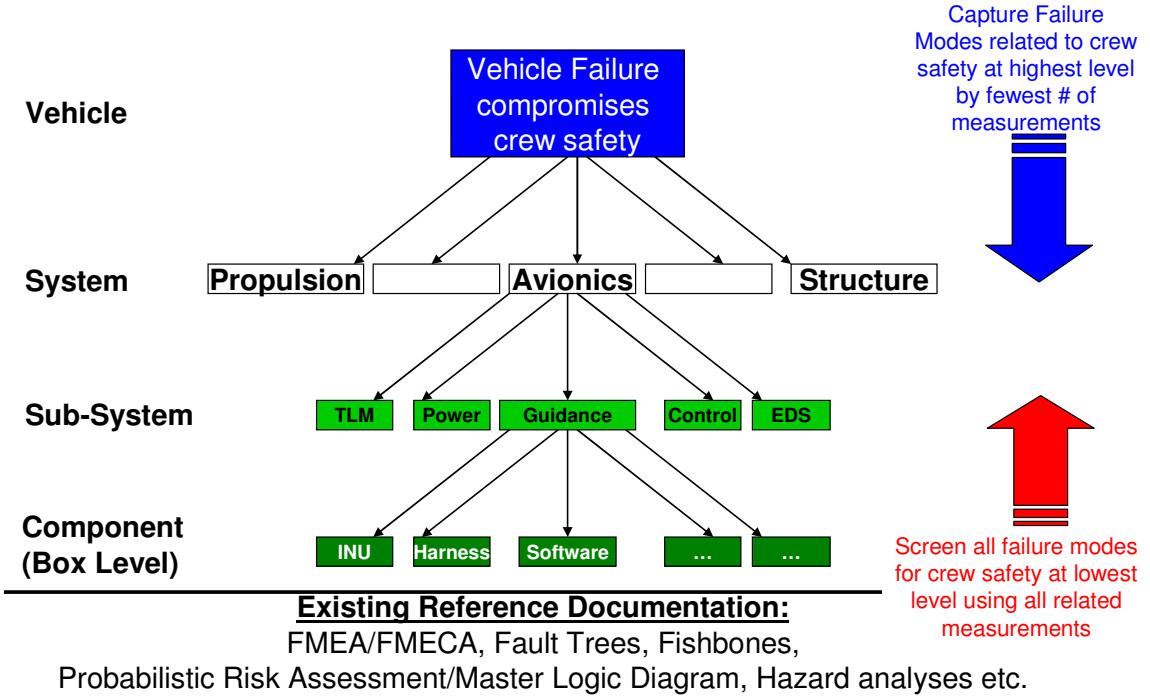

Figure 3. Bottom-up approaches start with specific failure modes and end with system level impacts.

For human spaceflight, the emphasis becomes crew safety. While system reliability provides a large measure of crew safety, the implications of any remaining risk in the design, manufacture, or operation of the LV dictate additional measures to ensure minimal overall crew risk. Thus, starting with crew hazards and evaluating the failure modes that contribute to those hazards is a top-down effort in contrast with the bottom up approach that begins with failure modes and assesses the impact of those failures on crew safety. The difference in perspective surfaces relevant failure modes that look at system level interaction and may be different from the reliability-focused, bottom-up assessment.

The top-down approach is consistent with NASA's Return to Flight approach after the Columbia accident, in contrast to the bottom-up approach taken after Challenger. The reality is that a combination of both approaches is needed to ensure thorough fault coverage, so it is anticipated that a validation of the top-down results will include a bottom-up assessment.

As shown in Figure 4, the sum of the time it takes to sense an emergency condition and generate an abort signal plus the time for the spacecraft to separate itself sufficiently from the LV must be less than the time it takes for that early indication of a problem to propagate itself to the point compromising crew safety (the Time to Criticality (TTC). The goal is to sense and respond to emergency conditions as quickly as possible.

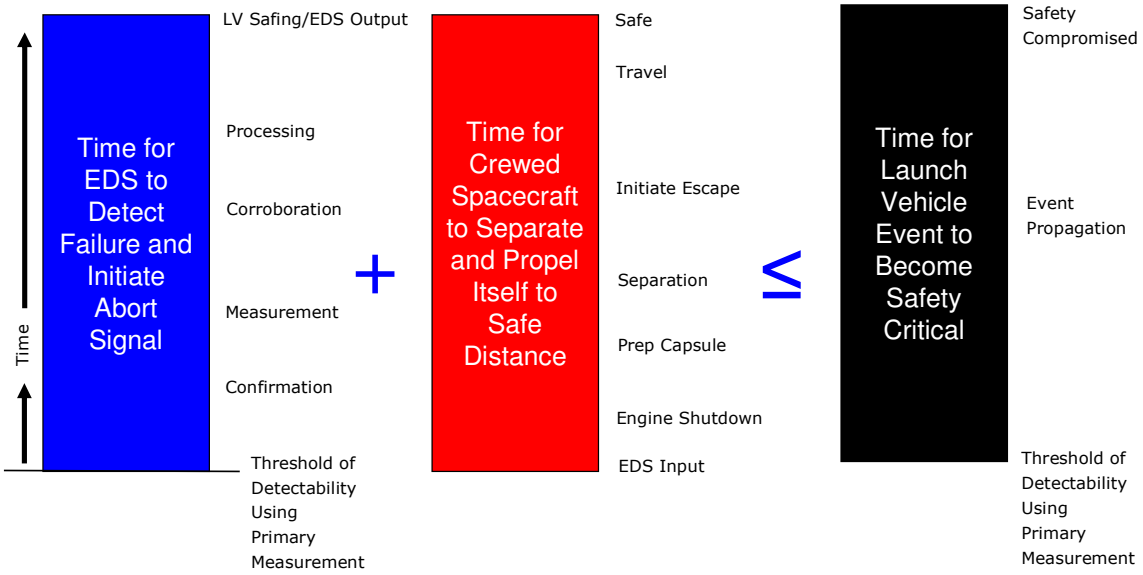

Figure 4. The goal is to sense and respond to emergency conditions as quickly as possible.

With this ultimate goal in mind, the EELV Fault Coverage Assessment process began by enumerating the specific hazards that could endanger the crew, taking a top-down view. Crew safety hazards are a result of spacecraft conditions, which are in turn a function of the environment around the spacecraft, to which the LV is a contributor. The conditions of the LV that contribute to crew safety hazards through this chain of connectivity was documented graphically to describe how each hazard links to a finite set of LV anomalous conditions. The majority of the LV hazard conditions are consistent with the existing PRA results, with the addition of crewed spacecraft-specific hazards such as spacecraft induced failures and crew sensitivity hazards; for example, excessive axial acceleration.

Since the crew hazard analysis links for the most part to components of the Master Logic Diagram, the underlying fault conditions are already documented. ULA performed a fresh validation of those fault conditions for both Atlas and Delta to ensure completeness, particularly given the crew safety perspective. Figure 5 shows that the process to accomplish this was an iterative process of evaluating the timeliness of measurements that would indicate a fault relative to the time to criticality of that fault condition. If the measurements (primary and corroborating) can provide timely indication of an impending hazardous condition, then that set of measurements is baselined for use in the EDS algorithms. If not timely enough, another pass through the process takes place performed, using subsystem level measurements with more likelihood of identifying the fault quickly. The tradeoff for this lower level measurement is breadth of coverage, since it is measuring only a subset of the higher-level system functionality. Where no timely measurement is possible, an assessment of the design of the system is performed to evaluate whether it is consistent with criteria for Design for Minimum Risk.

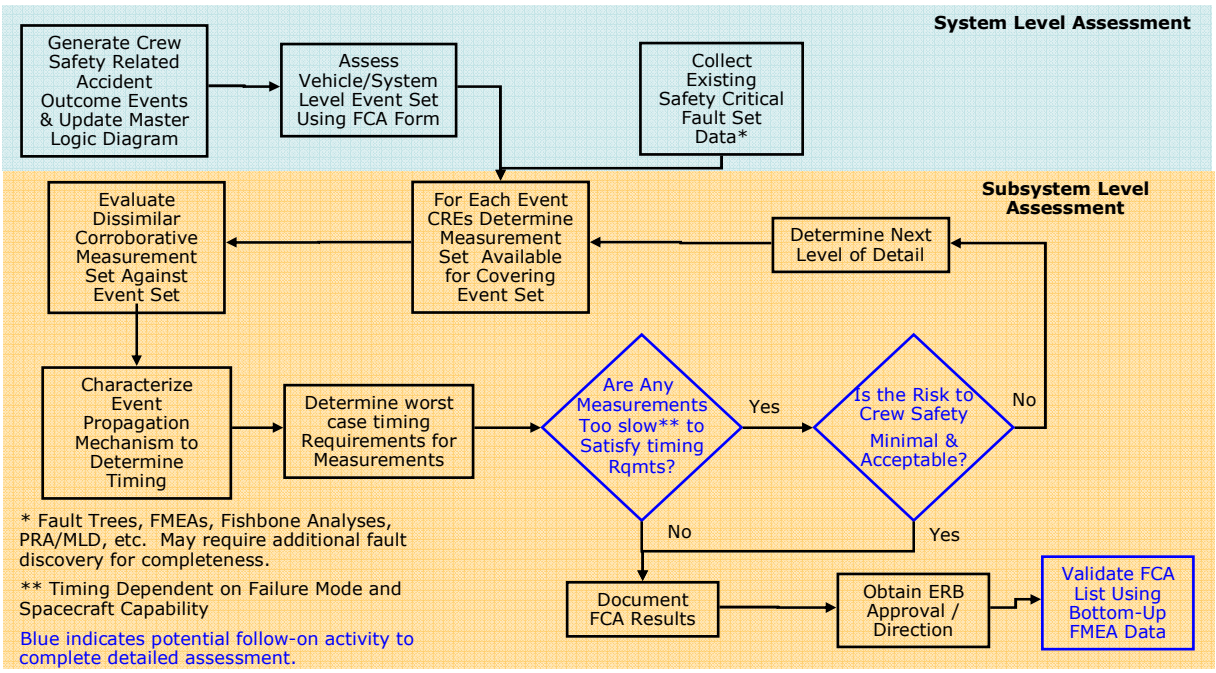

Figure 5. Fault conditions validation ensures completeness from the crew safety perspective.

V. Overview of the Proposed EDS Architecture for EELV

A. Background

Atlas V and Delta IV EELVs have been in service for 8 years. They are existing designs with long and successful flight histories. As such, the EDS must be an "add-on kit" to the existing designs; it cannot be built into a new design from the start. One very important goal, therefore, is to minimize impacts to the existing vehicles in order to preserve the flight-proven design. This goal must be carefully balanced with providing adequate emergency detection capability via the added system. Too much change threatens the existing demonstrated performance and reliability while too little change provides inadequate protection to the crew of the spacecraft.

Also important is controlling the overall complexity of the added system. The EDS must not be overly complicated in its ability to discern a failure and issue an abort signal to the spacecraft. An overly complex system has the potential to falsely declare an abort or, worse, not declare a valid abort. A minimum number of sensors and interfaces, which still address adequate safety, must be employed to address this constraint. Use of high-level sensors helps limit overall system I/O and complexity. Conversely, an overly simple system may not be robust enough to avoid declaring an abort for sensor-only failures (not vehicle failures). This area is addressed by applying sensor fault tolerance, voting, and corroboration, such that no single measurement failure will generate an abort.

The function of EDS is to detect and act on any monitored failure at the earliest opportunity and at the highest level of measurement capability as time permits for a given failure scenario. High-level sensors are preferred (i.e., attitude, rates, acceleration, etc.) as they offer broad fault coverage and address numerous failure modes. However, lower-level sensors may be required to provide earlier awareness and timing margin.

With these constraints in mind, the basic approach is to add new electronic monitoring boxes that access existing vehicle sensors to assess (via software algorithms) if the LV is performing acceptably or not (and if not, issue an abort signal to the spacecraft). Existing sensors are preferred (versus adding new ones) wherever possible as their data are based on previous flights and they have known performance. Anomalous trends are easier to detect with known sensor performance.

B. Current Architecture Considerations

As the EDS is critical for human safety, it must be a minimum of single fault tolerant (including transducers/sensors, transmission paths, processing, etc.). This level of fault tolerance matches the existing LV architecture. This includes single fault tolerance for issuing a false abort signal as well as single fault tolerance

against preventing initiation of a valid abort signal. Thus, failure detection by sensors is expected to be corroborated via separate, independent measurements as much as possible.

To meet the above requirements, ULA uses an overall EDS "Series-Parallel" approach. Two physically separate processing units provide parallel coverage. Either can independently detect a failure and generate an abort signal. One of the two units functions under a single failure scenario. To guard against accidental abort, series (multiple) inhibits as well as high-level signal encoding are used for issuing signals. No single EDS failure will cause an unintentional abort. In addition, there is a fail-safe design approach within each EDS unit such that internal failures do not generate or require an auto-abort. Fail-safe in this context means no auto-abort action. As there are two physically separate units, there is no need to generate an auto-abort for failures within one unit because the remaining unit is fully functional. Faults within EDS are not grounds for an auto-abort and are not an indication of off-nominal LV performance. Online/offline health and status of each EDS unit are provided to the spacecraft.

The following system-level features are included in the architecture:

1. Two fully redundant, physically separate chains,
2. Independent unit power, redundant sensor monitoring (1553, analog and discrete) including GNC/GPS sources,
3. Self-checking pair processor sets to perform EDS as well as Autonomous Flight Safety System (AFSS) and Flight Termination System (FTS) functions,
4. Interfaces to provide real-time telemetry status and EDS health and status to/from the spacecraft (including the spacecraft-sourced abort command), and
5. Propulsion system shutdown signals for LV safing during an abort.

Figure 6 depicts a system-level architecture. The EDS component internal designs and architecture are based on existing, heritage technology, and proven designs already in use on the LV. New technology is not required. Existing design standards, practice, and experience are being used to development the EDS, which leverages proven design-to-production engineering and manufacturing processes.

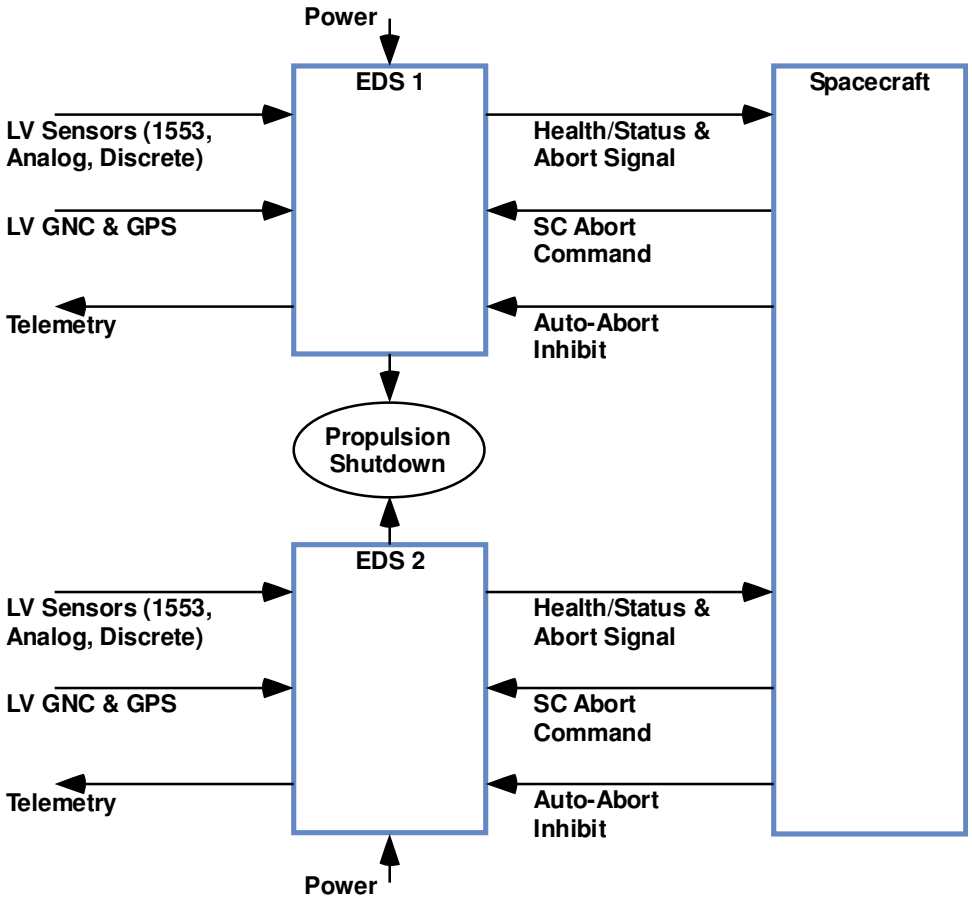

Figure 6. Overall EDS System Architecture

C. Spacecraft Interfaces

The EDS must support the Atlas V and Delta IV EELVs with a common design. In addition, it must support multiple spacecraft providers, each with individual interface requirements. This requires a generic and flexible LV interface in order to accommodate the various users. Programmable RS-422 interfaces are planned as they can convey a large amount of data over a small and manageable electrical interface. They also allow for robust message protocols, which minimizes the likelihood of acting on potential errors. As the interface is programmable, it will allow specific data to be routed to the spacecraft depending upon requirements.

The EDS supports a LV auto-abort mode (LV detected faults), but it must also support spacecraft-originated aborts as well. Spacecraft aborts can be auto-detected in spacecraft hardware or via manual crew interaction (i.e., button push), with the resultant command sent to the LV EDS to initiate the abort mode. The EDS also supports an "Auto-Abort Inhibit" function from the spacecraft. If a condition is detected by the LV that is not an immediate auto-abort but is trending towards an abort threshold in the future, the crew has the ability to inhibit an abort for this condition and allow the mission to continue. While inhibited, if the condition does transition into the abort limits, no action is taken by EDS. If the inhibit is removed while the condition is inside the abort limits, an auto-abort will occur. This inhibit feature is not required on a per-measurement basis but rather on a per-abort-criteria (group) basis, so that select failures may be inhibited without losing total EDS monitoring. This reduces the overall complexity by not having to provide an inhibit function for every single measurement on the LV. As an example, suppose a subsystem monitored by three measurements indicates an issue and generates an appropriate caution signal. The Flight and Ground Teams determine the situation is not a concern and the crew desires to inhibit the possible abort. The "three measurement subsystem" is inhibited (not each measurement) so this entire monitoring "leg" can no longer cause an abort action. All other monitoring continues in case a separate issue occurs which EDS must take action on. It is also possible to "un-inhibit a previously inhibited abort criteria if warranted.

EDS health and status data are transmitted to the spacecraft and displayed in the crew area. EDS provides typical items such as trajectory, position, and attitude to the spacecraft displays, along with overall health of the various subsystems. Specific data content will be worked out with each spacecraft provider to optimize displays and monitoring. Data sent to the spacecraft will likely be somewhat high-level and provided only if useful in real time decision making by the flight crew (i.e., a subset of total vehicle data). EDS down links full LV telemetry data to the Ground Flight Control Team for use in anomaly resolution.

D. Prototype EDS Testing

The Atlas System Integration Laboratory (SIL) currently performs preliminary testing of a prototype EDS. The prototype consists of existing flight-proven Single Board Computers (SBC) utilizing self-checking pair microprocessors. It is connected to the LV 1553 control data bus as a Bus Monitor. The prototype EDS monitors the 1553 bus traffic, looking for data from monitored measurements, and inputs the necessary data into the EDS software algorithms. The algorithms perform sensor voting, down-select, and pass/fail limit checking (including persistency). The software outputs an abort signal when the correct quantity of sensors, with persistency, is out of pre-defined allowable limits. This abort signal triggers a shutdown of the LV propulsion subsystem. It is routed to the spacecraft interface for notification of the abort mode. Using the SIL, various failure modes can be injected into the system and the associated response monitored. Failure scenarios currently addressed include loss of thrust, excessive rates/attitude, off-nominal trajectory performance, and propellant tank leak issues. This initial prototype-testing phase is planned to continue through November 2010.

VI. Summary

The CCDev EDS system is an evolved technology similarly demonstrated on previous Atlas Mercury, Titan Gemini, and Apollo systems. EDS is the key technology to enable flight-proven, demonstrated, and reliable EELV to provide a safe crew transportation alternative to ISS and perhaps other destinations. ULA works in conjunction with NASA and other potential spacecraft providers toward demonstrating the ability to detect anomalous conditions on the LV and provide a timely abort signal to the crew. The EDS takes advantage of the latest state-of-the-art sensors and computing power to provide the most reliable system architecture. It will ultimately provide the safest possible ride to orbit for our future commercial crew astronauts.