

JSC SMA FLIGHT SAFETY OFFICE

Gary Johnson: Lessons Learned from 50+ Years in Human Spaceflight and Safety

April 30, 2018

SMA Engineering Contract
Product 5, Delivery 2
JS-2018-009
NNJ13RA01B



Record of Revisions/Changes

Revision	Description	Date

Table of Contents

Introduction.....	5
Redundancy can help or hinder.....	6
Apollo 10 (May 1969): Fuel Cell Failure.....	6
Apollo 12 (November 1969): Lightning Strike.....	6
Skylab 3 (July 1973): Propellant Leak and Rescue Mission.....	7
Space Shuttle Orbiter Electrical System.....	7
Expect the unexpected, and never stop learning.....	9
Apollo 13 (April 1970): Oxygen Tank Explosion.....	9
Apollo 14 (January 1971): Docking Problem.....	10
Apollo 15 (July 1971): Propulsion System Electrical Short.....	10
Documenting and sharing information: communication is key.....	12
Apollo-Saturn Mission 201 (February 1966): Loss of Reaction Control System.....	12
Apollo Environmental Control System (April 1966): Fire.....	12
Apollo 8 (December 1968): Launch Pad Electrical Test	13
Apollo 11 (July 1969): Service Module Entry	14
Skylab 2 (May 1973): Emergency Docking Procedure.....	15
Apollo-Soyuz Test Project (Spring 1975): Service Module Inspection.....	16
Human factors and crew error.....	17
Apollo 10 (May 1969): Inadvertent Lunar Module Abort.....	17
Skylab 4 (November 1973 – February 1974): Loss of Control During Entry.....	17
Apollo-Soyuz Test Project (July 1975): Second Docking and CM Entry.....	18
Test as you fly, fly as you test, and the value of real-time testing.....	20
Apollo 7 (October 1968): Electrical Short.....	20
Apollo 16 (1972): Lunar Rover Anomalies.....	20
Apollo 16 (April 1972): Delayed Lunar Descent.....	20
Politics is the enemy of good design.....	22
Space Shuttle Main Engine Electrical Design.....	22
Space Shuttle Avionics Computers.....	22
Automatic versus manual control.....	24

Drawings help, but remember to inspect actual hardware.....	26
Apollo 4 (1967): Launch Pad Instrumentation Electrical Noise.....	26
Mars Viking Test (1975): Test Stand Instrumentation Electrical Noise.....	26
Hazard analysis is critical.....	28
Apollo Mission A-003 (1965): Little Joe II Booster Fin Failure.....	28
Apollo-Saturn Mission 201 (February 1966): Loss of Reaction Control System.....	28
Apollo Environmental Control System (April 1966): Fire During Test.....	29
Apollo 1 (January 1967): Fire and Loss of Crew.....	29
Apollo 13 (April 1970): Oxygen Tank Explosion.....	30
Skylab 3 (July 1973): Propellant Leak and Rescue Mission.....	30
Killing “Death Star:” be persistent in advocating for safety.....	31
Working with the Russians.....	34
Summary and Conclusions.....	36
Acronyms.....	38
Sources.....	39
Appendix A: Gary Johnson Career History.....	43

Introduction

Future spacecraft designers and managers need to be aware of problems, corrective actions, and the resulting lessons learned to avoid experiencing the same problems in new programs. Fewer and fewer people with firsthand experience of the design, test, and operations of past programs, such as Apollo, are available today to pass on their experience. This white paper, sponsored by the Johnson Space Center (JSC) Safety and Mission Assurance (SMA) Directorate Flight Safety Office (FSO), will discuss the major lessons I learned during my 50+ years (and counting) working in human spaceflight.

I worked on all the major human spaceflight programs beginning with Apollo. I started my career in 1964 at NASA's Manned Spacecraft Center (MSC), which is now JSC, in the Engineering and Development Directorate Power Distribution and Sequencing Section, where I was responsible for the design and testing of the Apollo Command and Service Module (CSM) sequencing system. I also served as the manager for the sequential subsystem for the Apollo CSM, Lunar Module (LM), and Skylab CSM, and I was a member of the Apollo-Soyuz Test Project (ASTP) Working Group 4.

Later, I was assigned to the Engineering Office, Space Shuttle Orbiter Project. After transferring to the Mission Operations Directorate, I served as the first Space Shuttle Orbiter Flight Controller for Electrical, General Instrumentation, and Lighting (EGIL). I was also the Branch Chief for the Mission Operations Directorate Mechanical and Payload Systems Branch and the Guidance and Propulsion Systems Branch.

My experience in the Safety, Reliability, and Quality Assurance (SR&QA) Directorate, later called the SMA Directorate, began in 1985 when I became the Deputy Director. I was subsequently the co-chairman of the NASA/Mir Joint Safety Assurance Working Group, the Deputy Director of Russian Projects in SR&QA, and the co-chairman of the International Space Station (ISS) Program Joint American-Russian Safety Working Group.

I retired from NASA in 2006, but returned as a consultant

in 2007 as a safety expert for the Constellation Program and a representative on the Orion Project Standing Review Board. I've also worked in the JSC SMA FSO since 2007. (For detailed career information, see Appendix A.)

My lessons learned are arranged according to themes, but many of the incidents I describe contain lessons on multiple themes. I hope this paper will communicate valuable experience to younger engineers, so they can continue to build on the lessons of the past to create even better human spaceflight programs.

Redundancy can help or hinder

At the beginning of any spacecraft program the reliability goals and the redundancy philosophy for safety should be established. On the Apollo Program, the reliability goals were identified for each function to be performed. For example, the reliability apportionment established for the Service Module (SM) post-separation from the Command Module (CM) was 0.999985 (or 15 failures/10-to-the-6 missions, the reliability terminology used in 1965). If the function was safety-critical, the design should have no single-point failures and should be fail-safe. The amount of subsystem redundancy was determined by the criticality, flight experience, and maturity of technology. As a result the redundancy varied. For example, fuel cells were a new technology for aerospace applications, while the electrical power buses and power contactors for switching were proven technology. Therefore, the redundancy level was three fuel cells and two main buses. For the alternating current (AC) power system the solid state inverters were a new technology for aerospace, and three inverters with two AC buses was the redundancy level. One inverter was always offline as a spare.

Apollo 10 (May 1969): Fuel Cell Failure

After docking with the Command and Service Module (CSM) and jettisoning the LM while the CSM was in lunar orbit, a caution and warning alarm sounded, and the Fuel Cell 1 AC circuit breaker tripped, due to a short in the hydrogen pump, causing the loss of Fuel Cell 1. The CM pilot told the commander he thought another one would go out as soon as they got to the back side of the moon. Halfway through the next night side pass, an alarm occurred on Fuel Cell 2 due to a fluctuation on the condenser exit temperature. With a minor electrical load reduction, Fuel Cell 2 continued to provide power.

Lesson: Critical systems should be two-fault tolerant. Consumables, like electrical power, which are required for crew safety should have an additional level of redundancy for missions beyond Earth orbit.

Redundancy saved the crew in this case, since without redundancy in the fuel cells, the crew would not have had enough power to return to Earth. The CSM could safely return with one fuel cell down.

Apollo 12 (November 1969): Lightning Strike

During the Apollo 12 launch on November 14, 1969 lightning struck the spacecraft. At 11:22 am, T+36 seconds, the crew saw a bright light. At T+36.5 seconds many errors occurred: Fuel Cells 1, 2, and 3 disconnected; Main Buses A and B were under-voltage; AC buses 1 and 2 overloaded. The warning lights and alarm came on in the cabin, indicating the failure of the Inertial Stabilization System. At T+52 seconds (13,000 feet) lightning struck the vehicle and the Inertial Measurement Unit platform tumbled.

The potential effect on the vehicle was induction into wiring, depending on the location and rate of change of potential and direct current (DC) flow in grounding. The high negative voltage spike (delta voltage/delta time) caused the Silicon Controlled Rectifiers to trip on the fuel cell and AC inverter overload sensors. Failures occurred in four SM Reaction Control System (RCS) helium tank quantity measurements, five thermocouples, and four pressure/temperature transducers.

Using power from the battery relay bus, the crew reconnected the fuel cells to Main Bus A and B, and reconnected the inverters to AC Bus 1 and 2. The mission continued.

Good structural electrical bonding among the Launch Escape System, CM, SM, Spacecraft LM Adapter, and Saturn V Inertial Unit prevented major damage to the systems and vehicle. The Launch Vehicle Instrument Unit computer provided ascent guidance and control since the CM computer, which was the backup for ascent, stopped working at the lightning strike. Ascent abort sensor processing (Emergency Detection System) was performed by the Instrument Unit avionics. Having the redundant computer for ascent guidance and

control located in the launch vehicle instead of the CM saved this mission. CM battery power prevented the loss of all electrical power when fuel cells disconnected from the main buses. This allowed the crew to recover and reset the fuel cell connections to the main buses.

Lesson: Redundant systems for critical functions should be dissimilar and/or located in different parts of the vehicle.

Skylab 3 (July 1973): Propellant Leak and Rescue Mission

During the rendezvous on July 28, 1973 Commander Alan Bean saw the first indication of a problem: the attitude was off about 25 degrees in yaw. According to fellow astronaut Owen Garriott, Jack Lousma “suddenly announced, ‘Owen, there goes one of our thrusters floating by the window.’”¹

The CSM RCS Quad B forward-firing positive-yaw engine oxidizer valve had leaked, and the nitrogen tetroxide had frozen into the shape of the thruster exhaust cone. The crew also reported a “snow storm” on the right side (Quad B side) of the spacecraft at the same time. The Quad was isolated, and the rendezvous had to be completed with only three of the four SM Quads. The crew members had not trained for this, but were able to complete the docking to Skylab.

Five days later after docking to Skylab, the Quad D engine package temperature had decreased, causing an alarm. The crew saw a “snow storm” blowing by the window and knew that something was leaking from Skylab. With guidance from the ground, the RCS engines were inhibited, and the isolation valves closed about 1 hour and 20 minutes later. This second oxidizer leak prompted a concern that the oxidizer portion of the SM RCS had a problem.

If this were true the remaining SM RCS Quads could fail, and preparations began at Kennedy Space Center (KSC) for a rescue mission. By eliminating subsystem tests the spacecraft CSM-119 could be mated with its Saturn 1B

launch vehicle the next week. Removing storage lockers allowed for two more crew couches to be installed under the existing three. Deleting the Countdown Demonstration Test meant the spacecraft and launch vehicle could be ready in early September. The Skylab Multiple Docking Adapter had been designed with a spare radial docking port, in case a rescue spacecraft might have to dock. Commander Vance Brand and Pilot Don Lind were assigned as the rescue crew.

While rescue preparations were underway, Engineering concluded that the SM Quads did not share a common problem. The only condition that would match the timeline of events and leakage rates experienced on Quad D was an improperly torqued Dynatube connector. A contingency procedure was developed so that if another SM RCS Quad failed, the CM RCS could be used to de-orbit and for control during entry. The mission was allowed to continue, and the Skylab rescue capability was available if needed.

The innermost and primary seal of a Dynatube connector is a mirror-finished, metal-to-metal seal. The second seal is a butyl O-ring. Tests showed that a finger-tight Dynatube connection would pass a preflight helium leak test. However, when the RCS system is pressurized prior to liftoff, the oxidizer penetrates the unmated primary metallic seal, and the O-rings alone seal the connection. Tests showed the butyl O-ring degrades and can start leaking when exposed to nitrogen tetroxide at flight temperatures and pressures. The butyl O-ring seal was considered a redundant seal, but did not actually provide redundancy, creating a false sense of security.

Lesson: Redundant systems must use compatible materials to be effective. Flight-critical fluid connections should have controls in place to insure proper torquing of connections, and seals should be compatible with the fluid they are trying to seal.

The program’s early planning to develop a Skylab rescue capability allowed a rescue mission to be developed quickly.

Space Shuttle Orbiter Electrical System

1 Hitt, Garriott, and Kerwin, *Homesteading Space: The Skylab Story*, page 239

During the Space Shuttle Program, the orbiter avionics were required to have an additional level of redundancy (three levels) compared with what was required for the Apollo Program (two levels). This was because the new digital avionics system had no proven flight experience. This also applied to other systems, so that launches could continue even if one system failed. (This supported not only safety, but the goal of the shuttle launching repeatedly with a quick turnaround, like an airline.)

The orbiter had three hydraulic systems and was powered by three auxiliary power units, three fuel cells, and three main electrical buses. Early in the design phase the orbiter contractor's manager for electrical systems and the NASA electrical power distribution engineers recommended not to require the extra redundancy (three levels) to the main DC bus system, since it was very reliable and had been flight proven. This recommendation was not adopted, and the orbiter power system was designed with three redundant systems. The additional level of redundancy added cost and complexity to the electrical power distribution systems. While redundancy is often beneficial, increasing the complexity of a system introduces the possibility for more problems and greater risk. Unnecessary redundancy can hinder a program's development by adding cost and introducing new issues.

Lesson: To minimize spacecraft complexity, weight, cost, and schedule the level of redundancy should depend on the criticality, flight experience, and technology maturity of the hardware. Unnecessary redundancy adds complexity, which increases cost and risk.

Expect the unexpected, and never stop learning

When you are responsible for a spacecraft crew safety system, even if you meet the program requirements for operation and redundancy, you need to imagine situations in which something unexpected happens or something unexpected fails. What if the Lunar Module batteries need to be charged (Apollo 13)? What if two of the three docking probe contacts fail to close, preventing probe retract (Apollo 14 and Skylab 2)? What if the electrical short only occurs in zero gravity (Apollo 15)? What if the launch vehicle structurally fails or the spacecraft upper deck sharp edges cut the parachute risers (Apollo Mission A-003)?

Apollo 13 (April 1970): Oxygen Tank Explosion

During trans-lunar flight at approximately 56 hours, one of the two SM oxygen tanks over-pressurized and exploded, causing the loss of oxygen in that tank and an oxygen leak in the remaining tank. This resulted in loss of all three fuel cells, loss of the primary oxygen source, and loss of electrical power to the CM except for the entry batteries. We know how the mission was able to continue with the use of the Lunar Module and the crew safely returned. My support was in the Mission Evaluation Room (MER) at the CSM Electrical Power Distribution and Sequencing position. When the explosion of the SM oxygen tank occurred, I was in the MER and did not leave until the next morning. By then the CSM was completely unpowered and the main activity was with the engineers supporting the active LM systems.

Prior to Apollo 13, I had thought about how to possibly use the CM's battery charger to charge the LM batteries if needed. I worked with the LM Electrical Power Subsystem Manager, and we developed a procedure using an on-board umbilical to electrically connect the battery charger output on a CM bus to the LM bus.

After the explosion of the SM oxygen tank, we later used this procedure in reverse to provide power to the unpowered CM from the LM.²

2 This was mentioned in the book *Apollo: the Race to the Moon* by Charles Murray and Catherine Bly Cox on page

Later I worked on the CM power-up configuration before the jettison of the LM before re-entry. This consisted of marking up a CM display panel drawing with switch and circuit breaker positions (marked red if the circuit breaker was to be closed and marked blue if it was to be open). The switch position was shown by a red arrow in the direction to be positioned. This information was provided to the Flight Control Team that converted the information to a checklist to be read to the crew. I still have the marked-up document, "V34-900101, Rev. AC, Controls & Displays – Main Display Console Panels drawing A1 & A2, SC 109 Thru 115A, 1-23-70." After the mission I was involved in the NASA investigation as to what caused the SM oxygen tank to explode. I still have the chart of total fuel cell electrical current that was used in the investigation.

Prior to launch, several conditions resulted in the oxygen tank failing during the mission. By design, the cryogenic oxygen tank required both electrical heaters to maintain pressure and fans to prevent stratification. The tank was a complex assembly with blind installation of the quantity probe, heater/fan assembly, and fill tube. This design left wiring insulation vulnerable to damage during assembly with no way to inspect after installation. The Teflon-insulated wiring was in close proximity to the heater elements and fan and is a combustible material in the oxygen tank. The Apollo 13 tanks had originally been installed on Apollo 11, but a change required the tanks to be removed. During removal of the oxygen shelf, one bolt was left in place causing the fixture to break and resulting in a two-inch drop of the shelf and tanks. Although a loosely fitting (due to loose specification tolerances) fill tube could have been displaced by this, all testing was passed. No cryogenic tests which would have revealed the problem were performed.

During the Countdown Demonstration Test the oxygen tank could not be emptied by the normal means of pressurized oxygen gas. A leak at the fill tube would cause this. Instead, the tank heaters were turned on to boil off the oxygen in the tank. The thermostatic

439. ("The MER had figured out a way to pass power from the LEM [or LM] to the CSM...")

switches were rated for 30 volts DC, but several years earlier the heater ground power supply voltage was raised to 65 volts to reduce the pressurization time. As the temperature increased, the thermostatic switch opened, and the higher voltage caused the contacts to weld closed. With the heaters continuously on, the temperature approached 1000 degrees and damaged the wire insulation, setting up the conditions for a short and ignition inside the tank. Ground personnel did not notice the continuous heater operation. During the prelaunch problem solving neither the Apollo Spacecraft Program Manager nor the KSC Director of Launch Operations knew the tank had previously been dropped or that the heaters had been on for eight hours straight.

Lesson: My biggest contribution to this event was the contingency procedure developed prior to the mission, which was used to provide critical electrical power from the LM to the CM. Try to anticipate unexpected problems that may arise and solve the problem in advance.

The design for critical hardware should avoid blind installation that prevents post-assembly verification. Materials associated with gaseous or cryogenic oxygen should be compatible. The design should specify tolerances that take into account the worst case stack-up and prevent problems due to tolerance variation. Changes to hardware operation should be verified to be within the hardware design limits. Ground test consoles should have both visual and audible alarm limits for critical operating parameters. Redundancy in life support, LM life support systems, propulsion, communication, and GNC allowed for the safe recovery of the crew.

Apollo 14 (January 1971): Docking Problem

Prior to the launch of Apollo 14 I was working as the Apollo Sequential Subsystem Manager and was concerned that the two small pyrotechnic batteries A and B could fail, as they were not able to be recharged like the entry batteries. I started thinking of an

alternative way to fire the pyrotechnics in case the batteries failed. I developed a procedure to fire the CM pyrotechnics by using the 16 mm camera cable that connected to a utility power outlet. One connector would be cut off, exposing the three wires. One 28-volt wire and one power return could then be inserted into the sequencer box access connector. Step 9 of the procedure addressed “No docking probe retract,” since retracting the CSM docking probe required firing a pyrotechnic.

After Apollo 14’s launch and trans-lunar injection the crew proceeded to dock to the LM. The crew made six attempts at capture (soft dock), which required two of three capture latches to close to apply power to the pyrotechnic to retract the probe, so the crew was unable to obtain hard dock with the LM.

After several docking attempts, I went back to the office to get the emergency procedure memorandum. To make sure the crew could do the procedure, Apollo astronaut Ken Mattingly went with the crew tool kit to a previously flown CM in the JSC Auditorium. He was able fix a cable and gain access to the Lunar Docking Events Controller connector J5 located in the right-hand equipment bay. This showed the procedure could be done. Mattingly and I hurried back and found out the crew had finally been able to dock after six unsuccessful attempts.

A discussion took place about continuing the mission as planned. If you were unable to obtain capture during docking of the LM ascent stage to the CSM in lunar orbit, you might not be able to transfer the crew to the CSM, so the Mission Control Center (MCC) would not have continued the mission unless a backup probe-retract procedure were available. However, knowing we had a backup procedure the MCC allowed the mission to continue.

Lesson: Anticipate how the system could fail and prepare potential work-arounds. You never know if they may be needed to continue a mission.

Apollo 15 (July 1971): Propulsion System

Electrical Short

During the mission, after trans-lunar injection and just after transposition and docking, the SM Propulsion System (SPS) thrust light illuminated with no engine fire command present. This light indicated the presence of a short to structure in the SPS ignition circuitry. Ignition would have occurred if the engine had been armed. This condition was a “No Go” for Lunar Orbit Insertion. I noted that the short indication first occurred briefly, just after Earth orbit insertion when the spacecraft was in zero gravity, and then occurred the second time as mentioned above after trans-lunar injection.

In reviewing the SPS circuitry the only place to find something floating in a closed cavity was the delta-V thrust panel switch. This switch contained a braided wire which could have a loose wire strand, and if it shorted to the case (ground) it would illuminate the SPS thrust light. This would explain what the crew was seeing. The MER Manager gave permission for me to go to the MCC to explain this theory of what might be causing the thrust indication.

I explained what I considered to be the cause of the indication to Dr. Christopher Kraft. Dr. Kraft said this sounded plausible, but that we needed to perform a test to prove the short was causing the light to illuminate, and not a fire command to the SPS. The crew procedure was modified for a test firing of the SPS during a mid-course correction. The successful firing verified that the short was isolated to the system A delta-V thrust switch and allowed implementation of an alternate procedure to safely fire the SPS engine and successfully continue the mission.³ Post-flight failure analysis showed that a loose wire strand from the braided wire inside the delta-V thrust panel was

3 Dr. Christopher Kraft stated in *NASA SP-350, Apollo Expeditions to the Moon*, “The Operations Team, working with Don Arabian, a legend in his own time, and Gary Johnson, an excellent young electrical engineer, isolated the short to one of two systems. A test firing was initiated by the crew to verify that the short existed on the ground side of one of two sets of valves. Procedures were then developed by the ground, working with the flight crew, and the mission continued.”

causing the short to structure.

Lesson: The flight environment can cause unexpected anomalies which would not have occurred on Earth. In this case, a short to structure occurred due to a loose piece of wire floating in zero gravity.

The SPS engine fire command is switch to structure (negative bus), while short to structure is more likely to occur. The engine fire command should require a positive voltage signal. Switch components that have an internal cavity should be free of possible sources of conductive debris.

Documenting and sharing information: communication is key

In a complex organization with many teams made up of many people, documentation enables information to be shared. Sharing information is key when many groups will be working on different aspects of one project, like a spacecraft. Any modifications to spacecraft design or installation need to be documented and communicated to the other systems and personnel. When significant anomalies happen, the results of formal board investigations should be shared widely to avoid repetition of the same mistakes. Mission reports should include significant mission anomalies and should be updated if a problem comes to light after the report is written. Flight operation changes to a crew checklist system procedure need to be reviewed by the engineers responsible for that spacecraft system. Drawings from a previous spacecraft program or mission must include all engineering changes to that drawing. A spacecraft project engineer, besides understanding his system, should know and work with the design, manufacturing, test, and operations personnel for that system, even though they may work under another organization, vendor, or launch center.

Apollo-Saturn Mission 201 (February 1966): Loss of Reaction Control System

During the uncrewed Apollo-Saturn (AS-201) mission after CSM separation, a short to power occurred causing the RCS commands to be transferred from the CM to the SM, resulting in the loss of RCS control. This transfer of command circuits to the shorted umbilical due to entry heating caused a large short and low voltage on Main Bus A and B till the circuit breakers opened. After the loss of the RCS, the CM went into a stable roll and did a ballistic entry instead of the planned lifting re-entry.

The cause of all this was a non-functional circuit that was routed through the CSM umbilical that was not deadfaced prior to separation, and it shorted, tripping the circuit breaker powering the Sequential Events Control Subsystem System B circuit causing loss of the redundant Earth Landing System (ELS). The non-functional circuit had been dropped from the drawings, but the wiring was left in the spacecraft and

was not disconnected from power. Since it was not on the drawing for the powered wiring going through the CSM umbilical, it was not deadfaced prior to guillotine of the umbilical.

Redundant NASA Standard Initiators, one powered by System A and one by System B (this source failed), were used on all critical pyrotechnic functions, including the ELS, and this allowed for recovery of the CM.

Lesson: Drawings should include all design changes, even disconnected or unused circuits. The lack of documentation in this case meant that the design drawings did not match the spacecraft, which made it more difficult to identify the problem.

Also, all non-functional circuits left in the spacecraft should be disconnected from both power and return. Careful review must be made to ensure all powered wiring through an umbilical to be guillotined must be deadfaced prior to cutting with the guillotine.

Apollo Environmental Control System (April 1966): Fire

On April 28, 1966 a fire occurred at the AiResearch Torrance Facility in California in the altitude chamber used to simulate the interior environment of the Apollo CM (100% oxygen at five psi). The Apollo Block 1 Environmental Control System (ECS) was undergoing a 500-hour mission-duration qualification test. The fire severely damaged the ECS and test setup equipment, but the damage was confined within the test chamber. The test was later repeated successfully and without incident, both with a new set of Block I hardware and then again with an ECS of the Block II configuration.

An MSC Fire Investigation Board was appointed on May 3, 1966 by Dr. Robert R. Gilruth, Director of the MSC, to independently investigate the cause of the fire. At the request of the Apollo Spacecraft Program Office, I was assigned to participate in the fire investigation to determine the ignition cause. I was working at the time as the CSM electrical power distribution project engineer.

I investigated the test setup wiring and the sequence of events leading to the start of the fire and interviewed the AiResearch instrumentation engineer in charge of the test. When the fire occurred, the chamber had been evacuated for several days to simulate a depressed cabin environment, which was part of the test profile, and was being repressurized with oxygen to five psi in preparation for the next test phase. The last change in configuration before the start of the fire was increasing the voltage on the steam duct heater, and 48 seconds later the chamber dome lifted due to the increased pressure from the fire.

The most probable cause of the fire was a failure of the commercial quality strip heater used to add heat to the steam duct (the line from the suit heat exchanger and glycol cooling evaporator to the vacuum source) to preclude freezing of water in the duct. This duct was wrapped with two strips of the heater tape and overwrapped with asbestos tape. During the interview the instrumentation engineer stated that the electrical technician had purchased the heater tape from Sears. This was the same type used to wrap a house's outside water line to prevent freezing. I was told not to put in my report that the electrical technician had installed Sears heater tape for the duct heater. No analysis had been done to see if the commercial tape wire insulation could withstand the temperature it would be exposed to. The steam duct heater wire had previously shorted outside the dome near a splice like the splice to the heater tape in the dome, where the wire was open and looked like it had arced.

I never saw the official board's report, because it was not distributed even to those that participated in the investigation. I had made a recommendation about a possible ignition source on the test setup wiring, but never found out if my recommendation was included.

Lesson: Information about mishaps should be shared, so that NASA can learn from its mistakes to possibly prevent future accidents. The investigation board's official report was classified, limiting knowledge of the incident and preventing the lessons learned from being widely understood.

This event should have been a wake-up call. It revealed issues that would appear again during the Apollo 1 fire (no engineering assessment of materials at 16 psi pure oxygen and no protection of Teflon wiring from physical damage to prevent arcs from shorts). Materials must be compatible with the environment (temperatures and pure oxygen exposure), but this commercial hardware had undergone no engineering analysis to show it was compatible with the test environment.

Apollo 8 (December 1968): Launch Pad Electrical Test

The Apollo Program Manager stated that if everything went well on the Apollo 7 mission, we would plan for Apollo 8 to be the first launch to go to the moon. NASA also thought the Russians would do a circumlunar flight before we did, so this launch and flight had particular pressure and concern. The AC system had electrical shorts on Apollo 7, but the cause had been identified and was thought to be fixed. However, the Program Manager directed that we run a test on the Apollo 8 spacecraft to carefully check out and test every AC load and component on the spacecraft, because he wanted to be absolutely certain nothing would go wrong with the AC system.

I was assigned to develop and run tests on the CSM AC electrical system and record the voltage, current, power factor, and wattage of every AC-powered load. I worked for about a week in Houston planning what needed to be done. I already knew and had been working closely with flight operations at the North American Rockwell Space Division (NARSD) Downey, California design and test division, as well as the KSC and NARSD launch processing CSM power distribution personnel. The CSM 2TV-1 and Spacecraft-008 vehicles (full-up vehicles) had been tested in the large vacuum chamber at JSC, so I ran my planned tests of the AC system on 2TV-1.

Then I went to KSC, and Apollo 8 was on the pad. I spent a week at KSC writing the test procedure. I had known and previously worked with the NASA and contractor

electrical power distribution engineering personnel, so they were very helpful in getting me the information I needed on the launch pad, such as spacecraft interfaces and required paperwork to develop the test on the AC system. I was very nervous at that time, even though I had run the test at JSC, because this was the first time I'd been responsible for a vehicle being tested at KSC on the pad for an upcoming moon mission, and making sure it worked with all the KSC ground support and connections for spacecraft checkout at the pad.

The test procedure was many pages. Even though I was very careful and worked closely with the NASA KSC and contractor engineers, I was sure they would carefully check my work as I was going through the required engineering and management approval signatures for the test. I assumed that the KSC engineers would carefully scrutinize the work of a young, visiting engineer from JSC. However, when this lengthy procedure started making its way through the signature chain, people signed off very quickly. They told me it seemed like I had checked with the right people and done the right things. I went through all the required signature chains for the test procedure, and no one had thoroughly checked my work. That made me even more nervous.

The test was scheduled for the third shift, meaning in the evening. I was out at the Saturn V launch pad in the White Room, sitting just outside the open crew hatch, with my test procedure and headset on to monitor the test, and the ground test crew was in the spacecraft. About halfway through the test, suddenly everything went black, and the lights in the White Room went off. I almost had a heart attack. I thought, "My goodness, what have I done?" Then I heard the control center say we had lost facility power, and I looked inside the hatch and saw all the spacecraft lights were still on, and everything was fine. The Florida Power and Light Company (which in those days we called "Florida Light and Flicker") had experienced a power failure, so the lights in the White Room had gone off, which caused everything to go dark. The spacecraft itself was on backup emergency battery power, so it was fine. It turned out there was nothing wrong with my test, but

at the time all I could think was, "You're responsible for scrubbing the Apollo 8 mission." That experience stuck with me a long time.

Lesson: On a critical task make sure your work is correct. Do not depend on someone else reviewing and checking your work. In this case, information was thoroughly documented and shared among organizations, but only one person was truly ensuring that the information was correct. Take the time to do your homework, and don't assume someone else will double check your work.

Apollo 11 (July 1969): Service Module Entry

About five minutes after CM/SM separation, the crew reported seeing the SM fly by to the right and a little above them, straight ahead. It was first visible in window number 4, then later in window number 2, and spinning. The CM should never have been close enough to see the SM after separation. During lunar return, if the SM contacted the CM in the entry corridor the result would be catastrophic, so this triggered an anomaly investigation. Photographs obtained by aircraft showed the SM entering Earth's atmosphere and disintegrating in the vicinity of the CM entry corridor. Radar tracking confirmed what the photographs had shown. The radar tracking data for the previous Apollo 8 and 10 lunar return missions were similar to Apollo 11, with the SM entering in the same corridor as the CM.

To prevent SM re-contact with the CM during entry, a System A and redundant System B SM Jettison Controller (SMJC) were located in the SM. As the Apollo Sequential Events Control System NASA Subsystem Manager, I was responsible for the design and development of the SMJC. Redundant signals from the crew operated a guarded CM/SM separation switch, which would initiate a sequence in each SMJC, firing all four -X SM RCS jets. Two seconds later it would fire the four RCS roll jets, and three seconds later would terminate the four RCS roll jets, while the -X RCS jets continued to fire. Electrical power for the SMJCs and the RCS came from the still-active fuel cells in the SM, and the RCS used the residual SM RCS propellant.

The investigation analysis showed that under certain conditions, such as propellant slosh after separation, re-contact could occur. We were lucky, as analysis showed that if the -X RCS jets were turned off after 25 seconds it would prevent any chance of re-contact. That change was then made to the SMJCs for the later Apollo missions.

This anomaly was not in any of the Apollo 11 mission reports, and I had forgotten about this close call prompting a design change to the SMJC. However, in December 2016 when looking back through my files, I found MSC-03466 “Apollo 11 Anomaly Report No. 3 Service Module Entry,” dated November 1970. Since the date is long after the Apollo 11 mission in July 1969, this is probably the reason the anomaly is not mentioned in any of the Apollo 11 mission reports.

I had previously been concerned that the Orion spacecraft SM currently being designed and built by the European Space Agency for NASA’s Orion Program did not have a requirement for an active controller after CM/SM separation. When I mentioned this, the Orion Program personnel said their analysis indicated that the present design met their requirements. The CM/SM separation force is provided by springs with the CM RCS firing after separation. No safety hazard report had been written to address the hazard of SM re-contact with CM during entry. When I rediscovered the Apollo 11 anomaly report, I passed the information along to the Orion Program. So far it has generated an action to develop a safety hazard report to cover SM re-contact with CM during entry.

Lesson: Lessons learned should be freely available and shared. Mission reports should be updated to include anomaly and failure investigations that occur after the mission. Also, because the crew had reported seeing the SM during the Technical Crew Debriefing, this information was stamped “confidential” and was prevented from appearing in the Apollo 11 mission reports. This example shows that the quality of the documentation and sharing of information from past programs can have a direct impact on future programs, which

need to be aware of all the potential hazards they may face.

Skylab 2 (May 1973): Emergency Docking Procedure

After Skylab rendezvous and approach, the first objective was a “soft docking” at Skylab’s forward port, engaging capture latches but not retracting the CM’s docking probe to obtain hard dock. Then the crew released the capture latches, backed away from Skylab, flew around to a stuck solar panel with the side hatch open, and tried to free the solar panel. Unable to free the solar panel, the crew closed the side hatch and proceeded with the final docking to Skylab.

After numerous attempts, the crew was unable to achieve soft dock. Movement after the previous soft dock may have damaged the capture latches. There was one more procedure in the checklist labeled “Final Docking Attempt.” Following the checklist, the crew members donned the pressure suits, depressed the cabin, opened the tunnel hatch, removed the probe cover, and cut the wires. They also connected the emergency retract cable to the Utility Power Outlet and the other end of the cable to the Lunar Docking Events Controller connector J5. After firing the probe retract pyro using utility outlet power, the commander was able to make direct contact, triggering the 12 structural latches and achieving hard dock.

The procedure for achieving hard dock when capture had failed was developed during the Apollo 14 mission (see “Expect the unexpected, and never stop learning”). After Apollo 14 a special cable was developed and stowed in the CM and the right-hand equipment bay panel was modified to allow quick access to the J5 connector. The procedure did not require removing the probe retract cover to cut wires, for which the crew had to be suited and the cabin depressed. Later, without coordinating with Engineering, the Flight Operations personnel changed the crew checklist to require the cutting of the probe wires.

The culture at the time was that only Flight Operations

and the crew were involved in developing the crew checklist procedure, and Engineering did not have the opportunity to review the crew checklist. The official Engineering interface with Flight Operations on crew procedures was via the Crew Procedure Change Request.

Lesson: Organizational culture should encourage interdepartmental communication. In this case, because organizations outside of Flight Operations could not review and approve crew procedures, the Skylab 2 crew used a much riskier procedure, which required donning suits and depressurizing the cabin. Engineering's procedure could have been performed using only the emergency probe retract cable without requiring access to the docking probe.

Sharing information across organizations can enable better, more informed decisions. A process change with regard to reviewing crew procedures occurred after the Space Shuttle *Challenger* accident when, over the objections of Flight Operations, the Space Shuttle Program approved the request from SR&QA to allow safety engineers to review the checklist to ensure the operational hazard controls were properly implemented.

Apollo-Soyuz Test Project (Spring 1975): Service Module Inspection

The later Apollo missions had a scientific instrument bay in the SM for conducting experiments in lunar orbit. Some experiments had booms extending out into space, and limit switches indicated whether the boom had been retracted far enough away to fire the SPS engine without that boom coming back and colliding with the SM. On one of those missions the limit switches were not sensing properly, which was found to be an installation problem and was later corrected.

When I was working on the ASTP doing the wiring inspection for the SM scientific instrument bay at the North American Aviation, Inc. plant at Downey, California, I was looking carefully at those same limit

switches because of the problem that occurred on the Apollo mission. I noticed that the little lever arm that's supposed to trip the switch was not making good contact with the boom piece, so I flagged that during the walk-around inspection. Then we checked to see how that issue had been missed. The quality team always inspected the vehicle to make sure it was built per the installation drawing, and it turned out that this was indeed per the installation drawing.

The explanation was the long time lag between the last Apollo flight, Apollo 17 in 1972, and ASTP in 1975. In response to the limit switch problem during the Apollo mission, an engineering order was attached to the drawing to correct the limit switch installation, instead of changing the actual drawing, which was more expensive. Often, many engineering orders were attached to a drawing. When those installation drawings were taken from the files to be used in ASTP, the engineering orders were not included.

The quality assurance personnel could only verify that the installation matched the drawing, not that it matched the intended design. However, the designer could see if the drawing was wrong. That was the beauty of both NASA and contractor design personnel performing vehicle inspections. After the Apollo 1 fire, NASA required a "Management Walk-Around Inspection" of all spacecraft prior to shipment to KSC, and this continued in the Space Shuttle Program.

Lesson: Design drawings should be updated following a design change. Engineering orders (attachments which show a change to a design) should not be overused. When an older design is being used, ensure that all of the subsequent modifications and changes have been documented and included.

Also, involving personnel that participated in previous missions or investigating past lessons learned can help avoid the repetition of past mission anomalies. For critical systems, the designers should be able to inspect the installation, to make sure it accurately follows the intended design.

Human factors and crew error

Human factors must be considered when designing space systems, to allow crew members to safely and successfully accomplish the mission. Sometimes this involves the design of the human-hardware interface, such as clearly labeling switches, protecting them from accidental activation, or accounting for the physical limitations of a space suit. Other times it involves operational considerations, such as managing training schedules or eliminating distractions during critical mission activities.

Apollo 10 (May 1969): Inadvertent Lunar Module Abort

Important mission objectives were to demonstrate the separation of the LM, fire the descent engines, and dock the LM, but a switch misconfiguration resulted in lunar lander control problems. During the LM last pass, within eight miles of the moon and prior to the jettison of the LM descent stage, the commander (while wearing a space suit) started to troubleshoot an electrical anomaly. The Abort Guidance System was inadvertently switched from “hold attitude” to “auto,” which caused the LM to look for the CSM and flip end over end.

The attitude indicator was going to the red zone and in danger of tumbling the inertial platform. The commander was able to grab the hand controller, switch to manual control, jettison the descent stage, control the LM ascent stage, and finally dock with the CSM.

Lesson: Several human factors contributed to the error:

- The crew member was distracted due to troubleshooting the LM electrical problem while involved in procedures for LM ascent/descent separation.
- The crew member had limited reach and visibility when fully suited with helmet and gloves.
- A critical switch was unguarded and susceptible to accidental activation.

Skylab 4 (November 1973 – February 1974): Loss of Control During Entry

On February 8, 1974 while preparing for entry, the crew inadvertently opened the Stabilization and Control System pitch and yaw circuit breakers instead of the SM Propulsion System pitch and yaw circuit breakers. The vehicle was in an apex-forward configuration for SM jettison. The commander attempted to orient the vehicle to the proper attitude for entry, heat shield forward. The control commands produced no effect due to the Stabilization and Control System being inadvertently unpowered, and the vehicle failed to change attitude. The crew switched to “manual RCS direct” and oriented the vehicle to the proper attitude. The inability to orient the heat shield forward would have caused the loss of the crew.

The crew members later stated that they had mistakenly pulled the wrong circuit breakers because both circuit breakers were located on the same panel with similar labeling. Also, they had not operated the CSM in three months, so the operations were not fresh in their minds.

Lesson: Good labeling and positioning of switches are important for mitigating crew error during high-activity periods. In this case, crew error caused a problem, but the crew members also saved themselves using a backup manual control system. Critical automatic functions should have a manual or unlike-redundancy backup.

Several human factors contributed to the error:

- Crew members were distracted while doing two things at once (troubleshooting the CM RCS system while involved in procedures for CM/SM separation).
- The crew was required to open circuit breakers at critical time for deadfacing power. Power deadface relays should have been designed to deadface all circuits.
- Circuit breakers should be labeled clearly, so that one is not mistaken for another.
- When all circuit breakers are located on the

same panel, the chances of pulling the wrong one increase.

- Training and simulation should be repeated or reviewed to re-establish proficiency after a significant time has passed.

Apollo-Soyuz Test Project (July 1975): Second Docking and CM Entry

On the last day of the joint mission the Docking Module pilot took control of the spacecraft to perform the second docking between the two spacecraft. The Soyuz had a sunlit Earth behind it, which caused poor docking target visibility and washout of the optical alignment sight reticle. The Docking Module pilot continued with the docking, but after docking he inadvertently bumped the left Rotational Hand Controller, firing a roll thruster after contact, which caused both vehicles to oscillate for a short time, folding them toward one another. The joint docking mechanism could have been damaged and a catastrophic depressurization of the Soyuz could have occurred. The Russians said this impact reached the design limits of the Soyuz docking system. The MCC in Houston apologized for the mistake.

A second issue occurred during entry and landing. Prior to the mission, a crew training and procedures engineer informed me, when I worked as the Sequential Subsystem Manager, that the commander, who had also commanded the Apollo 10 mission, had insisted that the checklist be the same as it was for Apollo 10 with regard to arming the ELS. Previously the crews had been concerned that the guarded ELS logic switch might fail, arming the ELS prematurely. This was a single-point-failure concern during the first seconds of flight. After Apollo 10 a change was made to rewire the ELS switches to have series redundancy, eliminating the single-point-failure mode. The new procedure kept the pyros armed after CSM separation and had been used on several missions. This prevented a critical step from having to be performed during the later, time-critical period.

The crew training and procedures engineer arranged for us to meet with the commander, so I could explain the

changes to him. We also tried to convince him to keep the ELS in automatic mode and to let the parachutes be deployed automatically. The commander refused to change the entry procedure and insisted that the crew would not forget to deploy the parachutes.

As the spacecraft was descending the crew got behind in the checklist, and the pyro buses were armed 20 seconds late at 37,000 feet. At 30,000 feet the ELS auto system should have been turned on, but wasn't, due to a miscommunication between the Docking Module pilot and CM pilot.

At 24,000 feet the commander should have turned off the RCS, but didn't, because he was waiting for the drogue parachutes to deploy. The drogue parachutes had not deployed because the auto ELS system wasn't on. The CM pilot manually jettisoned the apex cover at 19,700 feet and deployed the drogues at 18,550 feet. (The drogues should have deployed at 24,000 feet.) At 10,000 feet the commander realized that the auto ELS was not on, and turned it on, so that the main chutes deployed. The delay caused the main chutes to be deployed at 7,150 rather than 10,000 feet. The commander also disabled the RCS.

The RCS was disabled much later than the correct altitude of 24,000 feet, but the cabin pressure relief valve opened automatically and correctly at 24,500 feet. During a 30-second period of high thruster activity after drogue parachute deployment, a mixture of air and propellant combustion products, water and nitrogen oxide, were sucked into the cabin. This would have been avoided if the RCS had been switched off at the correct time.

At about 16,000 feet the commander closed the RCS propellant isolation valves, per the checklist. Closure of the propellant isolation valves allowed the toxic nitrogen tetroxide oxidizer trapped between the valves and the thrusters to boil off as the thrusters operated for 23 additional seconds before the RCS was inhibited by the operation of the RCS disable relay at an altitude of about 9,600 feet. The toxic nitrogen tetroxide vapors trapped between the propellant isolation valves and

the solenoid valves were sucked into the cabin.

One of the positive roll thrusters was two feet away from the steam vent through which outside air was pulled into the CM close to the CM pilot. This exposed the crew to a high level of nitrogen tetroxide, since emergency oxygen masks were not available until landing. The CM pilot passed out, but revived when the commander put an oxygen mask on him after landing. The exposure resulted in a two-week hospital stay for the crew.

Lesson: Crew training should include human factors awareness. In the docking event, the crew member didn't take his own human limitations into account when he attempted to dock without having adequate visibility.

Crew training should reflect the current vehicle configuration and the latest crew procedures. In the entry event, the crew didn't correctly follow the entry procedure because the commander wanted to use the old procedure he knew instead of the updated procedure. He also ignored the advice of the engineers to enable the automatic system. This resulted in errors which endangered the crew.

Test as you fly, fly as you test, and the value of real-time testing

As analysis and modeling techniques have improved, spaceflight programs have tended to rely more and more on this less expensive approach, as opposed to the more expensive process of testing. However, because of the unknown space environment testing is required to confirm the analysis and models.

It is important to understand the flight environment and to test flight hardware to that environment whenever possible. The qualification test configuration should be the same as the flight configuration. Ground testing personnel should be available to support critical mission phases in real time, especially for missions beyond Earth orbit.

Apollo 7 (October 1968): Electrical Short

During the Apollo 7 mission, the first flight after the Apollo 1 fire, while on orbit during a loss of signal, the AC bus 1 and 2 momentarily shorted out, causing automatic disconnect of the AC inverters. The AC power loss turned off the internal panel lights and all AC-powered equipment (pumps and fans). The short was associated with the cryogenic oxygen tank fans being automatically switched off by the pressure switches. The crew turned the automatic system off. Post-flight analysis identified the SM motor switches used to switch the three-phase 115-volt AC power as the source of the short. The motor switches were only environmentally sealed, not hermetically sealed, and were not sufficiently tested for the vacuum environment. While exposed to vacuum, a leak in the environmental seal caused the pressure to drop to the threshold for corona arcing, causing the shorting of AC power.

Lesson: The flight environment must be thoroughly understood, and flight hardware should be tested according to that environment as much as possible.

Electrical switching components exposed to vacuum should be hermetically sealed to prevent shorting due to corona.

Apollo 16 (1972): Lunar Rover Anomalies

During Apollo 16 multiple, intermittent battery instrument anomalies occurred during Lunar Rover Vehicle (LRV) operation in the low-temperature environment on the moon. The Marshall Space Flight Center (MSFC) Director asked the JSC MER to independently investigate the cause of the LRV problems, since MSFC's investigation board had not identified a cause.

I was working as the Sequential Subsystem Manager, and my investigation of the grounding circuitry revealed that the small 22-gauge return wires to the meters and ampere-hour integrator were crimp spliced with the large 12-gauge battery return wire (total of five wires in the splice). An open circuit to ground and power return would explain the anomalies seen in flight.

The number of these return wires and the size difference exceeded the JSC spacecraft requirements on the splicing of different gauge wires in a single splice, as large differences can result in a loose connection on some of the small-gauge wires. The investigation also revealed that the qualification LRV that was tested in a thermal vacuum chamber had solder connections, not the crimp splices as used on the LRVs.

Lesson: The vehicle's qualification test configuration should be the same as the flight configuration, even for small things like wire splices, because changes that seem small on the ground can have significant unforeseen consequences in a flight environment.

Apollo 16 (April 1972): Delayed Lunar Descent

After Lunar Orbit Insertion the LM undocked from the CSM in preparation for starting the lunar descent. The CSM performed system checks of the primary and secondary SPS pitch and yaw gimbal actuators in preparation to perform the circularization burn. Oscillations were detected in the secondary yaw gimbal actuator. Proper operation of both primary and secondary were required for the mission to continue with a lunar landing. The LM crew was told to go back and stay in close proximity to the CSM while

troubleshooting was performed on the secondary yaw actuator. The LM would need to be docked to the CSM if the primary SPS gimbal actuator failed, in order to return to Earth from lunar orbit.

Tests and analysis showed that the redundant system was still usable and safe, had it been required for an SPS engine burn. Therefore, the LM was given a go to proceed with the powered lunar descent and landing after a six-hour delay.

Lesson: Having personnel from design, test, and operations available to support flight operations can be beneficial. In this case, engineering analysis and testing could be performed in real time to enable the mission to continue.

Politics is the enemy of good design

The political interests of NASA centers can motivate decisions that are in the best interests of the center, but not in the best interests of the overall design or of safety. A spacecraft contractor that wants to use a particular hardware subcontractor may work to show that its hardware is the best, even if the customer has a cost concern about that subcontract, and even when it compromises the overall systems design and safety. The following examples from the early development and design of the space shuttle illustrate this problem.

Space Shuttle Main Engine Electrical Design

Why was the orbiter designed for 117 volts AC power instead of the aerospace standard of 115 volts?

The Power Distribution and Control Branch in the Control Systems Development Division was responsible for the AC power and distribution for the orbiter being developed by Rockwell Space Division. As a redundancy improvement over Apollo, the AC inverter would be single phase 115 volts, using three inverters to power a three-phase AC bus. The vendor's design was similar to the design used in commercial aviation. After the design was well underway, we were informed that the MSFC Space Shuttle Main Engine (SSME) controllers under contract were designed to receive 115 volt, three-phase AC power. This was because the SSME contracts were awarded early when the proposed orbiter design called for AC generators in the aft to provide electrical power. Later when the orbiter contract was awarded, the design removed the AC generators and electrical DC power was provided by fuel cells.

We informed MSFC that the power in the aft compartment would be DC power. MSFC did not want to change the SSME controller design, due to cost and schedule, and insisted on receiving AC power, rather than the DC power located in the aft compartment. I don't know the actual figures, but I suspect the SSME controller cost and schedule change was greater than the cost and schedule change to the orbiter AC inverter. It was probably the correct decision for cost and schedule, but looking at it from an integrated power distribution design standpoint, the DC power

would have been a more reliable power source and lower safety risk.

Rockwell had to change the inverter design to provide the non-aerospace standard 117 volts, which was required because of the two-volt line drop from the forward compartment AC bus to the SSME controllers. All AC powered equipment in the orbiter had to change to accept 117 volts instead of the standard 115 volts. This was a less reliable source of power for the SSME controller due to the three small-gauge wires, long wire run with many connectors (forward avionics bay to aft compartment SSME controller), and need for each phase to be protected by a three-ampere circuit breaker. This compares to a design of two wires (power and return) from the aft avionics bay to the SSME controller. Electrical DC power to the aft avionics bay from the forward distribution assembly was via two very large-gauge wires, each protected by 200 ampere fuse. During ascent on STS-93 a short on AC bus 1 phase A caused the loss of SSME 1 Controller A and SSME 3 Controller B.

Lesson: NASA centers tend to compete with each other, and may not want to take each other's advice, especially if it involves redoing work. These factors may influence spacecraft design. Also, this example shows cost and schedule considerations taking precedence over design and safety.

To avoid this situation, NASA Headquarters would have to review both centers' proposals and insist on the design with less safety risk. This would be challenging to implement.

Space Shuttle Avionics Computers

Why were the computers air cooled, while the avionics were on cold plates?

In the orbiter contract Rockwell had stated that IBM would provide the orbiter avionics computers. IBM was very expensive compared to the other bidders for the orbiter computers, but told NASA these would be the flight-proven IBM computers flying on the B-52s. The B-52 computers were air cooled, like all aircraft

avionics. The orbiter avionics were on cold plates, which would not be affected if the orbiter crew cabin became depressurized, but because the IBM computers were the less efficient air-cooled design, they would fail if the cabin were depressurized. Also, the air inlet filters had to be periodically cleaned. IBM's orbiter computer design was nothing like its aircraft computers, so the argument that the design was flight proven was no longer valid.

After the shuttle had been flying for several years, NASA considered converting the computers to a cold plate design, which would involve removing the air ducts and adding cold plates, but the idea was rejected as too expensive.

Lesson: Contractors' business interests may influence design decisions, with detrimental effects. Also, either the hazard analysis in this situation was insufficient or the additional risks posed by the IBM design were not sufficiently communicated, resulting in a poor design decision.

Automatic versus manual control

Manual crew control as a backup for automated systems has the potential to save the crew and/or mission when in-flight anomalies occur. However, the addition of manual crew control capabilities comes at the expense of budget and schedule and can introduce new risks associated with potential human error. Risk benefit trades must be performed to determine what types of manual crew control capabilities should be incorporated into new spacecraft designs to mitigate risks to flight crew and mission success while staying within programmatic constraints.

On the Apollo spacecraft, backup capability was provided for crew safety functions, even if the system provided a level of unlike redundancy. This saved the crew and the mission on several occasions.

Manual backup controls saved the LM crew on Apollo 10 (see “Redundancy can help or hinder”). Later, the Apollo 12 crew manually reset an automatic function to save the mission. Crew members used power from the battery relay bus to reconnect the fuel cells to Main Bus A and B and reconnect the inverters to AC Bus 1 and 2 (see “Redundancy can help or hinder”).

Manual backup to automatic control also saved the crew on Skylab 4. The commander switched to manual control, so he could maneuver the spacecraft to the proper entry attitude (see “Human factors and crew error”).

Manual backup to the automatic redundant Earth Landing System saved the crew on ASTP when the apex cover had to be jettisoned manually so that the drogue parachutes would deploy (see “Human factors and crew error”).

Lesson: Critical automatic functions should have a manual or unlike-redundancy backup.

Figure 1 summarizes the history of manual control. It shows the systems on each vehicle which provided manual control, whether those systems were used, and whether they were used during nominal operations or a contingency event.

Capability		Program				
		Mercury	Gemini	Apollo	Space Shuttle	Soyuz
Pre-launch/Ascent	Abort Initiation	✓	✓	✓	✓	X
	Abort Inhibit	X	✓	✓	✓	X
	Manual Steering	X	X	✓ (2 nd & 3 rd stage)	✓ (post MET 1:30)	X
	Manual Throttling and Shutdown	X	X	✓ (3 rd stage)	✓	X
On Orbit	Abort Initiation	✓	✓ ^C	✓	✓	✓ ^C
	Attitude Control	✓ ^C N	✓ ^C N	✓ ^C N	✓ ^C N	✓ ^C
	Translation Burns		✓ ^N	✓ ^N	✓ ^N	✓ ^C
	Rendezvous		✓ ^C	✓ ^N	✓ ^N	✓ ^C
	Docking/Undocking		✓ ^N	✓ ^N	✓ ^N	✓ ^C N
Lunar Descent/Ascent	Abort Initiation			✓		
	Abort Inhibit			✓		
	Attitude Control			✓ ^C N		
	Translation Burn			✓ ^C N		
Entry/Landing	Attitude Control	✓ ^C	✓ ^C	✓ ^C	✓ ^N	✓ ^C
	Parachute Deployment	✓ ^C	✓	✓ ^C	✓ ^N (drag chute)	X
	Landing Gear Deployment				✓ ^N	
	Runway Steering				✓ ^N	

- ✓ Manual capability was provided
 - N - used for nominal operations
 - C - used in a contingency event
- X Manual capability was NOT provided
- Capability not applicable to the program

Figure 1. History of the Use of Manual Control
(Source: History of Manual Crew Override, page 2)

Drawings help, but remember to inspect actual hardware

During a problem investigation, try to inspect the actual hardware involved, if possible. If the problem is electrical noise or electromagnetic interference, remember to investigate the grounding system first. If the electrical problem occurs on unrelated hardware, the ground system is often common, and that is the first place to investigate. (In addition to the following examples, also see the LRV incident in the section “Test as you fly, fly as you test, and the value of real-time testing.”)

Apollo 4 (1967): Launch Pad Instrumentation Electrical Noise

Apollo 4 was the first uncrewed test flight of the Saturn V launch vehicle. Apollo 4 was an “all-up” test, meaning all rocket stages and spacecraft were fully functional on the initial flight. The mission objective was to demonstrate structural and thermal integrity and compatibility of launch vehicle and spacecraft, as well as to test the adequacy of the Block II command module heatshield design for lunar return entry conditions.

When Apollo 4 first arrived at the pad at KSC for testing and checkout, the Apollo spacecraft personnel observed a lot of electrical noise on their instrumentation system. After a lot of work, they still couldn’t figure out what was wrong, so they asked the MSC MER Manager to send a team to help determine what the problem was. I was on this team, since I always worked on the electrical system. I began with looking at the drawings and saw that the spacecraft was well designed, in the sense that it had an “I ground” for the grounding of all low-level instrumentation. It had an “E ground” for the grounding all electrical power, and both were separated from each other. According to the drawings, this system would be isolated all the way down to the base of the Saturn V and the mobile launcher, where they would be tied together.

In the mobile launcher the two grounds, electrical power return “E” and instrumentation “I,” were tied together to go to the main ground to make sure everything was grounded. I went over the drawings and

met with the KSC engineer, then we started at the top and walked down the grounds, opening up the various junction boxes. When I got all the way down to the base, which was in a closed compartment underneath the mobile crawler, and opened up the junction box, a link was missing between the “E” and “I” ground. The “E” ground, the power return, was grounded. The “I” ground was floating. It wasn’t connected to the “E” ground, and the link to tie them together was missing. That immediately explained the noise on the instrumentation system. Thankfully it was an easy fix, and the testing of the spacecraft and launch vehicle could continue.

Lesson: Physical hardware, as well as design drawings, should be inspected during problem investigations. This area is often overlooked. When there is electrical noise in the electrical/instrumentation system, the first step is to look at the grounding/power return design and inspect the hardware.

Mars Viking Test (1975): Test Stand Instrumentation Electrical Noise

While the Mars Viking Landers 1 and 2 were undergoing testing at the Martin Denver facility prior to shipment to KSC for launch processing, an electrical noise problem occurred that the engineering and test personnel were unable to isolate and fix. The NASA JSC Manager of the Programs Operations Office responsible for the MER received a call from JSC Director Kraft’s office to go to Denver to help solve the problem, and I was on this team.

We were briefed by the Viking Program’s engineering personnel and given the drawings/schematics of the test stand electrical and grounding system. This sounded very much like the Saturn V spacecraft electrical noise problem we had investigated before, so I first looked at the grounding drawings and noted they had an “E ground” for electrical power return and an “I ground” for the instrumentation, a good design. I went to the test stand with a Martin test electrical engineer to physically inspect the E and I grounds. They

consisted of two large cables that came down the test stand and went outside the building.

The facility is located on the side of a mountain, and the climate is very dry, so a water well was used to provide a good ground. Both cables went down this well, and I asked for the cover to be removed. Using a flashlight that I shined down the well, I could see water at the bottom. I asked the engineer to wiggle the cables, and the water did not move. That was the source of the problem: both the E and I grounds were floating, acting like antennas picking up electromagnetic interference. The solution was to add water to the well and add a step in the test checklist to verify that the cables were in the water. They thanked us, but were embarrassed that such a simple fix solved their problem.

Lesson: As in the previous example, drawings are often examined for issues in the design, but checks of the installation or setup are often overlooked. Any time you have electrical noise in the electrical/instrumentation system, first look at the grounding/power return design. Don't just look at drawings; physically examine the setup to make sure everything is in place.

Hazard analysis is critical

Hazard analysis was not routinely performed during the Apollo Program and was not fully accepted in the broader NASA community until the *Challenger* accident. Engineering safety hazard analysis should not only be performed for flight systems, but also for critical spacecraft ground tests. Also, the hazard analysis should be repeated when there is a subsequent design change. Pessimistic thinking can help reveal risk areas and motivate preparations for emergencies.

Apollo Mission A-003 (1965): Little Joe II Booster Fin Failure

Apollo Mission A-003 used a boilerplate spacecraft (BP-22) launched from Launch Complex 36 at White Sands Missile Range on May 19, 1965. The mission was a high-altitude test of the abort system, and the Little Joe II had six Algol solid rocket motors, making this the largest solid rocket motor launch at that time. Concern about the reliability of the abort signal from the launch vehicle led to using a loss of signal/open circuit rather than an electrical signal being sent. Three abort signals were to be sent in two-of-three voting in the spacecraft sequencer to initiate the abort. A radio frequency command was sent to the launch vehicle for the abort, which powered a relay opening the normally closed contacts, causing loss of signal to the spacecraft.

Shortly after liftoff one of the Little Joe fins failed hard-over, and the faster it went forward the faster it spun around till centrifugal force caused the launch vehicle to structurally fail approximately 25 seconds after liftoff. The launch vehicle breakup caused the open circuit/loss of signal, and the spacecraft sequencer initiated an automatic abort of the BP-22 spacecraft. The spacecraft separated from the launch vehicle at a high roll rate. The drogue chute had steel cables as risers, which was beneficial, since the spacecraft upper deck was damaged from the risers lashing around in the process of damping out the roll rate. The lower part of the main risers had a fine steel overwrap. Concern about spacecraft dynamics during parachute deployment causing damage to the parachute risers from upper deck sharp edges resulted in the changes to the parachute risers.

The abort command from the launch vehicle implemented as an open circuit allowed this signal to also be an indication of launch vehicle structural integrity. This concept was carried forward to the Saturn 1B and the Saturn V launchers. The three Emergency Detection System abort circuits to the CM were routed 120 degrees apart along the inside of the outer structure, with open circuit being the abort command. Two out of three of the circuits being open would initiate an automatic abort. The change to steel cables for the drogue chute risers is probably the reason the spacecraft was safely recovered.

Lesson: Engineering safety analysis should indicate what the abort signal to spacecraft should be if the launch vehicle structurally fails. Parachute risers should be designed for the worst case environment.

Apollo-Saturn Mission 201 (February 1966): Loss of Reaction Control System

After CSM separation, entry heating led to an electrical short, causing the RCS commands to be transferred from the CM to the SM, resulting in the loss of RCS control. After the loss of the RCS the CM went into a stable roll and did a ballistic entry instead of the planned lifting re-entry.

The cause of all this was a non-functional circuit (Criticality 3) that was routed through the CSM umbilical that was not deadfaced prior to separation, and it was powered from the Sequential Events Control Subsystem System B circuit breaker, causing loss of the redundant Earth Landing System (Criticality 1). The non-functional circuit had been dropped from the drawings, but the wiring was left in the spacecraft and was not disconnected from power. Since it was not on the drawing for the powered wiring going through the CSM umbilical, it was not deadfaced prior to guillotine of the umbilical. The redundant Earth Landing System allowed for recovery of the CM.

Lesson: Hazard analysis should be performed on critical systems. All non-functional circuits, if left in the spacecraft, should be disconnected from

both power and return and should be identified on spacecraft drawings. Careful review should ensure all powered wiring through an umbilical to be guillotined is deadfaced prior to cutting with the guillotine.

Also, Criticality 3 functions (which are not essential for crew or vehicle survival) should not be allowed to affect Criticality 1 functions (which are essential for the operation of the vehicle and/or the survival of the crew).

Apollo Environmental Control System (April 1966): Fire During Test

See the full summary of this event in “Documenting and sharing information: communication is key.” The hardware used in the test had undergone no engineering analysis to show it was compatible with the test environment. Hazard analysis would probably have revealed that the commercial heater tape insulation could not withstand the temperature to which it would be exposed.

Lesson: Hazard analysis should be performed on critical test configurations. The compatibility of materials with the environment (temperatures and pure oxygen exposure) must be assessed. This error should have led to greater awareness of this issue, but similar problems occurred the following year during the Apollo 1 fire.

Apollo 1 (January 1967): Fire and Loss of Crew

At 6:31 pm on Friday, January 27, 1967 at KSC during a simulated countdown for the AS-204 mission, a fire broke out in the CM and quickly caused the loss of the crew, Virgil Grissom, Ed White, and Roger Chaffee. I was in the JSC MCC on the Electrical Power System Console in the Staff Support Room alongside my flight controller counterpart monitoring the test at KSC. The test was running long due to numerous problems. Because the MCC was just monitoring the test being run from KSC, after 5:00 pm the flight control personnel in the Staff

Support Room left for the day. I and the North American Space and Information Systems flight controller on the Environmental Control Systems Console were the only ones left.

We heard the scream of fire on the headset and the KSC personnel trying to get to the CM. Ground personnel grabbed the available gas masks, but passed out after entering the smoke-filled White Room around the CM, because the masks were for filtering hypergolic propellant fumes and were not closed, oxygen-providing masks. I was hopeful, thinking the crew members were in their spacesuits and would be okay, but I heard the KSC test conductor on the headset tell Dr. Christopher Kraft to go to a private phone. My heart sank, as I knew it meant the crew didn’t survive. Dr. Kraft was monitoring the test at the Flight Director Console in the Mission Operations Control Room. He then announced on the Flight Director loop to lock the doors, that no one was to leave, and that we were allowed one call to our spouse to say we would not be home, but not to say anything else. He later came back to the Staff Support Room and told us they would be playing back the data and to concentrate on reviewing it.

I had noticed at about the time of the report of fire that we had a short on Main DC Bus A and B. That indicated that the short must have a load connected to both main DC buses. The following day I went over all the schematics to identify the wires dioded to both main buses. The next week I was asked to go to KSC for the investigation. I was assigned, along with a photographer, to go through the wiring in the CM to identify the ignition source.

A significant part of the left-hand lower equipment bay was gone (metal, plumbing, wiring, etc.). This was where the fire started and was the hottest, because the most oxygen was present. The most probable initiator was an electrical arc occurring near the floor in the lower forward section of the bay. Here, instrumentation power from a Teflon-insulated wire powered by Main Bus A and B was routed over metal plumbing and under a coolant control access panel, just below the left crew

couch.

The wire harness, a twisted pair of wires, and power and power return had an extra Teflon overwrap for protection from the panel door and the metal plumbing. However, the last closeout photo of that area before the fire showed that the extra Teflon wrap had slipped down, and was not keeping the wire away from the plumbing. The wire harness had no extra protection from the panel door opening/closing or from ground test personnel or crew at the time of the test. The wire looked like it was touching the bottom of the panel door.

Spacecraft movement was noted during the test, as the commander was reconnecting the communications cable, and the damage could have happened at this time. A simulation showed that he would have had to put his foot down, off the crew couch, to reconnect the cable, and would have placed his foot near this wire.

The crew cabin was pressurized to 16.7 psi with pure oxygen. The side hatch consisted of a two-piece, inward opening (pressure sealing) hatch. The fire increased the pressure, which made the hatch more difficult to open, so the crew was unable to open the hatch to escape. It took 90 seconds to remove the hatch from the outside and get them out.

No engineering safety hazard analysis was performed on the ground test configuration. If performed, it probably would have identified that the materials inside the cabin were not certified for the environment and that no protective gear or training was available for fighting a fire on the spacecraft level at the launch pad.

Lesson: Hazard analysis should be performed on critical test configurations. All tests at 100% oxygen should be defined as hazardous. Emergency training should be required for all test support personnel, and test areas should be equipped with appropriate emergency, fire-fighting, or rescue equipment. The selection and placement of materials inside the spacecraft must be compatible with the spacecraft environment. The crew ingress/egress hatch should be a single, outward-opening

hatch requiring only five seconds to open.

Apollo 13 (April 1970): Oxygen Tank Explosion

See the full incident summary in the section “Expect the unexpected and never stop learning.” The thermostatic switches were rated for 30 volts DC, but several years earlier the heater ground power supply voltage was raised to 65 volts to reduce the pressurization time. As the temperature increased, the thermostatic switch opened and the higher voltage caused the contacts to weld closed. No engineering safety hazard analysis of the voltage change to the thermostatic switch was performed.

Lesson: Hazard analysis should be repeated following a design change.

Skylab 3 (July 1973): Propellant Leak and Rescue Mission

See the full incident summary in the section “Redundancy can help or hinder.”

Lesson: Hazard analysis should be performed on redundant systems, to ensure they provide the expected redundancy. Had the analysis been performed, it would have revealed that a system that appeared to be single-fault tolerant was actually zero-fault tolerant in effect, because the backup system would not work.

The programs’ early planning to develop a Skylab rescue capability is what allowed a rescue mission to be developed so quickly. This is a good example of reaping the benefits of planning ahead for something to go wrong.

Killing “Death Star:” be persistent in advocating for safety

In July of 1982, Congress mandated a Shuttle/Centaur Program to launch Galileo and Ulysses satellites by May of 1986 and subsequently to collaborate with the U.S. Air Force for Department of Defense (DOD) missions. In order to pair these two existing programs, the shuttle propellant fill/drain/dump system had to be modified. The Centaur also required multiple design changes to integrate with the shuttle payload bay, including modifications of the tank, the fill/drain/dump system, the integrated support system, and software updates.

I became the Deputy Director of SR&QA in October 1985. In November a senior safety engineer informed me of significant safety concerns about the Shuttle/Centaur Program, which no one in management had addressed. One concern was the tank and propellant systems not meeting the required factors of safety. Another was the overpressurization of the liquid oxygen system from excessive surge pressure, such as a water hammer effect from liquid oxygen loading termination.

The Space Shuttle Program Payload Safety Panel Chairman had disapproved the Shuttle/Centaur payload non-compliance reports, but that the decision was overturned by NASA Headquarters after an appeal by the NASA Lewis Research Center (LeRC). Other safety-critical, single-point failures existed in this program as well, with credible concerns as to the reliability of the system.

In preparation for the Shuttle/Centaur Program Level 1 (NASA Headquarters) Review on January 16, 1986 at KSC, I wrote a memorandum to the manager of the National Space Transportation System regarding the JSC SR&QA position on Centaur.⁴ This memorandum outlined multiple safety problems that SR&QA believed needed to be resolved prior to the first Centaur flight scheduled approximately four months later.

At the Level 1 Program Review I presented the JSC SR&QA position, and the NASA Headquarters Head of Human Spaceflight directed me to coordinate with LeRC. This was discouraging, since JSC SR&QA and the Payload Safety Panel had been working with LeRC with

no agreement to correct the safety non-compliance reports.

In early January 1986 the commander for one of the Centaur missions, Rick Hauck, was working on an issue with redundancy in the helium actuation system for the liquid oxygen and liquid hydrogen dump valves. Hauck believed that the program was willing to compromise on the margins in the propulsive force being provided by the pressurized helium, which concerned him enough that he raised the issue with the Chief of the Astronaut Office, John Young. “John Young called this mission, ‘Death Star’” recalled Hauck. “That was his name for this mission, which he said with humor, but behind humor, there’s a little bit of truth. I think it was conceded this was going to be the riskiest mission the shuttle would have flown up to that point.”⁵

John Young and Rick Hauck “went to a board [Space Shuttle Program Control Board] to argue why this was not a good idea to compromise on [the helium actuation system], and the board turned down the request.” Back in the Crew Office, Hauck told the other crew members, “NASA is doing business different from the way it was done in the past. Safety is being compromised, and if any of you want to take yourself off this flight, I will support you.”⁶

On January 28, 1986 the *Challenger* disaster occurred. I was surprised and disappointed that the next scheduled mission, this “Death Star,” with all of the open safety concerns was delayed but not canceled. At a Payload Safety Review Panel meeting, more safety concerns were raised. LeRC stated that a redesign would create schedule problems that NASA Headquarters would have to direct.⁷

In March I conducted an SR&QA audit of the safety-critical avionics. Significant findings included:

- Acceptance testing without released test procedure.
- Automatic test equipment used on checkout often

5 Frederick H. Hauck Oral History Interviews

6 Ibid.

7 Documented in memorandum NA/86-M035

4 Memorandum NA/86-M007

indicated “Test Passed” when parameters were out of limits.

- Control unit tested on unreleased software.
- Critical avionics box certified for flight with open failures and wavers.

When I asked the responsible engineer why he signed off on the flight certification with open failures, he said his manager directed him to sign. LeRC told me this was not true. I did not mention this in my written report, because I did not want the engineer to be disciplined for what he conveyed to me in private.

On March 4 John Young wrote to the Centaur mission commanders Rick Hauck and Dave Walker about the Centaur mission. The handwritten note said, “But also never forget that: a. Running the pressure up & down during ascent, b. Venting H₂ during ascent, c. pressurized stabilized pressure vessels, d. spot-welded pressurized propellant tanks are not good ideas... Please do NOT invite me to any more briefings on Centaur. The engineering logic in them makes my head hurt.”⁸ Despite this sentiment, Hauck reported that John Young would ask him about the “Death Star” at the Monday morning status meetings.

On April 8 three members of the House Appropriations Committee Surveys Investigation Staff met with me regarding Centaur safety concerns. They asked me questions about my audit results and the problems I had reported.⁹ They also requested copies of the other two memos, documenting the SR&QA position and the concerns raised at the Level 1 Program Review at KSC.

The JSC Engineering Propulsion and Power Division Systems Branch Deputy Chief had concerns about Centaur’s compatibility with the shuttle. He believed that the inherent Centaur design, with common bulkhead pressure-stabilized tanks combined with a highly active cryogenic vent and pressurized duty cycle, did not meet human spacecraft standards and

represented an undue hazard to the shuttle.¹⁰

On May 22, 1986 Rick Hauck presented the concerns to management, that even after the proposed safety modifications had been implemented, the Shuttle/Centaur flight still represented significant additional risk to the orbiter and crew. Attempts to integrate an uncrewed upper stage into the shuttle resulted in compromises which created undue risk, and the ability to reduce the risks to an acceptable level was questionable.¹¹

On June 6, 1986 a draft of a Shuttle/Centaur presentation destined for the NASA Administrator was reviewed in a meeting chaired by the Space Shuttle Program Office (Level 2) at JSC with personnel from Headquarters, LeRC, KSC, and the Jet Propulsion Laboratory.¹² The briefing highlighted two significant hazards:

- Loss of pressure control of oxygen or hydrogen tanks. (This would be a catastrophic failure, and end-to-end pressure control could not be verified by testing.)
- Rupture of lines/components due to pressure surges during normal system transients, and pressure surges due to system malfunction or inadvertent operations not included in design requirements.

The presentation concluded that even with the best possible solutions, Centaur represented significant additional risks to the shuttle. This was the JSC position, not LeRC’s position, and the word “significant” was ultimately deleted. The safety assessment stated, “No technical barriers have been identified which prevent Centaur integration into [the shuttle] with minimal additive risk.” I spoke up to say that this was not safety’s position, but the chart was not changed.

On June 13, 1986 NASA Headquarters sent out this Shuttle/Centaur presentation for review and comment, in preparation for its presentation to the

8 Handwritten notes on memorandum DA8-86-44

9 Memorandum NA/86-M052 documented the audit results

10 Documented in memorandum EP2-86-M55.

11 Rick Hauck, “Centaur Risk”

12 Draft of “Shuttle/Centaur Presentation to the Administrator”

NASA Administrator on June 19. I recommended adding the wording “tank rupture hazard increased during dumps.” Regarding tank pressure control, I added “end-to-end pressure control is highly sensitive to assumptions regarding fluid dynamics which cannot be test verified.” On the summary chart I added, “additive safety risks are inherent to Centaur, cannot be eliminated, and represent significant increase over that accepted for previous payloads.” None of my comments were incorporated into the presentation.

On June 16 a telecon was held with NASA Headquarters regarding Centaur. I wrote a memo to document that I had communicated the JSC SR&QA position that “even if all the proposed safety modifications are made...the program must accept a safety risk greater than any previous shuttle payload and most shuttle systems... The overall position of this office is not to fly Centaur on the space shuttle.”¹³

On June 19, 1986 the revised charts were presented to the NASA Administrator, and I attended this meeting sitting next to Commander Rick Hauck. At the meeting DOD, LeRC, the JSC Engineering Propulsion and Power Division Chief, and planetary representatives favored continuing Shuttle/Centaur, but I stated that the risk was too high. Many arguments were made under much scrutiny, but I held my position regarding the safety hazards. The astronauts also expressed concerns, but were somewhat resolved to flying the mission. The Administrator left to have a separate, closed-door meeting. I felt very discouraged, as it seemed the program would continue, based on the presentation and the position of the other organizations.

Later that day I learned that the Administrator had canceled the program. That made my day! Hard work and persistence had paid off.

Lesson: If you believe something is unsafe, be persistent in reporting your concerns, again and again if necessary. Advocating for the cancellation of this program was an extraordinarily difficult task that faced considerable opposition. Even

with the recent loss of *Challenger*, significant safety hazards were not receiving enough attention, influenced in part by schedule pressure. Although other organizations had concerns with the Shuttle/Centaur Program (Payload Safety Panel, Engineering, Crew Office), I as the SR&QA representative voiced opposition to the mission at the Administrator’s review.

13 Memorandum NA/86-M082

Working with the Russians

When working with Russian partners, cultural differences, approaches to education, the value placed on experience, the willingness to accept different paths to a common goal, and differences in design philosophy are all important in communicating well and developing trust. One cultural difference is that Russians believe it's bad luck to shake hands in a doorway. Another is that even numbers are bad luck; for example, flowers should always be given in odd numbers. Knowing these small things can make relationships with any international partners go more smoothly.

Knowing the differences in U.S. and Russian educational systems can help minimize misunderstandings. The U.S. education system emphasizes reading, writing, and written responses in tests. In contrast, the Russian system focuses more on auditory learning with lectures and oral exams. As a result, most Americans learn to write things down to remember them. The Russians tend to consider writing things down an unnecessary step. They have grown up with the expectation of being told something once and being able to remember, and they tend to have great memories.

In our Shuttle/Mir joint working groups, the Russians usually gave verbal presentations on their Soyuz/Mir systems, and we took notes to remember what we were told. We used viewgraphs/PowerPoint charts or other written material to describe the orbiter systems. One factor may have been a lack of paper, as the Russians would write notes on the backs of used paper, and when visiting Russia we had to bring any paper we used with us. We noted this and eventually brought enough paper that we could share it with our counterparts.

One example of this difference causing working/communication challenges is when NASA astronauts train in Russian at Star City. They might listen to classroom lectures and take oral exams without any written material. This can be difficult and upsetting, especially with limited proficiency in the Russian language. Another example is when NASA astronaut Shannon Lucid gave her debrief after returning from her mission on Mir. She stated that when the two

cosmonauts were preparing for an EVA outside the Mir station, they told Shannon a list of things to do if the ground called. Shannon asked them to wait a minute while she wrote the instructions down, but they said no, you will remember.

Documentation may not be as necessary for the Russians, since they experience less turnover in experienced personnel. They rely on experts in their organization to remember things. In the U.S. where personnel turnover is higher, good documentation is required to capture knowledge. Because many experienced Russian designers are aging and passing away, they are now doing more written documentation to pass on the knowledge to the younger engineers, whereas in the past the design expert would verbally pass on the information.

Differences in spacecraft design philosophy and lack of understanding why a test requirement was necessary caused a significant conflict early in ISS assembly. The Russian power system was designed to minimize the potential for electrical shorts to structure (28 Vdc power with return isolated from structure) and use integrated ground testing to identify electromagnetic interference issues. The U.S. power system used a single-point ground to structure to minimize potential electromagnetic interference and relied more on component-level testing. The Russians relied extensively on test data and were very reluctant to accept our modeling and simulation data. During the Shuttle/Mir Program any U.S. electrical hardware had to be sent first to Russia to be installed and operated in the Mir test facility before being allowed to be launched and operated on Mir. The Russians generally rely more on testing than NASA does, as opposed to analysis.

Early in ISS assembly the U.S. had electrical cables that needed to be installed on the Russian Segment. The cables were loaded onto the orbiter to be launched to the ISS. The Russians said they would first need to be tested in the ground test facility. The NASA ISS Program Manager argued that it was U.S. hardware, and it was launched over the strong objections of the Russian ISS Manager. The Russians said this hardware was not to

be used or operated on the Russian Segment, even if it was on the ISS. This resulted in the Joint American Russian Safety Working Group developing a process to address hardware being launched to the ISS without joint certification. The process was called “yellow tag,” because the hardware would be launched with an attached, visible yellow tag stating, “Not to be used or operated till ground confirms certification.”

Unlike NASA, the Russians record the human errors committed by each cosmonaut during ground training and in flight, creating a human-performance/human-error database. The information is useful for human factor engineers and safety personnel and is used to improve procedures, training, and the design of spacecraft controls and displays. The Russian chairman of the Joint American/Russian Safety Working Group estimated that 10-15% of spacecraft anomalies are due to crew error. Several space shuttle commanders agreed that 10% sounded right. In the early days of NASA, crew errors were a very sensitive subject and usually only discussed during private crew debriefs. This approach hindered data collection, analysis, and dissemination.

A good working relationship requires the development of mutual trust, a willingness to accept that your counterpart has a successful history of human spaceflight, and the attitude that we can learn from each other. Part of this trust is good communication. Be careful not to say that something can be done, if further approvals or constraints are involved. Make sure to communicate these issues, so if changes occur your Russian partners know why, and do not feel they were misled in order to reach an agreement.

In addition to the working relationship, getting to know each other’s life and family experience can help. We spent time with our Russian colleagues after work, inviting them to our homes to share meals, go shopping, and visit local sites both in the U.S. and Russia.

Summary and Conclusions

Human spaceflight is challenging and dangerous. The history of our successes and failures must be communicated in order to prevent, or at least reduce, future accidents. The lessons in this paper are from

my personal experience, but they will apply to future programs as NASA continues to send humans into orbit and beyond. Table 1 summarizes the themes and the lessons in this paper.

Table 1. Summary of Themes and Lessons

Chapter/Theme	Mission	Event	Lesson
Redundancy can help or hinder	Apollo 10	Fuel cell failure	Critical systems should be two-fault tolerant.
	Apollo 12	Lightning strike	Redundant systems for critical functions should be dissimilar and/or located in different parts of the vehicle.
	Skylab 3	Propellant leak	Redundant systems must use compatible materials to be effective.
	Space Shuttle Program	Electrical Power System redundancy	Level of redundancy should be based on criticality, flight experience, and technology maturity. Unnecessary redundancy adds complexity, which increases cost and risk.
Expect the unexpected, and never stop learning	Apollo 13	Oxygen tank explosion	Contingency procedures should be developed prior to the mission.
	Apollo 14	Docking problem	Anticipate how the system could fail and prepare potential work-arounds.
	Apollo 15	Propulsion system electrical short	The zero-gravity flight environment can create unexpected failures that would not have occurred on Earth.
Documentation and sharing information: communication is key	Apollo-Saturn Mission 201	Loss of RCS	Drawings should include all updates, even disconnected/unused circuits.
	Apollo ECS	Fire	Lessons learned should be freely available and shared.
	Apollo 8	Launch pad electrical test	Don't count on anyone double-checking your work. Even when information is thoroughly documented and shared, in this case only one person was ensuring the information was correct.
	Apollo 11	SM entry	Lessons learned should be freely available and shared.
	Skylab 2	Emergency docking procedure	Organizational culture should encourage interdepartmental communication.
Apollo-Soyuz Test Project	Service module inspection	Documentation should be updated following a design change, and all documentation should stay together. Allowing designers to inspect completed hardware can help to catch errors.	
Human factors and crew error	Apollo 10	Inadvertent LM abort	Crew distraction, visibility, and mobility in the suit can impact the human-machine interaction.
	Skylab 4	Loss of control during entry	Good labeling and positioning of switches are important for mitigating crew error during high-activity periods.
	Apollo-Soyuz Test Project	Second docking and CM entry	Crew training should include human factors awareness and should reflect the current vehicle configuration. Crew members should listen to the advice of the engineers who designed the system.

Table 1. Summary of Themes and Lessons (continued)

Chapter/Theme	Mission	Event	Lesson
Test as you fly, fly as you test, and the value of real-time testing	Apollo 7	Electrical short	The flight environment must be thoroughly understood, and hardware should be tested to that environment if possible.
	Apollo 16	Lunar Rover anomalies	The vehicle's qualification test configuration should be the same as the flight configuration.
		Delayed lunar descent	Making personnel from design, test, and operations available to support flight control at the MCC can be beneficial.
Politics is the enemy of good design	Space Shuttle Program	SSME electrical power design	Center competition can impact design. Cost and schedule had greater influence than design and safety.
		Avionics computers	Contractor's business interests can impact design decisions.
Automatic versus manual control	Apollo 10	Inadvertent LM abort	Critical automatic functions should have a manual or unlike redundancy backup.
	Skylab 4	Loss of RCS control	
	Apollo-Soyuz Test Project	CM entry	
Drawings help, but remember to inspect actual hardware	Apollo 4	Launch pad instrumentation electrical noise	Physical hardware, as well as design drawings, should be inspected during problem investigations.
	Mars Viking Test	Test stand instrumentation electrical noise	
Hazard analysis is critical	Apollo A-003	Booster fin failure	Hazard analysis should indicate what the abort signal to spacecraft should be if the launch vehicle structurally fails. Parachute risers should be designed for the worst case environment.
	Apollo-Saturn Mission 201	Loss of RCS	Hazard analysis should be performed on critical systems. Non-functional circuits should be disconnected from power and return and identified on drawings.
	Apollo ECS	Fire	Hazard analysis should be performed on critical test configurations.
	Apollo 1	Fire and loss of crew	
	Apollo 13	Oxygen tank explosion	Hazard analysis should be repeated following a design change.
	Skylab 3	Propellant leak	Hazard analysis should be performed on redundant systems, to ensure they provide the expected redundancy.
Killing "Death Star"	Shuttle/Centaur Program	Cancellation of program	If you believe something is unsafe, be persistent in reporting your concerns, again and again if necessary. Safety organizations can make a difference. Schedule pressure can cause management to accept otherwise unacceptable levels of risk.
Working with the Russians	Career experience	Cultural differences	Become familiar with cultural customs and symbols.
		Educational differences	Oral versus written learning and memory.
		Value of experience	Reliance on experts versus documentation.
		Design and organization	Different doesn't mean wrong. Emphasis on testing and tracking of crew errors.
		Trust	Establish trust based on honesty and never commit to anything you're not completely sure you can deliver.

Acronyms

AC	Alternating Current	MER	Mission Evaluation Room
ASTP	Apollo-Soyuz Test Project	MET	Mission Elapsed Time
CM	Command Module	MSC	Manned Spacecraft Center
CSM	Command and Service Module	MSFC	Marshall Space Flight Center
DC	Direct Current	NARSD	North American Rockwell Space Division
DOD	Department of Defense	NASA	National Aeronautics and Space Administration
ECS	Environmental Control System	psi	Pounds per Square Inch
EGIL	Electrical, General Instrumentation, and Lighting	RCS	Reaction Control System
ELS	Earth Landing System	SAIC	Science Applications International Corporation
FSO	Flight Safety Office	SM	Service Module
H ₂	Hydrogen	SMA	Safety and Mission Assurance
ISS	International Space Station	SMJC	Service Module Jettison Controller
JSC	Johnson Space Center	SPS	SM Propulsion System
KSC	Kennedy Space Center	SR&QA	Safety, Reliability, and Quality Assurance
LeRC	Lewis Research Center	SSME	Space Shuttle Main Engine
LM	Lunar Module	STS	Space Transportation System
LRV	Lunar Rover Vehicle	U.S.	United States
MCC	Mission Control Center		

Acknowledgments:

Joanna M. Opaskar, Senior Communications Analyst/Editor, for the ability to convert a technical discussion into a report understandable by others.

Timothy A. Kassebaum, Senior Systems Safety Engineer, for the ability to identify and summarize the key safety lessons.

Dennis W. Pate, Senior Human Factors Engineer, for human factors support to the report.

General References

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

History of Manual Crew Override, Revision A. JSC SMA Flight Safety Office, 7 March 2013.

Significant Incidents and Close Calls in Human Spaceflight. JSC SMA Flight Safety Office. <https://sma.nasa.gov/SignificantIncidents/?SMAInsidePortal=true> (accessed 11 April 2018)

Apollo Mission A-003

NASA Program Apollo Working Paper No. 1175, Flight Data Report For Apollo Mission A-003 (BP-22). NASA Manned Spacecraft Center, 26 July 1965.

Apollo-Saturn Mission 201

“AS-201.” *Kennedy Space Center Science, Technology, and Engineering Space Flight Archives*. <https://science.ksc.nasa.gov/history/apollo/as-201/as-201.html> (accessed 10 April 2018)

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

NASA JSC-09423 Apollo Program Summary Report. April 1975. pg 2-17.

“Trip Report on testing to investigate the cause of the main buses shorting on the Spacecraft 009.” NASA Memorandum, To: EE/Ralph Sawyer, From: EE4/Power Distribution and Sequencing Section. 19 April 1966.

Apollo Environmental Control System Fire

“ECS Fire at AiResearch on April 28, 1966 Torrance, Calif.” Manned Spacecraft Center Fire Investigation Board Meeting, AiResearch Torrance Facility, 10 May 1966.

“Report on travel performed by Gary W. Johnson and Robert E. Munford, JUN 2, 1966 with enclosed ‘REPORT TO FIRE REVIEW BOARD ON TEST SET-UP WIRING.’” NASA Memorandum, To: EE/Chief, Instrumentation and Electronic Systems Division, From: EE4/Power Distribution and Sequencing Section.

Apollo 1

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Johnson, G. W. “Apollo 1 Case Study, Course Number BA-604.” NASA JSC Safety and Mission Assurance Training Program, July 2007.

Murray, C. and C. B. Cox. *Apollo: The Race To The Moon*. Simon and Schuster, 1989. Chapter 14.

Senate Report No. 956, Apollo 204 Accident, Report of the Committee On Aeronautical and Space Sciences United States Senate with Additional Views. 30 January 1968.

Apollo 4

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Apollo 7

“Apollo 13 Review Board Data/Test Request 12: Provide oxygen tank anomalies from previous flights, Apollo 7 Momentary Loss of AC Buses.”

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Godwin, R., ed. *Apollo 7: The NASA Mission Reports*. Apogee Books, 2000. pg 120, 208.

NASA Manned Spacecraft Center Apollo 13 Investigation Team Memorandum PT030. 14 May 1970.

Apollo 8

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Apollo 10

Godwin, R., ed. *Apollo 10: The NASA Mission Reports*. Apogee Books, 1971.

Stafford, T. P. *We Have Capture*. Smithsonian Institution Press, 2002.

Apollo 11

“MSC-03466, Apollo 11 Anomaly Report No. 3 Service Module Entry, November 1970.” *NASA Apollo 11 Technical Crew Debriefing, Volume II*. 31 July 1969.

Apollo 12

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

NASA JSC-09423, Apollo Program Summary Report. NASA, April 1975. pg 2-38.

NASA MSC-01540, Analysis of Apollo 12 Lighting Incident. NASA, February 1970.

Apollo 13

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Murray, C. and C. B. Cox. *Apollo: The Race To The Moon*. Simon and Schuster, 1989.

NASA MSC-02680, Apollo 13 Mission Report. NASA, September 1970.

“V34-900101, Rev. AC, Controls & Displays – Main Display Console Panels drawing A1 & A2, SC 109 Thru 115A.” North American Aviation, Inc., Space and Information Systems Division, 23 January 1970.

Apollo 14

Apollo 14 Mission Commentary – Air/Ground Transcript. NASA, 31 January 1971.

“Emergency procedure to fire CSM pyrotechnics if both pyrotechnic buses have failed.” Memorandum EB8-1/71-042, To: PA/Assistant Program Manager for Flight Safety, From: EB8/Manger, CSM/LM Sequential Subsystem, 28 January 1971.

NASA MSC-04112, Apollo 14 Mission Report. NASA, May 1971.

“SPAN/Mission Evaluation Action Request Control Number CL-100 R2.” 3 February 1971.

Apollo 15

Cortright, E. M., ed. *SP-350, Apollo Expeditions to the Moon*. NASA, 1975.

“Gary W. Johnson Oral History Interviews.” *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

NASA Certificate of Commendation. To Gary Johnson, December 1971.

NASA MSC-05161, Apollo 15 Mission Report. NASA, December 1971.

Scott, D. and A. Leonov. *Two Sides of the Moon: Our Story of the Cold War Space Race*. St. Martin's Press, 2004.

Apollo 16

Godwin, R., ed. *Apollo 16: The Nasa Mission Reports, Volume One*. Apogee Books, 2002. pg 27.

NASA JSC-09423, Apollo Program Summary Report. NASA, April 1975. pg 2-48.

NASA MSC-07230, Apollo 16 Mission Report. NASA, August 1972.

Apollo Lunar Rover Vehicle

Apollo 16 Flight Evaluation. 14 July 1972. pg xxxi, 20-1.

"Gary W. Johnson Oral History Interviews." *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

MSC-07684, Apollo 16 Mission Anomaly Report No. 9: Lunar Roving Vehicle Electrical System Meter Anomalies. Manned Spacecraft Center, January 1973.

Skylab 2

"Docking Probe Auxiliary Retract Method." North American Rockwell Corporation, Space Division Master Change Request A13613, 19 March 1971.

"Emergency procedure to fire CSM pyrotechnics if both pyrotechnic buses have failed." Memorandum EB8-1/71-042, To: PA/Assistant Program Manager for Flight Safety, From: EB8/Manger, CSM/LM Sequential Subsystem, 28 January 1971.

"Final Skylab Entry Checklist, add detailed revision BACKUP PROBE RETRACTION." Crew Procedures Change Request, 7 February 1973.

NASA Exceptional Service Medal Award. To Gary Johnson, 15 April 1974.

"NASA Inventions and Contributions Board Award for Skylab Emergency Docking Probe Retract Mechanism and Procedure." NASA JSC Memorandum, To: Gary W. Johnson, From: AH5/Chief, Awards Office, 15 April 1975.

"SPAN/Mission Evaluation Action Request Control Number CL-100 R2." 3 February 1971.

Skylab 3

Compton, W. D., and C. D. Benson. *NASA SP-4208, Living and Working in Space: A History of Skylab*. NASA, 1983.

Hitt, D., O. Garriott, and J. Kerwin. *Homesteading Space: The Skylab Story*. University of Nebraska Press, 2008.

JSC-08662, Skylab Mission Report Second Visit. NASA, January 1974.

NASA JSC-08478, Skylab 1/3 Technical Crew Debriefing. NASA, 4 October 1973.

"Skylab Problem Tracking List – No. 43 DOY 209 and No. 51 DOY 214." *Skylab 1/Skylab 3 Summary Report*. 26 September 1973.

Skylab 4

"Gary W. Johnson Oral History Interviews." *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

JSC-08809, Skylab 1/4 Technical Crew Debrief. NASA, 22 February 1974.

Apollo-Soyuz Test Project

Brand, V. E-mail to Gary W. Johnson. 18 April 2015.

"Cancellation of Earth Landing System Logic Switch on Panel #1 Rewire." Apollo Spacecraft Program Office

Configuration Control Board Directive 34610, 8 December 1970.

Ezell, E. C. and L. N. Ezell. *On Mars: Exploration of the Red Planet, 1958-1978--The NASA History*. Dover, 2009.

"Gary W. Johnson Oral History Interviews." *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

"Leave pyro bus armed from CM/SM sep to splashdown." Crew Procedural Change Request, CSM ENTRY C/L, 31 August 1971.

NASA JSC-09823, ASTP Technical Crew Debrief. NASA, 8 August 1975.

NASA JSC-10607, Apollo-Soyuz Mission Evaluation Report. NASA, December 1975.

NASA JSC-10638, Apollo-Soyuz Mission Anomaly Report No. 1. NASA, December 1975.

NASA SP-4209, The Partnership: A History of the Apollo-Soyuz Test Project. NASA, 1978.

"Rewire Earth Landing System Logic Switch on Panel #1." Apollo Spacecraft Program Office Configuration Control Board Directive 34610, 23 November 1970.

Scott, D. and A. Leonov. *Two Sides of the Moon: Our Story of the Cold War Space Race*. St. Martin's Press, 2004.

Stafford, T. P. *We Have Capture*. Smithsonian Institution Press, 2002.

Mars Viking Test

"Gary W. Johnson Oral History Interviews." *NASA JSC Oral History Project*. 3 May 2010. http://www.jsc.nasa.gov/history/oral_histories/JohnsonGW/johnsongw.htm (accessed 10 April 2018)

Shuttle/Centaur Program

"Centaur-Ulysses/Galileo Flight Rules Review." John Young handwritten notes on Memorandum DA8-86-44, To: Distribution, From: DA8/Centaur-Ulysses/Galileo Lead Flight Director, 4 March 1986.

"Concerns on Centaur Compatibility with Shuttle." Memorandum EP2-86-M55, To: EP/Chief, Propulsion and Power Division, From: EP2/Deputy Chief, Systems Branch, 19 May 1986.

"Frederick H. Hauck Oral History Interviews." *NASA JSC Oral History Project*. 20 November 2003. https://www.jsc.nasa.gov/history/oral_histories/HauckFH/hauckfh.htm (accessed 26 April 2018)

Hauck, R. "Centaur Risk." NASA Flight Crew Operations Directorate, 22 May 1986.

Hill, D. and H. R. Smith. *Bold They Rise: The Space Shuttle Early Years, 1972-1986*. University of Nebraska Press, 2014.

"JSC SR&QA Position on Centaur." Memorandum NA/86-M007, To: GA/Manager, National Space Transportation System, From: NA/Director, Safety, Reliability, and Quality Assurance, 15 January 1986.

"NASA-S-86-01932, Shuttle/Centaur Presentation to the Administrator." Final version presented to the Administrator, 19 June 1986.

"Shuttle/Centaur Presentation to the Administrator." Initial draft presented at JSC for review, 6 June 1986.

"Telecon with NASA Headquarters, Code D, Haggi Coehn, on Centaur Safety." Memorandum NA/86-M082, To: Memorandum for the Record, From: NA/Deputy NA/Director, Safety, Reliability, and Quality Assurance, 16 June 1986.

"Trip Report of Shuttle/Centaur Program Meetings." Memorandum NA/86-M035, To: NA/Director, Safety, Reliability, and Quality Assurance, From: NA/Deputy Director, Safety, Reliability, and Quality Assurance, 12 March 1986.

"Trip Report Shuttle Centaur Avionics Audit." Memorandum NA/86-M052, To: NA/Director, Safety, Reliability, and Quality Assurance, From: NA/Deputy Director, Safety, Reliability, and Quality Assurance, 3 April 1986.

Appendix A: Gary Johnson Career History

Education:

- Bachelor of Science in Electrical Engineering, Oklahoma State University, 1964
- Masters in Business Administration, University of Houston at Clear Lake, 1979



Career Experience:

- 1964-1969: NASA JSC (formerly Manned Spacecraft Center), Houston, Texas. Project Engineer in the Power Distribution and Sequencing Section.
- 1969-1974: Subsystem Manager for the Sequential Subsystem for the Apollo Command and Service Module, Lunar Module vehicles, and the Skylab CSM.
- 1971-1974: Group Leader for the Power Controls and Lightning Group in the Power Distribution and Control Branch. Test subject for space suits.
- 1974-1975: Subsystem Manager for the Apollo-Soyuz Test Project electrical and sequential subsystems and member of the ASTP Working Group Number 4.
- July 1974-January 1975: Assigned to the Engineering Office, Space Shuttle Orbiter Project. Project Manager for Shuttle Avionics Lab electrical power distribution.
- 1975-1978: Head, Equipment and Installation Section in the Power Distribution and Control Branch of the Control Systems Development Division in the Engineering and Development Directorate.
- March 1978-September 1978: Special Assistant to the Director, Office of the Director.
- October 1978-June 1981: Deputy Chief, Electrical, Mechanical, and Environmental Systems Branch, Flight Control Division. Served as the Orbiter Flight Control Team Electrical, General Instrumentation, and Lighting (EGIL) flight controller during the first shuttle flight.
- June 1981-July 1983: Chief, Mechanical and Payload Systems Branch, Systems Division.
- July 1983-October 1985: Chief, Guidance and Propulsion Systems Branch, Systems Division.
- October 1985-May 1997: Deputy Director, Safety, Reliability, and Quality Assurance Office. Also served

as ISS Phase 1 NASA/Mir Program Joint Safety Assurance Working Group NASA Co-chairman from 1992 to 1998.

- May 1997-July 2003: Deputy Director of Russian Projects in SR&QA. Co-chairman of the ISS Program Joint American-Russian Safety Working Group.

- July 2003-January 2006: Associate Director for Technical, SMA Directorate.

Member JSC Quality Systems Panel and NASA Quality Leadership Forum.

- April 2006-April 2010: Applied Research and Engineering Sciences Corporation Senior Risk Management Specialist.
- March 2007-June 2010: SAIC technical consultant on the Constellation Program. Member of Orion Crew Exploration Vehicle Standing Review Board for Safety.
- June 2007-present: SAIC/J&P Technologies SMA Contract technical consultant for the Flight Safety Office.

Technical Papers:

- Johnson, G.W. *NASA TND-7951, Apollo Experience Report: Command and Service Module Sequential Events Control Subsystem*. April 1975.
- Johnson, G.W. and B. Sotnikov. *NASA Phase 1 Program Joint Report*, Section 6: Safety Assurance Process. January 1999.
- Johnson, G.W. *NASA/TP-2010-216131, Worldwide Spacecraft Crew Hatch History*. Office of SMA Assessments Team, August 2010.
- Johnson, G.W. "25th Anniversary of the Challenger Disaster: A Tragedy Waiting to Happen." *International Association for the Advancement of Space Safety Newsletter*, March 2011.
- Johnson, G. W. "Safety of Astronauts on Soyuz: Experience and Lessons Learned." *International Association for the Advancement of Space Safety Newsletter*, May 2011.
- Johnson, G. W. "Columbia: A Tragedy Repeated." *International Association for the Advancement of Space Safety Magazine*, Issue 6, Winter 2013.

This is a product of the JSC SMA Flight Safety Office (FSO). Our reports assemble and clarify the best-available data from multiple sources to help SMA decision makers develop a fully informed and integrated perspective of key factors involved in the risk-based decision process. For further information, please contact:

Nigel Packham, Ph.D., NASA

Manager, SMA Flight Safety Office

JSC Safety & Mission Assurance Directorate

Nigel.Packham-1@nasa.gov

Bill Stockton, SAIC

Task Order Lead, FSO Team

Science Applications International Corp.

William.P.Stockton@nasa.gov

SAIC

