Evolution of Abort Management of Crewed Launch Vehicles from Mercury ASIS to Commercial Crew EDS

Gary Herbella[1] and Rick Mingee[2]
United Launch Alliance, Centennial, CO

Tom Heinsheimer[3]
Colbaugh & Heinsheimer Consulting, Inc., Rolling Hills Estates, CA

The 1960's Mercury Atlas program employed an on-board emergency detection and automatic abort system called ASIS (Abort Sensing and Implementation System) that monitored precursors of catastrophic missile failure in order to automatically abort the flight if needed. The system design was based upon the knowledge that catastrophic failures of Atlas missiles were endemic. When astronaut John Glenn flew the Friendship 7 spacecraft on Mercury-Atlas-6, February 20, 1962, the success rate of the Mercury Atlas was 50%. ASIS was driven by dual imperatives — to protect the astronaut in case of imminent disaster, and to avoid erroneous flight abort of a healthy rocket. It monitored only 13 measurements, carefully selected for their broad fault coverage, reliability, and predictability.

Fifty years later, Atlas V, as one example of a Commercial Crew launch vehicle, will be safeguarded by the Emergency Detection System (EDS). The Atlas launch vehicle on-board data processing capability is orders of magnitude greater than that of the 1960's, and the Atlas vehicle has flown over 110 times through 28 years since the last failure that would have posed an immediate safety risk to a crewed spacecraft. However, the basic security and reliability concerns remain the same. Current NASA human spaceflight experience is primarily with a very different, reusable launch system which has unique failure modes and unique abort modes. As launch services to Low Earth Orbit transition to the next generation, the experience of both expendable and reusable solutions become important contributors to reliable and safe human space launch systems.

This paper explores the influence upon the EDS design of 50 years of launch vehicle experience, including Atlas, Delta, Titan and Shuttle. It describes the similarities and differences between the ASIS and EDS solutions, including design drivers, implementation technology, available measurements, and measurement monitoring strategy.

I. Launch Vehicle Emergency Detection

A. Emergency Detection Principles

Launch vehicles are inherently hazardous, with highly dynamic components creating a controlled explosion of thousands of gallons of combustible, often cryogenic liquids. The Atlas D booster that launched the Mercury astronauts weighed over 260,000 lb at liftoff, with over 360,000 lb of thrust. Today's Atlas V (without Solid Rocket Boosters) weighs over 730,000 lb at liftoff, with over 860,000 lb of thrust. During the past quarter century, the science behind rocketry has improved the design, production, and operation of liquid fueled rockets to a rate of launch success well beyond that experienced in the first quarter century of the technology. At one time it was common to carry a '20-vehicle rolling average' as a measure of the reliability of a launch system. Today there are launch systems with close to one hundred consecutive successes, and most of the failures that occur are not the catastrophic explosions that pose the greatest threat to a human crewed spacecraft. But there is still no question that the crew of a spacecraft needs to know that the launch vehicle under them is operating correctly and

[1] Systems Engineer, Project Engineering, United Launch Alliance, Denver, CO 80127, AIAA Senior Member
[2] Sr. Staff Engineer, Avionics Systems, United Launch Alliance, Denver, CO 80127, AIAA Senior Member
[3] Senior Business Strategist, Colbaugh & Heinsheimer Consulting, Inc., Rolling Hills Estates, CA 90274, AIAA Senior Member

will, should it fail, provide them the opportunity to escape before their lives are endangered. That is the function of the Emergency Detection System.

The basic principles of launch vehicle emergency detection are consistently illustrated in the selection of measurements that are monitored in real time. The highest level of monitoring which will capture as many lower level failures as possible is the most efficient method of providing a high level of crew safety. Key measurements include vehicle rates and accelerations in all three axes, as well as propellant tank pressures. In addition, specific high-energy engine characteristics such as turbopump speed can give warning of impending engine failure. The system must be capable of identifying when any of those key measurements exceed a safe-operation threshold, and then must respond promptly to allow the crew of the spacecraft the maximum amount of time to escape to a safe distance.

The following sections outline the emergency detection systems of each of the launch vehicles in NASA's human spaceflight programs, including concepts of operations and capabilities.

B. Mercury-Atlas Abort Sensing and Implementation System (ASIS)

The ASIS implementation for Mercury Atlas was simple but effective, focusing on a set of 13 measurements that covered a wide range of failure modes. Three types of sensors were used; pressure switches, rate gyros, and electrical circuit components[4].

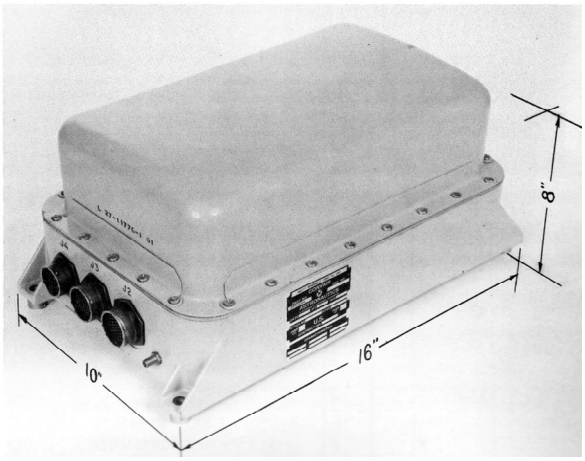

Figure 1. ASIS Flight Hardware

Pressure sensors monitored the fuel injection pressures of all three Atlas engines, liquid oxygen tank pressure, main bulkhead differential pressure, and sustainer engine hydraulic pressure. The flight control system was monitored by evaluating the outputs of two sets of three rate gyros, each with an over-rate indicator. In addition, the ASIS monitored electrical power levels.

ASIS was armed at liftoff, which allowed it to command an abort from that point on. The engine shutdown functionality was delayed until liftoff plus 30 seconds, and the system was disarmed at sustainer engine cutoff.

To accommodate Range Safety destruct commands, ASIS received a signal from the range safety receivers that indicated a destruct command had been received. ASIS then started a 3-second timer, which delayed arming of the range safety destruct system, shut down Atlas engines and initiated the abort sequence. The 3-second delay allowed the Mercury capsule to eject and reach a safe separation distance from the launch vehicle before the actual destruct occurs.

ASIS functions were monitored open-loop during the Mercury Atlas 1 mission (MA-1) on July 29, 1960. The mission itself failed, though ASIS performed nominally, generating an abort signal 1-second prior to booster explosion. A closed-loop ASIS was employed on the MA-2 mission on February 21, 1961. Telemetry indicated that ASIS performed nominally and did not generate an abort indication. MA-3, on Aril 25, 1961, was an unintentional but effective test of the ASIS ability to accommodate a Range Safety destruct command. When the booster failed and a destruct command sequence was sent, ASIS performed as designed and generated a timely abort command which resulted in successful recovery of an undamaged test spacecraft[5].

---

[4] T.F. Heinsheimer, "Flight Safety Systems for Advanced Manned Space Missions II", Instrumentation Laboratory, Massachusetts Institute of Technology, Cambridge Mass.; September 1962, pg 26.

[5] T.F. Heinsheimer, "Flight Safety Systems for Advanced Manned Space Missions II", Instrumentation Laboratory, Massachusetts Institute of Technology, Cambridge Mass.; September 1962, pp31-33.

ASIS was used for all remaining Mercury-Atlas flights, included the historic flights carrying John Glenn, Scott Carpenter, Wally Schirra, and Gordon Cooper (MA-6 – MA-9).

C. Gemini-Titan Malfunction Detection System (MDS)

Development of the functional requirements for the Gemini-Titan MDS, shown in Figure 2[6], involved detailed failure mode analyses. Determination of which of these failure modes should result in an automated abort or left to the crew to evaluate a manual abort was a function of the time-criticality of certain failures. Engine chamber pressure, tank pressure, and vehicle rate thresholds were defined for both crew display and automated abort indications.

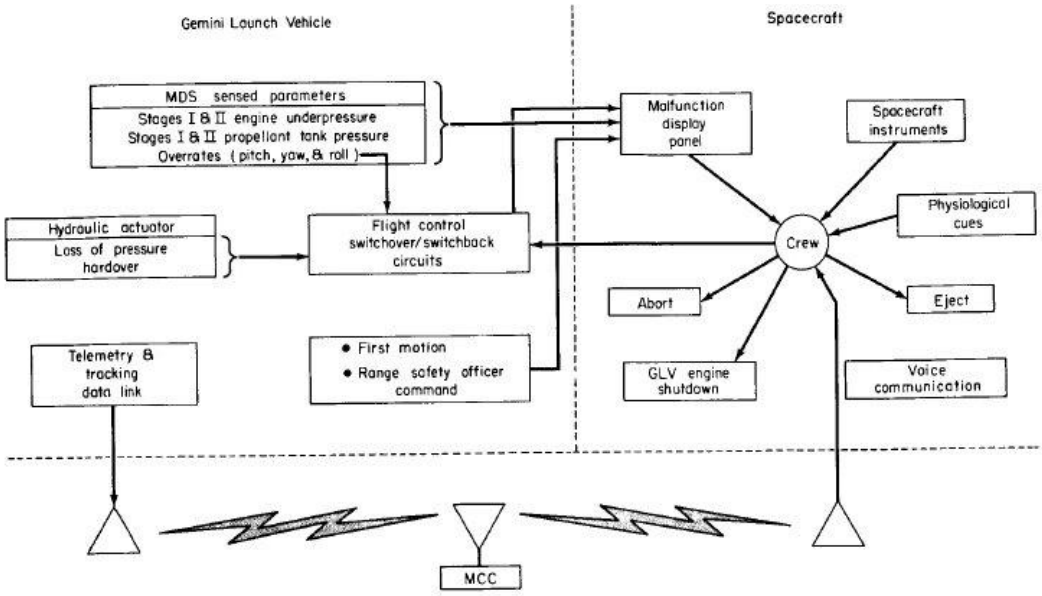

Figure 2. Gemini-Titan MDS Schematic

The assessments of failure modes resulted in a catalog of failure modes and their time criticality, which was provided to NASA for training purposes. Structural safety was ensured by imposing a 1.25 margin of safety above the specified wind environment. Winds were measured prior to each launch to develop flight rules and models.

The Titan II Gemini design relied more on the flight crew to initiate engine shutdown and ejection or abort, based on data provided by the MDS on a display in the spacecraft. It operated in either primary or backup mode, manually switched depending on whether the system itself malfunctioned in either mode[7].

The Gemini MDS was a key player in one of the most nervous moments of the Gemini program. On December 12, 1965, astronauts Wally Schirra and Tom Stafford were sitting aboard Gemini VI, ready to fly. The engines ignited at 9:54am. Lacking indication of upward movement after an inadvertant tail plug ejection had started an airborne timer, the MDS had stopped the engines. Given the state of the launch vehicle after this hot-fire abort, the rules called for the crew to eject, since it wasn't clear whether it was stable on the launch pad or had been released. The crew had not sensed motion, so Schirra made the decision not to eject. The crew exited the launch vehicle after it was safed, and the launch team reached a satisfactory conclusion of the cause investigation, allowing a successful launch three days later.

---

[6] Walter D. Smith; "Gemini Launch Vehicle Development"; NASA SP-121 Gemini Midprogram Conference, February 23-25, 1966, pp108-110.

[7] Joseph F. Wambolt; Aerospace Corp interview 8/2/2001, pp3-5

D. Apollo-Saturn V Emergency Detection System (EDS)

The Apollo Saturn Emergency Detection System, Figure 3[8], had two modes of operation, automatic abort and manual abort.

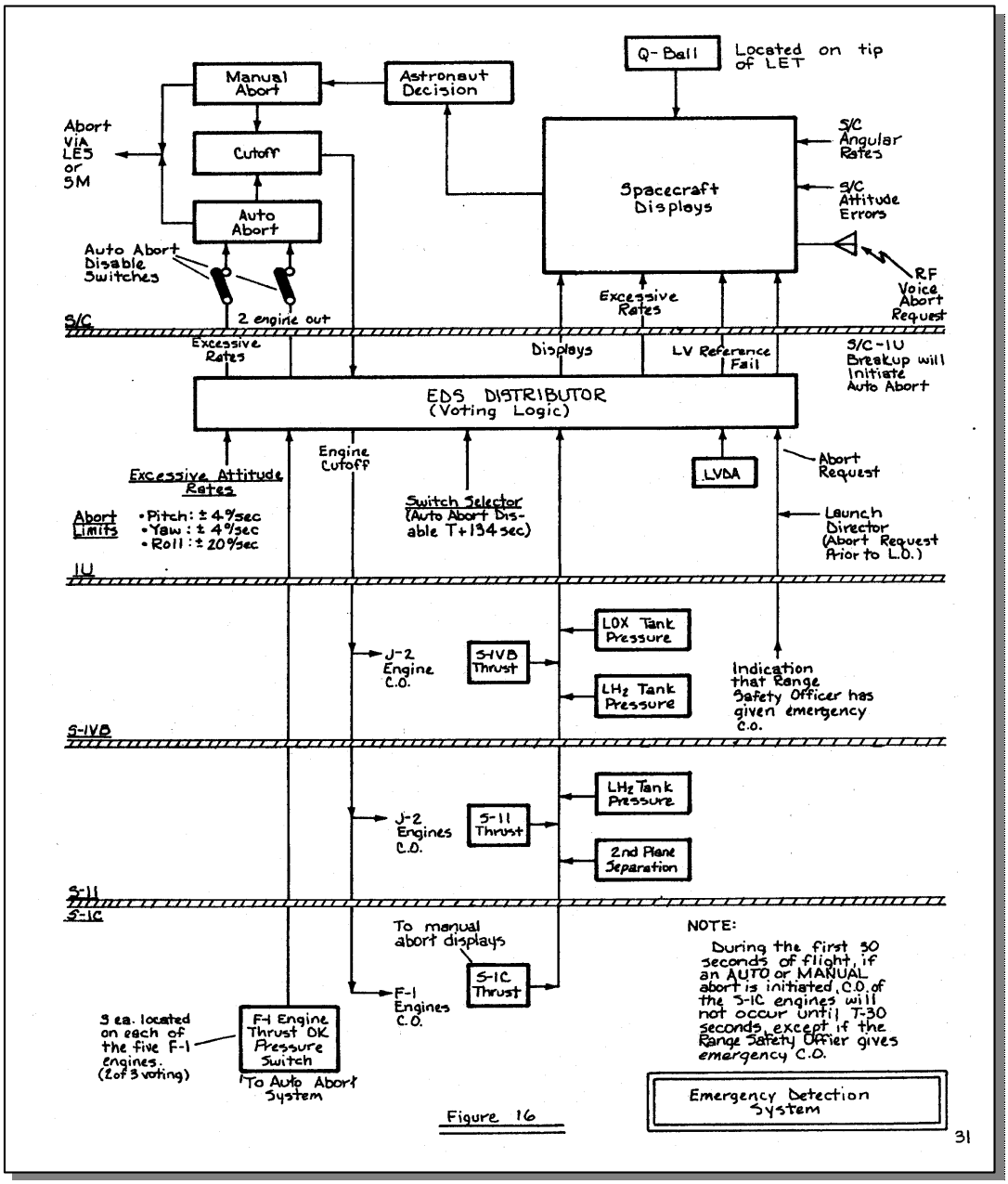

Figure 3. Apollo Emergency Detection System Overview

Automatic mode used on-board monitoring of thrust (on two or more engines) and vehicle overrate conditions that could result in a rapid vehicle breakup. If acceptable conditions were exceeded, the system would shut down the engines, trigger the separation ordnance, and ignite the spacecraft escape motors.

[8] NASA Marshall Spaceflight Center, "Technical Information Summary Apollo-11 (AS-506)", June 25, 1969, pg 31

Manual mode displayed EDS information to the crew and required the crew to use either their own senses or information from the ground to evaluate the overall situation and initiate an abort if necessary. The conditions displayed included lights indicating engine status, stage separation, overrate, and guidance malfunction, as well as angle of attack and propellant tank pressure information. There was also a red 'Abort' light that could be illuminated by the Launch Control Center (while the vehicle was on the pad) or, after liftoff, either by flight controllers or range safety officers via uplink.

Three sets of triply redundant dedicated rate gyros monitored Saturn V rates and provided those data to a control signal processor. An EDS distributor provided data to spacecraft displays and used relay and diode logic as required to generate the automatic abort sequence. Multiple engine shutdown functionality was enabled by a timer 30 seconds after liftoff. The EDS automatic abort mode was deactivated 100 seconds after liftoff.

> "EDS was much more sophisticated than the pure analog system found in Mercury — it included triple redundant digital modules and sensors that allowed two of three voting logic. Sensors monitored tank pressures, attitude rates, engine pressures, which directly correlates to thrust, as well as breakwires to detect premature staging. It also provided situational awareness of launch vehicle health to the crew via caution and warning indications and other displays. "
>
> Bullman, J., Langford, G., Benik, M., Effenhauser, R., Bedell, D., Foster, D., et al. (2004). *OSP-ELV Human Flight Safety Certification Study Report, Volume 1, Draft 3, pg 31.*

E. Space Transportation System (STS) Caution and Warning System (CWS)

The Shuttle system poses a different problem than an expendable launch vehicle with spacecraft. Generally, any STS off-nominal condition during ascent requires some manual operation to reconfigure redundant systems around the failed component. Shuttle lacks a true escape system, so 'abort' in shuttle terminology generally means 'revert to a backup flight plan'. Whether it's 'abort to orbit' (ATO), Transatlantic Landing (TAL), or 'Return to Launch Site' (RTLS), the crew is along for the ride, with the only alternative being a risky 'bail-out' under very limited conditions.

The STS Caution and Warning system supports the abort decision process by presenting on cockpit displays a variety of data that tell the crew when systems are off nominal. 120 signals are monitored by the Caution and Warning system, each providing upper and lower limit exceedence detection.

The STS CWS is a relatively high level function, relying on a distributed health management process to provide key elements. The Space Shuttle Main Engines were monitored throughout their operation by the Advanced Health Management System (AHMS), developed by Pratt & Whitney Rocketdyne and flown initially in June 2007. AHMS is a modification among other modifications of the SSME Controller that performs high pressure turbopump synchronous vibration redline monitoring.

F. Commercial Crew Transportation System – Atlas/Delta Emergency Detection System (EDS)

The Atlas/Delta EDS approach is an "add-on kit" to the existing and currently flying Atlas V and Delta IV vehicles which contains its own processors and software logic. The EDS monitors the health of the launch vehicle, with "health" being determined by monitoring various sensors located throughout the launch vehicle such as acceleration, attitude errors, rates, tank pressures, etc. In the event of a major anomaly, EDS terminates propulsion and issues an abort signal to the spacecraft. The spacecraft processes the abort signal and is in charge of separation and escape system activation. The spacecraft also has the ability to initiate an abort, as well as inhibit the launch vehicle auto-abort mode.

The EDS is a single fault tolerant architecture, consistent with the existing launch vehicle avionics architecture. An overall EDS "Series-Parallel" approach is used to address the fault tolerance. Two physically separate EDS processing units (EPU) provide parallel coverage (either of which can independently detect a failure and generate an

abort signal to the spacecraft). To guard against accidental abort, multiple (series) inhibits as well as high-level digital signal encoding are used for issuing signals to the spacecraft.

Table 1 in Section G, extended from a similar table included in the Bullman Report[9], draws a comparison of expected EDS monitored functions in relation to previous vehicle configurations. Many of the measurement types baselined for monitoring are common with EDS predecessors. Due to the availability of a digital data bus, additional measurements can be added with little or no physical interface modifications. The only limiting factors are processing bandwidth and the latencies inherent in the software cycle time required to process the additional data.

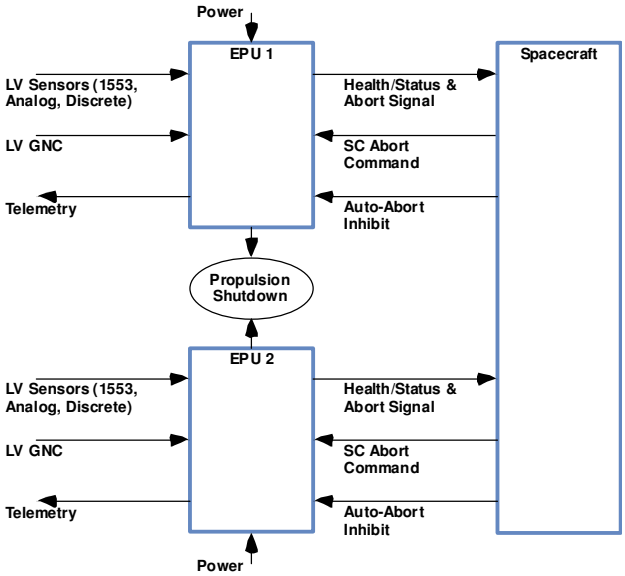

Figure 4. Atlas/Delta Emergency Detection System Diagram

The EDS processor architecture is based on the currently flying Atlas V guidance computer (Fault Tolerant Inertial Navigation Unit – FTINU). A common Single Board Computer (SBC) design will be used for the EPUs and future upgraded guidance computer for overall production and cost efficiencies. This design utilizes MIL-STD-1750A self-checking-pair (SCP) 16-bit processors. Unique algorithms which perform Abort/GO calculations on the various sensor suites are hosted on this SBC. Fault tolerance is provided via a two-channel architecture arranged in an active/hot-spare (standby) configuration.

The current EDS architecture allows data/commands between launch vehicle/spacecraft to be conveyed via three different types of circuits; 1553 databus, RS-422 digital stream or discretes. The spacecraft can choose which type best suits the interface. It is likely that discretes will not be used solely on their own as abort signals due to the small amount of information which can be conveyed (i.e. on or off only), however such a very simple interface could be implemented if needed. Digital data transmission will include robust communications protocol, error checking and message checksum/CRC.

At the end of 2010 during the CCDev1 phase, ULA demonstrated the basic functionality of the EDS, using a prototype EDS testbed environment comprised of existing Atlas V avionics associated with its mature Systems Integration Laboratory (SIL), including a number of representative failure scenarios. The EDS prototype utilized an existing FTINU SBC with self-checking-pair microprocessors (the same configuration planned for the actual EDS), connected to the launch vehicle 1553 control data bus as a Bus Monitor. The various algorithms performed sensor voting, down-select and pass/fail limit checking (including persistency). The software output the abort signal when the correct quantity of sensors, with persistency, was out of pre-defined allowable limits. The overall demonstration performance was excellent and with architectural and hardware/software designs highly relevant to the planned configuration.

G. Summary

Table 1 shows the parameters used to monitor the various crewed launch systems built in the United States. Some measurements are common to nearly all systems, implying an inherent ability to detect crew safety critical failure modes with key performance criteria.

[9] Bullman, J., Langford, G., Benik, M., Effenhauser, R., Bedell, D., Foster, D., et al. (2004). *OSP-ELV Human Flight Safety Certification Study Report, Volume 1, Draft 3, pg 49*

Parameter	Mercury Redstone	Mercury Atlas	Gemini Titan	Apollo Saturn IB	Apollo Saturn V	STS	CTS EDS	Comments
Electrical power	X	X				X	I	Bus voltage/power not being directly monitored, however effects of loss of power are; such as comm errors, databus loss, LRU health, etc
Booster-SC Electrical Interface		X			X		Y	EDS interfaces directly with SC providing GO/ABORT status continuously during mission. SC can initiate abort over this interface
Attitude Rates	X	X	X	X		X	Y	Roll/Pitch/Yaw rates derived from single fault tolerant inertial measurement block in GNC system
Angle of Attack				X	X	X	P	Currently under assessment. Derived from same GNC sensors as Attitude Rates
LV Guidance			X	X	X	X	Y	Guidance system monitored for comm errors, databus loss, loss of total function, etc. Design is single fault tolerant so first failure is loss of redundancy with NO Abort, second failure would require Abort.
Structural Failure				X			N	No direct monitoring of structure (e.g. strain gages). Structural failures such as leaks or breakup monitored indirectly via tank pressure sensors, breakwires, etc
Hydraulic Pressure		X				X	N	Only the Stage 1 uses hydraulics (in the actuator system) Stage 2 uses electro-mechanical actuators and has no hydraulic components. Loss of hydraulic function determined via actuator position (if monitored) or GNC rates.
Fuel/Oxidizer Tank Bulkhead Differential Pressure	X	X					Y	Differential pressure is calculated in EDS software via reading multiple pressure sensors from each tank
Stage 1 Fuel Injector Pressure		X	X				N	Not a monitored function
Stage 1 Fuel Tank Pressure			X				Y	Each tank uses the same single fault tolerant ullage pressure monitoring approach
Stage 1 Oxidizer Tank Pressure		X	X				Y	Each tank uses the same single fault tolerant ullage pressure monitoring approach
Stage 1 Engine Thrust OK	X		X	X	X	X	Y	Redundant speed sensors provided engine health/thrust data. Thrust determined via acceleration derived from single fault tolerant inertial measurement block in GNC system. Additional engine health monitors also in place.
Stage 2 Fuel Injector Pressure			X				N	Not a monitored function

Stage 2 Fuel Tank Pressure			X	X	X		Y	Each tank uses the same single fault tolerant ullage pressure monitoring approach
Stage 2 Oxidizer Tank Pressure			X	X	X		Y	Each tank uses the same single fault tolerant ullage pressure monitoring approach
Stage 2 Thrust OK			X	X	X	X	I	Thrust determined via acceleration derived from single fault tolerant inertial measurement block in GNC system
Stage 3 Engine Under-pressure					X		NA	2-Stage LV, No Stage 3
Stage 3 Oxidizer Tank Pressure					X		NA	2-Stage LV, No Stage 3
Stage 3 Fuel Tank Pressure					X		NA	2-Stage LV, No Stage 3
Stage 3 Thrust OK				X	X		NA	2-Stage LV, No Stage 3
Staging			X	X	X	X	Y	First stage / Second stage separation monitored by sensing errors in all databus communications to the First stage, after the separation command is issued.
Engine Helium Pressure						X	N	Not a monitored function
Engine Helium Regulator output Pressure						X	P	Currently under assessment, potential to measure Helium bottle supply used for tank pressurization and engine control, may or may not be regulator output
Fuel Manifold Pressure						X	N	Tank ullage pressure sensing (see above) used instead
Oxidizer Manifold Pressure						X	N	Tank ullage pressure sensing (see above) used instead
Engine Controller						X	I	Several avionics LRU's are monitored, not just the "engine controller" unit
Turbopump Temperature						X	N	Not a monitored function
Turbopump seal purge pressure						X	N	Not a monitored function
Turbopump Coolant Liner Pressure						X	N	Not a monitored function
Engine Actuator Position					X		P	Currently under assessment, possible comparison of actual position to commanded position

Table 1. Historic List of Parameters Monitored for Emergency Detection Purposes, from the Bullman Report with Additional Atlas/Delta Entries

H. Conclusions

The similarities that exist between the functions monitored in 1962 and those proposed to be monitored in 2015 are somewhat expected. The nature of launch vehicles in general has not changed significantly in those 50 years. Very similar systems imply very similar monitoring of safety critical faults. In fact, the development of the CTS EDS followed many of the same steps and processes employed in the development of the Mercury-Atlas and Gemini-Titan system.

The biggest difference in 50 years of evolution, is that today's digital electronic systems provide a great deal more flexibility in both what to monitor and how to monitor it. Analog measurement fed into an EDS solution provide a simple and prompt method of identifying that an off-nominal condition has occurred. However, though there is some inherent delay in digitizing a signal and transmitting the results to an on-board processor, the ability to define specific thresholds for different phases of flight for each sensor provides enhanced system optimization. Use of standard data buses and communication protocols also provides flexibility and maturity to the solution.

The CTS Emergency Detection System will add a critical enhancement to the Atlas and Delta launch vehicles that will provide additional protection in case of a launch failure.

.