National Aeronautics and Space Administration

Recurring Causes of Human Spaceflight Mishaps during Flight Tests and Early Operations

NESC Academy

May 14, 2020

Team Members:

Tim Barth
KSC/NASA Engineering and Safety Center

Steve Lilley
Glenn/NASA Safety Center

Donna Blankmann-Alexander
KSC/Abacus Technology Corporation

Barbara Kanki
Ames/Human Factors

Blake Parker
KSC/ASRC Aerospace

Background

- **Recurring cause study goal: Using selected flight test/early operations mishap investigations, identify recurring cause patterns and provide results to current human spaceflight programs to inform and stimulate their mishap risk management efforts.**
  - **"The NESC gains insight into the technical activities of programs/projects through…systems engineering reviews and independent trend or pattern analyses of program/project technical problems, technical issues, mishaps, and close calls within and across programs/projects." (NESC Management Plan)**
  - **"The NSC will conduct …special studies…at the request of Centers, programs and projects to provide trends within Centers, programs, projects, or facility activities." (NSC Implementation Plan)**
- **Modeled after NESC recurring anomaly studies for Space Shuttle and ISS programs using Problem Reporting and Corrective Action (PRACA) database**
- **Study results can provide current human spaceflight programs with data and examples to seed discussions and questions such as:**
  - **What else can be done within my area of responsibility to ensure crew safety?**
  - **What are we doing now that needs to be improved?**
  - **What could be stopped and replaced with a better approach?**
  - **What is working in other systems than can be extended to my system?**
- **This presentation is a summary of the recurring cause study results**
  - **11 findings, 1 observation, and 3 recommendations**
  - **Complete report is available as a NASA Technical Memorandum (NASA/TM 2020-220573)**





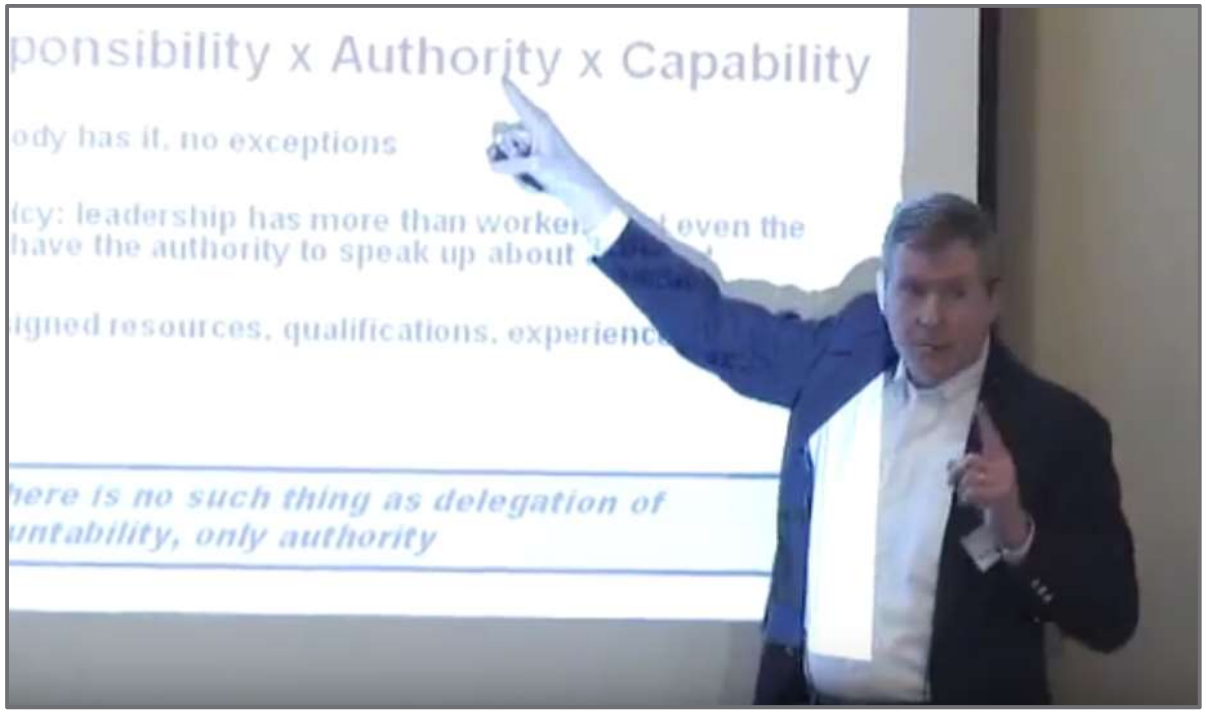




Safety Accountability vs. Responsibility

NESC and NSC common goal: *safety through engineering and technical excellence*

- **Everybody is responsible for safety, but is everybody accountable for safety?**
- **Accountability = Responsibility x Authority x Capability (Bryan O'Connor)**
- **The difference between responsibility and accountability is that responsibility can be shared while accountability cannot. Being accountable not only means being responsible for something but also ultimately being answerable for your actions.**



https://www.youtube.com/watch?v=t-jlwW7ppvA

National Aeronautics and Space Administration

Excerpt from the STS-1 System Failure Case Study

"Tragedy has marred the start of every human spaceflight program since three American astronauts were lost in the 1967 Apollo-1 fire: a Russian cosmonaut died when his spacecraft, Soyuz 1, plummeted to Earth after a parachute deployment failure; NASA's Space Shuttle Program endured an inauspicious beginning when three technicians were asphyxiated in the aft compartment while preparing STS-1 for launch; and the first commercial spaceflight suffered a setback when three Scaled Composites employees perished while performing a cold flow nitrous oxide test. In addition, the first orbiting space station, Skylab, was nearly lost during Skylab-1, and a ground crew fatality was narrowly avoided during preparations for the Ares 1-X test flight in the Parachute Refurbishment Facility at KSC."

National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

October 2011 Volume 5 Issue 9

Tough Transitions

March 1981: Twelve years had passed since astronauts first landed on the moon, six years had passed since the legendary Apollo program had come to a close, and a new chapter in human spaceflight was about to begin. Space Shuttle Columbia, the first reusable launch system and orbital spacecraft, would soon embark upon its maiden voyage. The Space Shuttle had been in development since the early 1970's, and its initial test flight, STS-1, was over two years behind schedule. As ground crews worked diligently to prepare for the launch, a group of technicians collapsed inside Columbia's nitrogen-filled aft compartment after a countdown demonstration test on March 19. STS-1 Pilot Bob Crippen recalled that day: "About a month before the first flight, John (Young) and I were at the Kennedy Space Center doing a Terminal Countdown Demonstration Test, which is pretty much a dry run of what actually goes on when you go launch a Shuttle. The test went great. John and I climbed out of the cockpit, went back to the crew quarters at the O&C Building, and we were patting each other on the back and said 'Hey, we're getting pretty close to flight.' That was when we got the bad news. There had been an accident at the Pad." Nitrogen exposure would claim three of the technicians' lives.

Figure 1: Space Shuttle Columbia prior to the STS-1 launch.

Background

Space Shuttle Program

NASA had been developing early designs for the space shuttle years before Apollo's first lunar landing in 1969. When President Richard Nixon authorized the development of reusable space exploration vehicles three years later, those designs became a springboard from which NASA launched the project known officially as the Space Transportation System (STS) and unofficially as the Space Shuttle Program. The Space Shuttle grew into a significantly more complex system than earlier human spaceflight programs. The vehicle's intricate launch and reentry configurations challenged flight crew safety considerations, and the decision to fly astronauts on the first (or any) launch rested upon successful test and quality control processes.

In June 1974, Rockwell International (now owned by The Boeing Company) began work on the first orbiter, which NASA named Enterprise in response to a massive write-in campaign by *Star Trek* fans. Enterprise never left the atmosphere, but flew approach and landing tests to help verify the reliability and redundancy of the Space Shuttle's design.

STS-1 Mission Objectives

The first operational orbiter, Columbia, arrived at Kennedy Space Center (KSC) atop a modified 747 in March 1979. On STS-1, its first mission, Columbia would carry a Development Flight Instrumentation package as its only payload. This package contained sensors and measuring devices that would record orbiter performance and log stresses encountered during each stage of the flight profile. The flight's primary mission objectives were to safely ascend into orbit, check all systems, and return to Earth landing as an unpowered glider.

Three Technicians Die Before Space Shuttle Columbia's Inaugural Launch

Proximate Cause:

- Oxygen-deficient environment in aft compartment renders workers unconscious and hampers rescue efforts.

Underlying Issues:

- Unclear and Incomplete Procedures
- Communications Breakdown
- Inadequate Controls and Recovery Systems
- Competing Operations Philosophies
- Failure to address recurring causes of earlier mishaps

http://nsc.nasa.gov/SFCS/

"No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state of the art."

Henry Petrosky, To Engineer is Human

National Aeronautics and Space Administration







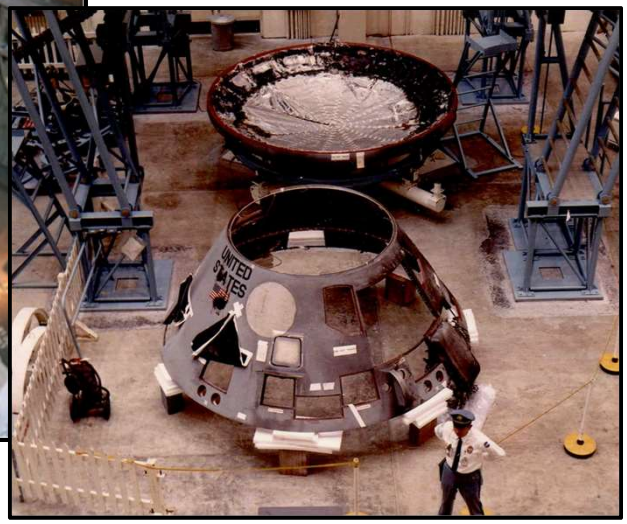


Human Spaceflight Mishaps

Apollo-1 Crew Module Fire at Launch Complex 34

January 27, 1967

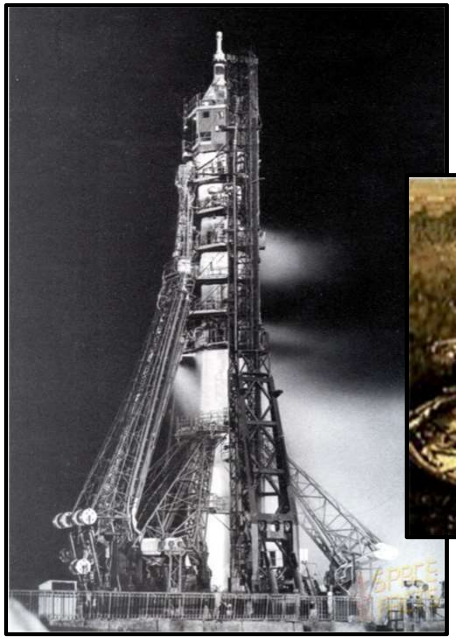
Loss of Flight Crew (3)



Soyuz-1 Main and Reserve Parachute Failures During Reentry

April 24, 1967

Loss of Flight Crew (1)



National Aeronautics and Space Administration

Human Spaceflight Mishaps (continued)

Skylab-1 Loss of Meteoroid Shield During Launch Ascent

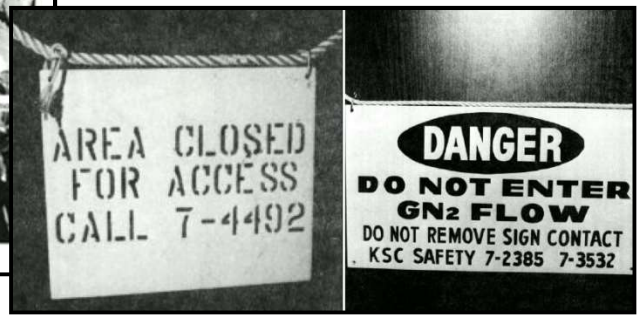
May 14, 1973

Rescue Mission Needed to Save the Orbital Workshop

STS-1 Oxygen Deficiency in Aft Compartment at Launch Complex 39A

March 19, 1981

Loss of Ground Crew (3)



National Aeronautics and Space Administration

Human Spaceflight Mishaps (continued)



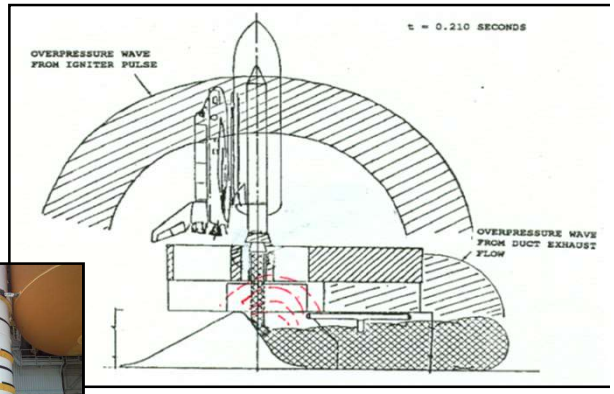






STS-1 SRB Ignition Over-Pressurization
April 12, 1981
Buckled RCS Oxidizer Tank Support Struts; Suppression System Redesigned for STS-2





Scaled Composites Ground Explosion During Cold Flow N2O Test
July 26, 2007
Loss of Ground Crew (3) and Ground Crew Injuries (3)

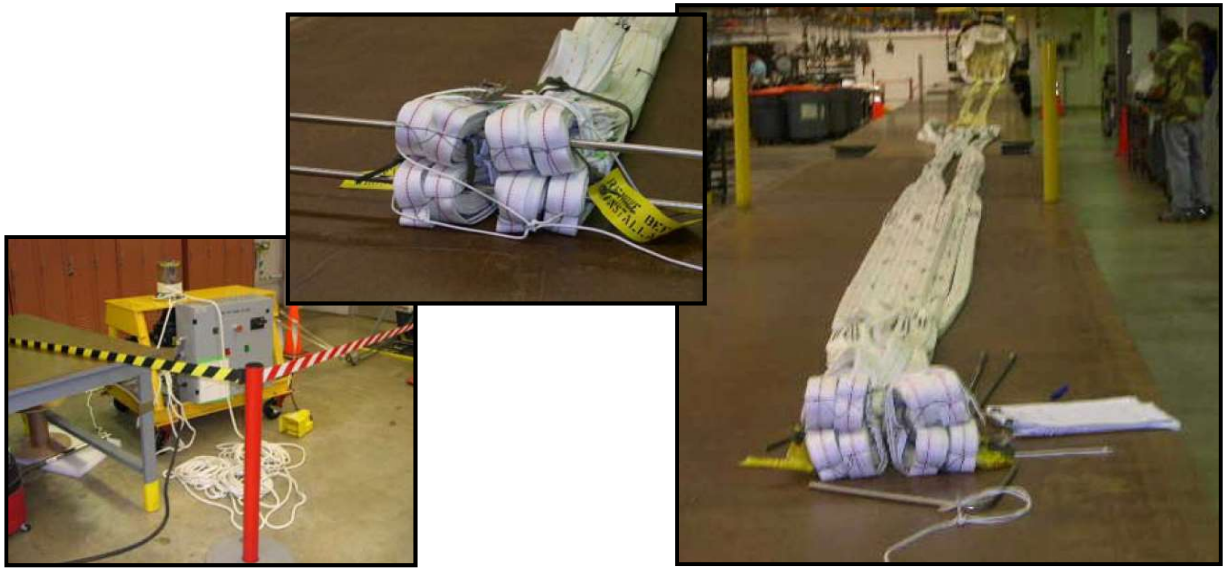

National Aeronautics and Space Administration

Human Spaceflight Mishaps (continued)

Ares-1X Steel Rod Mishap During Static Strip Test at KSC Parachute Refurbishment Facility

September 5, 2007

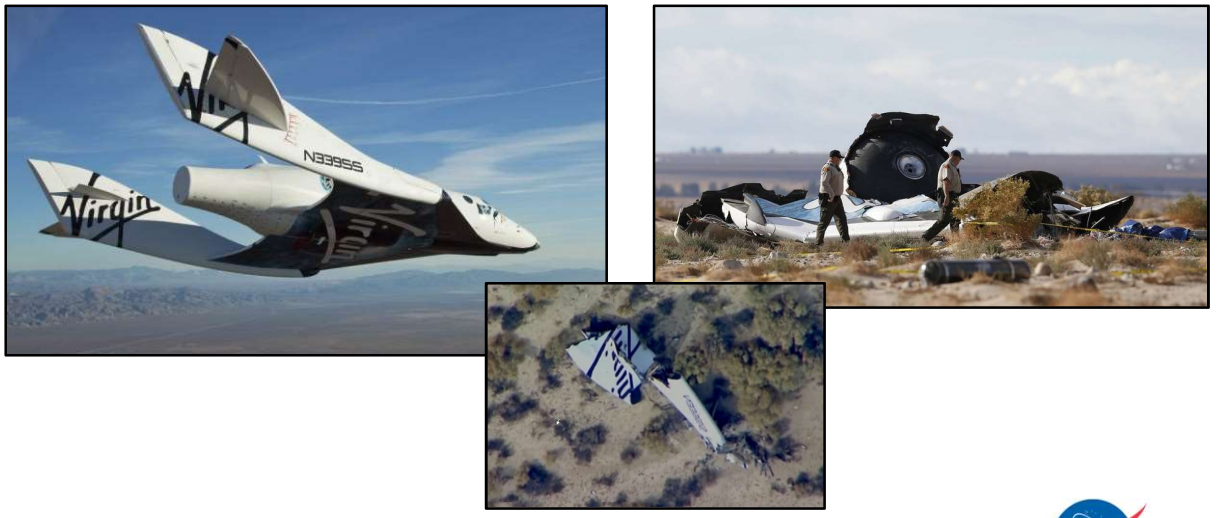
Ground Crew Injury (1)



SpaceShipTwo Test Flight Mishap

October 31, 2014

Loss of Flight Crew (1), Flight Crew Injury (1), and Loss of Spacecraft



National Aeronautics and Space Administration

Systemic, Fundamental, or Underlying Safety Issues

Excerpts from the *Report of the Shuttle Processing Review Team* (i.e., the "Perry Committee" Report), June 1993:

- **"Overall, we were forced to conclude that the bulk of the incidents (particularly the more perplexing ones) were one-of-a-kind events, symptomatic of a more fundamental predisposition to error. In other words, developing specific fixes to preclude the recurrence of these specific incidents will probably have only a minimum impact on reducing the frequency and severity of incidents in the future. Most of the incidents are best viewed as symptoms of more fundamental problems that must be addressed within the broader context of the turnaround processing system."**

- **"The causal patterns of human-initiated incidents during orbiter turnaround operations are complex. Several causal factors are likely to contribute to a typical incident…Although analyses of incidents as they occur should enhance system learning and preclude these specific errors from recurring, they are not likely to address the root causes of most incidents."**

"No matter what measures are taken, doctors will sometimes falter, and it isn't reasonable to ask that we achieve perfection. What is reasonable is to ask that we never cease to aim for it."
Dr. Atul Gawande, Complications





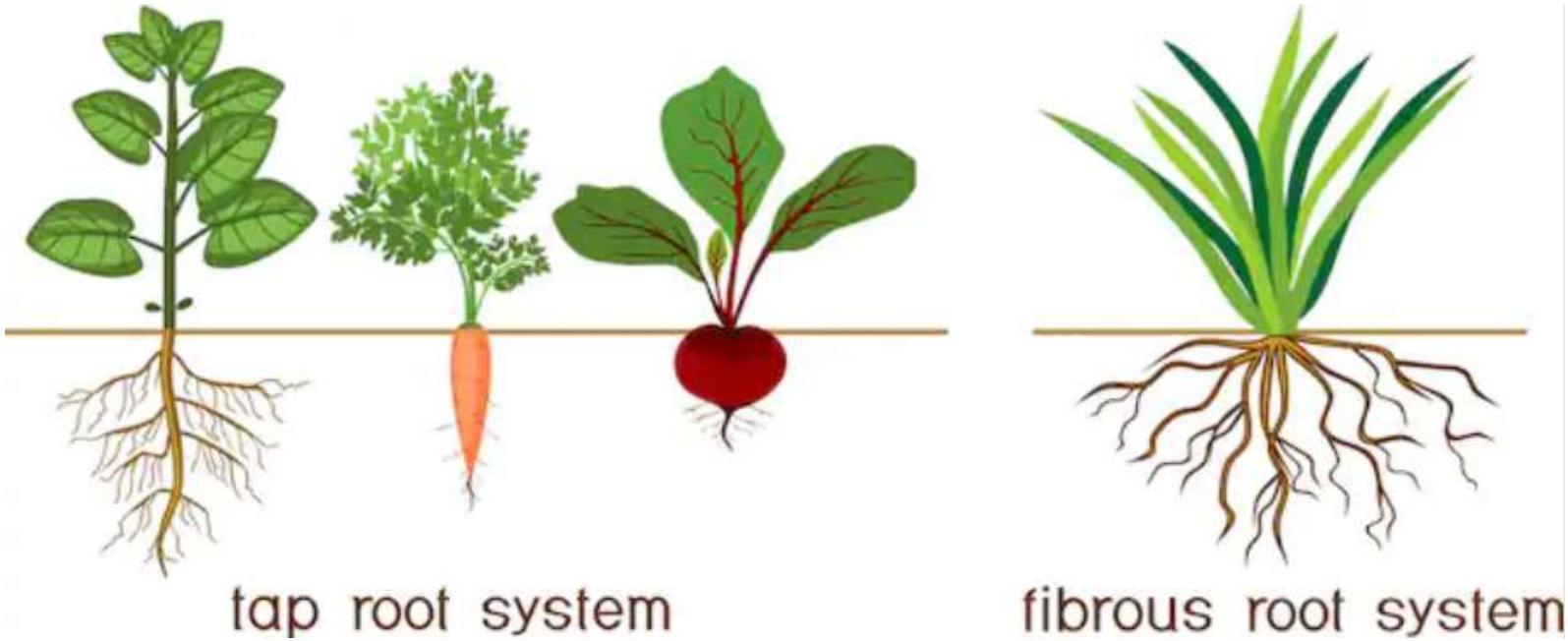




Systemic, Fundamental, or Underlying Safety Issues

Root Cause(s) in Complex Systems

Carrots, Dandelions, and Crabgrass



"I would hasten to add there isn't a root cause. It's a bad term. There are many causes and contributing factors, and to say that there's just one, I would doubt you could ever show an event that there was just one cause. There might be one principal cause, but there are many that, you know, contribute to in sum total end up with a bad event. And you have to look at the myriad of things that contribute to a bad event."

Former Astronaut Dr. James Bagian during an 8/9/10 NPR panel discussion on "What Can be Done to Avoid Man-Made Disasters"

Taxonomy of Potential Causes

Organizational Factors →

- SL; Senior Leadership (8)
  - SL1; Organizational Culture LTA
  - SL2; Resource ($ & staff) Allocation LTA
  - SL3; High Level Policy-Guidance LTA
  - SL4; High Level Org Perf Msmt LTA
  - SL5; Customer-Stakeholder Relat Mgmt LTA
  - SL6; Supplier-Subcont-Reg Relat Mgmt LTA
  - SL7; Internal Relationship Mgmt LTA
  - SL8; Strategic-Succession Planning LTA
- ES; Enabling Systems (8)
  - ES1; Adminstrative Controls LTA
  - ES2; Budget Controls LTA
  - ES3; Schedule Controls LTA
  - ES4; Tech Ctrls-Proc Chng Ctrls-Risk Mgmt LTA
  - ES5; Human Resource Systems LTA
  - ES6; Procuremt-Logistics-Matl Ctrl Systems LTA
  - ES7; Int Cont Imp & Org Learning Systems LTA
  - ES8; Cust-Stakeholder Feedback Systems LTA
- DS; Design & Development Systems (7)
  - DS1; Support Equip-Tool Des & Dev LTA
  - DS2; System-Part Des & Dev LTA
  - DS3; Task Des & Dev LTA
  - DS4; Wkspace-Work Env Des & Dev LTA
  - DS5; Procedure Des & Dev LTA
  - DS6; Training Course Des & Dev LTA
  - DS7; Organizational Des & Dev LTA
- TS; Training Systems (5)
  - TS1; System Training LTA
  - TS2; Task Technical Training LTA
  - TS3; Emerg-Contingency Trng LTA
  - TS4; Safety-HF Awarens Trng LTA
  - TS5; Leader-Team Skills Trng LTA

Dual Role Factors →

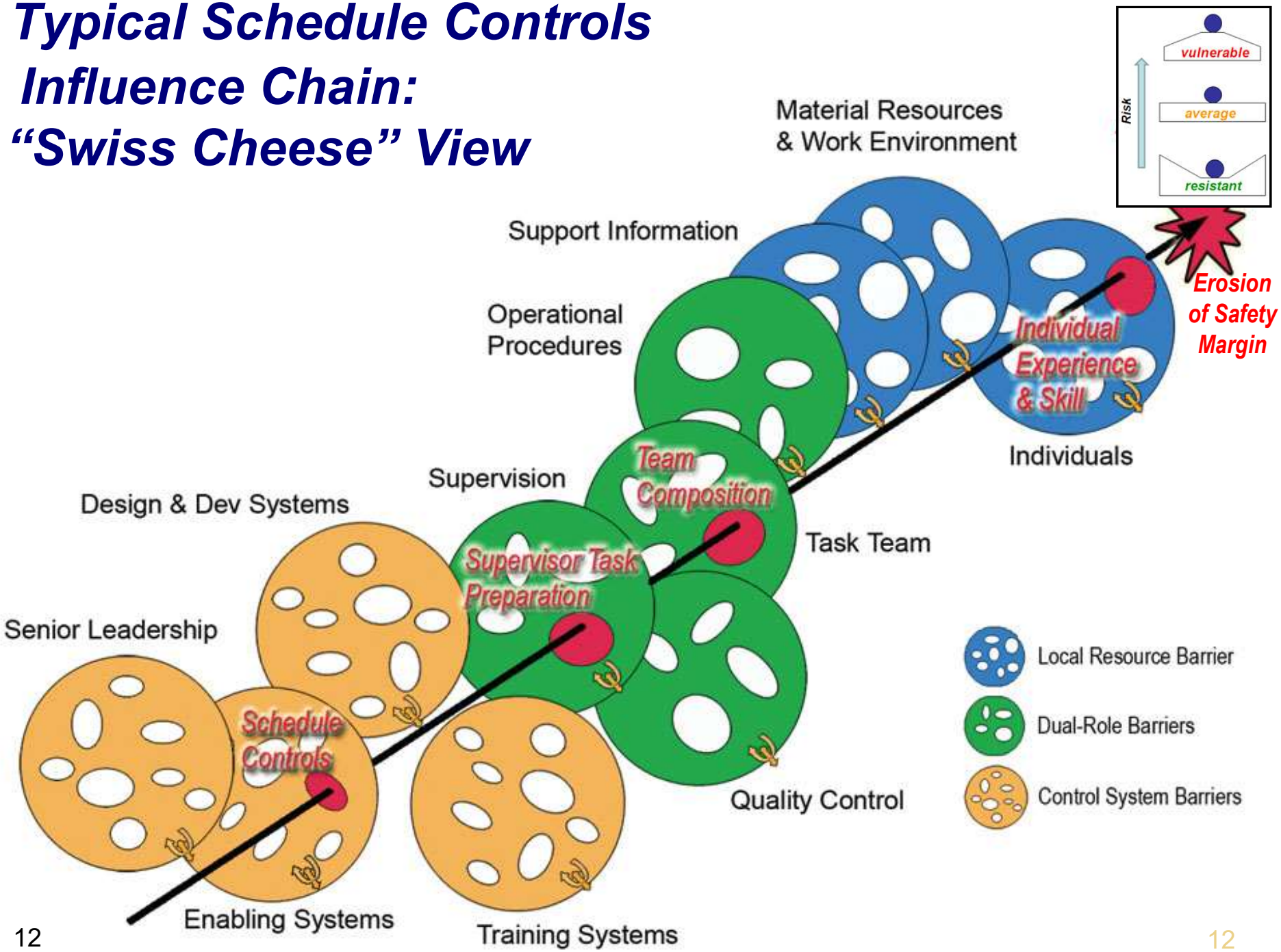
- SV; Supervision (4)
  - SV1; Supv Task Preparation LTA
  - SV2; Supervision During Task LTA
  - SV3; Poor Supv Example-Excess Risk Taking
  - SV4; Supv-Employee Relationship Mgmt LTA
- QC; Quality Control (5)
  - QC1; Insp-Surv-Audit Reqmts LTA
  - QC2; Insp-Surv-Audit Instructions LTA
  - QC3; Insp-Surv-Audit Techniques LTA
  - QC4; Missed-Cursory Insp-Surv-Audit
  - QC5; Statistical Methods LTA
- TT; Task Team (6)
  - TT1; Team Composition LTA
  - TT2; Team Authority-Preps LTA
  - TT3; Team Communication LTA
  - TT4; Accepted Team Practices LTA
  - TT5; Team Adaptability-Flexibility LTA
  - TT6; Teamwork-Morale LTA
- OP; Operational Procedures (4)
  - OP1; Unavailable Procedures
  - OP2; Incomplete Procedures
  - OP3; Incorrect-Conflicting Procedures
  - OP4; Unclear-Misunderstood Procedures

Local Resource Factors →

- SI; Support Information (5)
  - SI1; Written Support Info LTA
  - SI2; Verbal Support Info LTA
  - SI3; Support Equip-Tool Feedback LTA
  - SI4; System-Part Feedback LTA
  - SI5; Worker-Work Env Sensory Signals LTA
- MW; Matl Resources & Work Env (7)
  - MW1; Supt Equip-Tool Reliability-Usability LTA
  - MW2; Supt Equip-Tool Unavail-Uncertified
  - MW3; System-Part Reliability-Usability LTA
  - MW4; System-Part Unavail-Uncertified
  - MW5; Infrequent-Unique Task
  - MW6; Workspace-Facility Work Env LTA
  - MW7; External Work Env LTA
- IN; Individuals (7)
  - IN1; Physical Factors
  - IN2; Cognitive Factors
  - IN3; Emotional Factors
  - IN4; Indiv Exp & Skills LTA
  - IN5; Accepted Indiv Work Practices LTA
  - IN6; Indiv Assertiveness LTA
  - IN7; Values-Attit-Disc LTA, Willful Viol, Disruptive Behavior

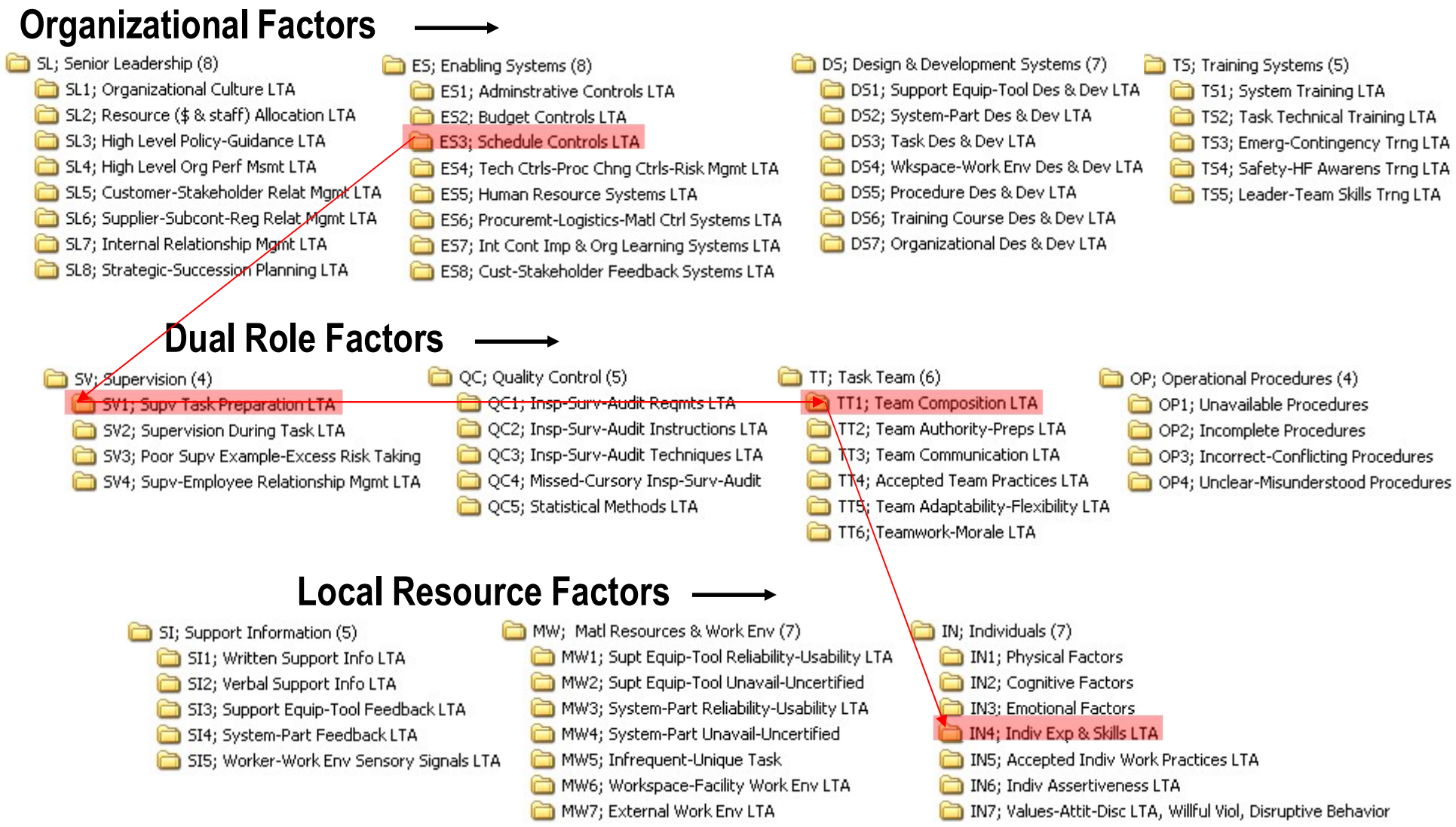
11

Typical Schedule Controls Influence Chain: "Swiss Cheese" View



12

Typical Schedule Controls Influence Chain: Taxonomy View



Study Results – Aggregate Analysis

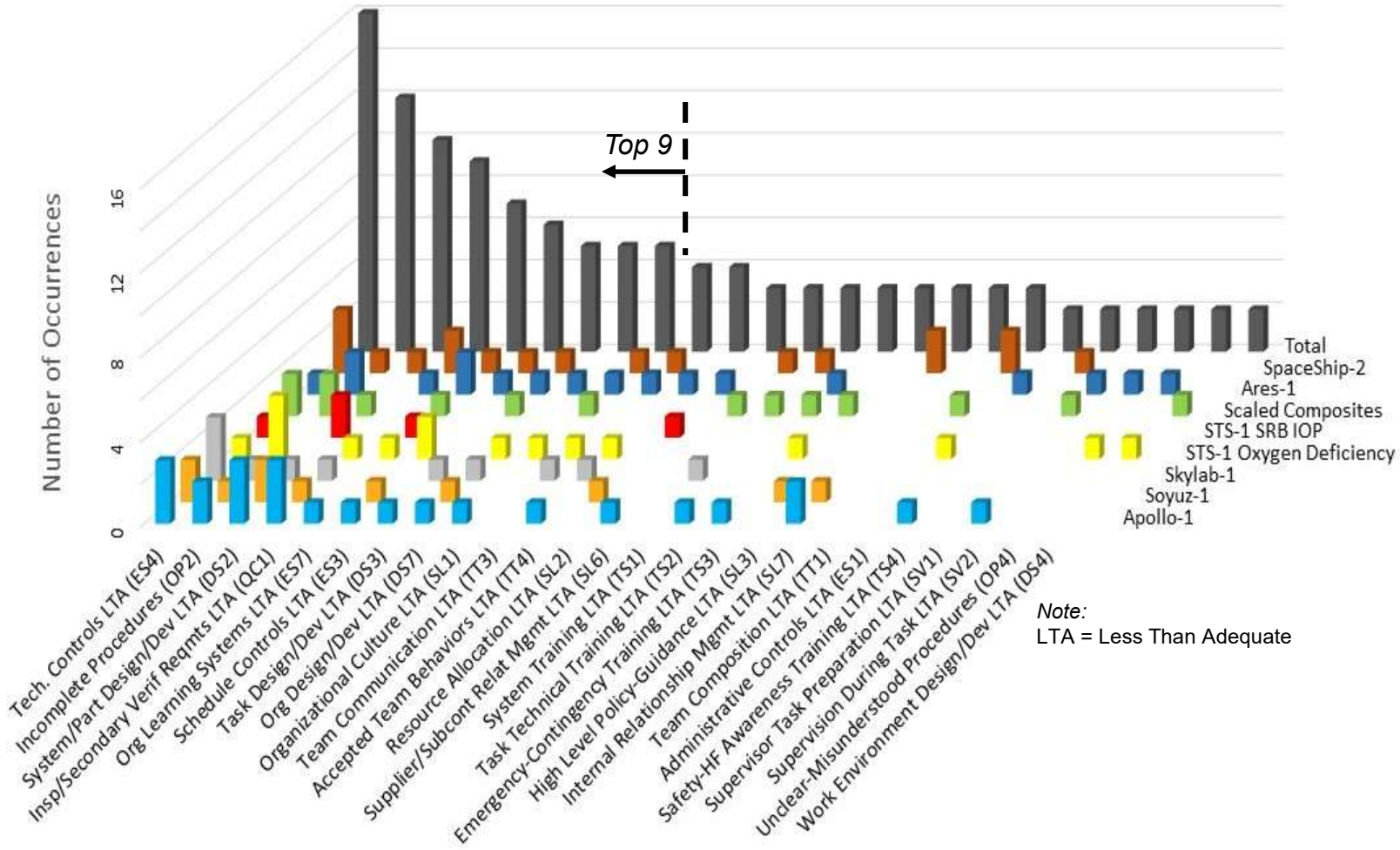
Finding:

For the eight mishaps included in the study, 180 causes were identified. The average number of causes per incident was 22.5. The number of causes per incident ranged from a minimum of eight causes for the STS-1 SRB IOP event to a maximum of 34 causes for the Apollo 1 fire.

Finding:

Twenty-five cause types occurred at least twice (or recurred at least once). The "top nine" most frequent recurring cause types occurred at least five times total in five different mishaps. Seventy-five of the one hundred and seventeen (65%) organizational and dual role recurring causes are included in the nine most frequently recurring cause types.

Pareto Analysis of Mishap Recurring Cause Types



Note:
LTA = Less Than Adequate

"Top 9" Recurring Cause Types

- **Inadequate technical controls and risk management practices**
- **Incomplete procedures**
- **System design and development issues**
- **Inadequate inspection or secondary verification requirements**
- **Inadequate organizational learning systems**
- **Inadequate schedule controls**
- **Inadequate task design/analyses processes**
- **Organizational design issues**
- **Organizational safety culture issues**





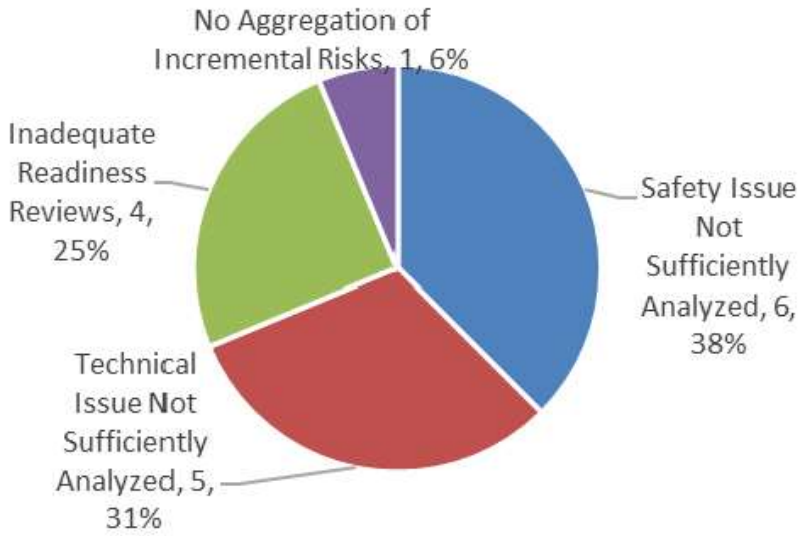




Study Results – Top 9 Recurring Cause Types (1 of 9)

Finding:

Sixteen occurrences of ***"inadequate technical controls or technical risk management practices"*** contributed to all eight (100%) of the incidents studied. Six of the sixteen occurrences (37.5%) were inadequate safety reviews/analyses with tools (e.g., hazard analyses or system safety analyses). Five of the sixteen (31.3%) were due to technical issues not being sufficiently analyzed with tools (e.g., failure modes and effects analyses (FMEA's), process-FMEA's, and quantitative risk assessments). Four of the sixteen occurrences (25.0%) were inadequate readiness reviews. The remaining single occurrence (6.2%) was a case where an aggregation of incremental technical risks was not performed.



"Risks identified are rarely realized, risks realized were rarely identified."
Aerospace Corporation Study, Technical Risk Identification at Program Inception"

Study Results – Top 9 Recurring Cause Types (1 of 9)

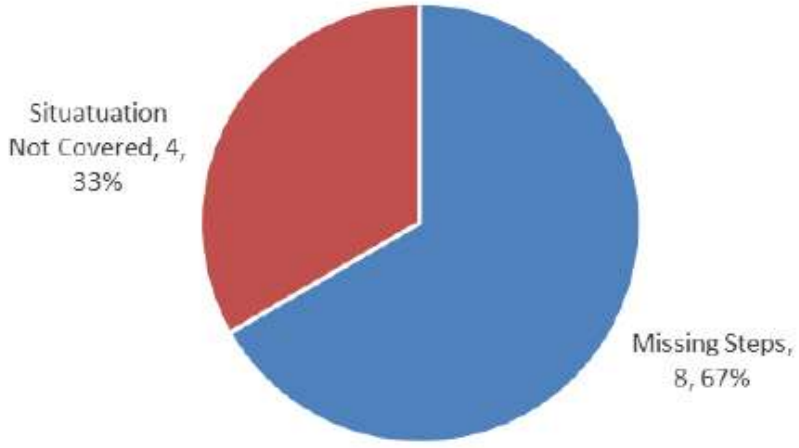
Examples:

- SpaceShipTwo. The system safety analysis (SSA) process was inadequate because it resulted in an analysis that failed to: (1) identify that a single human error could lead to unintended feather operation during the boost phase, and (2) consider the need to more rigorously verify and validate the effectiveness of the planned mitigation measures [ref. 16].
- Soyuz 1. The process failure mode of the primary and secondary parachute's malfunction (stuck in its container due to damage incurred during TPS baking) and the consequences of that failure were not considered in the design of the parachute system [refs. 7, 8].
- Ares-1X. Even though the parachute riser lines were approximately four times longer than the riser lines on the SSP orbiter drag chute, there was no requirement for engineering to perform a first-time loads analysis of the test setup or a readiness review for the initial Ares-1X parachute static strip test [ref. 15].
- Skylab 1. “Despite six years of progressive reviews and certifications, two major hazards eluded discovery until actual flight: aerodynamic load effects on the meteoroid shield and aeroelastic interactions between the shield and its external pressure environment during launch escaped otherwise rigorous design, research and test engineers working under experienced and competent leadership” [ref. 9].

Study Results – Top 9 Recurring Causes (2 of 9)

Finding:

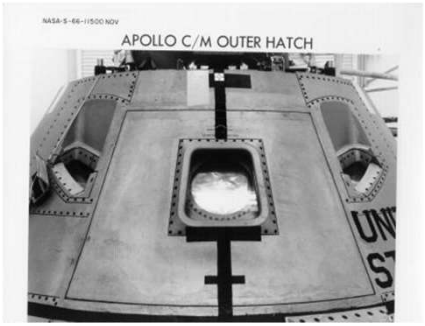
Twelve occurrences of ***"incomplete procedures"*** affected seven of the eight incidents studied (87.5%). When issues with incomplete procedures were identified as a cause of an incident in this study, eight (67%) of those occurrences were attributed, more specifically, to missing steps in the procedure to satisfy hazardous constraints, describe the test setup, and communicate cautions and warnings. The remaining four (33%) occurrences were attributable to the situation not being covered by a written procedure (e.g., emergency or contingency situation).



"How do we achieve engineering excellence? I see it in terms of four guiding principles: clearly documented policies and procedures, effective training and development, engineering rigor, and open communication. All are necessary to enable people to perform at their best in the unique context of NASA, a high-reliability organization that builds one-of-a-kind systems."

Chris Scolese, former NASA Chief Engineer and GSFC CD

Study Results – Top 9 Recurring Causes (2 of 9)



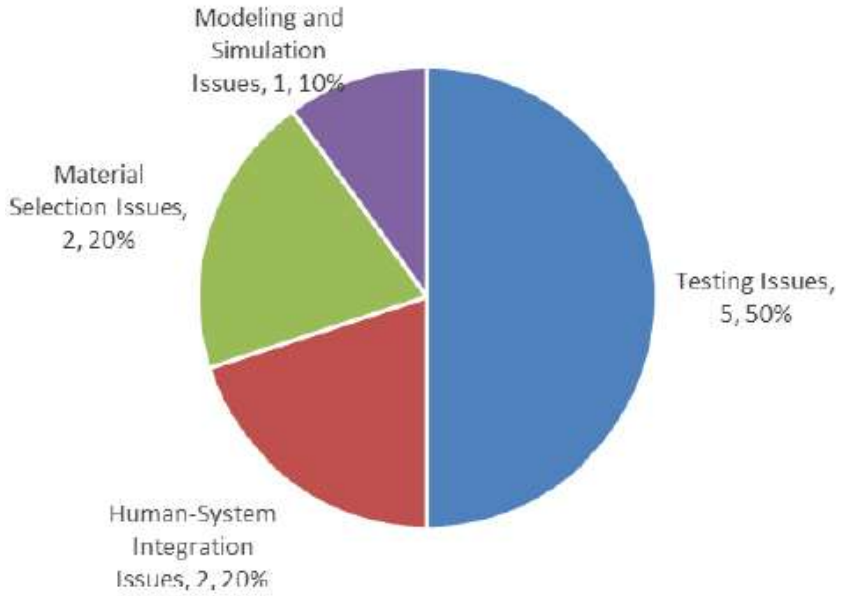
Examples:

- Apollo 1. Adequate safety precautions were not established or observed for this test. Contingency preparations to permit escape or rescue of the crew from a Command Module fire were not made.
- STS-1 Oxygen Deficiency. Atmosphere checks or air purge verifications were not in the safety procedure.
- Scaled Composites. Material Safety Data Sheet (MSDS) documents, in their most basic form from N_2O suppliers, caution against pressure shock. There were no warnings in the work instructions about the dangers of pressure shock. There was no designated hazard control area. Workers were allowed to stand behind a chain link fence in close proximity to the N_2O tank during the test.
- SpaceShipTwo. According to Scaled Composites engineers and test pilots interviewed, the boost phase was a high-workload phase of flight, and duties were divided between the pilot and the copilot. The copilot would unlock the feather at 1.4 Mach, with or without a callout, as indicated on the PF04 test card. Because of the workload, the speed was not crosschecked by the pilot flying [ref. 16]. Also, there was “no warning, caution, or limitation in the SpaceShipTwo pilot operating handbook (POH) that specified the risk of unlocking the feather before 1.4 Mach.”

Study Results – Top 9 Recurring Cause Types (3 of 9)

Finding:

Ten occurrences of the ***"system design and development issues"*** cause category were found to contribute to six of the eight (75%) incidents studied. Five of the ten (50%) system design/development issues were related testing issues (e.g., inadequate testing and verification of system interfaces). This finding included several violations of the "test like you fly and fly like you test" approach. Inadequate system design and development included two of ten (20%) human-system integration issues, and two of ten (20%) material selection issues. The final issue occurred once (one of ten, 10%), and was a modeling and simulation issue related to using subscale testing data to anchor the launch vehicle environments model.



"The single most important factor leading to the high degree of reliability of the Apollo spacecraft was the tremendous depth and breadth of the test activity."
George Low









Study Results – Top 9 Recurring Cause Types (3 of 9)

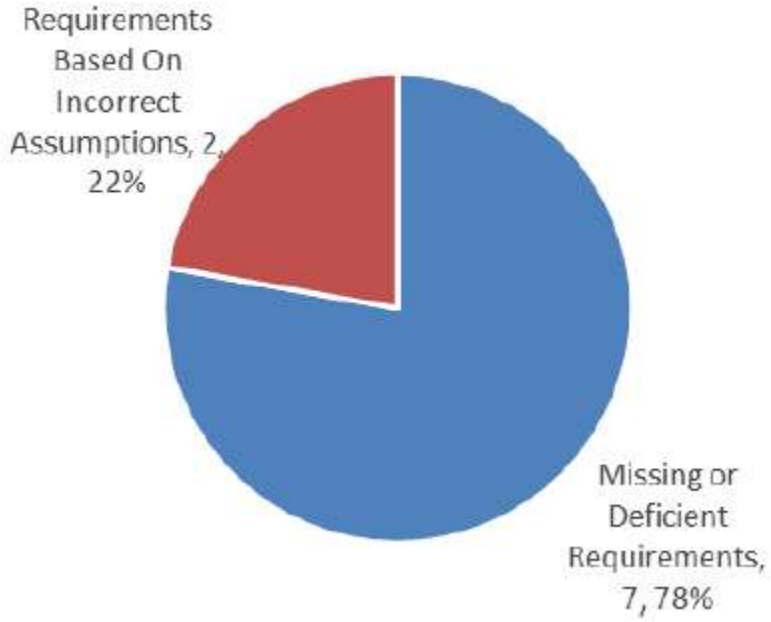
Examples:

- Apollo 1. Teflon wire coating was chosen for superior insulation, chemical inertness, and fire resistance. However, the soft, unprotected, thick-wall Teflon coating was susceptible to creep, cold-flow deformation, and abrasion. The Teflon coating was abraded during installation and from contact with adjacent hardware during training activities. Electrical wiring was exposed, which contributed to command module technical problems during tests.
- Soyuz 1. “In retrospect, the Soyuz 1 flight should not have been carried out at that time. The spacecraft was insufficiently tested in space conditions, and it was certainly not ready for the ambitious first mission it was scheduled to accomplish.”
- Scaled Composites. The N_2O tank design included several materials that were incompatible with the propellant, and the tank lacked a pressure relief protection to prevent rapid over-pressurization.
- STS-1 SRB Ignition Over-Pressurization. System Integration, which is responsible for defining the liftoff environment, accepted the Tomahawk ignition test as a sufficient simulation of SRB IOP. Engineers did not fully appreciate the effect of the differences between the SRB and the Tomahawk ignition characteristics.

Study Results – Top 9 Recurring Cause Types (4 of 9)

Finding:

Nine occurrences of ***"inadequate inspection or secondary verification requirements"*** affected six of the eight (75%) incidents studied. Seven of nine (77.8%) of those occurrences were attributed to absent or inadequate inspection requirements for known issues related to materials, safety, and contamination. The remaining two of nine (22.2%) occurrences were attributable to basing inspection requirements on incorrect assumptions.











Study Results – Top 9 Recurring Cause Types (4 of 9)

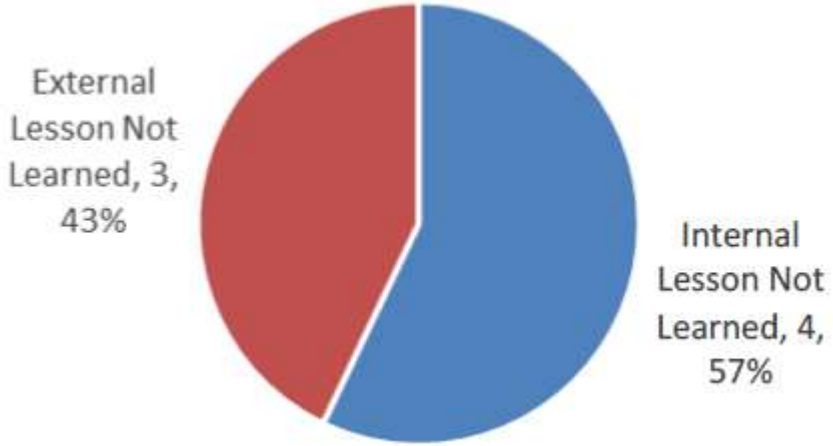
Examples:

- Apollo 1. Inadequate attention was given to the inspection of the wire bundles for abrasion or deformation.
- Soyuz 1. There was no requirement to inspect the parachute container for contamination or damage.
- Skylab 1. There was no system feedback (e.g., a visual cue) to the technicians, quality inspectors, and engineers that a “tight fit” had not been achieved during rigging. There were also inadequate requirements for quality inspections.
- STS-1 Oxygen Deficiency. Applicable safety documents did not have sufficient requirements for atmosphere checks or verification of an air purge before reentry of the orbiter aft compartment by technicians. There was no oxygen deficiency monitoring system in the aft compartment.

Study Results – Top 9 Recurring Cause Types (5 of 9)

Finding:

Seven occurrences of ***"inadequate organizational learning systems"*** affected six of the eight (75%) incidents studied. The lessons were present within human spaceflight programs or in related industries, but they were not shared, found, and/or heeded. Four of seven (57.1%) occurrences were internal lessons not learned, where "internal" refers to within the current or previous human spaceflight programs. This failure was sometimes due to restricted or classified information. Three of seven (42.9%) of the occurrences were external lessons not learned, where "external" refers to lessons outside the human spaceflight programs and related aerospace industry.

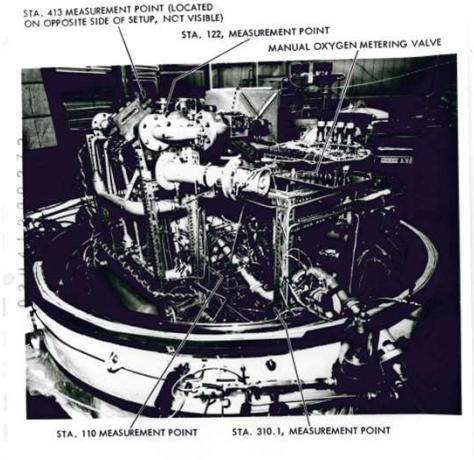


"There's no shortage of lessons, but learning is the issue"
T.K. Mattingly

Study Results – Top 9 Recurring Cause Types (5 of 9)

SpaceShipTwo Feather Lock System

Command Module ECS test rig



Examples:

- SpaceShipTwo. Human reliability issues and probability estimates are well-documented in related literature and human-system integration design guidance based on many years of experience within DOD and commercial aviation, NASA space flight operations, and the nuclear industry. The likelihood of a pilot error in deploying the feathering system should not have been considered “remote” or “zero,” especially when it was recognized that the consequences were catastrophic.
- Apollo-1. There was an electrical fire of an Apollo command module ECS test rig in a vacuum chamber in 1966. The test was conducted under a lower atmospheric pressure (i.e., 5 psi to simulate cabin pressure in space versus 16.7 psi for the LC 34 test), but in a 100% O_2 environment. The test incident report was classified and inaccessible to personnel without clearance.
- STS-1 Oxygen Deficiency. In 1967, Apollo 1 Congressional hearings uncovered a problem at KSC with timely submittals of operational checkout procedures to the safety organization for review. STS-1 procedures had the same problem. It was unclear whether the issue “slipped through the cracks” between the Apollo Program and SSP or corrective actions proved to be ineffective.





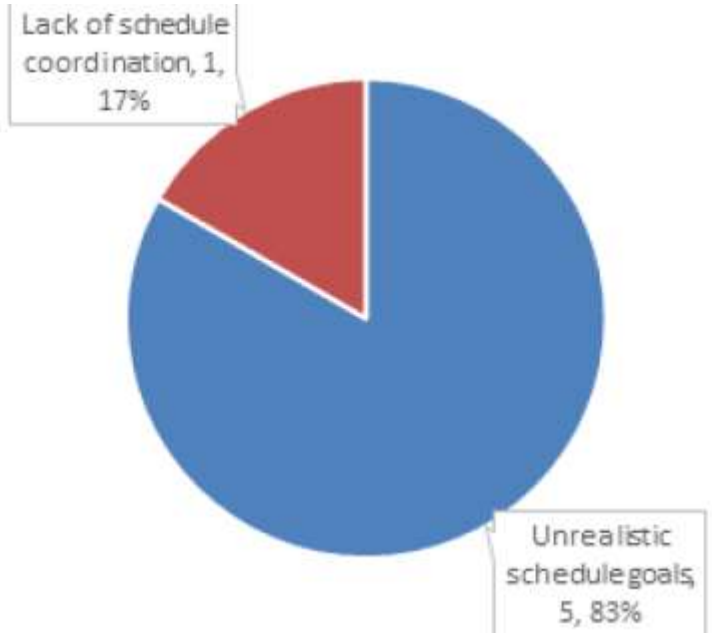




Study Results – Top 9 Recurring Cause Types (6 of 9)

Finding:

Six occurrences of ***"inadequate schedule controls"*** affected five of the eight (62.5%) incidents studied. Five of the six (83.3%) occurrences were related to overly optimistic/aggressive schedules, and the remaining (one of six, 16.7%) occurrence was related to a lack of communication/ coordination between the overall master schedule and local shop area schedules.



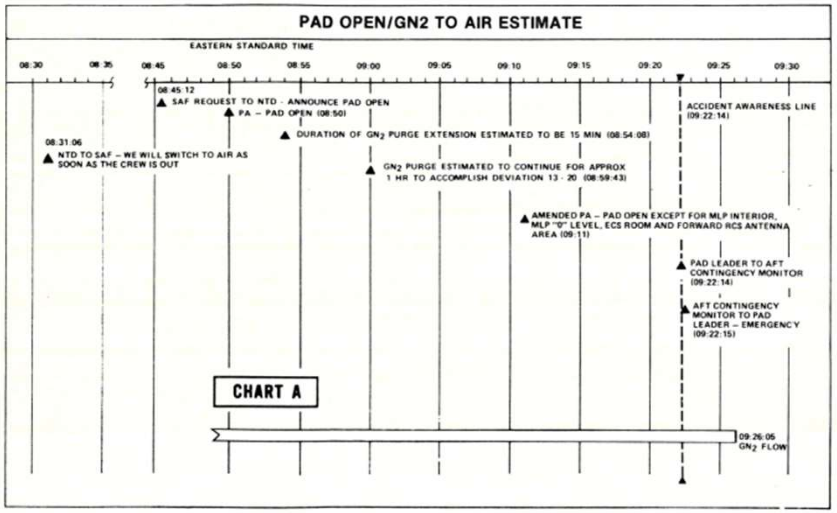
"We were too gung ho about the schedule and we locked out all of the problems we saw each day in our work...Not one of us stood up and said, 'Dammit, stop!"

Gene Kranz to his team on the Monday morning following the Apollo-1 fire

Study Results – Top 9 Recurring Cause Types (6 of 9)

Examples:

- STS-1 Oxygen Deficiency. The shop schedule was followed instead of the integrated schedule. The shop schedule showed the deviation as being hazardous, but the integrated schedule did not. Schedule motivation created a practice of allowing non-hazardous, non-critical path "side work" to be performed in parallel with hazardous operations, which increased risk and susceptibility to an incident. "Scheduling of side work during hazardous operations should be prohibited as a matter of practice. Where exceptions must be made, they should be placed under stringent firing room and/or safety controls, and coordinated with all involved parties" [ref. 10].
- SpaceShipTwo. The pressure to approve experimental permit applications within a 120-day review period interfered with the Federal Aviation Administration's (FAA's) ability to thoroughly evaluate the SpaceShipTwo experimental permit application.
- Apollo-1. The command module was shipped to KSC with excessive open work items. "There is an inference that the design, qualification, and fabrication process may not have been completed adequately prior to shipment to KSC" [ref. 19].



STS-1 mishap report timeline of GN2 purge continuing after pad was re-opened for work.

Shuttle Workforce Message from Bob Crippen

www.youtube.com/watch?v=5vfyZtVPvfs





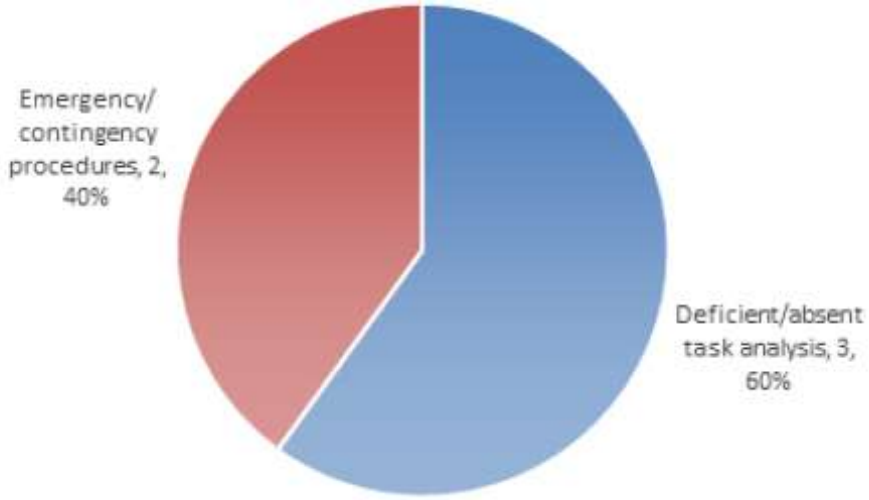




Study Results – Top 9 Recurring Cause Types (7 of 9)

Finding:

Five occurrences of ***"inadequate task analysis and design processes"*** affected five of the eight (62.5%) incidents studied. Three of the five (60%) occurrences were related to missing or deficient task analyses, and the remaining two of five (40%) occurrences were related to inadequate designs of emergency or contingency operations.











Study Results – Top 9 Recurring Cause Types (7 of 9)

Examples:

- Apollo-1. The astronauts requested that the emergency egress simulation be added to the end of the plugs out test because they were three weeks from launch and had not practiced an emergency escape. The plugs out test did not require all the hatches to be closed and locked.
- Skylab-1. Stowing and rigging the large, lightweight MS to the OWS proved extremely difficult, requiring the coordinated action of a large group of technicians. Despite considerable adjustments to the assembly of the various panels, a tight fit between the shield and the OWS wall could not be made.
- Ares-1X. The initial parachute strip test setup combined components (i.e., forklift, capstan winch, nylon break ties, and a nylon towline) in an untested combination. The nylon tow line used to extract the parachute released a dangerous amount of stored energy to the steel rods upon failure.





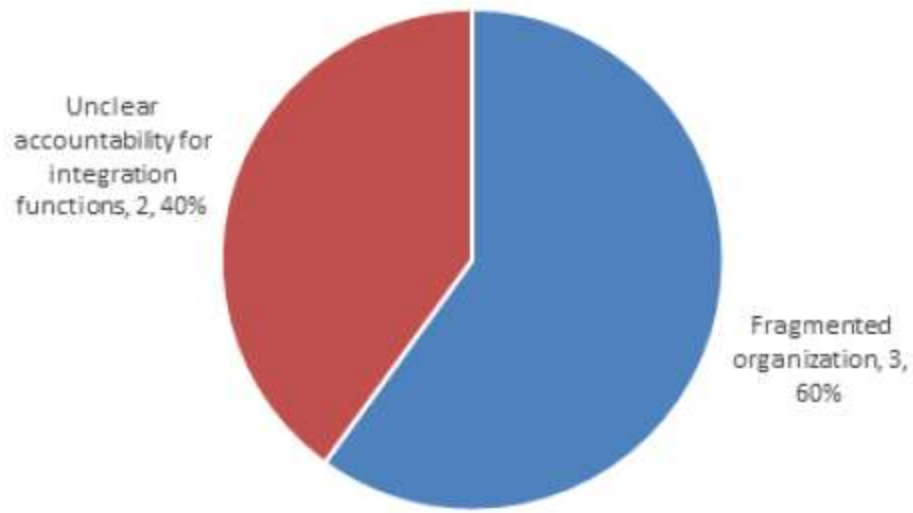




Study Results – Top 9 Recurring Cause Types (8 of 9)

Finding:

Five occurrences of ***"organizational design issues"*** affected five of the eight incidents studied (62.5%). Three of the five (60%) occurrences were related to fragmented organizations due to competing projects and priorities. The remaining two of five (40%) occurrences were related to unclear accountability of technical integration functions during design and operations.











Study Results – Top 9 Recurring Cause Types (8 of 9)

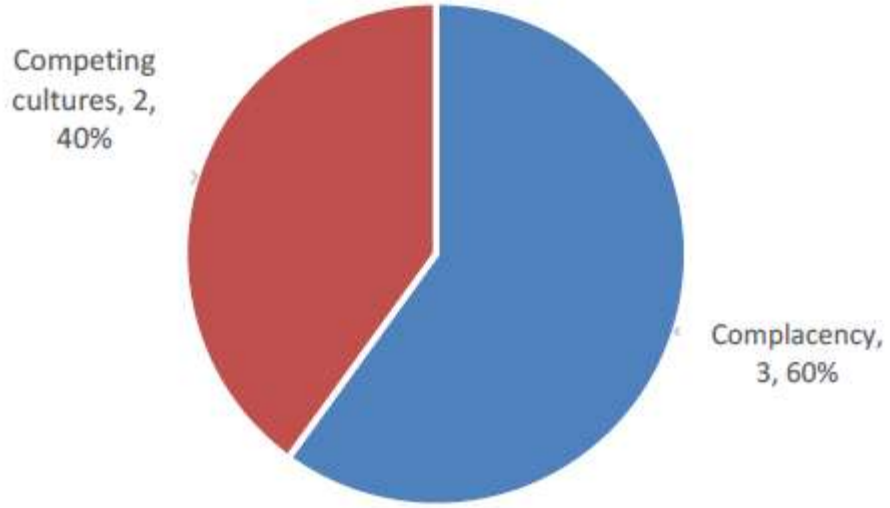
Examples:

- Apollo-1. North American Aviation's (NAA's) organization was too fragmented and unintegrated. NAA's organizational deficiencies were noted and presented to NAA's president 13 months prior to the Apollo 1 fire. A NASA report was issued that was critical of NAA's continued failure to meet committed schedule dates with required technical performance and within cost. "It is our view that the total Engineering, Manufacturing, Quality, and Program Control functions are too diversely spread and in too many layers throughout the Space and Information Systems Division to contribute, in an integrated and effective manner, to the hard core requirements of the programs" [ref. 6].
- Skylab-1. There was no designated systems or chief engineer for the meteoroid shield. "Organizationally, the meteoroid shield (MS) was treated as a structural subsystem. The absence of a designated project engineer for the shield contributed to the lack of effective integration of the various structural, aerodynamic, aeroelastic, test, fabrication, and assembly aspects of the MS system. Complex, multi-disciplinary systems such as the meteoroid shield should have a designated project engineer who is responsible for all aspects of analysis, design, fabrication, test and assembly" [ref. 9].
- Ares-1X. The Ares-1X integrated product team (IPT) process was not defined or formalized. There was no defining requirement for team membership and no defined roles and responsibilities. Membership was at the IPT lead's discretion. In some cases, a necessary discipline may be missed (e.g., Safety or GSE design).

Study Results – Top 9 Recurring Cause Types (9 of 9)

Finding:

Five occurrences of ***"organizational safety culture issues"*** affected five of the eight (62.5%) incidents studied. Three of the five (60%) occurrences were related to organizational complacency regarding known, documented safety issues. The remaining occurrences (two of five, 40%) involved competing cultures: a centralized versus distributed command and control culture during ground tests and a research versus operational culture.



"Carelessness and overconfidence are more dangerous than deliberately accepted risk."

Wilbur Wright, 1901

National Aeronautics and Space Administration

Study Results – Top 9 Recurring Cause Types (9 of 9)

Examples:

- Ares-1X. Two serious injuries occurred in December 2006 during STS-116 SRB retrieval operations, and investigators questioned the safety culture and leadership of the Solid Rocket Booster Element (SRBE) organization. The same organizational safety culture issues affected the Ares-1X mishap in the Parachute Refurbishment Facility (PRF). Smaller, isolated facilities like the PRF often have less safety surveillance and independent monitoring than the other more integrated facilities, which can contribute to culture drift. A video recording was made of the Ares 1-X parachute static strip test which showed examples of complacency, disengagement, and lack of discipline related to organizational safety culture.
- STS-1 Oxygen Deficiency. Different cultures were emerging associated with two competing operations philosophies: centralized operations controlled and coordinated through the firing room versus decentralized operations controlled and coordinated at the local work areas.
- Scaled Composites. Scaled Composites was complacent regarding the documented hazards of N_2O. Earlier OSHA findings related to system safety were not addressed. “Serious Violation, ($18,000.00 penalty): The employer failed to provide for correcting the unhealthy or unsafe conditions, and other work practices and procedures associated with the use of nitrous oxide chemical compound prior to a TST equipment apparatus test on 7/26/2007. This failure contributed to the serious injuries suffered by six employees working at the site.”

Human Spaceflight SME Review

JSC:
- Bo Bejmuk
- Wayne Hale
- Gary Johnson
- Steve Lilley*

MSFC:
- Jim Blair
- Bob Ryan
- Don Hull*

WebEx:
- Mike Blythe
- Nancy Currie-Gregg
- TK Mattingly

KSC:
- Jay Honeycutt
- Bob Lang
- Charlie Mars
- Gerry Schumann
- Bob Sieck
- Tip Talone
- John Tribe
- Donna Blankmann-Alexander*
- Barbara Kanki*
- Tim Barth*

**Facilitators*

Anomaly Investigation

Examples of little-known but significant human spaceflight anomalies:

- Apollo Mission A-003 Little Joe II Launch Abort*
- Apollo Mission A-201 Command Module Reaction Control System Loss*
- Apollo 7 Mission AC Electrical Bus Short
- Apollo 10 Inadvertent LM Abort and Fuel Cell Failure
- Apollo 14 Docking Problem
- Apollo 15 Service Propulsion System Engine and Main Chute Failure
- Apollo 16 SPS Secondary Yaw Gimbal Actuator Oscillations
- Apollo 16 Lunar Rover Anomalies
- Skylab 2 Hard Dock Problem
- Skylab 3 Propellant Leak on Service Module
- Skylab 4 Command Module Loss of Pitch/Yaw RCS Control
- Apollo-Soyuz Mission Command Module Crew Exposure to N_2O_4
- STS-1 Negative Margins in Orbiter Wing During Ascent
- STS-51F Abort Request Command Near Miss**
- STS-55 Experiment Valve Near Miss**
- STS-53 Approach Near Miss**
- STS-41C Dynamic Standby Computer Failure Near Miss
- STS-93 Launch Scrub
- STS-93 SSME Injector Anomaly
- STS-114 Debris Strike***
- STS-121 External Tank (ET) Engine Cut-Off (ECO) Sensor Anomaly *(see next slide)*

** A NASA report exists, but it is not readily available.*

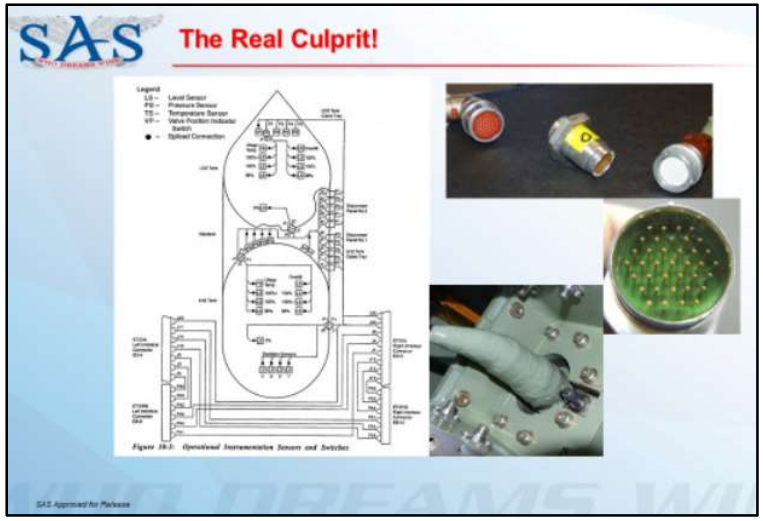
*** "near miss" term used where no record of a NASA close call investigation was found in NMIS going back to 1985*

**** NESC report available*

Anomaly Investigation (continued)

STS-121 External Tank (ET) Engine Cut-Off (ECO) Sensor Example

- ECO sensor issues initially appeared during ET tanking tests before STS-114 launch (first return-to-flight mission after Columbia accident)
- The same sensor issues were the cause of STS-121 initial launch attempt scrub
- *"It wasn't the point sensor box in the orbiter; it wasn't the sensors in the bottom of the ET. It was the pin connectors on the pass through where the wiring went from inside to outside of the hydrogen tank. Something we thought we had exonerated early on. We had jumped to an erroneous conclusion early in the troubleshooting and spent over a year working on the wrong problem. Somebody from a different program pointed out – much later than STS-121 – that the Delta program had a similar problem which was caused by pin connectors in the tank wall pass through and they had solved their problem by soldering the wires together. Which is what we did. Which solved the problem. After almost two years of work."*



from Wayne Hale's blog:
https://waynehale.wordpress.com/2018/03/16/sts-121-the-hardest-launch-part-2-electrical-problems/

Final Report Observation

Many potentially severe technical anomalies, problems, and other events occurred during tests and operations without any surviving record of detailed investigation and troubleshooting results, event sequences, causes of potential failures, and corrective actions.









Final Report Recommendations

- **Encourage human spaceflight organizations to internalize the mishap recurring cause study results and determine whether additional mishap risk reduction actions are warranted.**

- **Consider organizing a knowledge-sharing forum focused on ensuring safe and effective ground processing and mission operations.**

- **Develop a strategy to capture significant events (anomalies, problems, system failures, technical issues, close calls) not already captured in existing databases in sufficient detail that engineers on existing and future programs have systematic context to apply lessons learned to their own work, and encode this strategy as requirements for the NASA Lessons Learned Process (NPR 7120.6).**

What Can I Do?

- **Learn how your systems and processes are designed to achieve safety goals and prevent failures.**
  - **Use your system as your context for decisions, to include software, hardware, liveware, and environment. Limit your scope to the safety controls in your system (technical, administrative), the requirements that created them, and the assumptions behind the requirements.**
  - **How healthy are your controls? Have the assumptions that created them changed?**

- **Use the five attributes of a healthy safety culture to guide your efforts.**
  - **Reporting culture: Has fear been driven out? Are failure, anomaly, and problem investigations and reports thorough enough to assess safety controls at the technical and risk ownership levels?**
  - **Flexible culture: Are changes to the system being captured in configuration control to include safety control effectiveness?**
  - **Just culture: For errors due to training or willful neglect, are we consistent in corrective actions?**
  - **Learning culture: Are we capturing and sharing expensive lessons?**
  - **Engaged culture: Are we vigilant, obsessed with the potential for failure but striving to recognize and encourage behaviors that enable success and create safety?**

- **Participate in technical reviews and constantly ask yourself questions such as: "Is the program/project making decisions that place cost or schedule ahead of safety, reliability, or quality?" or "Are we being asked to prove it is unsafe instead of proving that it is safe?"**
  - **Optimum balance at this decision/review level is the future of mission assurance and flight safety. No longer is it sufficient to measure safety in terms of lack of a negative outcome (no disasters for years now). Measurements of fewer and fewer mishaps become increasingly less informative and hide latent conditions that increase safety risk. Instead, look at upstream conditions that reflect organizational attention to mission assurance and safety.**









Dr. Jonathan Clark: "Turning Badness Into Goodness"

- **January 27, 1967: Apollo-1 fire**
  - **July 16, 1969: Apollo 11 launch**
- **April 24, 1967: Soyuz-1 parachute failures**
  - **October 25, 1968: Soyuz-2 launch**
- **May 14, 1973: Skylab-1 loss of meteoroid shield during ascent**
  - **May 25, 1973: Skylab-2 launch**
- **March 19, 1981: STS-1 oxygen deficiency mishap**
  - **April 12, 1981: STS-1 launch and SRB ignition over-pressurization close-call**
- **September 5, 2007: Ares-1X static strip test mishap**
  - **October 28, 2009: Ares-1X test flight**

"A ship in harbor is safe, but that is not what ships are built for."
John A. Shedd









Final Report

NASA/TM–2020-220573
NESC-RP-12-00823

Recurring Causes of Human Spaceflight Mishaps during Flight Tests and Early Operations

Timothy S. Barth/NESC
Langley Research Center, Hampton, Virginia

Steve K. Lilley
Glenn Research Center, Cleveland, Ohio

Barbara G. Kanki
Ames Research Center, Moffett Field, California

Donna M. Blankmann-Alexander
Abacus Technology Corporation, Chevy Chase, Maryland

Blake Parker
ASRC Aerospace, Greenbelt, Maryland

- ***Final report is available on NESC Academy website or by emailing Tim or Steve***
  - ***Available soon on NTRS***
- ***Approx. 50 pages + Appendices***

Additional Resources

- **NASA Safety Center**

http://www.nasa.gov/offices/nsc/home/

  - System Failure Case Studies
  - Think Safety Articles
  - NASA Mishap Investigation Board Reports
  - Risk Management Handbook
  - SMA Technical Excellence Program (STEP)
  - Quality Audit, Assessment, and Review (QAAR)
  - IV&V Services

- **NASA Engineering and Safety Center**

http://www.nasa.gov/offices/nesc/home/

  - Independent Assessment Reports
  - Technical Bulletins
  - On-line NESC Academy
  - DDT&E Best Practices Report
  - Readiness for Crewed Flight Report

- **NASA OCE/OCKO**
  - NASA Lessons Learned Information System (LLIS)
  - APPEL Courses and Case Studies
  - Shuttle Knowledge Console
  - NASA Standards and Handbooks

"We must challenge our assumptions, recognize our risks, and address each difficulty directly and openly so that we can operate more safely and more successfully than we did yesterday, or last month, or last year. We must always strive to be better, and to do better."

Chris Scolese, Former NASA Chief Engineer and GSFC Center Director, Day of Remembrance Memo, January 29, 2009