A Review of Spacecraft Safety: From Vostok to the International Space Station

Robert P. Ocampo and David M. Klaus

Aerospace Engineering Sciences, University of Colorado Boulder, Boulder, Colorado.

ABSTRACT

As the U.S. manned space program begins its transition from government to commercial enterprise, the safety of the crew, ground, and general public is of paramount concern. A catastrophic accident early in NASA's Commercial Crew Development (CCDev) program could derail the nascent commercial space industry, leaving the United States wholly reliant on Russia for manned launch services. To reduce this risk, lessons learned from past space programs should be assimilated into current commercial practice. This article traces the evolution of manned spacecraft hardware safety, from Vostok to the International Space Station, with the hope that a review of yesterday's spacecraft will benefit tomorrow's space travelers.

INTRODUCTION

In 2010, NASA established the Commercial Crew Development (CCDev) program to stimulate the development of commercial spacecraft for manned missions to and from the International Space Station (ISS). To help ensure crew, passenger, ground personnel, and public safety (as well as programmatic success), it was decided that spacecraft developed in this program should not exceed an overall Loss of Crew probability distribution of 1 in 270.[1]

To fulfill this requirement while meeting budget and schedule constraints, commercial space companies must rely on past "lessons learned" to inform present-day design decisions. A summary of these lessons, culled from 290 manned space flights spanning the last half century, is described in this article.

MERCURY

Project Mercury, America's first manned spaceflight program, utilized a single-seat capsule built by the McDonnell Aircraft Company. The capsule was launched on top of a modified tactical missile—the Redstone rocket in the case of early suborbital flights and the Atlas D for later orbital missions. While both missiles had a less than exemplary track record prior to their first manned launches (81% and 75%, respectively, as of May 1961[2,3]) they were favored for the accelerated Mercury program because of the significant experience base associated with their launch and operations.

Both the Mercury Redstone and Mercury Atlas D shared many broad design characteristics with their unmanned predecessors. However, both manned launch vehicles were built to higher quality standards and more conservative design margins. The structure of each rocket, for example, was built to withstand 1.5 times the anticipated loads.[4] In addition, both manned vehicles contained additional redundancy and instrumentation to ensure no single failure could lead to the loss of the mission.[5] However, if the manned rocket *were* to fail catastrophically, an integrated launch escape system was tasked with automatically separating the spacecraft from the launch vehicle.

Risk was further mitigated through extensive ground and flight testing. Hardware was tested iteratively—first at the component level, then as a completed subsystem, and finally as an integrated vehicle.[6] Components that could not be adequately tested on the ground, such as the ablative heat shield or the launch escape system, were tested in flight using the Little Joe or Big Joe boosters.[3] As a final precaution, both Mercury Redstone and Mercury Atlas boosters were flown in an unmanned configuration several times prior to their first manned launch.

Organizational procedures also served to improve astronaut safety. Spacecraft and launch vehicle were built with parts identified by a "Mercury stamp," thereby ensuring only qualified components were used in the vehicle.[6] Workers were actively encouraged to meet high standards of workmanship, and those that met certain high performance criteria were awarded with marks of distinction.[3] As further incentive, Mercury astronauts made a point of visiting NASA contractors so workers would associate a "face" with the vehicle they were building.[3]

Despite the effort made to improve both booster and capsule reliability, each manned Mercury launch suffered its share of hardware failures. In many of these situations, the astronaut successfully served as a final line of defense against mission failure. Originally, the Mercury spacecraft was intended to be fully automated; the astronaut would fly as a passenger, not as a pilot. However, the astronauts strongly objected to this "spam-in-a-can" design, and a small viewport and manual control system were added to the spacecraft. This allowed the human astronaut to serve as a backup to the automated flight control. This design choice proved particularly effective during the last manned Mercury mission, allowing Gordon

DOI: 10.1089/space.2013.0015

Cooper to pilot his Faith 7 spacecraft through reentry after his automatic stabilization and control systems were lost.[3]

The man-rating* process for Project Mercury proved to be a significant challenge, both in terms of schedule and cost: With roughly 80,000 critical parts in the capsule and booster, the first manned Mercury Redstone launch took place over a year behind schedule and cost 40% more than its unmanned predecessor.[3] Despite these modifications, the reliability of the Redstone only increased from 81% (the success rate of the rocket prior to 1961) to 84% (the reliability estimate of the Mercury Redstone rocket).[2] Ultimately, however, the man-rating process for Mercury proved effective because all six astronauts returned safely from their Mercury flights.

GEMINI

Gemini was intended to bridge the gap between Mercury and Apollo, with missions designed to parse out the techniques and technologies required for rendezvous, docking, long-duration flight, and extravehicular activity (EVA). McDonnell Aircraft was once again selected to build the two-person spacecraft, which was launched on a modified Titan II intercontinental ballistic missile. Later missions incorporated the use of an Agena upper-stage booster, which served as a docking target and third-stage booster for the Gemini spacecraft.

Like the Atlas and Redstone rockets before it, Titan II was originally designed for military applications, then later adapted for manned use. These modifications included the addition of redundant hydraulic, electrical, and flight control systems; an upgraded factor of safety for structural components (1.25); and the inclusion of a malfunction detection system.[4] Oxidizer standpipes and mechanical accumulators were also added to the booster to eliminate longitudinal "Pogo" oscillations that often occurred during launch.[7]

Prior to its first manned launch, the Titan II booster had accrued a significantly higher success rate than either Mercury Redstone or Mercury Atlas and benefited from concurrent reliability improvements initiated by the manned Dyna-Soar-Titan II program. Moreover, Titan II boosters assigned for manned use were built in a facility separate from other missile production lines to further improve quality.[8]

The Gemini spacecraft inherited a number of flight-proven subsystems from its Mercury predecessor. "Lessons learned" during Mercury capsule design and construction were captured and faithfully passed down to Gemini engineers (a process aided by the fact that the same contractor, McDonnell Aircraft, build both vehicles). However, the *location* of these subsystems differed substantially in the newer spacecraft. Due to the thrust limitations of the Mercury launch vehicle, the Mercury capsule incorporated integrated systems, attached in the manner of a "layer cake." While this technique significantly decreased mass, it made spacecraft testing and checkout burdensome. In contrast, the Gemini spacecraft utilized a separate "service module" containing modularized subsystems, a design that significantly expedited and improved verification and checkout.[7]

Unlike its programmatic predecessor, Gemini lacked an escape tower. Instead, the capsule incorporated ejection seats designed to separate the crew from the spacecraft during a launch and landing emergencies. This abort system methodology was chosen ostensibly to simplify and "modularize" the design, but proved difficult to implement in practice (a malfunction during testing destroyed a test dummy).[7] Notably, ejection could only be initiated manually, a technique in line with the greater flight control authorities allotted to astronauts during Gemini[9] and very much appropriate given the Titan II's hypergolic propellants. The decision to incorporate manual ejection capabilities proved well-founded when a tower plug prematurely separated from the Gemini 6-Titan II rocket prior to liftoff. Although mission rules called for an ejection, the astronauts (appropriately) elected to remain in their spacecraft, thereby salvaging the mission.[7]

Originally intended as an add-on to Mercury, Gemini suffered from significant cost overruns as it developed into its own full-fledged, stand-alone program. Because of budget constraints and schedule pressures, Titan II engine test firings were curtailed and quality assurance and reliability testing programs were eliminated, replaced instead with cheaper enhanced qualification testing. The effects of such a fast-paced program were not inconsequential: Thrusters aboard Gemini 7 failed towards the end of flight because those installed were of an older design known to have problems.[7]

Although all 10 Gemini missions ended with the crews' safe return, Gemini 8 nearly ended in catastrophe. Upon docking with its Atlas Agena target, a stuck thruster in the spacecraft began rolling the spacecraft at a rate that threatened to cause the crew to lose consciousness. After manually shutting down the thruster and activating the reentry control system, the crew was able to stabilize their spacecraft and initiate an emergency landing in the Pacific Ocean.[7]

APOLLO

The Apollo program safely landed 12 men on the moon between 1969 and 1972. The three-man crew utilized two separate spacecraft on their lunar missions: the Command and Service Module (CSM), which served as primary crew quarters and Earth-entry vehicle, and the Lunar Module (LM), which provided two astronauts with lunar landing and ascent capabilities. Both the CSM and LM were launched on the Saturn series of vehicles. Saturn IB rockets were utilized for low-earth orbit missions; Saturn V rockets were used primarily for lunar voyages.

Unlike boosters used in Mercury and Gemini, the Apollo Saturn rocket was designed *explicitly* for manned use.[10] Man-rating features

*"Man-rating" (later "human-rating") was initially aimed at improving the reliability of launch vehicles for human use and at increasing safety through the addition of escape/abort systems. Later references began including "human in the loop" design aspects driven by ergonomics and human factors, which essentially extended the focus from protection of the crew (and public) to include utilization of the crew in the design. The term has also evolved from being posed as guidelines to what are now a set of requirements.[1] The first vehicles found to be deemed man-rated in the literature were the X-series of experimental rocket planes.[4,20]

were built into the vehicle from the start (rather than being grafted on later), with redundant systems eliminating most single point failures. Moreover, the vehicle's design was inherently conservative: The Saturn series of rockets relied on state of the art (*not* cutting edge) technologies and margins that were considered "lavish even by aerospace standards."[11] And, if the booster *were* to fail catastrophically, an emergency detection system and abort tower were available to rapidly separate the spacecraft from the launch vehicle.[9]

The nascent Saturn rockets had an attendant disadvantage, however: a knowledge base for the rocket did not exist prior to Apollo.[10] To validate the Saturn's design while maintaining the pace necessary to meet President Kennedy's lunar landing goal, engineers employed a technique known as "all up testing" in which *all* stages of the vehicle were flown live on each launch. In this manner, a successful test of the lower stages could provide flight data for the upper stages. This technique largely contributed to Saturn's accelerated man-rating process.[†,12]

Once in orbit, the crew traveled to and from the moon in the CSM and LM. Despite their inherent complexity—the combined CSM/LM had over 3 million parts[12]—both spacecraft were designed to extremely high standards of reliability. North American Aviation, charged with designing the Command Service Module, utilized proven technologies and employed redundant components wherever possible. The Lunar Module, built by Northrop Grumman, aimed for reliability through simplicity[13]; the fixed ascent engine on the LM, for example, utilized a pressure-fed engine hypergolic fuel and oxidizer, thereby negating the need for an igniter (and thus removing a potential failure mode).[13] Even the Lunar Roving Vehicle, utilized in later Apollo missions to extend the astronaut's travel range, adhered to strict man-rating requirements. Through design and operations, the Lunar Roving Vehicle was single-fault tolerant to Loss of Mission and dual-fault tolerant to Loss of Crew.[14]

Although Apollo successfully met its goal of landing men on the moon before 1970, the program was not without its share of failures. In 1967, a fire in the command module during a "plugs-out" test claimed the lives of astronauts Gus Grissom, Ed White, and Roger Chaffee. A frayed wire beneath the command module pilot's seat is thought to have triggered a spark, and the CSM's high pressure, 100% oxygen crew environment—coupled with an abundance of flammable materials in the cabin—contributed to the fire's rapid, lethal spread.[15] A second failure of the CSM—this time involving a high pressure oxygen tank—nearly claimed the lives of a second crew 3 years later when an oxygen tank in the Apollo 13 service module exploded halfway to the moon, forcing the crew to retreat to their lunar module. The LM, though not designed for such a contingency, successfully served as a "lifeboat" and the crew returned to Earth safely.[16]

[†]The rocket's man-rating was also aided by Saturn's modular design. Because many stages were interchangeable (the S-IV earth departure stage, in some derivation, appeared on the Saturn 1, the Saturn 1B, and the Saturn V), data accrued during early unmanned Saturn 1 and Saturn 1B launches could be applied to later manned launches of the Saturn V. Given the S-IV's early and frequent success, NASA felt confident launching men to the moon on the very first manned Saturn V.[12]

SKYLAB

The Skylab space station, launched in 1973, hosted three separate American crews over the course of a 9-month period. During 28-, 59-, and 84-day missions, Skylab astronauts conducted experiments in astronomy, physiology, biology, and remote sensing. Leftover Saturn hardware served as both the station's backbone and its transportation infrastructure: A modified Saturn S-IVB stage, boosted by an unmanned Saturn V rocket, functioned as the station's orbital workshop and crew quarters, and an Apollo Command and Service Module (CSM), launched on a Saturn IB booster, provided crew transportation to and from the station.

During its launch to orbit, Skylab suffered critical damage to its electrical and thermal protection systems. A micrometeoroid shield, used to both protect and cool the station, broke loose, knocking out one of two primary solar arrays. Initially engineers feared that such damage was beyond repair; however, by deploying a temporary "parasol" and manually deploying the station's remaining solar array, Skylab astronauts were able to restore the station to near-nominal functionality. A more permanent sunshade—the "Marshall sail"—was subsequently installed by the 2nd Skylab crew. In-flight maintenance and operational procedures mitigated the effects of later coolant system leaks and Control Moment Gyro failures.[17]

Designed to support crews of astronauts for upwards of a year, Skylab was subject to numerous man-rating requirements. Only parts that had already been proven in space or rigorously tested on the ground could be used on board the station. Moreover, NASA limited its selection of Skylab contractors to those that had successfully flown flight hardware in the past. As a final safeguard, components that were deemed critical were designed as single-fault tolerant or exceptionally reliable.[18]

All three Skylab crews completed their missions and returned to Earth safely. However, several hardware failures on board the Apollo spacecraft threatened to curtail two of the missions. The first Skylab crew was forced to initiate a "hard dock" maneuver to link their spacecraft to the space station when capture latches on the CSM port failed to engage.[17] During the second manned Skylab mission, two of the four Reaction Control System jets on the Service Module failed in orbit, threatening to strand the crew in space. A potential rescue mission was initiated but never launched because the crew managed to deorbit their spacecraft with the remaining Reaction Control System jets.[17]

SPACE SHUTTLE

From 1981 to 2011, the US Space Shuttle—the world's first partially reusable spacecraft—performed a variety of missions in Low Earth Orbit (LEO). Over the course of 135 flights, shuttle crews deployed and retrieved satellites, performed experiments in Spacelab and Spacehab scientific modules, resupplied the Soviet Mir space station, and helped assemble the ISS.

Launched in a multistage, parallel-burn configuration, three Space Shuttle Main Engines, fueled by an External Tank (ET) and augmented by twin Solid Rocket Boosters (SRBs) provided thrust to the crewed Orbiter during ascent. During landing, the winged Orbiter returned to Earth as an unpowered glider, landing on a runway.[19]

Given the diversity of its mission objectives and the complexity of its flight operations, shuttle development proved extremely challenging. Building a reusable spacecraft necessitated major advances in thermal protection, computer avionics, and propulsive engineering.[20] One engineer is quoted as stating that the Space Shuttle Main Engines "required a greater step forward in technology over the Saturn engines used in Apollo than the Saturn engines did over their predecessors."[19] Yet despite the vehicle's heavy reliance on unproven technologies, the space shuttle was never tested in an unmanned configuration; both its first Approach and Landing Test *and* its first launch were manned. To certify the shuttle as safe for flight, NASA relied solely on ground testing in conjunction with model analysis.[21]

If critical components were to break down in flight, redundant spares provided fault tolerance[22]; if engines were to fail during launch, several abort modes were available. As a last resort, the crews of the first four "developmental" flights had the option of ejecting if a catastrophic malfunction were to occur. In 1988 (after the Challenger disaster), a sliding pole escape system was added to the orbiter to allow for crew bailout during certain phases of compromised launch and landing operations.[23]

The Space Shuttle was the only NASA program to lose crew members in flight. In 1986, the orbiter Challenger broke apart 73 seconds after launch. Heated gas from an SRB field joint breached both primary and secondary O-ring seals, impinging upon and destroying the ET-SRB attachment strut. This event led to the aerodynamic destruction of the vehicle and loss of the entire crew.

Seventeen years later, the orbiter Columbia disintegrated during re-entry, killing all seven crewmembers on board. Insulating foam from the ET broke loose during launch, colliding with and damaging the thermal protection system on the shuttle wing leading edge. During re-entry, heated plasma breached the affected wing, melting the spacecraft's aluminum structure and destroying the vehicle.

Both accidents were presaged by anomalies that indicated serious weaknesses in the shuttle system: O-ring "blow-by" occurred 10 times prior to Challenger; ET foam shedding was identified six times prior to Columbia.[21,24] The Rogers Commission and the Columbia Accident Investigation Board—the investigatory boards formed in the wake of the two shuttle accidents—asserted that engineers had disregarded these anomalies in the face of budget and schedule pressures.[21,24] NASA responded by modifying shuttle hardware, upgrading safety standards, and revamping its Safety, Reliability, and Quality Assurance programs.

INTERNATIONAL SPACE STATION

The ISS is a modular space laboratory designed and built by the United States, Russia, Japan, Canada, and partner nations from the European Space Agency (ESA). The first ISS module was launched in 1998; after extensive delays following the space shuttle Columbia disaster, the station was completed in 2011.

Although structurally unified, ISS is *programmatically* divided into Russian and U.S. Orbital Segments (ROS and USOS, respectively, with ESA, CSA, and JAXA hardware being considered part of the USOS). Such segmentation offers dissimilar failure tolerance to critical and catastrophic hazards.[25] If all four U.S. Control Moment Gyros were to fail, for example (as one did in 2002 and again in 2006), thrusters on the Russian Service Module can provide backup attitude control. The benefits of segmentation, however, come at a price: hardware built in one country must integrate cohesively and safely with hardware created elsewhere—a significant challenge given that *system-wide* testing and verification of the ISS was not accomplished prior to the start of ISS assembly.[25]

During its 14 years in orbit (as of November 2012), the ISS has suffered a number of critical component failures.[25] In 2004, the Elektron oxygen generator broke down, forcing the crew to rely on Solid-Fuel Oxygen Generator "candles" for oxygen—the very same candles responsible for the fire on Mir. Two years later, a similar Elektron unit began leaking potassium hydroxide, a toxic irritant; although the situation was eventually stabilized, the crew on board was obliged to don masks and surgical gloves as a precautionary measure until the atmosphere was cleared.

External hazards, such as Micrometeoroid and Orbital Debris (MMOD), have also posed threats to the ISS. In 2009 and 2011, large pieces of debris nearly collided with the station; and in 2012, a small MMOD object actually struck (but did not penetrate) a window on the ISS cupola. Although the ISS design was intended to meet a 95% probability of no penetration of pressurized compartments, certain Russian segments, originally designed for the Russian Mir2 station, were not designed to this same standard.[25]

Despite the criticality of these incidents, according to ESA, station-wide safety procedures remain underdeveloped.[26] There remains no unified ISS Safety Authority, and political sensitivities continue to limit international information transfer. Nevertheless, the United States expects to support the USOS until at least 2020, while Russia hopes to eventually utilize their segment as the building block of a third-generation space station.[27]

CONTRASTING THE U.S. AND SOVIET/RUSSIAN SPACE PROGRAMS

Although the technical aspects of spaceflight remain the same whether one launches from Baikonur or Cape Canaveral, significant philosophical differences separate the Soviet/Russian and U.S. space programs. These differences are driven in large part by programmatic and socio-political influences.[28–35]

- Historically, the Soviet/Russian space program has been less open to the public and more accepting of risk than its U.S. counterpart.
- The Soviet/Russian space program has approached spacecraft design from an evolutionary, rather than a revolutionary, perspective—the current Soyuz spacecraft and Soyuz rocket

are part of an engineering lineage that stretches back 40+years.
- Having more experience with long-duration spaceflight than the United States, the Soviets/Russians are accustomed to relying on repair as a means of ensuring spacecraft reliability.
- The Soviet/Russian program assigns less autonomy to their cosmonauts, relying instead on flight controllers on the ground and/or automated systems on the spacecraft for critical decisions and actions. In contrast, the United States typically allows considerably more crew control of spacecraft and launch vehicle functions.

Despite these differences, the Soviet/Russian and U.S. programs have comparable flight safety records, with each having lost only 2 crews in 50+years of spaceflight.

VOSTOK/VOSKHOD

The Soviet Vostok program succeeded in launching the first manned spacecraft, the first multi-orbit and multiday missions, and the first set of tandem spaceflights. The single-seat capsule (Vostok 3KA) was launched on a variant of the R-7 Inter-Continental Ballistic Missile (ICBM) known as the Vostok-K (8K72K). Like its American counterpart (see *Fig. 1*), the Mercury-Atlas, the R-7 had a relatively poor track record prior to its first manned launch, succeeding only 57% of the time. (According to Hall,[29] a leading Soviet space historian, it was Soviet practice to carry out "more flight-testing than trouble shooting before flight tests"; this may in part explain the R-7s relatively low early success rate. Nevertheless, most Soviet engineers considered the launch vehicle to be the weakest link of the Vostok program.[30]) As such, ejection seats, which were nominally used during landing, were also made available for ascent emergencies.

To improve the reliability of the vehicle during flight, a strict quality control and testing program was put in place for Vostok. Every aspect of the spacecraft's fabrication underwent "painstaking examination" and a "complete cycle of factory tests" before being delivered to the launch site.[30] Parts that passed inspection were then logged as "suitable for 3KA" to differentiate them from unmanned R-7 missile components (a technique analogous to one used in Project Mercury).

Functional redundancy and design margins also served to improve spacecraft safety. The spacecraft's pressurization and control systems were designed to withstand a single fault,[30] and life support consumables were sized to last until the natural decay of the vehicle's orbit (thereby mitigating the effects of spacecraft retrorocket failure—a very real risk given its occurrence on the unmanned Korabl-Sputnik 1). Notably, Vostok differed from the Mercury capsule in that manual control did not serve as a means of redundancy.

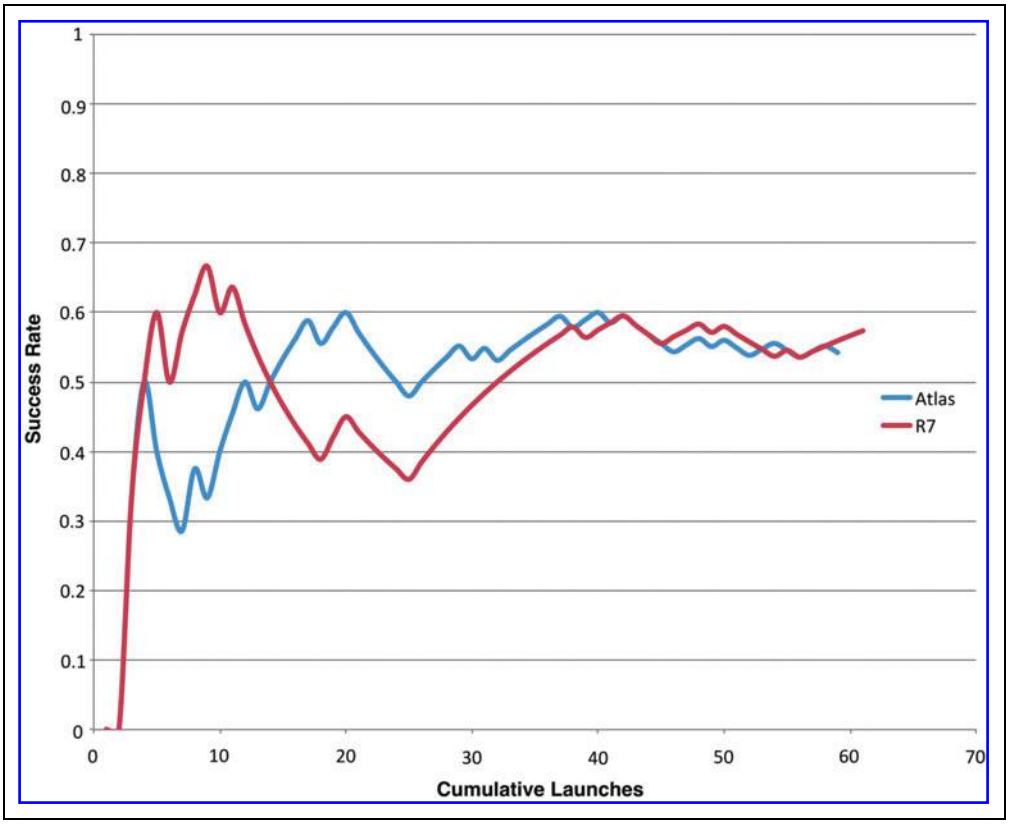

Fig. 1. R-7 and Atlas cumulative success rates prior to their first manned launch. Data taken from "Space Launch Report".[36]

In 1964, Vostok was succeeded by Voskhod, an upgraded multi-crewed capsule with redundant re-entry rockets, an added descent braking engine, and in one instance, an EVA airlock. In order to accommodate multiple crew members, Voskhod cosmonauts were launched without ejection seats, abort tower, or pressure suits.

Both Voskhod flights and all six Vostok flights ended with the cosmonauts' safe return; however, several close-calls occurred during re-entry. On Vostok 1, 2, 5, and Voskhod 2, the instrument module failed to disconnect from the descent module, causing the spacecraft to tumble until the dynamic pressure of re-entry could separate the two segments. Voskhod 2 also suffered from a failure of its automated re-entry system, forcing the two cosmonauts to rely on their backup manual re-entry system. The spacecraft landed several thousand miles off course, and the cosmonauts were not recovered until 48 hours after landing.

SOYUZ

The Soyuz spacecraft has been the mainstay of the Soviet/Russian manned space program. First launched in 1967, Soyuz has supported 115 crews on six different spacecraft variants (Table 1 shows a summary of Soyuz missions as of late 2012). Although it was originally designed for the Soviet manned lunar program and actually flew several unmanned Zond circumlunar flights,[30] Soyuz has since proven its merit as a space station transfer vehicle, shuttling crews to Salyut, Mir, and the ISS. (During the 1970s, six Soyuz missions ended prematurely due to rendezvous or docking failures; however, in the intervening years, Soyuz has since improved its track record.[34])

The Soyuz spacecraft is launched on top of the Soyuz booster, a derivative of the R-7 ICBM. Throughout the years, this launch vehicle has proven exceedingly reliable—with 700+ launches to its credit, the Soyuz booster maintains a success rate that exceeds 97%.[36] Despite this exceptional track record, all manned Soyuz missions are launched with an automatic Launch Escape System (SAS); additionally, all Soyuz subsystems are designed to be one fault tolerant to loss of mission, and two fault tolerant to loss of crew.[30] As a final precaution, all spacecraft systems undergo thorough testing prior to flight.[34]

Table 1. Soyuz variants, launch dates, and launch numbers, as of the end of 2012

Soyuz Variant	Year(s)	Launches
Soyuz 7K-OK/OKS	1967–1971	10
Soyuz 7K-T	1973–1981	26
Soyuz 7K-TM	1975	3
Soyuz-T	1976–1986	15
Soyuz-TM	1986–2002	33
Soyuz-TMA	2003–2012	22
Soyuz-TMA-M	2010–2012	7

During the last four decades, the Soyuz spacecraft has undergone a series of modifications aimed at incrementally improving cost, safety, and mission assurance. However, these changes have been evolutionary, rather than revolutionary in nature; as such, the current design retains (and benefits from) both state of the art hardware and flight-proven subsystems.‡

Nevertheless, Soyuz has suffered its share of critical and catastrophic failures, primarily in the early years of its history. In 1975, the Soyuz 18a booster failed to stage, leading to the automated separation of its capsule prior to orbital insertion. Eight years later, cosmonauts aboard Soyuz T-10a were the first to survive a pad abort after their Soyuz booster caught fire on the launch pad.

Critical and catastrophic incidents have also occurred during re-entry and landing. Cosmonauts on Soyuz 23 landed in a freezing lake and were rescued only a few hours before their consumables were depleted. In 1967, cosmonaut Vladimir Komarov perished when his parachute failed to deploy on Soyuz 1. Four years later, three cosmonauts died when a pressurization valve aboard their Soyuz 11 spacecraft inadvertently opened during re-entry. Both catastrophic incidents have been attributed to a flawed quality control system.[30]

SALYUT

In 1971, the Soviet Union launched Salyut 1, the world's first space station. In the decade to follow, the original Salyut was succeeded by six first-generation and two second-generation Salyut stations. Of these nine space stations, three were destroyed during launch or in the early days of its mission.[31]

Due to Salyut's close ties with the military Almaz space station, many details regarding Salyut hardware remain classified. However, evidence suggests that a number of subsystems used in Salyut were first flight-tested in the manned Soyuz and unmanned Zond programs.[32]

No cosmonauts were lost while aboard Salyut space stations; however, several critical incidents occurred, including a small electrical fire aboard Salyut 1, a (potential) Environmental Control and Life Support System failure on Salyut 5, and a fuel leak on Salyut 7.[31] In 1985, a cosmonaut, Vladimir Vasyutin, was evacuated from the station prior to the completion of his mission. Additionally, six missions to Salyut stations were curtailed by rendezvous or docking failures.

MIR

The Soviet (later, Russian) Mir was the first space station to be assembled on orbit in piecemeal fashion. The first module, the base block, was launched in 1986; six additional modules were added in the decade that followed. Presaging the docking mishaps that would plague Mir in the 1990s, the first three modules to be added—Kvant 1, Kvant 2, and Kristall—all suffered from initial automated docking failures before successful re-rendezvous and attachment.[35]

‡Many Soyuz components were previously or concurrently incorporated on Kosmos, Zond, Progress, and Salyut spacecraft.[30]

Table 2. Near-miss, critical, and incidental events on Mir

Type	Category	Mission	Year	Event
Collisions	Near-misses	Progress M-7	1991	Passes within 5 m of station
		Progress M-33	1997	Passes within 10 m of station
	Incidental	Soyuz TM-17	1993	Collides with Kristall
		Progress M-24	1994	Collides with Mir
	Critical	Progress M-34	1997	Causes depressurization of Spektr
Fire	Incidental	Mir EO-17	1994	Vika oxygen fire
		Mir EO-23	1997	SFOG oxygen fire
Medevac	Critical	Soyuz T-14	1985	Medevac due to crew illness

SFOG, Solid-Fuel Oxygen Generator.

During its 15 years in orbit, Mir greatly exceeded its design lifetime, in some cases by over a decade. Yet despite Mir's longevity, subsystem failures proved constant during its later years of operations, particularly with respect to the life support and thermal control systems.[37] Redundancy, resupply, and crew maintenance succeeded in mitigating the effects of many of these failures. Table 2 shows a summary of critical mishaps and failures onboard Mir.

Mir suffered from several critical and near-catastrophic fires. In 1994, a fire in the Vika oxygen-producing systems broke out on Mir, but was smothered before it could spread. Three years later, another oxygen fire started in Kvant 1. Although the crew extinguished the fire before it could engender catastrophe, the fire severely charred the walls of the module and generated significant levels of toxic smoke.[37,38]

Mir also suffered a number of collisions and "near-misses" with manned Soyuz transfer ferries and unmanned Progress freighters. Mir suffered much smaller collisions as well, namely in the form of MMOD. In 1994, Mir passed through the remains of the Swift–Tuttle comet and was impacted over 60 times.[35] Progress M-7 and Progress M-33 narrowly avoided collision with Mir when automated control was lost during final approach. Progress M-24 and Soyuz TM-17 actually struck the station but did not cause life-threatening damage. In 1997, Progress M-34 collided with Spektr during a test of the manual docking system, causing depressurization of the module. Only by sealing Spektr from the remaining habitat modules was the crew able to avert disaster.

Mir was deorbited in 2001, after being visited by 39 crews from 12 countries. Modules for the follow on Mir 2 were eventually utilized on the Russian segment of the ISS.[39]

SUMMARY

Of the 290 manned missions launched by the governments of the United States and Soviet Union/Russia between 1961 and 2012, only four have resulted in catastrophic (i.e., fatal) in-flight accidents. This amounts to a success rate of over 98%. If commercial spaceflight is to succeed in the United States, a similar (or better) safety record must be achieved. This goal can be achieved, in part, by assimilating "lessons learned" from past government space programs.

In addition to (and in conjunction with) past lessons learned, the following "best practices" should also be considered:

- Quality assurance programs (e.g., testing, evaluation, and inspection) significantly improve vehicle reliability. In those instances where testing and thorough evaluation of inspection or test results has been limited or curtailed (e.g., Mercury, Vostok/Voskhod, pre-Challenger Space Shuttle, early Soyuz), risk has increased significantly; in some cases to the point of catastrophe.[3,24,30,40]
- Design techniques such as redundancy, fault tolerance, factors of safety, design margins, and Design For Minimum Risk must be carefully incorporated into the vehicle to safeguard the crew. Although no vehicle can be made perfectly safe, these techniques, when given proper consideration, reduce risk. A nearly redundant spacecraft (the lunar module) helped saved the crew of Apollo 13, while conversely, an O-ring design that was not fully fault tolerant doomed the crew of Challenger.
- When design techniques fail to eliminate a hazard, operational procedures can save the crew, particularly during long-duration missions. Skylab, Salyut, Mir, and ISS missions have all been saved or extended because of in-flight uploaded software patches or operational workarounds.
- Significant crew and controller training has been a staple of both U.S. and Soviet/Russian space programs since the start of the space age, and has contributed significantly to mission success.
- Ejection seats and/or abort modes should be carefully considered during the early design phase of the spacecraft and/or launch vehicle. Although aborts have only been performed three times in the last half century (Soyuz T-10a pad abort; Soyuz 18a; STS-51-F Abort To Orbit), they have saved the crew on each occasion.

These techniques do not come cheaply and may take commercial aerospace companies significant time, money, and effort to assimilate. However, by increasing safety and mission success, they may well serve to drive costs down in the long run.

ACKNOWLEDGMENTS

This work was supported in part by the William F. Marlar Memorial Foundation and from related efforts with the Sierra Nevada Corporation (SNC) and the FAA Center of Excellence for Commercial Space Transportation (COE CST).

AUTHOR DISCLOSURE STATEMENT

Mr. Robert Ocampo's doctoral research is funded in part by the Sierra Nevada Corporation and Professor Klaus is supported in part by SNC and the FAA COE CST. Although SNC and the FAA have

supported efforts related to this study, neither entity explicitly endorses or rejects the findings of this research. The presentation of this information is in the interest of invoking technical community comment on the results and conclusions of the research.

REFERENCES

1. NASA. ISS Crew Transportation and Services Requirement Document. NASA CCT-REQ-1130, 2012.
2. Cassidy, J., Johnson, R., Leveye, J., & Miller, F. The Mercury-Redstone Project. NASA, 1964.
3. Swenson, L. Grimwood, J., & Alexander, C. This New Ocean: A History of Project Mercury. NASA, 1966.
4. Bond, A. A Review of Man-Rating in Past and Current Manned Space Flight Programs. Houston: Eagle Engineering/LEMSCO, 1988.
5. French, J., & Bailey, F, Jr. Mercury Project Summary: Including Results of the Fourth Manned Orbital Flight. NASA, 1963.
6. Burkhalter, B., & Sharpe, M. Mercury-Redstone: the first American man-rated space launch vehicle. Acta Astronautica 1990;21:819–853.
7. Hacker, B. & Grimwood, J. On the Shoulders of Titans: A History of Project Gemini. NASA, 1977.
8. Franzini, B., & Fragola, J. Human rating of launch vehicles: historical and potential future risk. Reliability and Maintainability Symposium (RAMS), 2011 Proceedings-Annual. IEEE, 2011.
9. Embrey, S. The Apollo Saturn emergency detection system. Washington, DC: Bellcom, Inc., 1966.
10. Harris, E., & Brom, J. Apollo Launch-Vehicle Man-Rating: Some Considerations and an Alternative Contingency Plan. NASA, 1965.
11. Murray, C., & Cox, C. Apollo, the Race to the Moon. New York: Simon and Schuster, 1989.
12. Bilstein, R. Stages to Saturn: A Technological History of the Apollo/Saturn Launch Vehicle. NASA, 1980.
13. Brooks, C., Grimwood, J., & Swenson, L. Chariots for Apollo: A History of Manned Lunar Spacecraft. NASA, 1979.
14. Young, A. Lunar and Planetary Rovers: The Wheels of Apollo and the Quest for Mars. Berlin: Praxis Publishing Limited, 2007.
15. Apollo 204 Review Board. Report of Apollo 204 Review Board to the Administrator Natioanl Aeronautics and Space Administration. Washington, DC: U.S. Government Printing Office, 1967.
16. Apollo 13 Review Board. Report of Apollo 13 Review Board. NASA, 1970.
17. Hitt, D., Garriott, O., & Kerwin, J. Homesteading Space: The Skylab Story. Lincoln, NE: University of Nebraska Press, 2008.
18. Belew, L. & Stuhlinger, E. Skylab: A Guidebook. Washington, DC: US Government Printing Office, 1973.
19. Stockton, W. & Wilford, J. Spaceliner. New York: Times Books, 1981.
20. Heppenheimer, T. History of the Space Shuttle: The Space Shuttle Decision, 1965–1972. Wahington, DC: Smithsonian Institution Press, 2002.
21. Columbia Accident Investigation Board. Report of the Columbia Accident Investigation Board, Volume I. NASA, 2003.
22. Williamson, R. "Developing the Space Shuttle" in Exploring the Unknown, Volume IV: Assessing Space. NASA, 1999.
23. NASA. Inflight Crew Escape System. http://spaceflight.nasa.gov/shuttle/reference/shutref/escape/inflight.html
24. Presidential Commission on the Space Shuttle Challenger Accident. Report to the President on the Space Shuttle Challenger Accident, 1986.
25. International Space Station Independent Safety Task Force. Final Report of the International Space Station Independent Safety Task Force. 2007.
26. Pelton, J. & Marshall, P. Space Exploration and Astronaut Safety. Reston, VA: American Institute of Aeronautics and Astronautics, 2006.
27. Zak, A. Russia to save its ISS modules. BBC News, 2009.
28. Portree, D. Mir Hardware Heritage. NASA, 1995.
29. Hall, R. & Shayler, D. The Rocket Men: Vostok & Voskhod. The First Soviet Manned Spaceflights. Berlin: Springer, 2001.
30. Chertok, B. Rockets and People, Volume 3: Hot Days of the Cold War. NASA, 2009.
31. Ivanovich, G. Salyut—The First Space Station: Triumph and Tragedy. Berlin: Praxis, 2008.
32. Gibbons, J. Salyut: Soviet Steps Toward Permanent Human Presence in Space. Washington, DC: DIANE Publishing, 2008.
33. Shelton, W & Titov, G. Soviet Space Exploration: The First Decade. New York: Barker, 1969.
34. Hall, R. & Shayler, D. Soyuz: A Universal Spacecraft. Berlin: Springer, 2003.
35. Harland, D. The Story of Space Station Mir. Berlin: Praxis Publishing Limited, 2005.
36. Kyle, E. Space Launch Report. www.spacelaunchreport.com/log2012.html
37. Burrough, B. & Murray, B. Dragonfly: NASA and the Crisis Aboard Mir. New York: Harper Collins Publishers, 1998.
38. Linenger, J. Off the Planet. New York: McGraw-Hill, 2000.
39. Bond, P. The Continuing Story of the International Space Station. Berlin: Springer, 2002.
40. Vaughan, D. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago: University of Chicago Press, 1997.

Address correspondence to:
Robert Ocampo
Aerospace Engineering
429 UCB
Boulder, Colorado, 80309

E-mail: robert.ocampo@colorado.edu