Commercial Crew Abort System Design Evolution and Validation

Ian Dawson[1], Brooke Mosley[2]

United Launch Alliance
Centennial, CO

New commercial crew vehicles require an emergency detection system for crew abort capability. This system is implemented to provide protection for the crew in the event that a catastrophic hazard occurs. The emergency detection system developed for the Atlas V is not unprecedented. The Space Shuttle program had several abort capabilities, as did the Apollo/Saturn vehicle. The underlying principles in designing an abort system remain very similar across programs and across time. The technology available to implement these systems has evolved and improved. The understanding of past failures to abort when needed also play into modern day abort system design. Launch vehicles include many complex integrated systems and subsystem components. Understanding the failure space of all these systems and their combination is a daunting and seemingly endless task. When in abort system design, there are two contrasting design perspectives that must be considered: "Failure Space" and "Success Space". The Failure Space case design is used where there are unknown outcomes, nonlinear time variant complex analyses that cannot be done in the time allotted, and unknown fault system interactions. The concern with designing in Failure Space is the inability to abort when necessary. Because this type of abort analysis is not well understood, it moves validation of these abort cases into effect-based validation. On the other hand, the Success Space case design is more straightforward. In this space the causes are understood, testing to determine abort success exists, execution of redundancy is clear, and the statistical analysis associated with assessed failure modes is clear. The concern on this design side is overachieving or inadvertent abort. The validation of Success Space abort design is cause-based where the cause of the failure can be detected and the abort sequence initiated properly. Abort system validation techniques can be polarized between the complex effect-based validation and the less complex cause-based validation. The first puts the designer in a qualitative risk based assessment world and the later places the designer in a logical limit based analysis world. It is imperative that the designers of an abort system can be successful in both of these types of failure spaces. The design of the Atlas V emergency detection system has required this and although the hope is that it will never be used, should it be called upon, it stands to be the most comprehensive emergency detection system in launch vehicle history.

I. Introduction

Any vehicle or machine used by humans will include an emphasis on the safety of its users in the design. Automobiles have airbags and blind spot monitors, microwaves have radiation shielding. These are protection features designed into a system, based on well-known failure modes and system characteristics. However, launch vehicles are so complex, and the environment they create for riders so extreme, that adding simple protection devices are inadequate to ensure the crew's safety. A different philosophy of safety focusing on detection and evaluation of vehicle state needs to be formulated and implemented.

For the Commercial Crew Program Atlas V vehicle, an Emergency Detection System (EDS) has been developed that allows for robust autonomous launch vehicle monitoring and abort decision-making capabilities. This required a shift in thinking from a launch service that provides critical national security payload transport to a launch service that would provide crew transport.

The Atlas V was originally designed with mission success for critical national security payloads in mind. This means that certain design decisions were made without consideration for how failure modes for a crewed flight might be detected, or most importantly for a crewed vehicle, how these modes may affect the payload.

[1] Propulsion Engineer, HLS Propulsion, ULA, P. O. Box 277005 Denver Co 80127, AIAA Member

[2] Mechanical Engineer, HLS Commercial Crew Safety and Reliability, ULA, P. O. Box 277005 Denver Co 80127, AIAA Member

For the EDS design to be successful, a rigorous understanding of the vehicle's many complex integrated systems had to be made. Only after that understanding was achieved could the EDS design phase begin, with two philosophies to be considered: should engineering design in "Failure Space", or design in "Success Space".

Failure Space design analysis is used when there are nonlinear time-variant complex system interactions, and unknown outcomes. Designing abort modes within this space invokes a considerable risk of an inability to abort when necessary due to a lack of complete understanding of a failure mode. Essentially, designing in this space would require the detection system to base its abort decision on detection of the effect of a failure, and not the cause of that failure. This shaves precious time out of an abort scenario; these milliseconds could determine whether the crew is safe or not.

Success Space design takes a different, more straightforward approach. However, failure causes must be well understood, abort success test methods must exist and be readily performed, redundancy should be designed in easily, and all employed analysis methods should be well grounded. Designing in this space yields a system which can detect the cause of a failure prior to propagating into catastrophe, but it has its drawbacks. Namely, over-emphasis of design in this space risks inadvertent aborts due to "overachieving". This tends toward perfectionism, where even the slightest off-nominal condition could be interpreted as a precursor to failure. Initially, this seems a safer approach than the alternative of not detecting a failure in time, but when considering the detrimental effects a boost phase abort has on an astronaut's physiology, this inadvertent abort risk needs to be limited.

Historically, ULA uses a success space design philosophy whenever possible. The mission success-driven culture requires the diligent prevention of failures to ensure that critical national security payloads entrusted to the launch vehicle make orbit. Success space design utilizes off-nominal operation, but does not consider multiple independent failures of systems. Failure space, on the other hand, is designing a system with every failure scenario, including propagation, in mind. This was needed when augmenting the previous mission success design philosophy and engineering culture to incorporate new crew safety paradigms.

There is no right way to design a launch vehicle failure detection system, and even in the same design group, there may be different polarizing opinions about which direction, i.e., which design space, should be pursued. In the case of the Atlas V vehicle failure detection system, ULA leveraged history, nurtured and utilized engineering intuition, and ultimately implemented a philosophy that combined both Success and Failure Space design for development of the EDS.

II. From Digital to Analog

The aerospace industry is in a time of unprecedented technological progress. Computer simulations of complex problems are no longer a flight of fancy, given the appropriate time and resources. It has been the drive of many industries to automate and digitize processes and even decision-making to yield more efficiency and a higher return. Launch vehicle design is no different.

Atlas V was one of the first launch vehicles to be significantly developed through Computer Aided Drafting and other modeling software tools. Because of this emphasis on computer based analysis, the expensive all-up system level testing of past rocket programs was greatly reduced without a negative impact to vehicle reliability. Through 50+ flights of the Atlas V, nearly all of the assumptions made during those early analyses have been validated or refined to yield a robust understanding of the vehicle's integrated systems.

For the Commercial Crew Program, this reliability presents a dilemma. How should a system be designed to detect failures that have never been experienced? What data should be monitored? How should the system be programmed to make autonomous decisions based on those monitored indicators?

In today's world, it is easy to jump to the "just do analysis" conclusion. Let computer simulations and models dictate what could go wrong and design EDS to look for those indicators. Now, factor in realistic cost and schedule limitations, and suddenly these analyses must become truncated such that they become relatively simple, binary decision processes. A monitored temperature sensor reads off-nominally hot, therefore there is a fire – Abort! In a complex system, off-nominal indications are not necessarily indicative of a failure, meaning this "digital" approach could lead to an inadvertent abort. What if the sensor has failed? Or there is a small jet of fuel or pressurant impinging upon the sensor? You don't immediately jump out of your car doing 75mph when the tire pressure warning light comes on, do you? You assess the situation. You look for other indications of a failure, like noise or vibration. Using these inputs as failure confirmation, and your experience, you make a decision to ignore it and continue on, or pull over and check tire pressures.

It is important to understand what these "other indications" are when it comes to EDS design. The experience aspect also needs to be addressed. With Atlas V being such a reliable vehicle, a significant number of the EDS design team has never experienced a failure or gone through the ensuing failure investigation/corrective actions. When evaluating a system fault tree and making decisions on credible failure modes, the team has to "learn experience" from launch vehicle failure case studies. Historical information cannot be taken at face value. Similarities in design and operation of the vehicle in the case study need to be evaluated for applicability of the case study failure to Atlas V. Oftentimes, this requires a deep dive into Atlas V design

through documentation and personal recollection to ensure an understanding of the systems well enough to make that determination.

While deep in the trenches of reviews that determine failure modes and their mitigations, the design team was also under pressure to analyze these failure modes and how they propagate. Then the question becomes, how does one team analyze every credible catastrophic failure on a rocket? The short answer is, it doesn't, but the long answer is a bit more complicated.

III. Analysis Paralysis versus Risk Acceptance

Ideally, abort detection would be designed using a Success Space design approach, such that the fault can be detected at the source of the failure. In this paper and during the development of the Atlas V EDS, the source of the failure is referred to as the Basic Initiating Event (BIE) as shown in Figure 1. For systems closely tied to vehicle control, like avionics, Success Space design is not only ideal, it is possible. However, the systems that the avionics command, such as tank pressurization, are one step removed from the control systems of the rocket. Valves execute commands, and it is harder to detect anomalies in these lower-level systems using the Success Space design approach of monitoring avionics. In many cases, the failure that is detected at this level is the outcome of the BIE. Here, the emergency detection system is forced to rely on indications of the failure outcome or Accident Initiating Conditions (AIC)s (ex. detection of an overpressure vs detection of a valve failure). Note: After the AIC on the failure timeline, is an Accident Outcome Condition or AOC, such as vehicle breakup or loss of vehicle control.

Developing the abort system to detect BIEs would allow for prevention of AOCs. In this case, the failure mode is detected and the control system has the ability to shut down that system and rely on system redundancy, or safely shut down the vehicle and initiate the abort sequence. This method uses Fault Isolation Detection and Recovery, or FIDR, to protect the crew from catastrophic conditions, and the benefits of doing this are obvious. Unfortunately, not all system faults can be detected at the BIE and there are practical limitations that prevent the EDS designer from designing in Success Space with simple cause-based validation.

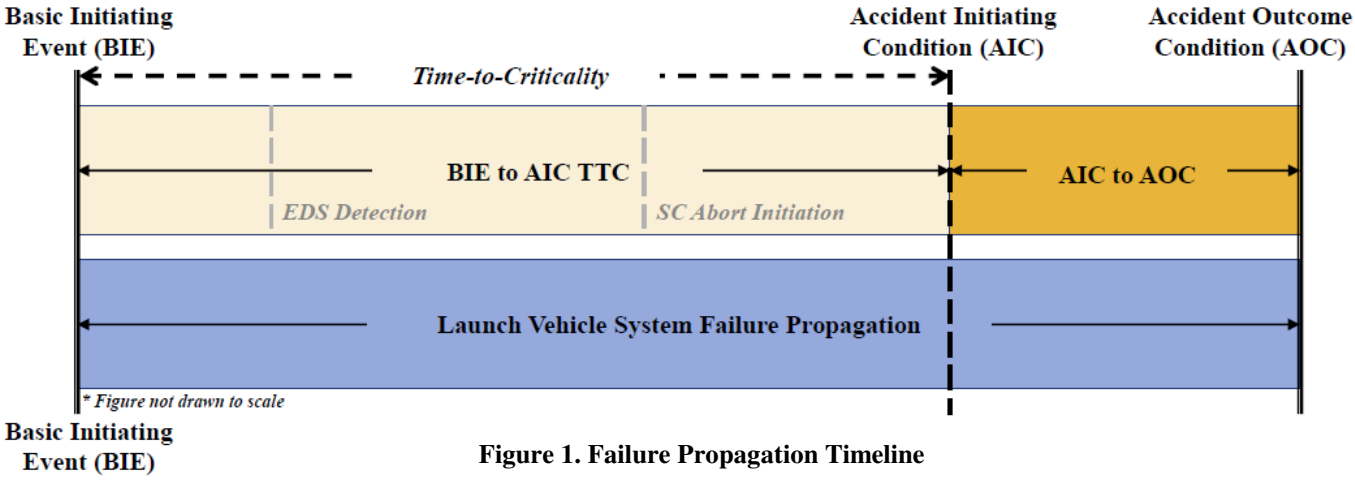

Figure 1. Failure Propagation Timeline

The downfall to designing a system in Success Space is that this rocket never flies because of design complexity and endless validation. Beyond avionics, there are too many basic initiating events in the propulsion systems alone, in varying forms and degrees of magnitude, to analyze with accuracy. The models required to do this are very complex and would only be reliable if anchored to failure data. This is when a development program finds itself in analysis paralysis. But wait, it gets worse! In addition to the complex analysis, the failure detection capability would have to be at the component, line, fitting, or mechanism level. This would weigh the rocket down with instrumentation to a degree where it wouldn't be able to lift its own weight off the ground. This is an extreme example where excessive analysis with the intent of designing the emergency detection systems using a Success Space methodology has occurred. The outcome is a program of PowerPoint charts, design memos, pretty PR pictures, and in the end all that remains is the formidable paper rocket.

Here is where the designer finds that there is no other option but to transition to a Failure Space design approach, i.e., can the failure be detected at the AIC? The sensors used to control the rocket: pressure transducers, thrust vector control indications, rate gyroscopes etc. are all good detectors of AICs. These sensors are entrusted with vehicle feeback control, thus designed to higher standards and requirements to undergo rigorous processes and procedures to ensure they do not fail or lie. These sensors are the flight computer advisors and, as such, they have the ability to report on vehicle health or a deterioration of this health. Determining how these sensors detect poor vehicle health, how fast, and how accurate is the function of Failure Space analysis. In this analysis, there is uncertainty in the failure mode propagation and timing that are accepted. Accepted uncertainty results in accepted risk. This risk is essential to allowing the rocket to fly. Unfortunately, as

in the case of BIEs, there are innumerable AICs that would need to be studied to be absolutely certain that every failure condition would be detected in an acceptable period of time. Using the tank pressurization example from before, there are innumerable leak rates and locations at different times in flight with different pressure conditions, and each would have a different outcome at a different time. Beyond that, there are also compounded failures. If there is a hole in a propellant tank, what does that do to the engine it feeds? Assume that the engine fails due to that condition. There is cavitation at a certain rate, and then propagation towards failure. However, other vehicle systems try to compensate for this deteriorating operation.

The list goes on and on and, depending on how creative the engineer is, it gets more and more complex and even diabolical. When car companies assess accident survivability, they look at front and side impacts at different speeds. They do not assess what happens when the car hits a deer, swerves off the road, flips down an embankment, side swipes a tree and lands in a river. Similarly, the EDS design team has chosen not to analyze every credible catastrophic failure. It has chosen to analyze a select set of failures, including integrated systems and propagation, at discrete times in the flight which encompass the vast majority of failures that could occur.

Without limiting types of failures assessed, there is trap that engineers find themselves in when trying to develop failure detection methods and systems. This is where risk trades come into play, engineering intuition is used and programmatic decisions are made. Has enough been done? Is this risk understood? Why is it acceptable? The truth is, not every fault can be designed out, many failures don't have a FIDR, and not every failure mode can be accurately understood.

With risk acceptance and crew safety in mind, the EDS solution that ULA has converged on for the Atlas V is a hybrid approach to covering failure modes that is somewhere between two extreme ends of the fault coverage spectrum. At one end of the spectrum, every fault is covered; this requires a very large budget and significant schedule where safety trumps all. A maximum fault coverage method also includes a lot of effect-based validation. This level of validation on a large number of failure modes is expensive and time consuming. At the other end of the spectrum, there is minimal fault coverage. This would be considered the least expensive approach, but one with little regard for crew safety. ULA has selected a fault coverage zone where effect-based faults are minimized and cause-based faults increase. This is a balanced compromise between covering failures (robust safety) and maintaining validation simplicity (reduced cost). Cause-based validation allows reduced cost because the analyst can validate an abort system by developing abort thresholds based on vehicle limits. When the limits are exceeded, analytically the vehicle cannot continue. Examples include: tank structural limits, avionics box communication failures, and engine structural limits. Effect-based validation requires the modeling and simulation of failure propagation through the vehicle. This is the most realistic form of failure validation; however, it also requires advanced simulation tools which considerably drives up cost and expands schedule. In addition, there is always a concern about the accuracy of the simulation tools developed due to their complexity.

IV. Design Simplicity

A principle that most engineers learn early on in their training is that the simplest solution is usually the best one. Sometimes complexity is a necessity, but in the case of EDS, simplicity is the baseline with complexity added only where needed for coverage or detection time. A method that can be understood by a wide range of disciplines prevents misunderstandings in the development and implementation process. Mistakes in development and implementation may not only result in a failure of the system to abort the crew when needed, they may also cause an abort that is not needed at all.

Taking a system of complex systems and targeting an overarching level of health monitoring that is both simple and effective is not unprecedented. Saturn V had a small number of abort triggers that were detected at the guidance level. Most failure modes propagate to guidance and control whether they are a loss of thrust due to a fire and explosion causing the propulsion systems to degrade, or a software issue that ultimately results in rates that exceed the control system authority. All failures propagate to a rocket falling out of the sky or to an unplanned trajectory.

The problem with detecting failures at this level is that many times it is too late to abort the crew in a controlled, predictable, survivable manner. What is desired in an emergency detection system is the opportunity to reliably detect failures at the earliest possible time. The Saturn V and the Atlas V are very different rockets designed several decades apart. Although the Atlas V has the advantage of improved technology and computing power, the health monitoring systems are actually quite similar in terms of simplicity and effectiveness.[1] Complex effect-based validation was not implemented for either program. What Atlas V has accomplished that the Saturn V could not, due to technology/computing limitations, is additional speed of detection of failure modes and more automation.

V. Algorithms on the Atlas

The Atlas V rocket has a structurally stable first stage with RP-1 and LO2 as propellants and a dual chamber RD-180 engine. The second stage is a pressure stabilized LO2/LH2 propelled two RL10 engine configuration.

In designing the algorithms that monitor vehicle health, ground rules were followed to ensure there was consistency in the philosophy used to develop each monitor. To ensure simplicity while also ensuring safety and reliability, detection of failures was designed to be accomplished at the earliest opportunity and at the highest level of measurement capability necessary to

maximize a successful abort outcome and minimize inadvertent aborts. Minimizing complexity in the algorithms precludes runaway schedules and budgets as well as inadvertent abort risk.

Crew safety is paramount in the design. The EDS system exists solely for the purpose of saving the crew in the event of a catastrophic failure. The design maximizes crew safety while also allowing flexibility. For example, there is a feature within flight software that allows the spacecraft to apply or remove a global Inhibit of the EDS Abort-response functionality depending upon flight rules and failure circumstance. Crew safety is the primary goal while operational flexibility remains an important feature that ultimately augments crew safety.

As a safety system not used for nominal flight, it may be acceptable to use systems, data, and or interfaces that are zero fault tolerant. The decision made by ULA in the design of the EDS was that it would be single fault tolerant, both to ensure that the abort system works when needed in failure environments that are unpredictable, and also to ensure that inadvertent aborts do not occur.

In the event of a catastrophic failure, the rocket itself begins to deteriorate where one failure could lead to many others. EDS is designed to detect a trigger and initiate the required abort sequence without detecting or requiring additional faults that occur subsequently. This reduces complexity of integration and execution without adding any risk.

A. Detection Methods Outside of the Control System

The abort triggers used by EDS require more than one measurement to declare an abort. Figure 2 summarizes the sensors used for the EDS. ULA's preference has been to use sensors already engrained within the control system as those sensors are redundant, highly reliable, and qualified to higher standards. This means that if a system is unhealthy it is a system that controls the rocket and it is absolutely necessary to abort. There are some systems that have the ability to deteriorate without losing the mission or endangering the crew. It is tough to draw the lines between a deterioration of health that may cause imminent danger to the crew versus an in-flight anomaly that can be flown through (mission success versus crew safety) without developing very complex intricate models. Control sensors go through a rigorous design and qualification process that ensures they will operate as expected.

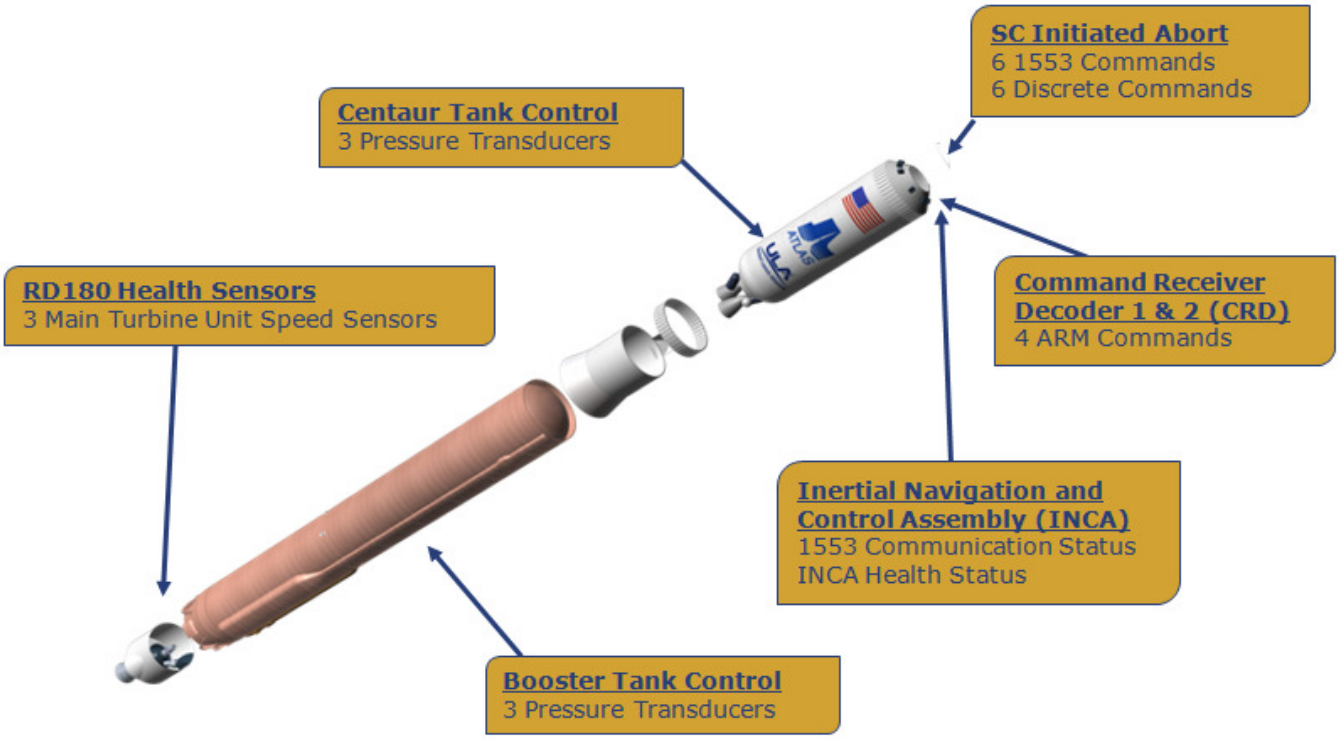

Figure 2. EDS Sensors on Atlas V

Using a telemetry sensor or a sensor tied to a system that is not critical to the control of the rocket increases the risk of false aborts. Steps are taken to increase the possibility of detecting an abort more quickly, but using a sensor that is outside of the control systems slides right back into the catastrophic failure category in the form of an inadvertent abort. Inadvertent aborts are considered catastrophic to the crew. Aborts that inadvertently occur have not been tested, the sequence of events is not fully understood, and the spacecraft could end up in a configuration that it was not required to be capable of surviving.

In developing the parameterized thresholds to be used in abort trigger exceedance checks, the designers must balance between competing objectives. On one hand, there is the desire to minimize false aborts by expanding abort thresholds based

on statistics or levels of operation. The other side to that is minimizing the emergency response time by tightening abort thresholds to be just around nominal operational characteristics. The optimal solution is somewhere in between the two objectives.

The following sections discuss the vehicle health monitors that will be implemented on the Atlas V that cover the majority of catastrophic failures that could occur.

B. External Monitors

The spacecraft has the ability to send abort commands to the launch vehicle that must be detected and acted upon by the Atlas V EDS.

EDS also monitors the Flight Termination System in the event that Range Safety must destruct the vehicle.

These external monitors respond to systems outside of the launch vehicle with situational awareness that the EDS cannot have. They are integrated into the overall success of the mission and safety of the crew.

C. Propulsion System Monitors

The Solid Rocket Motors are not monitored during ascent. SRMs are the divas of the propulsion world; either they are ignited, pressurized, and providing thrust, or they are not. There is no reliable detection method that would provide the time needed to abort safely; in response, there is no way to turn a solid off. Failure to ignite or catastrophic failures of the SRMs are detected by axial acceleration or rate monitor (see the Flight Control Monitor section) sometime after the AIC.

The RD-180 engine has failure modes that can fail uncontained resulting in a rapid deflagration of the engine and adjacent systems during ascent. Based on analysis, early detection of these failure modes can be seen at the turbomachinery prior to the AIC and subsequent AOC. EDS monitors first stage RD-180 engine pump speeds during boost phase. Loss of thrust conditions from the main engine are monitored by axial acceleration (see the Flight Control Monitor section).

The RL10 engine is not monitored during second stage flight. The sensors available for engine health monitoring are not tied to the control system. The result of an RL10 engine failure is not catastrophic to the crew until it propagates to the system as a whole. Those failures are detected both by tank pressure monitoring (see Structural Integrity Monitor), axial acceleration, and body rates.

D. Flight Control Monitor

As discussed earlier, all launch vehicle failures will result in loss of acceleration or body rates, but with the proper selection of thresholds, exceedances can be detected sooner with a minimal increase of risk of inadvertent abort. Waiting for the launch vehicle to start falling from the sky may be too late to start an abort and keep the crew safe. The EDS monitors axial and lateral accelerations, body rates, and engine actuator commands. Actuator commands are monitored for abnormal commanding which may indicate an abortable condition.

E. Structural Integrity Monitor

The booster tanks have LO2 and RP-1 ullage pressure monitors. The booster tanks are structurally stable and require proper pressurization during boost phase to maintain structural integrity and RD-180 engine run box conditions. EDS monitors tank ullage pressures to detect indications of pressurization conditions that could cause structural failure of the tanks or improper RD-180 run box conditions.

The second stage LO2 and LH2 tanks are pressure stabilized and require proper pressurization during ascent and second stage flight operations. The EDS monitors tank ullage pressures to detect indications of pressurization conditions that could cause structural failure of the tanks or improper RL10 engine inlet conditions.

F. Avionics Monitors

The safety-critical avionics systems involve bus communication between the flight control computer, control units, and engine controllers. The EDS monitors these safety-critical avionics systems for bus transmission errors and problems with communication between these units.

The flight computer itself also has health indicators of possible failed redundancy or the internal inertial measurement sensors. The EDS monitors the Flight Control Computer health and Inertial Measurement health for loss of vehicle control due to a sick computer, or hazardous loss of accelerometer or gyroscope sensor accuracy.

G. Staging Monitors

A launch vehicle fairing is used to protect mission-critical avionics systems from atmospheric effects during accent. The EDS monitors this fairing's breakwires to determine if inadvertent launch vehicle fairing jettison has occurred, which could render mission-critical avionics systems inoperable.

Once the booster stage has completed, it is commanded to separate from the rest of the vehicle, falling back to Earth. The EDS monitors for an expected loss of communication to a booster avionics control unit, which will occur when the booster physically separates from the second stage and severs the communication bus.

VI. Emergency Detection System Validation

There are two opposing philosophies to validating proper thresholds and timing as they apply to abort system detection and execution. There is the test-based philosophy where the goal is to test early and often, possibly fail, learn from this, and fix things that are found early in the program. The alternative is to analyze, learn and discuss, evaluate the systems at subcomponent levels as they mature, fix or prevent failures that are known, and perform an "all-up" test toward the end of the program when all of the plausible concerns have been fleshed out. Both approaches have their own schedule and cost risks, and both require a trade on failure acceptance versus failure prevention.

There are only a couple modern rocket systems that utilize failure detection and abort systems. The Saturn V program had an automated failure detection system and, although designed in the 1960s, there are many parallels to the outcome of the design being used on the Atlas V.

Early in the Saturn V program, NASA Associate Administrator George Mueller went toe-to-toe with Wernher von Braun on how to test Saturn V systems while keeping the program on-track. This has some similarities to the budget and schedule pressures industry is facing today. Von Braun advocated a test program where incremental changes were introduced into a system, tested in flight, then evaluated and approved before additional changes or systems were incorporated. S-IC would be launched with dummy upper stages and if it succeeded, then the next test would be of an S-IC stage and live S-II, with a dummy S-IVB, and so on. In 1963, George Mueller saw a program behind schedule and looked for ways to get it back on track to put humans on the moon by 1969. His approach was the "all-up" method where a vehicle would launch with a minimum of dummy components. He effectively turned a 10 vehicle unmanned test program into 2, with the third vehicle being Apollo 8, the first manned lunar orbiting mission. His gamble paid off. Even with the second test, Apollo 6, experiencing an anomaly in every stage of the vehicle, Apollo 11 would not have made its historic landing in 1969 had George Mueller not demanded that a certain higher level of risk be accepted in order to accelerate the test program.[2]

As briefly mentioned above, Saturn V included a simple EDS that monitored for excessive attitude rates and 2-engine out during S-IC operation.[3] Thresholds and computer voting logic were designed to avoid inadvertent automatic abort scenarios during the tumultuous S-IC boost phase. Fortunately, this system was never tested in flight. Even when Apollo 12 experienced two lightning strikes within 20 seconds during S-IC boost phase, with electrical systems including the vehicle's digital computer showing a multitude of faults, the guidance programming was able to discern fact from fault and keep the vehicle pointed in the right direction. During post-flight investigation, it was determined that computer programming checks and redundancy, along with automatic abort system design thresholds were adequate to ensure proper safety margin in future similar events.[4]

Saturn V is a successful example of cause versus effect-based validation. In many cases, the analytical technology simply did not exist to perform an effect-based validation of the system. Moreover, what did exist was so time consuming that the rocket would never have launched. Saturn V's auto abort modes relied upon attitude rate thresholds dictated by structural limits, and 2-engine out on S-IC, which would have put the vehicle on a ballistic trajectory. As described above, Atlas V EDS has taken a similar approach, even though the simulation capability exists today to do some complex effect-based validation. By comparing Atlas V EDS validation philosophy to that of Saturn V, confidence is instilled that the right approach was selected, with the right amount of rigor, to develop a solution that will successfully carry astronauts to orbit.

VII. Summary

Rockets and politics typically don't get along, but former Secretary of Defense Donald Rumsfeld paraphrased an idea he heard from former NASA Administrator William R. Graham that is very transferable to the discussion of launch vehicle safety: "…there are known knowns: there are things we know we know. We also know there are known unknowns: that is to say we know there are some things we do not know. But there are also unknown unknowns: the ones we don't know we don't know."[5] This perfectly describes complex system interactions as seen in launch vehicles.

The things that we know, through analysis, discussion, historical parallels, and testing we can design for or monitor with a high degree of confidence in Success Space. We have to accept that there are things we will not know, the known unknowns, because analyzing every failure scenario, or designing in Failure Space and performing effect-based validation, is impractical. Likewise, we must accept that we cannot determine all failure propagation scenarios, the unknown unknowns.

As the Atlas V EDS has been developed, everything was leveraged from qualitative historical data, to reliability numbers and statistics in order to validate the system and understand risks before accepting the design. There has been a convergence on a middle ground approach where ULA has avoided getting tangled up in strenuous effect-based validation by evaluating and accepting a certain level of risk in the EDS. The takeaway should not be that designing in Failure Space is bad and designing in Success Space is good; it should also not be the contrary. The Atlas V EDS was designed in Failure Space using

effect-based validation, and it was also designed in Success Space using cause-based validation. A balanced combination of the two is essential in creating a system that is both effective and practical. Using this approach, the Atlas V Emergency Detection System provides an extra level of safety that will keep our astronauts safe, give the best probability for overall mission success, and ultimately meet all schedule and budget constraints imposed.

References

[1] Saturn V Flight Systems Analysis *Saturn V Launch Vehicle Emergency Detection System Analysis, SA-504*. The Boeing Company Space Division Launch Systems Branch, 1968.

[2] Cortright, Edgar M. "Chapter 3.4." *Apollo Expeditions to the Moon*. Washington D.C.: NASA Scientific and Technical Information Office, 1975.

[3] Herbella, Gary. Hensheimer, Tom. Mingee, Rick. *Evolution of Abort Management of Crewed Launch Vehicles from Mercury ASIS to Commercial Crew EDS.* AIAA 2011-7128. AIAA Space 2011 Conference.

[4]Godfey, R. et al. *Analysis of Apollo 12 Lightning Incident*. NASA-TM-X-62894. NASA. 1970.

[5] Rumsfeld, Donald. *Known and Unknown: A Memoir.* Sentinel Publishing. 2011.