Original Article
https://doi.org10.56094/jss.v58i1.216

International System Safety Society

www.jsystemsafety.com

Journal of System Safety

Established 1965 Vol. 58 No. 1 (2023)

The Difficulties with Replacing Crew Launch Abort Systems with Designed Reliability

Shaun R. Ryan[ab]

[a] *Corresponding author email: shaun.r.ryan@lmco.com*
[b] *Lockheed Martin Space; Sunnyvale, California, USA*

Keywords
launch, crew, abort, human spaceflight

Peer-Reviewed
Gold Open Access
Zero APC Fees

Online: 22-Feb-2023

Cite As:
Ryan S., The Difficulties with Replacing Crew Launch Abort Systems with Designed Reliability. Journal of System Safety. 2022;58(1):19-24. https://doi.org10.56094/jss.v58i1.216

ABSTRACT

As the space industry continues to innovate and new paradigms arise to challenge the status quo, human spaceflight is now perceived as safer and more accessible than ever before. This has led to a new line of thinking in which crewed launch vehicles should be reusable and reliable like commercial airplanes, forgoing the need for an abort system. This paper will counter that line of thought with an analysis of the spectrum of coverage historical crew abort systems provided during launch and use historical data from launch rate successes and failures to glean insight into what reliability in the human spaceflight industry can expect when designing the vehicles of the future. This historical launch vehicle reliability will then be compared to system safety standards used in the commercial aviation industry to understand if future designs truly need a crew abort system. Through this analysis, the rationale for why these crew abort systems have historically been used can be better understood.

INTRODUCTION

While a lot of attention is focused on performance and capabilities of launch vehicles, crew launch abort systems are often overlooked. While maybe not as flashy as tonnage to low earth orbit or pushing boundaries with complex combustion cycles, crew safety is critically important in human spaceflight. The danger of human spaceflight is not isolated to the vacuum of space but extends down to the ascent phase as well. The earliest crew abort systems on launch vehicles used aircraft-derived ejection seats. Featured in the Gemini and Vostok programs, ejection seats have a very limited window of effectiveness. They must be deployed at an altitude high enough for the parachutes to fully unfurl, which renders them ineffective for pre-launch aborts and for the first few seconds of flight. Additionally, once launch vehicle speeds and aerodynamic forces become too great, the ejection itself could result in loss of crew. Subsequent programs like Mercury, Soyuz, and Apollo transitioned to the use of crew launch abort systems using rocket motors attached to the capsules. These designs leveraged the pre-existing reentry functionality of crew capsules, repurposing them for a suborbital return. With this design philosophy,

rocket motors affixed to the capsule would quickly accelerate the crew away in the event of launch vehicle failure. Once a sufficient distance is reached, reentry devices such as parachutes would deploy to land the crew capsule. This system has the advantage that it is designed to be used on the pad as well as on ascent, propelling the capsule to a sufficient altitude for parachute deployment in the event of an on pad failure. This design philosophy is still used today on the Orion, Starliner, and Crew Dragon capsules.

APOLLO CREW LAUNCH ABORT COVERAGE

A good example of the coverage that a crew launch abort system can give can be found in the system used on the Apollo missions. The ascent phase of the mission was considered an especially dangerous part of the mission (Lyndon B. Johnson Space Center [JSC], 1972), so a great deal of planning went into their crew launch abort scenarios. The four main ascent related abort modes considered for the mission are shown in Figure 1 below.

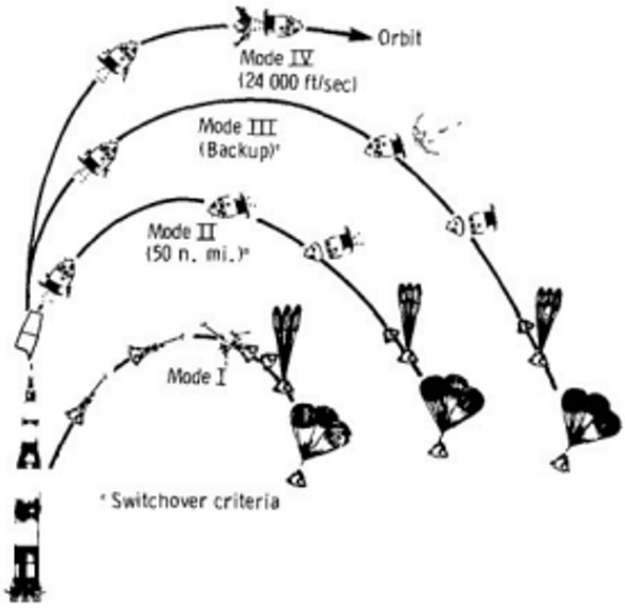

Figure 1: Apollo Abort Modes (JSC, 1972)

The first mode, or Mode I, was used for the major atmospheric phases of the flight. It was armed before launch to cover any pre-launch failures of the launch vehicle, with the vehicle fully loaded with propellants and after the crew boarded the command service module (Marshall Space Flight Center [MSFC], 1969). This mode lasted until the first few minutes in flight, at which the launch escape tower was jettisoned. If activated during this phase, the command module would separate from the service module as the launch escape tower fires. Once a safe distance away, the parachutes would fire, and the command module would hopefully land somewhere along the ground track (depending on when it was activated).

The second mode, Mode II, covers the phase of ascent after the highest atmospheric loads are experienced. Occurring after launch escape tower jettison, this mode relies on the traditional separation of the command service module and launch vehicle. After separation the command service module would maneuver itself clear of the launch vehicle and orient itself for landing. The service module would be jettisoned, and the command service module would return on a suborbital trajectory.

The third mode, Mode III, is a contingency mode used to prevent the command module from a land landing as the capsule was only designed to safely land on water. This would be executed in a similar way as the second mode, but with an additional retrograde burn by the command service module to constrain its down range landing to a pre-designated site (JSC, 1975).

The fourth mode, Mode IV, is essentially an abort to orbit. Once far enough along in its flight but still on a suborbital trajectory, an additional burn from the launch vehicle or service module would be performed to boost the command service module into orbit. Once in orbit a landing site could be designated and a return from orbit would be performed.

This crew abort plan was envisioned to provide the maximum possible coverage for all phases of the ascent. While never required to be used, it shows a great example on how to mitigate against a catastrophic failure of a launch vehicle.

THE SPACE SHUTTLE

The Space Shuttle program marked a major shift in design philosophy, with a new emphasis on reusability (Jones, 2018). The shuttle was a launch system consisting of a reusable space-plane based orbiter, a large expendable external tank, and two refurbishable solid rocket boosters (John F. Kennedy Space Center [KSC], 2022). This mindset shift also

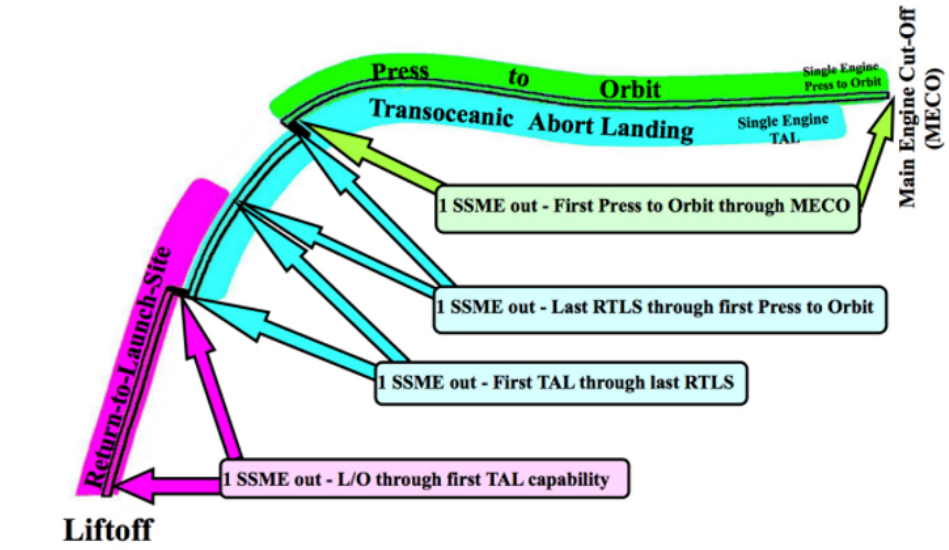

Figure 2: Space Shuttle Abort Modes (Henderson et al., 2011)

affected the crew launch abort planning for the shuttle. There was a new focus on robustness of the system which NASA thought could reduce the need for a crew launch abort system (Henderson & Nguyen, 2011). Instead, the in-flight abort scenarios utilized the intact orbiter for coverage throughout ascent profiled in Figure 2.

The first major mode is the Return to Launch Site (RTLS) abort. RTLS involves pitching the orbiter around to decrease down range trajectory. The burn is continued after the pitch around to give the shuttle extra velocity to enable a glide back to the launch site. The orbiter is then pitched down so that the external tank can be safely detached. The shuttle then performs its final unpowered glide back to the landing strip at the launch site. This abort mode is active from solid rocket booster separation until it is too far downrange to successfully glide back.

The second major mode is Trans-oceanic Abort Landing (TAL), in which the shuttle lands in pre-selected runways in Europe or Africa. For TAL, the ascent profile would remain very similar to a nominal launch, except with an earlier Main Engine Cutoff (MECO). The external tank would be separated in a way to minimize the risk of debris from a tank rupture impacting the orbiter. Then the orbiter would glide to a landing site.

The third major mode is an Abort to Orbit (ATO) in which the shuttle would continue to press on and achieve a stable orbit. Then the orbiter could select a more favorable landing time and location. Additionally, there is a small window for an Abort Once Around (AOA) in between modes. In a contingency AOA scenario, the shuttle would achieve just high enough velocity to make it once around the earth to then land back in the continental United States.

All these scenarios were developed for if one of the space shuttle's main engines were out. The picture of this abort plan becomes more clear when you look at the pre-Challenger contingency abort scenarios in Figure 3.

For the shuttle, contingency abort scenarios are for when two-out-of-three or three-out-of-three of the main engines are out. It is here that we can see the black out zones that are created when there is a catastrophic failure with the shuttle. While these focus on main engine out scenarios, Figure 3 makes it more clear that any major failures that occur in the solid rocket boosters would most certainly result in a loss of the crew, like what we tragically saw with Challenger in 1986. The shuttle design offered no protections for the crew in the event of launch vehicle destruction on the pad. In a stark difference to the Apollo philosophy, the shuttle attempted to design away the need for a crew launch abort system

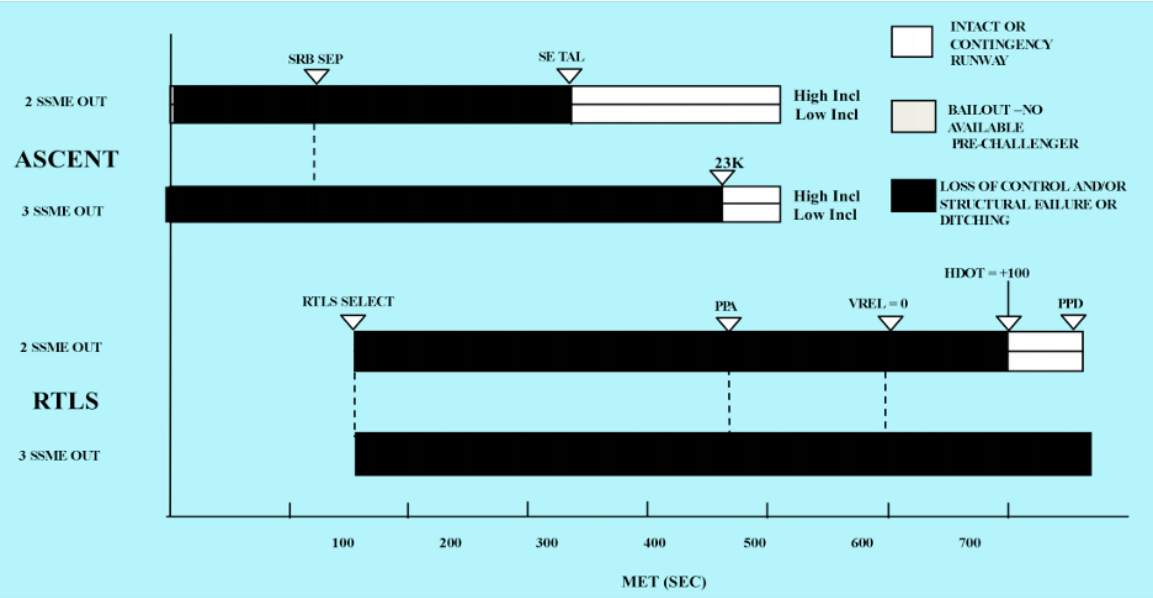

Figure 3: Pre 1986 Shuttle Contingency Aborts (Henderson et al., 2011)

assuming their vehicle was like a commercial airliner and their attempt failed (Jones, 2018).

REAL WORLD RELIABILITY OF LAUNCH VEHICLES

While there have since been technological advancements since the shuttle was designed, it is useful to look at the data from historical launch vehicles. This can be used to give a little insight into the human spaceflight industry and how it has performed. Using data from incidents and close calls in crewed space launches, a rough reliability of launch vehicles can be shown. For this paper the word reliability is being used in a general sense, divorced from probabilistic calculations. Below is a table of close calls and incidents that occurred during launch and ascent, sourced from NASA data with a focus on aborts and loss of crew/mission.

As of the writing of this paper, Soyuz has conducted 147 crewed launches and 3 resulted in aborts. This gives it a very rough reliability of about 99.97%, not taking into account uncrewed launches. For the shuttle's 135 launches and 2 ascent related incidents it gets a back of the envelope calculation at 99.99%. These two "reliability" numbers show how often an abort system was used to save the crew or crew was lost without such a system in place. While these numbers definitely don't tell a complete story, they will be useful to keep in mind as a basis of comparison. For an outside example, ULA calculated their reliability of the Atlas V 401 to prevent loss of crew as 99.96% (Patton & Barr, 2009). This value

Table 1: Close Calls and Incidents (JSC, 2019)

Mission	Incident/Close Call
STS-51L	Combustion gas leak in the solid rocket motor resulted in vehicle destruction. Loss of crew.
Soyuz T-10-1	Fuel spill ignited the launch vehicle while on the pad. Crew abort system activated. Crew saved
STS-51F	Faulty sensors resulted in premature engine shutdown and forced an Abort to Orbit. Auto-shutdown of second engine overridden to ensure AOA succeeded. Crew saved.
Soyuz 18-1	First stage failed to separate cleanly, and the vehicle was sent off course. Crew launch abort system activated. Crew saved.
Soyuz MS-10	Collision of boosters during staging resulted in destruction of the second stage. Crew abort system activated. Crew saved.

Probability (Quantitative)	Per flight hour 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable	Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor	Major	Severe Major	Catastrophic
	JAA	Minor	Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	• slight reduction in safety margins • slight increase in crew workload • some inconvenience to occupants	• significant reduction in safety margins or functional capabilities • significant increase In crew workload or in conditions impairing crew efficiency • some discomfort to occupants	• large reduction in safety margins or functional capabilities • higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely • adverse effects upon occupants	• all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D	Level C	Level B	Level A

Figure 4: Failure Severity as Related to Probability Objectives (SAE International, 1996)

shows that the oversimplified method above still falls within the range of numbers calculated using more traditional and robust reliability analysis.

RISK BASED ON AIRCRAFT STANDARDS

When new crewed space launch vehicle concepts are designed without crew launch abort systems, the comparison to commercial aviation is often made. The claim is that launch vehicle technology has sufficiently advanced enough that a risk posture similar to aviation can be adopted. In order to examine this claim, it is important to understand the thresholds that the aviation industry has adopted.

SAE's ARP 4761 is the de facto standard for System Safety in commercial aircraft design and manufacturing. In Figure 4 we can see that the probability objective for a catastrophic hazard in an aircraft is 1.0E-9, or 1 in a billion chance of occurrence per flight hour. To accurately gauge how the Soyuz and Shuttle compare to this, the previously calculated reliability should be normalized per each launch vehicle's ascent time for an ISS mission. The ascent times tend to be short, with the Soyuz at 0.15 hours (National Aeronautics and Space Administration [NASA], 2010), the Shuttle at 0.14 hours (NASA, 2007), and the Atlas V 401 at 0.20 hours (United Launch Alliance [ULA], 2022). If you take the ascent time for the vehicles and multiply by their total number of launches you can get a total hours accumulated per vehicle. Using the very simple formula below (eq. 1), the resulting launch vehicle normalized probability per flight hour objectives can be seen in Table 2.

$$\frac{(100 - Calculated\ Reliability)/100}{Cumulative\ Flight\ Hours} = Adjusted\ Probability\ Per\ Flight\ Hour \quad (eq1)$$

In this case, the Adjusted Probability Per Hour represents the probability a catastrophic event occurs that could result in loss of the crew per every flight hour. So for every flight hour, each of the launch vehicles would need to have a catastrophic failure less than the probabilities in Figure 4. The calculated Adjusted Probabilities Per Hour for the crewed launch vehicles do not compare favorably to the ARP 4761

Table 2: Adjusted Probability Per Ascent

Vehicle	Calculated Reliability	Ascent time (Hours)	Total Crewed Launches	Cumulative Flight Hours	Adjusted Probability Per Hour
Soyuz	99.97%	0.15	147	22.05	1.4E-5
Shuttle	99.99%	0.14	135	18.90	5.3E-5
Atlas V 401	99.96%* *From ULA	0.20	40* *No Crewed Launches to date so uncrewed used as a stand-in	8.00	5.0E-5

probability objectives for catastrophic hazards. The Soyuz comes in at the best with a probability of 3 in 200000. Then it is the Atlas V 401 with a probability of 1 in 20000. Lastly is the Shuttle with a probability of 53 in 1000000. These far exceed the probability thresholds for a catastrophic hazard by a significant margin.

These calculations are highly dependent on the data set used as well as an oversimplified definition of reliability. However, they remain useful as a litmus test between the commercial aviation and crewed spaceflight industries.

CONCLUSION

Crew launch abort systems are still a much-needed mitigation against launch vehicle failures in today's space industry environment. Crewed launch vehicles still have a way to go to meet commercial aircraft levels of reliability. The probability objectives from aviation system safety standards are a useful yardstick to measure how far vehicles have to go moving forward. Additionally, programs from the past can show us the risks we are assuming by leaving large black zones in crew launch abort capabilities. There is still a long road ahead before crew launch abort systems should be eliminated from designs.

REFERENCES

[1] Lyndon B. Johnson Space Center. (1972). Apollo Experience Report - Abort Planning. (Hyle, Foggatt, & Weber.) Retrieved from https://ntrs.nasa.gov/api/citations/19720017278/downloads/19720017278.pdf

[2] Marshall Space Flight Center. (1969). Saturn V Flight Manual SA-507. Retrieved from https://history.nasa.gov/afj/ap12fj/pdf/a12_sa507-flightmanual.pdf

[3] Lyndon B. Johnson Space Center. (1975). Apollo-Soyuz Test Project Recovery Requirements JSC-09436. Retrieved from https://history.nasa.gov/astp/documents/Astp-recoveryreq.pdf

[4] Jones, H. W. (2018). NASA's Understanding of Risk in Apollo and Shuttle. 2018 AIAA SPACE and Astronautics Forum and Exposition. https://doi.org/10.2514/6.2018-5235

[5] John F Kennedy Space Center. Space Shuttle Era Facts. Retrieved 2022, from https://www.nasa.gov/pdf/566250main_SHUTTLE%20ERA%20FACTS_040412.pdf

[6] Henderson, E. M. and Nguyen, T. X. (2011) Space Shuttle Abort Evolution. AIAA SPACE 2011 Conference & Exposition. https://doi.org/10.2514/6.2011-7245

[7] Lyndon B. Johnson Space Center. (2019) Significant Incidents & Close Calls in Human Spaceflight. Retrieved 2022, from https://sma.nasa.gov/SignificantIncidents/

[8] Patton, J. A. and Barr, J. D. (2009). Atlas and Delta Capabilities to Launch Crew to Low Earth Orbit. AIAA SPACE 2009 Conference & Exposition. https://doi.org/10.2514/6.2009-6729

[9] SAE International. (1996). GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT (ARP4761). https://www.sae.org/standards/content/arp4761/

[10] National Aeronautics and Space Administration. (2010). Soyuz Launch Overview and Timeline. Retrieved 2022, from https://www.nasa.gov/mission_pages/station/structure/elements/soyuz/timeline_overview.html

[11] National Aeronautics and Space Administration. (2007). STS-121: Ask the Mission Team - Question and Answer Session. Retrieved 2022, from https://www.nasa.gov/mission_pages/shuttle/shuttlemissions/sts121/launch/qa-leinbach.html#:~:text=It%20takes%20the%20shuttle%20approximately,8%2D1%2F2%20minutes

[12] United Launch Alliance. (2022). Atlas V to Launch Starliner OFT-2. Retrieved 2022, from https://www.ulalaunch.com/missions/next-launch/atlas-v-starliner-oft-2