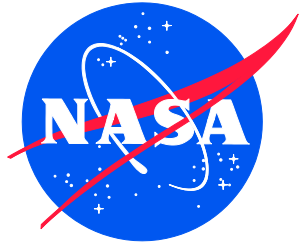


NASA/TM-2020-220573  
NESC-RP-12-00823



# 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*

## NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.

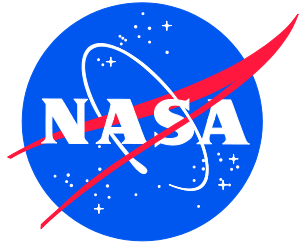
- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at <http://www.sti.nasa.gov>
- E-mail your question to [help@sti.nasa.gov](mailto:help@sti.nasa.gov)
- Phone the NASA STI Information Desk at 757-864-9658
- Write to:  
NASA STI Information Desk  
Mail Stop 148  
NASA Langley Research Center  
Hampton, VA 23681-2199

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*

National Aeronautics and  
Space Administration

Langley Research Center  
Hampton, Virginia 23681-2199

March 2020

## **Acknowledgments**

The study team thanks the following human spaceflight experts for their contributions during an initial review of the study results: Bo Bejmuk, Wayne Hale, Gary Johnson, Mike Blythe, Nancy Currie-Gregg, and T. K. Mattingly from Johnson Space Center (JSC); Jim Blair and Bob Ryan from Marshall Space Flight Center (MSFC), and Jay Honeycutt, Bob Lang, Charlie Mars, Gerry Schumann, Bob Sieck, Tip Talone, and John Tribe from Kennedy Space Center (KSC). These personnel (except Mike Blythe) are NASA or contractor retirees associated with the identified Centers but are not currently employed by a specific program at those Centers.

Special thanks to Jenny Twining, a research assistant at NASA Ames Research Center who supported the study by performing an independent analysis of the Aerospace Safety Advisory Panel (ASAP) recommendations.

The study team also thanks the peer reviewers for their contributions: Bob Beil, Tim Brady, Steve Gentz, Jon Holladay, Robert Johnson, Robert Moreland, Cynthia Null, Joe Olejniczak, Mike Watson, and Scott West.

<p>The use of trademarks or names of manufacturers in the report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.</p>
--

Available from:

NASA STI Program / Mail Stop 148  
NASA Langley Research Center  
Hampton, VA 23681-2199  
Fax: 757-864-6500





## **NASA Engineering and Safety Center Technical Study Report**

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

#### **Abstract**

An analysis of recurring causes underlying human spaceflight mishaps that occurred during flight tests and early operations was performed. Eight mishaps from the Apollo, Soyuz, Skylab, Space Shuttle, and Constellation Programs (i.e., the Ares-1X test flight) and commercial suborbital systems were included in the study. Detailed event analyses were performed for the historical mishaps and aggregate data analyses conducted to identify recurring issues. The nine most frequent issues were inadequate technical controls or risk management practices, incomplete procedures, system design and development issues, inadequate inspection or secondary verification requirements, failures of organizations to learn from previous incidents, inadequate schedule controls, inadequate task analyses or design processes, flaws in the design of organizations, and issues with organizational safety cultures.

**December 17, 2019**

## Report Approval and Revision History

NOTE: This document was approved at the December 17, 2019, NRB. This document was submitted to the NESC Director on January 22, 2020, for configuration control.

Approved: _____	<i>Original Signature on File</i>	1/23/20
	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Timothy S. Barth, NESC Integration Office, KSC	12/17/19
1.1	Minor editorial changes to multiple appendices	Timothy S. Barth, NESC Integration Office, KSC	2/28/20

# Table of Contents

## Technical Assessment Report

1.0	Notification and Authorization .....	7
2.0	Signature Page .....	8
3.0	Team List .....	9
3.1	Acknowledgments .....	9
4.0	Executive Summary .....	10
5.0	Assessment Plan .....	13
6.0	Precursor Activities.....	13
7.0	Background.....	14
7.1	Mishaps Included in the Recurring Cause Study .....	14
7.1.1	Apollo 1 Command Module Fire at Launch Complex (LC) 34.....	14
7.1.2	Soyuz 1 Main and Reserve Parachute Failures during Reentry.....	15
7.1.3	Skylab 1 Loss of Meteoroid Shield and Solar Array during Launch Ascent.....	16
7.1.4	STS-1 Oxygen Deficiency in Orbiter Aft Compartment at LC 39A .....	16
7.1.5	STS-1 SRB IOP .....	17
7.1.6	Scaled Composites Ground Explosion during Cold Flow N <sub>2</sub> O Test .....	18
7.1.7	Ares 1-X Steel Rod Ejections during Parachute Static Strip Test .....	18
7.1.8	SpaceShipTwo Premature Feather Flap Deployment during Test Flight .....	19
7.2	Methodology .....	20
8.0	Recurring Cause Study Results.....	21
8.1	Aggregate Analysis Results .....	21
8.2	Most Frequent Recurring Cause Types.....	23
8.2.1	Inadequate Technical Controls or Technical Risk Management Practices .....	23
8.2.2	Incomplete Procedures.....	24
8.2.3	System Design and Development Issues .....	25
8.2.4	Inadequate Inspection or Secondary Verification Requirements.....	26
8.2.5	Inadequate Organizational Learning Systems.....	28
8.2.6	Inadequate Schedule Controls.....	29
8.2.7	Inadequate Task Analysis and Design Processes.....	30
8.2.8	Organizational Design Issues.....	31
8.2.9	Organizational Safety Culture Issues.....	32
9.0	Confidence Building and Exploratory Analysis Activities.....	33
9.1	Comparisons to Historical Ground Operations Safety Reports .....	33
9.2	Comparison to ASAP Recommendations Analysis .....	36
9.3	Comparison to Mishap Recurring Causes during Late Space Shuttle Operations.....	38
9.4	Human Spaceflight Experts Review .....	40
10.0	Using the Mishap Recurring Cause Study Results .....	41
10.1	Developing Effective Mishap Risk Reduction Strategies.....	41
10.2	Human Spaceflight Knowledge Sharing Forum .....	43
10.3	NESC and NSC Activities .....	44
11.0	Findings, Observations, and Recommendations .....	44
11.1	Findings .....	44
11.2	Observations .....	46
11.3	Recommendations.....	46

12.0	Acronyms and Nomenclature List .....	46
13.0	References.....	48
Appendix A.	Taxonomy of Causes/Factors in Mishaps, Close Calls, Anomalies, and other Adverse Events .....	51
Appendix B.	Apollo 1 Mishap Analysis.....	58
Appendix C.	Soyuz 1 Mishap Analysis.....	73
Appendix D.	Skylab 1 Mishap Analysis.....	85
Appendix E.	STS-1 Oxygen Deficiency Mishap Analysis .....	94
Appendix F.	STS-1 SRB IOP Close Call Analysis.....	98
Appendix G.	Scaled Composites Mishap Analysis .....	101
Appendix H.	Ares 1-X Mishap Analysis .....	109
Appendix I.	SpaceShipTwo Mishap Analysis.....	122
Appendix J.	Aggregate Data Analysis.....	139
Appendix K.	Examples of ASAP Recommendations for Human Spaceflight Programs .....	179
Appendix L.	OCE Knowledge Sharing Forum Presentation.....	190
Appendix M.	Shuttle Processing Mishap Recurring Cause Study during Late Operations Phase .....	202
Appendix N.	Examples of NESC Assessments that Address Mishap Recurring Causes.....	234

### **List of Figures**

Figure 7.1-1.	Apollo 1 Command Module Fire at LC 34 .....	15
Figure 7.1-2.	Soyuz 1 at the Launch Pad and Descent Module Debris .....	15
Figure 7.1-3.	Skylab 1 Damaged Meteoroid Shield and Solar Array Systems.....	16
Figure 7.1-4.	STS-1 Stack at LC 39A and Orbiter Aft Access Opening .....	17
Figure 7.1-5.	STS-1 Launch and Sketch of SRB IOP Wave .....	17
Figure 7.1-6.	Steel N <sub>2</sub> O Storage Tank and Explosion Site .....	18
Figure 7.1-7.	Parachute Riser Strip Test Setup.....	19
Figure 7.1-8.	SpaceShipTwo Flight Configurations .....	19
Figure 8.1-1.	Dual Role Model.....	22
Figure 8.1-2.	Pareto Analysis of Recurring Cause Types.....	22
Figure 8.2-1.	Breakdown of “Inadequate Technical Controls or Technical Risk Management Practices” .....	23
Figure 8.2-2.	Breakdown of “Incomplete Procedure Issues” .....	24
Figure 8.2-3.	Breakdown of “System Design and Development Issues” .....	26
Figure 8.2-4.	Breakdown of “Inadequate Inspection or Secondary Verification Requirements” .....	27
Figure 8.2-5.	Breakdown of “Inadequate Organizational Learning Systems”.....	28
Figure 8.2-6.	Breakdown of “Inadequate Schedule Controls”.....	29
Figure 8.2-7.	Breakdown of “Inadequate Task Analysis and Design Processes” .....	30
Figure 8.2-8.	Breakdown of “Organizational Design Issues”.....	31
Figure 9.1-1.	Distribution of Mishap Causes during Apollo Operations.....	34
Figure 9.2-1.	Comparison of Most Frequent Mishap Recurring Cause Types to ASAP Recommendation Types.....	37

Figure 9.3-1. Comparison of Early Human Spaceflight and Late SSP Operations Mishap Recurring Cause Studies .....	39
Figure A-1. Dual Role Taxonomy .....	51
Figure A-2. Methodology for Single Event Analysis .....	52
Figure B-1. Apollo 1 Mishap Influence Chain Map.....	60
Figure C-1. Soyuz 1 Mishap Incident Influence Chain Map.....	75
Figure D-1. Skylab 1 Mishap Incident Influence Chain Map.....	87
Figure E-1. STS-1 Oxygen Deficiency Mishap Influence Chain Map.....	97
Figure F-1. STS-1 SRB IOP Close Call Influence Chain Map .....	100
Figure G-1. Scaled Composites Mishap Influence Chain Map .....	102
Figure H-1. Ares 1-X Mishap Influence Chain Map .....	112
Figure I-1. SpaceShipTwo Mishap Influence Chain Map.....	127

### List of Tables

Table 8.1-1. Number of Causes per Incident.....	21
Table 9.4-1. Examples of Undocumented Investigations of Human Spaceflight Adverse Events or Significant Anomalies .....	40
Table 10.1-1. Inadequate Schedule Controls Influence Chain Analysis .....	42
Table 10.1-2. Organizational Safety Culture Issue Influence Chain Analysis .....	43
Table A-1. Detailed Dual Role Taxonomy Categories.....	53
Table B-1. Apollo 1 Mishap Influence Chain Summary.....	58
Table C-1. Soyuz 1 Mishap Influence Chain Summary.....	73
Table D-1. Skylab 1 Mishap Influence Chain Summary.....	85
Table E-1. STS-1 Oxygen Deficiency Mishap Influence Chain Summary .....	94
Table F-1. STS-1 SRB IOP Close Call Influence Chain Summary.....	98
Table G-1. Scaled Composites Mishap Influence Chain Summary .....	101
Table H-1. Ares 1-X Mishap Influence Chain Summary .....	109
Table I-1. SpaceShipTwo Mishap Influence Chain Summary .....	122
Table J-1. Number of Causes for All Categories .....	139
Table J-2. “Inadequate Technical Controls/Technical Risk Management” Summary Table.....	141
Table J-3. “Inadequate Technical Controls/Technical Risk Management” Influence Chain Analysis .....	147
Table J-4. “Incomplete Procedures” Summary Table.....	148
Table J-5. “Incomplete Procedures” Influence Chain Analysis .....	152
Table J-6. “Inadequate Inspection/Secondary Verification Requirements” Summary Table .....	153
Table J-7. “Inadequate Inspection/Secondary Verification Requirements” Influence Chain Analysis .....	155
Table J-8. “Inadequate Schedule Controls” Summary Table.....	156
Table J-9. “Inadequate Schedule Controls” Influence Chain Analysis.....	158
Table J-10. “Inadequate Organizational Learning Systems” Summary Table.....	159
Table J-11. “Inadequate Organizational Learning Systems” Influence Chain Analysis.....	162
Table J-12. “System Design and Development Issues” Summary Table.....	163
Table J-13. “System Design and Development Issues” Influence Chain Analysis.....	169
Table J-14. “Inadequate Task Analysis and Design Processes” Summary Table.....	170

Table J-15.	“Inadequate Task Analysis and Design Processes” Influence Chain Analysis.....	172
Table J-16.	“Organizational Design Issues” Summary Table.....	173
Table J-17.	“Organizational Design Issues” Influence Chain Analysis.....	175
Table J-18.	“Organizational Safety Culture Issues” Summary Table.....	176
Table J-19.	“Organizational Safety Culture Issues” Influence Chain Analysis.....	178
Table K-1.	ASAP Recommendations.....	179

# Technical Study Report

## 1.0 Notification and Authorization

The goal of this study was to analyze recurring cause trends or patterns from human spaceflight mishaps that occurred during flight tests and early operations. The recurring issues identified during the study have been communicated to current human spaceflight programs to inform and stimulate proactive efforts to reduce the likelihood and/or severity of mishaps during ground and flight operations. The key stakeholders are current and future NASA human spaceflight programs, including the Artemis Program (consisting of the Multi-Purpose Crew Vehicle (MPCV), Space Launch System (SLS), Exploration Ground Systems (EGS), Human Landing System (HLS), and Gateway/Lunar Orbital Platform) and the Commercial Crew Program (CCP). Commercial suborbital and orbital spacecraft and launch vehicle operators are additional stakeholders, and two mishaps from commercial space activities were included in the study.

The study was performed by the NASA Engineering and Safety Center (NESC) and the NASA Safety Center (NSC). Independent studies are within the scopes of both organizations, as reflected in their respective organizational documents. “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” [ref. 20]. “The NSC will conduct...special studies...at the request of Centers, programs, and projects to provide trends within Centers, programs, projects, or facility activities” [ref. 21].

The NSC has developed and implemented a Safety and Mission Assurance (S&MA) Technical Excellence Program. Similarly, a founding principle of the NESC is “safety through engineering excellence.” Safety encompasses the safety of flight and ground crews, the broader NASA workforce, high-value flight and ground systems, and the public. Together, the common goal of the NESC and the NSC is to improve safety through engineering and technical excellence.

## 2.0 Signature Page

Submitted by:

*Team Signature Page on File – 1/29/2020*

---

Dr. Timothy S. Barth                      Date

Significant Contributors:

---

Mr. Steve K. Lilley                      Date

---

Dr. Barbara G. Kanki                      Date

---

Mrs. Donna M. Blankmann-Alexander      Date

---

Mr. D. Blake Parker                      Date

Signatories declare the study results compiled in the report are factually based on data extracted from program/project documents, contractor reports, independent investigation reports, and open literature.



### 3.0 Team List

Name	Discipline	Organization
<b>Core Team</b>		
Tim Barth	NESC Lead/Systems Engineering	LaRC
Steve Lilley	NSC Co-Lead/SMA	GRC
Donna Blankmann-Alexander	Human Factors	KSC/Abacus Technology Corp.
Barbara Kanki	Human Factors	ARC
Blake Parker	SMA	KSC/ASRC Aerospace
<b>Business Management</b>		
Loutricia Johnson	Program Analyst	LaRC/MTSO
<b>Support</b>		
Melissa Strickland	Project Coordinator	LaRC/AMA
Linda Burgess	Planning and Control Analyst	LaRC/AMA
Jonay Campbell	Technical Writer	LaRC/SGT
Guy Kemmerly	Technical Writer	LaRC/AMA

### 3.1 Acknowledgments

The study team thanks the following human spaceflight experts for their contributions during an initial review of the study results: Bo Bejmuk, Wayne Hale, Gary Johnson, Mike Blythe, Nancy Currie-Gregg, and T. K. Mattingly from Johnson Space Center (JSC); Jim Blair and Bob Ryan from Marshall Space Flight Center (MSFC), and Jay Honeycutt, Bob Lang, Charlie Mars, Gerry Schumann, Bob Sieck, Tip Talone, and John Tribe from Kennedy Space Center (KSC). These personnel (except Mike Blythe) are NASA or contractor retirees associated with the identified Centers but are not currently employed by a specific program at those Centers.

Special thanks to Jenny Twining, a research assistant at NASA Ames Research Center who supported the study by performing an independent analysis of the Aerospace Safety Advisory Panel (ASAP) recommendations.

The study team also thanks the peer reviewers for their contributions: Bob Beil, Tim Brady, Steve Gentz, Jon Holladay, Robert Johnson, Robert Moreland, Cynthia Null, Joe Olejniczak, Mike Watson, and Scott West.

## 4.0 Executive Summary

Engineer and author Henry Petroski wrote in his book, *To Engineer is Human*, “No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state of the art” [ref. 27]. It is important to thoroughly analyze and learn from human spaceflight’s historical mishaps to advance the state of the art in system safety and thereby “raise the bar” for flight and ground crew safety. Eight mishaps that occurred during testing and early operations (including inaugural missions) of the Apollo, Soyuz, Skylab, Space Shuttle, and Constellation (i.e., the Ares 1-X test flight) Programs as well as commercial suborbital systems were included in the study. Each program began with a tragedy or near-tragedy on the ground or during flight.

This study included a task to review and evaluate mishap study reports provided to previous human spaceflight programs. One of the reports was a Shuttle Processing Productivity and Error Prevention Report from 1981 [ref. 24], which contained the following:

“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 goal of this study was to identify those fundamental, systemic, or underlying problems that, if addressed within the broader context of the organizational support systems, would have a maximum impact on reducing the frequency and/or severity of incidents, especially those in the integrated test flight and early operational phases. If human spaceflight programs have truly learned from past failures, the state of the art should have advanced to the point where tragedies need not occur at the beginning of every new program.

In this study, the number of mishap cause recurrences was an indicator of the relative significance and pervasiveness of the corresponding systemic safety issue. The nine most frequently recurring causes were analyzed in additional detail. These top nine recurring causes were:

- Inadequate technical controls or technical risk management practices (e.g., inadequate readiness reviews, technical issues or safety hazards not sufficiently analyzed with failure modes and effects analyses (FMEAs), process FMEAs, hazard reports, risk analyses, and similar methods; inadequate aggregation of incremental technical risks).
- Incomplete procedures (e.g., missing steps; situations or scenarios not adequately covered by written procedures).
- System design and development issues (e.g., testing, human-system integration, material selection, and modeling and simulation issues).
- Inadequate inspection or secondary verification requirements (e.g., missing or deficient requirements; requirements based on incorrect assumptions).

- Inadequate organizational learning systems (e.g., unlearned lessons within or outside human spaceflight organizations).
- Inadequate schedule controls (e.g., unrealistic schedule goals; lack of schedule coordination).
- Inadequate task analysis and design processes (e.g., missing or deficient task analyses; emergency/contingency procedure issues).
- Organizational design issues (fragmented organizations; organizations with unclear accountability for integration functions).
- Organizational safety culture issues (e.g., complacency and competing internal cultures).

Mishap investigation boards are tasked primarily with recommending clear, actionable, and feasible options to prevent the recurrence of specific incidents. The types of causes listed above are seldom identified as root causes, so they may be overlooked or inadequately addressed by actions resulting from an individual investigation board's findings and recommendations.

Systemic safety risk mitigation requires a broad systems perspective looking across different types of mishaps and close calls. Actions addressing systemic safety issues should be more proactive and preventive than reactive and corrective. The focus of efforts to address systemic issues is to make the organizational support systems and processes more robust and resilient to prevent many different types of mishaps. The closer spacecraft and launch vehicles operate to their design limits, potentially operating within design margins, the more robust the organizational systems and processes must be to compensate.

An unprecedented number of human spaceflight systems are rapidly approaching crewed test flights and operations, including two Commercial Crew Program (CCP) providers, three Artemis Programs (i.e., the Multi-Purpose Crew Vehicle (MPCV), Space Launch System (SLS), and Exploration Ground Systems (EGS) Programs), and at least two commercial suborbital space tourism operators. Two additional Artemis Programs (i.e., the Human Landing System (HLS) and the Gateway/Lunar Orbital Platform) are moving quickly forward. At least one commercial suborbital operator is planning to begin crewed operations with passengers in 2020.

Former NASA Chief Safety Officer Bryan O'Connor reminded personnel supporting the design, development, and/or operations of human spaceflight systems that "everybody is responsible for safety; no exceptions" [ref. 30]. Depending on their authority and capability, however, each person shoulders a different amount of accountability. The primary recommendation from the study team is for personnel supporting human spaceflight programs to internalize the mishap recurring cause study results, consider their personal degree of safety accountability, and determine whether additional mishap risk reduction actions are warranted. Personnel should have an opportunity before crewed flights begin to step back from their busy schedules and technical challenges and ask questions like "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 subsystems than can be extended to my subsystem?" Hopefully, the results from this study will provide the data and examples necessary to seed those discussions.

Rocket science and brain surgery are sometimes singled out as the most challenging and demanding of human feats because system complexity levels are extremely high and error margins are extremely low. Surgeon and author Atul Gawande wrote, “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” [ref. 28]. Human spaceflight is, by its very nature, a risky endeavor. The systems, processes, and decision-making will sometimes falter, and tragedies will occur. Although it is true that the only way to achieve a perfect safety record is to never fly, human spaceflight organizations should never cease aiming for perfection when it comes to crew safety.

## 5.0 Assessment Plan

The elements of the assessment plan were to:

- Perform single event analyses for the Apollo 1, Soyuz 1, Skylab 1, Space Transportation System (STS)-1, and Ares 1-X mishaps, and any additional mishaps that occurred during flight tests and early operations. Identify the causes as well as the relationships between the causes.
- Perform aggregate data analyses to identify the most frequently recurring cause types.
- Compare the most frequent recurring causes with the top issues documented in previous mishap studies, including but not limited to the KSC Apollo studies [refs. 22, 23], the Space Shuttle Productivity and Error Prevention Report [ref. 24], the Report of the Shuttle Processing Review Team [ref. 25], and the Shuttle Mishap Recurring Cause Study (see Appendix M).
- Analyze Aerospace Safety Advisory Panel (ASAP) recommendations for human spaceflight programs using the same taxonomy (see Appendix K).
- Provide examples from NESC assessments of actions taken to address the systemic issues identified in the recurring causes.

## 6.0 Precursor Activities

The human spaceflight mishap recurring cause study evolved from several previous NASA activities. In the early 1990s, a joint contractor and NASA Shuttle Processing Human Factors Team was chartered. This team developed a taxonomy of mishap causes and contributing factors [refs. 1, 2]. The SSP team collected and analyzed data on common or recurring types of causes for ground processing mishaps. From 1996 to 2007, a database of 1,254 causes in 335 mishaps was developed. In addition to supporting numerous risk mitigation efforts in SSP ground operations, the human factors database also provided useful information to support the design and development of new flight systems, ground systems, ground support equipment, procedures, and work sites. For example, the SLS and MPCV human-system integration requirement (HSIR) documents include requirements to improve ground crew interfaces with flight systems [refs. 3, 4]. The NASA Spaceflight Human-System Standard, Volume 2: Human Factors, Habitability, and Environmental Health, was updated to include a new section titled “Ground Assembly Design and Emergency Egress Operations” [ref. 5]. The processes and capabilities for ground system design teams were enhanced to include human factors engineering assessments, expertise, design visualizations, ergonomic evaluations with motion capture technologies, and a comprehensive checklist.

Development of an improved approach for evaluating systemic safety issues was motivated by the Space Shuttle *Columbia* disaster on February 1, 2003. The “influence chain mapping” methodology [ref. 18] incorporated many lessons learned from the Shuttle Processing Human Factors Team. The methodology was applied to ground processing mishaps after successful SSP return to flight. Recurring causes were evaluated, and 12 proactive mishap risk reduction initiatives were implemented to contribute to safe SSP fly-out for flight and ground crews (see Appendix M).

## **7.0 Background**

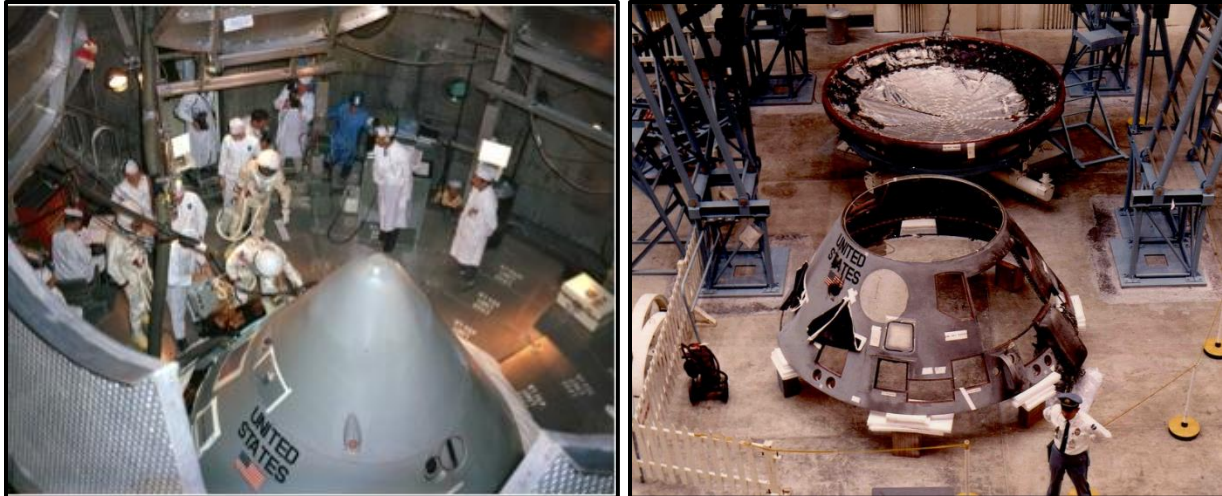
Major mishaps and significant close calls have marred the start of every human spaceflight program since three American astronauts were lost in the January 27, 1967, Apollo 1 fire. A Russian cosmonaut died when his spacecraft, Soyuz 1, plummeted to Earth after parachute deployment failures on April 23, 1967. A dangerous extravehicular activity (EVA) saved Skylab 1 after its meteoroid shield was damaged during launch ascent on May 14, 1973. NASA's SSP endured adversity on March 19, 1981, when three technicians were asphyxiated in the aft compartment while preparing STS-1 for launch. On April 12, 1981, a major flight failure was narrowly avoided due to underestimation of solid rocket booster (SRB) ignition over-pressurization (IOP) during the STS-1 launch. On July 26, 2007, three Scaled Composites employees perished when the cold flow nitrous oxide (N<sub>2</sub>O) test rig they were operating exploded. During preparations for the Ares 1-X test flight in the Parachute Refurbishment Facility (PRF) at KSC, a ground crew fatality was missed by inches on September 5, 2007. On October 31, 2014, the SpaceShipTwo copilot was killed and the pilot was injured during a test flight.

### **7.1 Mishaps Included in the Recurring Cause Study**

The goal of this study was to identify recurring causes in mishaps that have occurred during the flight test and early operational phases of human spaceflight programs, and to make design and operational recommendations, as appropriate, for the CCP, the Artemis Programs (i.e., SLS, MPCV, HLS, Gateway/Lunar Orbital Platform, and EGS), and commercial suborbital and orbital operators to proactively reduce the risks of serious mishaps before their initial crewed flights. The adverse events include four mishaps during ground operations and four mishaps during flight operations. Several human spaceflight experts interviewed by the study team mentioned additional mishaps, close calls, anomalies, and significant technical issues that occurred during earlier programs. However, formal investigation reports were available for only the eight events described in the following sections. Each undocumented investigation represents a missed opportunity for organizational learning. Additional details on each documented event are included in Appendices B through I.

#### **7.1.1 Apollo 1 Command Module Fire at Launch Complex (LC) 34**

The fire that led to the loss of three astronauts on January 27, 1967, was probably caused by an electrical arc from a Teflon-coated wire near the floor of the capsule [ref. 6]. The delicate wire was powered by the main power bus. Post-mishap interviews revealed a notable amount of traffic capable of damaging wiring insulation. The choice of the insulating material (while it was a superior heat insulator) made it unusually susceptible to damage from friction. Since a decision was made to conduct Apollo operations in a 100% oxygen environment pressurized to 16.7 psi, as had been done in the Mercury and Gemini capsules, previous successes in those programs served to effectively conceal the risks of combustibles in the cabin. Images of the Apollo 1 command module before and after the tragedy are shown in Figure 7.1-1.



***Figure 7.1-1. Apollo 1 Command Module Fire at LC 34***

The presence of combustibles in the oxygen-rich environment put this ground test at a high likelihood of a fire if an ignition source was present. The crew hatch was not designed for rapid emergency egress. The ground crew needed almost 5 minutes to open the hatch after the cockpit fire. The Apollo hatch was a new design following an incident with the Mercury/Gemini hatch design. Eliminating previous hazards introduced new hazards [refs. 6, 19].

### **7.1.2 Soyuz 1 Main and Reserve Parachute Failures during Reentry**

Early in the “space race,” following several American successes, Russia was trying to regain the lead it had following Yuri Gagarin’s historic first human flight to orbit the Earth. To mark the 50<sup>th</sup> anniversary of the Bolshevik Revolution, Russia was eager to launch the new Soyuz 1 spacecraft. Despite more than 100 critical problems identified by engineers, a series of failed hardware tests, and three non-crewed flight failures, the crewed vehicle was launched.

Figure 7.1-2 contains images of the Soyuz 1 mission on the launch pad and the descent module debris at the landing site.



***Figure 7.1-2. Soyuz 1 at the Launch Pad (left) and Descent Module Debris (right)***

On April 23, 1967, after overcoming several problems in orbit, the main and reserve parachutes failed on reentry, causing the vehicle to crash and killing the single cosmonaut on board. The parachute container had been damaged during a thermal protection system (TPS) baking process. Inspectors found the same problem with the Soyuz 2 parachute container. If the Soyuz 2 crew



had been launched to attempt a rescue of the Soyuz 1 crew, as was contemplated, both crews would very likely have been lost [refs. 7, 8].

### **7.1.3 Skylab 1 Loss of Meteoroid Shield and Solar Array during Launch Ascent**

Sixty-three seconds into deployment, there was a complete loss of the Skylab 1 meteoroid shield (MS) around the orbital workshop (OWS). A shield designed to protect the lab from micrometeoroids was damaged when it came loose during launch on May 14, 1973. This resulted in the loss of one of the two solar array systems (SAS-2) on the workshop and a failure of the interstage adapter to separate from the S-II stage of the Saturn V launch vehicle. Figure 7.1-3 contains images of the Skylab 1 MS damage, the primary solar shield, and the fully deployed SAS-1 panel after it was released during an EVA.



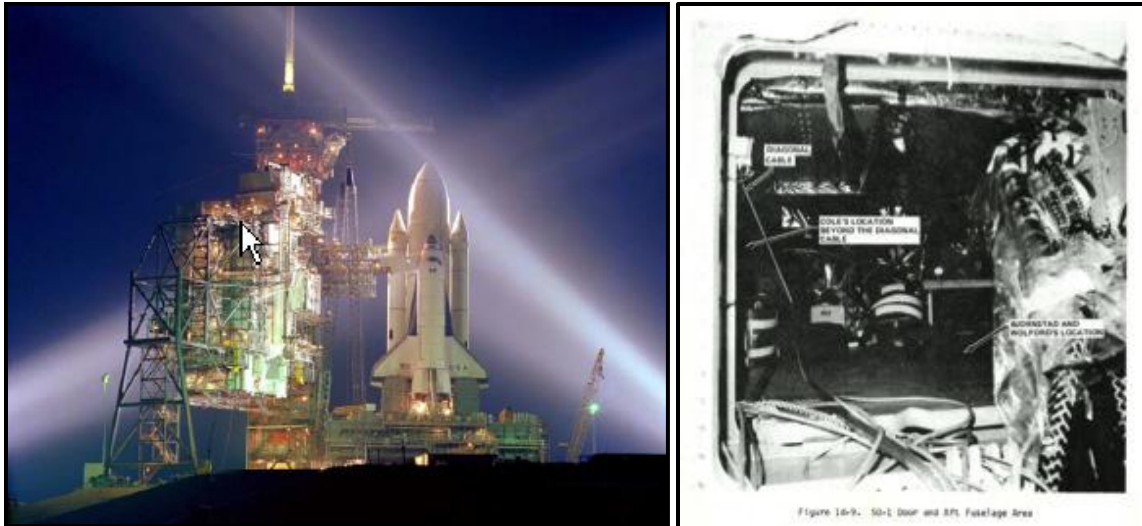
***Figure 7.1-3. Skylab 1 Damaged Meteoroid Shield (left) and Solar Array Systems (right)***

The meteoroid shield was designed to be stowed in an auxiliary tunnel that was subject to the supersonic freestream during ascent. The shield material and stowage method were new, and launch effects were not understood. Skylab 1 was ultimately saved during a successful repair mission (SL-2) [ref. 9].

### **7.1.4 STS-1 Oxygen Deficiency in Orbiter Aft Compartment at LC 39A**

During a simulated countdown involving the flight crew at the launch pad on March 19, 1981, many tasks unrelated to the simulation were being worked around the orbiter. All the tasks were managed from the firing room, but deviations to the standard procedures had to be made to accommodate the concurrent activities. In fact, more than 500 deviations were authorized. One activity was a nitrogen purge in the orbiter aft section to perform a leak check. The activity was not labeled hazardous on the schedule, so there was minimal review by safety personnel. Figure 7.1-4 contains images of the STS-1 stack at LC 39A and the opening for the orbiter aft compartment access.



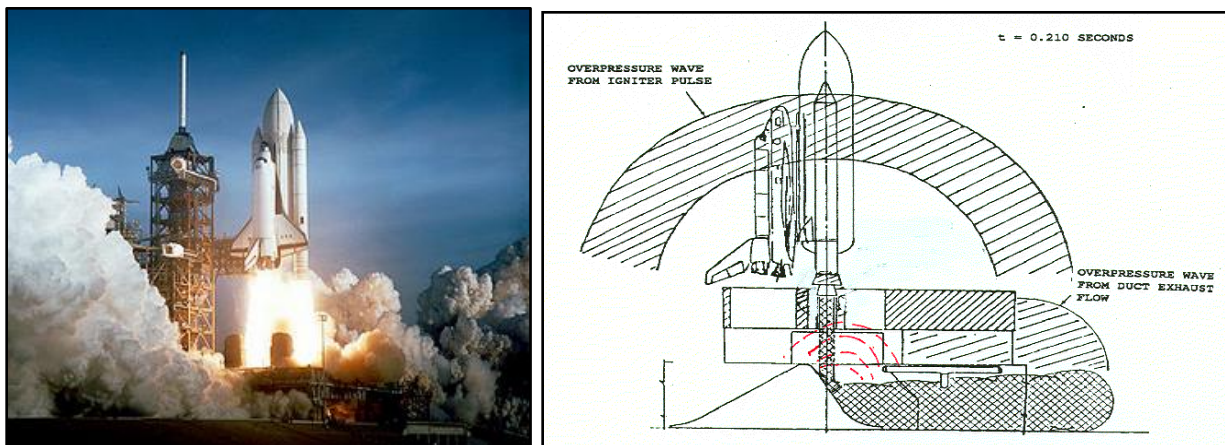


**Figure 7.1-4. STS-1 Stack at LC 39A (left) and Orbiter Aft Access Opening (right)**

When the test conductors in the firing room announced “all clear” at the end of the countdown test, technicians were permitted into the aft section of the orbiter, which still contained a deadly nitrogen atmosphere from the purge. Three technicians died and two technicians were seriously injured [ref. 10].

### 7.1.5 STS-1 SRB IOP

During the launch of STS-1 on April 12, 1981, a significantly low estimate of the pressure spike generated by the reflection of the SRB IOP wave resulted in nearly catastrophic damage to the orbiter. The SRB IOP was anticipated, but prelaunch modeling was conducted using Tomahawk missile motor data to validate the models, and the SRBs have much higher ignition pressures. Figure 7.1-5 contains an image of the STS-1 launch and a sketch of the IOP wave.



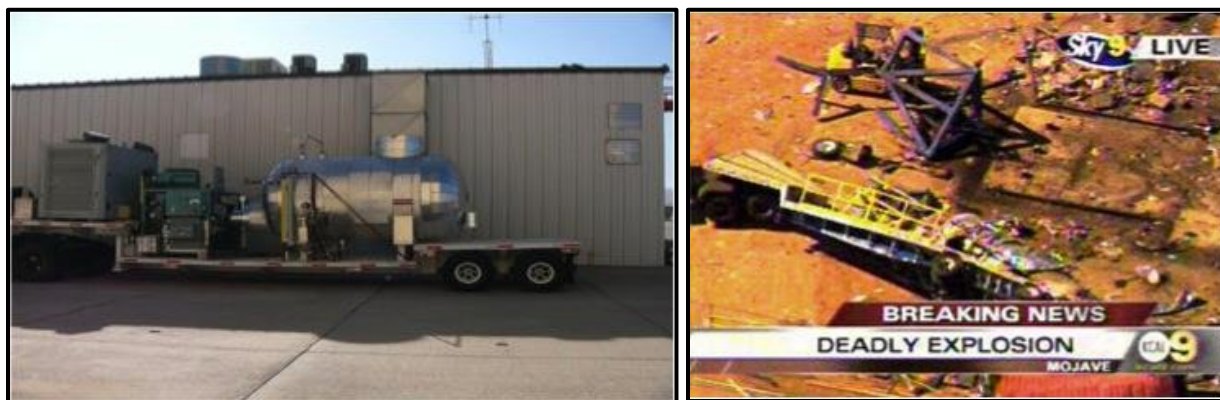
**Figure 7.1-5. STS-1 Launch (left) and Sketch of SRB IOP Wave (right)**

The powerful pressure wave buckled a strut that supported an oxidizer tank for the reaction control system (RCS) and overextended the orbiter body flap used to control pitch attitude during reentry. Rupture of the oxidizer tank would have destroyed the vehicle and killed the flight crew. Although STS-1 was a successful test flight, the LC 39A sound suppression system had to be redesigned for STS-2. STS-1 Commander John Young later said that if the crew had known

about the damaged body flap, they would have flown the orbiter to a safe altitude and ejected [refs. 11-14].

### **7.1.6 Scaled Composites Ground Explosion during Cold Flow N<sub>2</sub>O Test**

Ground operations for SpaceShipOne included testing a steel tank carrying approximately 10,000 lb of N<sub>2</sub>O (see Figure 7.1-6). While testing in the desert at approximately 105 °F on July 26, 2007, the N<sub>2</sub>O tank exploded, killing three ground crew members and injuring three others. The ground crew was reportedly unaware that N<sub>2</sub>O above 96.8 °F becomes a supercritical fluid and is much easier to ignite than in its gaseous state. Furthermore, the N<sub>2</sub>O was being transferred to a composite tank. N<sub>2</sub>O decomposes most composite materials and produces a vapor that is also explosive [ref. 29].



*Figure 7.1-6. Steel N<sub>2</sub>O Storage Tank (left) and Explosion Site (right)*

### **7.1.7 Ares 1-X Steel Rod Ejections during Parachute Static Strip Test**

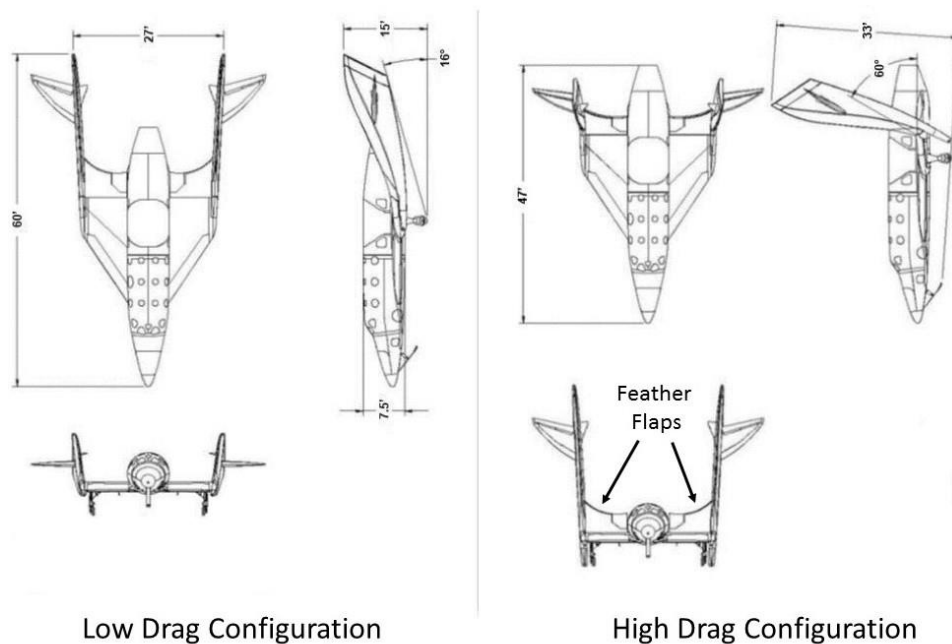
SRB recovery parachute risers were being tested on September 5, 2007, in a refurbishment facility just prior to delivery. There was a rush to complete the testing so the parachute system could be installed on the Ares 1-X vehicle and meet the planned launch schedule. It was the first time this type of test had been performed with this specific riser design, so a new test strategy and procedure had to be developed. The test procedure was a tailored version of a standard SSP test procedure. The load on the risers was generated by a winch and transferred to the riser through steel rods (see Figure 7.1-7). At some point during the test, steel rods were ejected from the risers, and one rod struck the operator at high speed across the legs. If the rod had struck the operator at a different angle or on a different part of his body, the results could have been lethal [ref. 15].



**Figure 7.1-7. Parachute Riser Strip Test Setup**

### 7.1.8 SpaceShipTwo Premature Feather Flap Deployment during Test Flight

To reduce speed in preparation for a safe landing, large flaps on the trailing edges of the wings were deployed to increase drag. These flaps were called “feather flaps” and deployed upward with the tail booms, as shown in Figure 7.1-8. During boost phase, as the spacecraft passed through transonic speeds, the aerodynamic loads pushing the feather flaps and tail booms upward were more powerful than the actuators could control, so the assembly was held in the low-drag position with locking pins. Once the spacecraft reached Mach 1.4, the locking mechanism could be safely disengaged. A test flight was conducted on October 31, 2014. During a workload-intensive period for the flight crew at the beginning of the boost phase with a speed approaching Mach 0.8, the copilot unlocked the feather flaps prematurely, and the tail assembly was destroyed. As a result, the spacecraft was lost and the copilot was killed. The pilot was injured but survived [ref. 16].



**Figure 7.1-8. SpaceShipTwo Flight Configurations [ref. 16]**

## 7.2 Methodology

The methodology used in this study involved performing a detailed analysis on selected mishaps from past human spaceflight programs. This event-specific analysis was typically based on the data collected in the formal mishap investigation board report and other related documentation. Except in recent mishaps, the study team was unable to follow up the board investigations with questions to collect additional data or obtain clarifications. Some investigation reports were more complete than other reports, so it was possible (even likely) that additional causes were present but not identified by the investigation board. Several additional technical issues and anomalies during early operations were suggested for inclusion in the study, but a formal investigation report was not found for those events (see Table 9.4-1 for examples).

The event-specific analysis involved classifying the causes and capturing their inter-relationships. For this study, a “cause” was defined as a factor with sufficient evidence to conclude that it contributed to the occurrence of the adverse event. This definition includes factors traditionally classified as contributing, proximate, probable, or root causes. Since the study team’s goal was to identify systemic safety issues, these distinctions were unimportant. Using this methodology, the “system” that failed during an event included the broader organizational system. Defining the scope and boundaries of the organizational system is an important step in applying the methodology. The broader system meets the criteria for a “complex” system. Systems can possess different types of complexity. Examples include *dynamic complexity* (changing over time), *interactive complexity* (modes of interaction between components can occur in nonlinear, nonintuitive ways), and *decompositional complexity* (structural decomposition of a system differs from functional decomposition).

In this study, a “cause” represents a cause category, type, or grouping. The specific causes were different for each event. A “recurring cause” was defined as a cause category that occurred in more than one mishap. To identify trends and make direct comparisons between different mishaps, the study team used the “dual role” taxonomy described in Appendix A (see Figure A-1 and Table A-1) to classify or categorize causes so similar causes could be identified across several events [ref. 18]. The analyst draws conclusions about the data during the cause categorization process. The analyst must determine the “best fit” category based on the evidence and overall context. The cause also needs to meet a minimum threshold level for the amount of objective data that supports the cause determination. These determinations were reviewed by the entire study team to ensure consistency.

The dual role taxonomy was based on a human factors taxonomy developed and used in SSP ground processing to support over 335 investigations during the last 15 years of the program. It included elements of cause taxonomies from the Department of Defense (DoD) and the aerospace and aviation industries. In addition, the taxonomy is based on the “Swiss cheese” model of active and latent barriers, controls, and defenses [ref. 17]. This enables the “influence” relationships between various causes to be captured and helps analysts identify preventive actions designed to reduce the likelihood and/or consequences of the systemic safety issues. A process flowchart depicting the steps in the influence chain mapping approach is also included in Appendix A (see Figure A-2).

The influence chain mapping methodology was specifically designed to step back from individual mishaps to evaluate causal trends and patterns to identify the most significant system-level safety issues. The influence chain approach complements root cause analysis methods,



helps identify all the causes of a mishap, explicitly models the influences between organizational systems and individual behaviors of frontline workers, and emphasizes *absent* barriers/controls in addition to *failed* barriers/controls. Completed influence chain maps for the eight mishaps in this recurring cause study are provided in Appendices B through I, and additional details on the methodology and examples are provided in reference 18.

## 8.0 Recurring Cause Study Results

To analyze recurrence, a taxonomy was used to classify all causes for each mishap. The frequency of occurrence of each cause type and how the causes tend to connect or happen together (their influence interrelationships) were evaluated. Overall trends in the aggregate data set were explored. For the most frequently recurring cause types, more detailed trends within the category were identified.

### 8.1 Aggregate Analysis Results

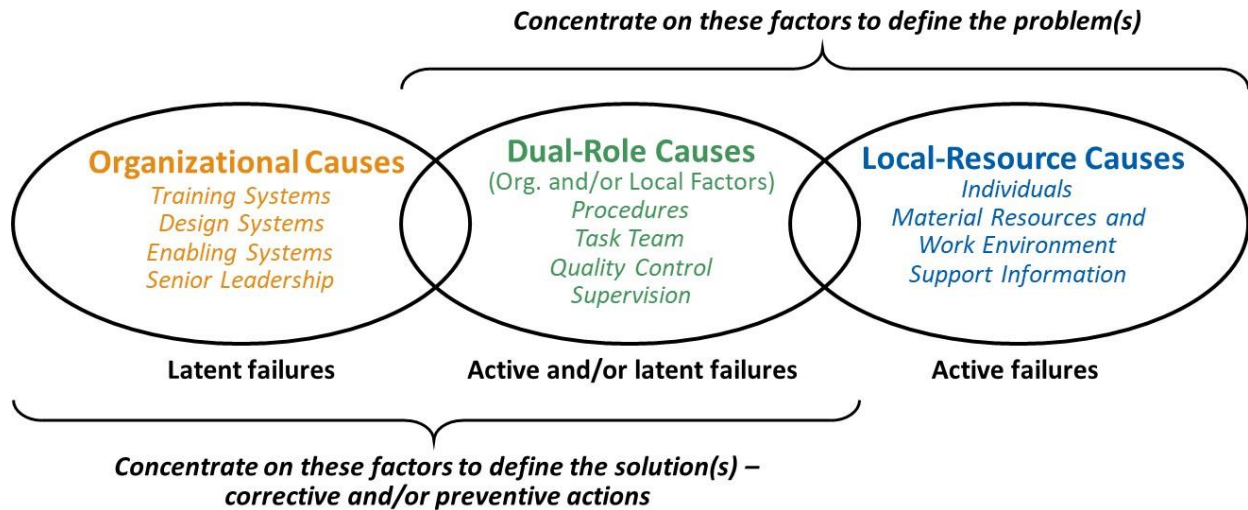
**F-1.** For the eight mishaps included in the study, 180 causes were identified. The average number of causes per incident was 22.5 (see Table 8.1-1). The number of causes per incident ranged from a minimum of eight causes for the STS-1 SRB IOP event to a maximum of 34 causes for the Apollo 1 fire.

*Table 8.1-1. Number of Causes per Incident*

Incident	Ground or Flight Ops	# of Causes
Apollo 1	Ground	34
Soyuz 1	Flight	16
Skylab 1	Flight	16
STS-1 Oxygen Deficiency	Ground	27
STS-1 SRB IOP	Flight	8
Scaled Composites	Ground	18
Ares 1-X	Ground	31
SpaceShipTwo	Flight	30
<b>Total</b>		<b>180</b>

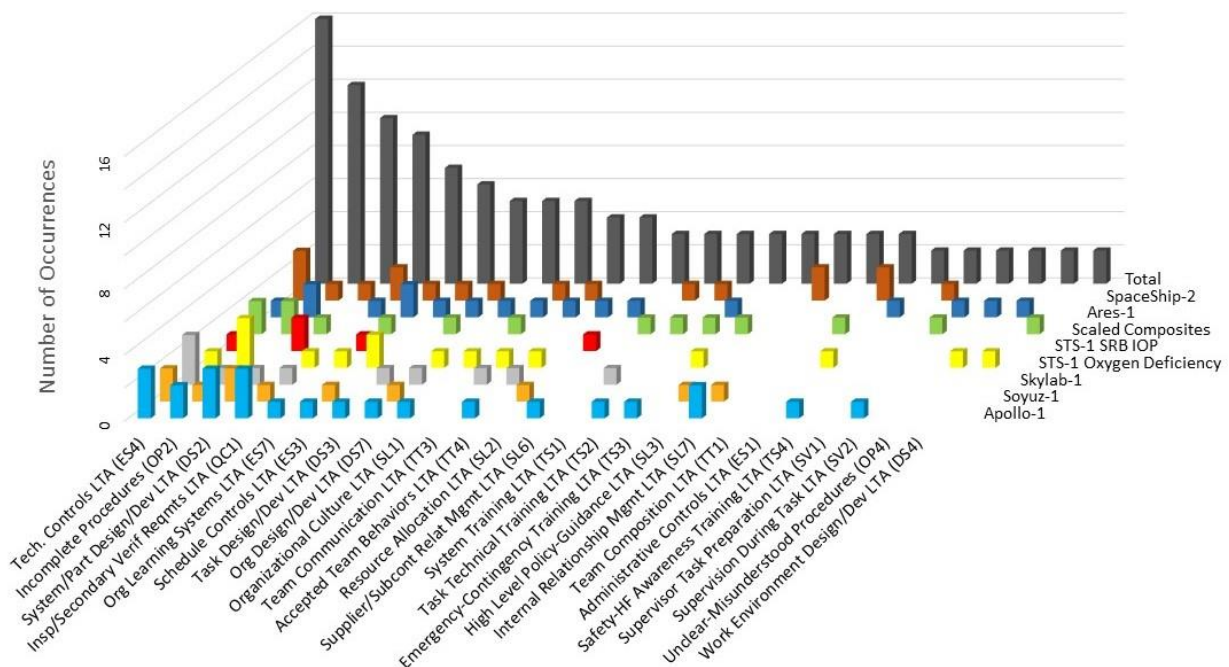
The investigation reports for the STS-1 SRB IOP and the Scaled Composites ground explosion were not as comprehensive as the other reports. The STS-1 SRB IOP investigation was an engineering report that did not evaluate organizational issues. The Scaled Composites report was a publicly available report written by the Occupational Safety and Health Administration (OSHA), which focused on compliance issues. The distribution of the 180 causes across the 66 categories in the taxonomy is included in Appendix J.

The dual role model that forms the basis of the taxonomy is depicted in Figure 8.1-1. The “local resource” causes were associated with resources necessary to perform the task at the time and location of the task. The “organizational system” causes were associated with the various systems in place to help ensure the tasks were completed safely, effectively, and efficiently. “Dual role” causes have characteristics of organizational system and local resource causes [ref. 18].



**Figure 8.1-1. Dual Role Model [ref. 18]**

During the analysis, all types of causes were considered. Local resource causes and dual role causes helped identify what went wrong during the mishap. Analysts concentrated on organizational system causes and dual role causes to develop recommendations for effective corrective and preventive actions. Since the study team’s goal was to identify recurring causes that represent systemic safety issues, the local resource cause types (i.e., individual factors, material resources and work environment, and support information) were not included in a Pareto analysis (see Figure 8.1-2). A total of 117 causes were considered actionable for purposes of addressing systemic or underlying safety issues.



**Figure 8.1-2. Pareto Analysis of Recurring Cause Types**

## 8.2 Most Frequent Recurring Cause Types

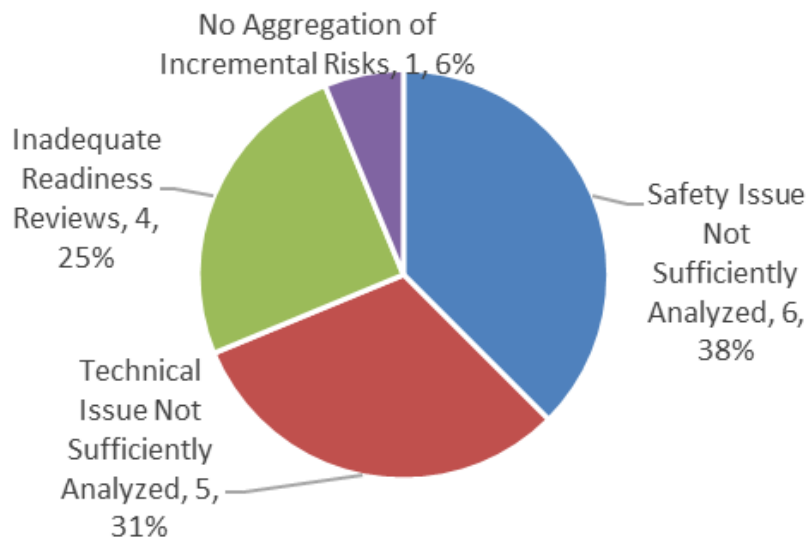
Figure 8.1-2 shows the recurring organizational system and dual role causes identified in the study, as discussed in Section 8.1. The recurring causes ranged from a maximum of 16 occurrences in all eight of the mishaps (“technical controls and technical risk management practices less than adequate (LTA)”) to a minimum of two occurrences in two of the mishaps for six cause types (“administrative controls LTA,” “safety-human factors awareness training LTA,” “supervisor task preparation LTA,” “supervision during task LTA,” “unclear/misunderstood procedures,” and “work environment design/development LTA”).

**F-2.** 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 117 (65%) organizational and dual role recurring causes are included in the nine most frequently recurring cause types.

Additional analyses of the top nine recurring causes are discussed in the following sections. Appendix J contains summary tables listing all occurrences of each top nine recurring type.

### 8.2.1 Inadequate Technical Controls or Technical Risk Management Practices

**F-3.** Sixteen occurrences of “inadequate technical controls or technical risk management practices” contributed to all eight (100%) of the incidents studied. Six of the 16 occurrences (37.5%) were inadequate safety reviews/analyses (e.g., inadequate hazard analyses or system safety analyses). Five of the 16 (31.3%) were due to technical issues not being sufficiently analyzed (e.g., inadequate failure modes and effects analyses (FMEAs), process-FMEAs, and quantitative risk assessments). Four of the 16 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 (see Figure 8.2-1).



**Figure 8.2-1. Breakdown of “Inadequate Technical Controls or Technical Risk Management Practices”**

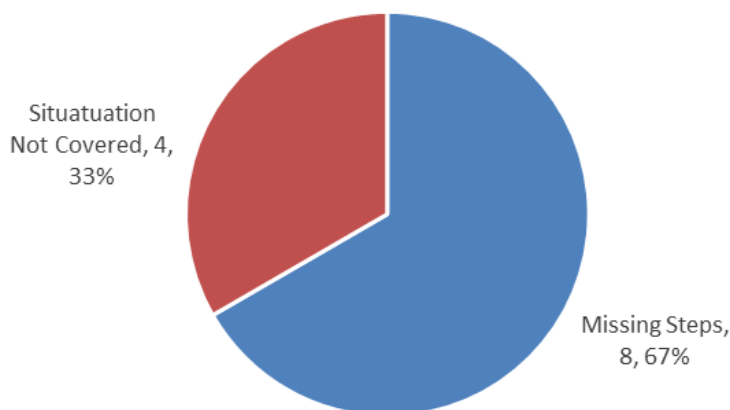
Examples of these technical controls and risk management issues are:

- SpaceShipTwo. The system safety analysis (SSA) process was inadequate because it 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 1-X. Even though the parachute riser lines were approximately four times longer than the riser lines on the SSP orbiter drag parachute, 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 1-X 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].

Table J-2 in Appendix J contains a complete listing of the technical controls/technical risk management causes identified in the study.

### 8.2.2 Incomplete Procedures

**F-4.** 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) (see Figure 8.2-2).



***Figure 8.2-2. Breakdown of “Incomplete Procedure Issues”***



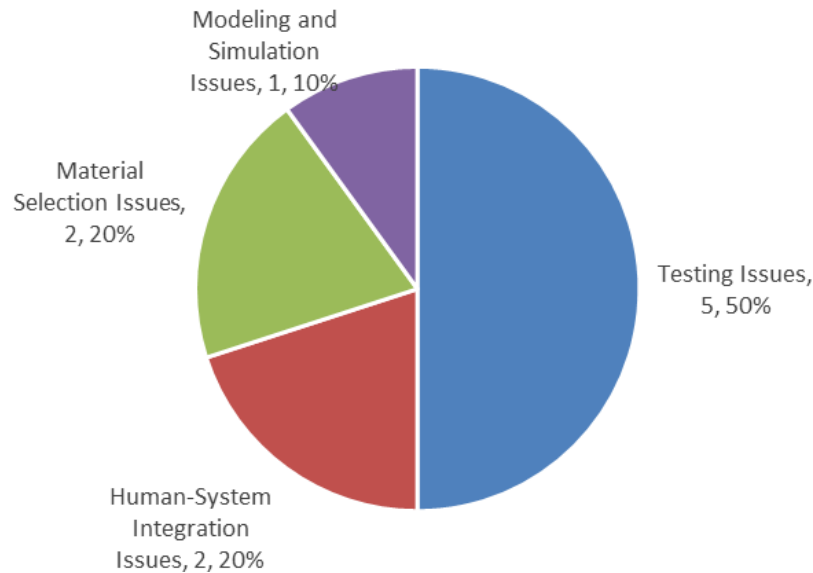
Examples of how incomplete procedures impacted the incidents studied are:

- Apollo 1. Adequate safety precautions were not established or observed for this test. Contingency procedures and preparations to enable escape or rescue of the crew from a command module fire were not made [ref. 6].
- STS-1 Oxygen Deficiency. Atmosphere checks and air purge verifications were not in the safety procedure [ref. 10].
- Scaled Composites. Material Safety Data Sheet (MSDS) documents, in their most basic form from N<sub>2</sub>O suppliers, caution against pressure shock. The work instructions contained no warnings about the dangers of pressure shock. There was no designated hazard control area. Workers were allowed to stand behind a chain link fence in proximity to the N<sub>2</sub>O tank during the test [ref. 29].
- 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 [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” [ref. 16].

Table J-4 in Appendix J contains a complete listing of the incomplete procedure causes identified in the study.

### 8.2.3 System Design and Development Issues

**F-5.** 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 (see Figure 8.2-3).



**Figure 8.2-3. Breakdown of “System Design and Development Issues”**

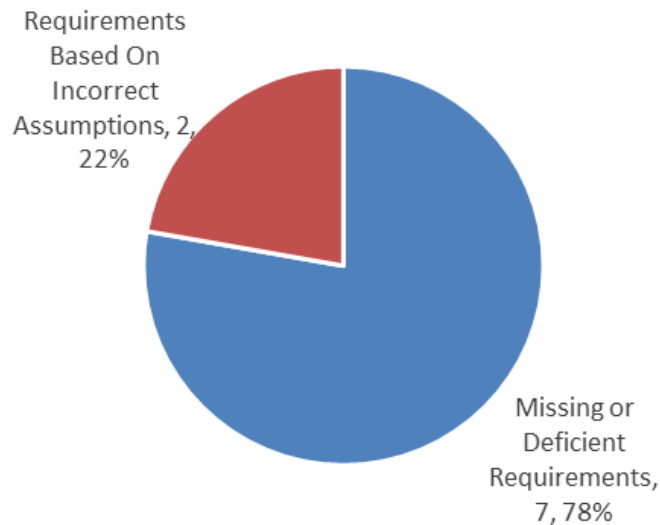
Examples of how “system design and development issues” impacted system safety are:

- 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 by contact with adjacent hardware during training activities. Electrical wiring was exposed, which contributed to command module technical problems during tests [ref. 6].
- 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” [ref. 7].
- Scaled Composites. The N<sub>2</sub>O tank design included several materials that were incompatible with the propellant, and the tank lacked a pressure relief protection to prevent rapid over-pressurization [ref. 29].
- STS-1 SRB IOP. 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 [ref. 11].

Table J-6 in Appendix J contains a complete listing of the system design and development causes identified in the study.

#### **8.2.4 Inadequate Inspection or Secondary Verification Requirements**

**F-6.** 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 material safety and contamination (see Figure 8.2-4). The remaining two of nine (22.2%) occurrences were attributable to basing inspection requirements on incorrect assumptions.



***Figure 8.2-4. Breakdown of “Inadequate Inspection or Secondary Verification Requirements”***

These secondary verifications were not necessarily the same as additional quality inspections, but were alternative ways to inspect for the same condition. Late in the SSP, an effort to convert quality inspections to other methods of secondary verification was pursued. The reason was that quality inspections were subject to errors. An example was the installation of washers on bolts for some of the hardware for the ferry flight. The quality inspector was to check for unused washers after the installation of a plate. The assumption was that, if the washers were not installed, they would be noticed in the work area by the inspector. A more reliable method was to measure the length of the exposed thread on the bolts after the assembly was complete. If the length of the exposed thread exceeded a minimum amount, then one or more washers had to be missing.

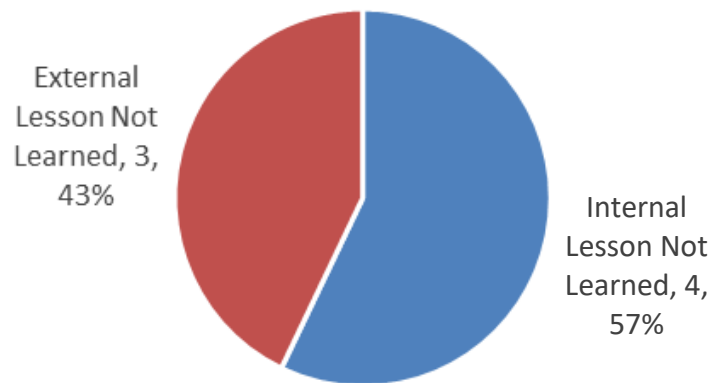
Examples of how “inadequate inspection or secondary verification requirements” impacted several incidents in the study are:

- Apollo 1. Inadequate attention was given to the inspection of the wire bundles for abrasion or deformation [ref. 6].
- Soyuz 1. There was no requirement to inspect the parachute container for contamination or damage [ref. 7].
- 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. Requirements for quality inspections were inadequate [ref. 9].
- STS-1 Oxygen Deficiency. Applicable safety documents had insufficient requirements for atmosphere checks or verification of an air purge before reentry of the orbiter aft compartment by technicians. The aft compartment had no oxygen deficiency monitoring system [ref. 10].

Table J-8 in Appendix J contains a complete listing of the inspection/secondary verification causes identified in the study.

## 8.2.5 Inadequate Organizational Learning Systems

**F-7.** 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 were not shared, found, and/or heeded. Four of seven (57.1%) occurrences were internal lessons not learned, where “internal” refers to 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 (see Figure 8.2-5).



**Figure 8.2-5. Breakdown of “Inadequate Organizational Learning Systems”**

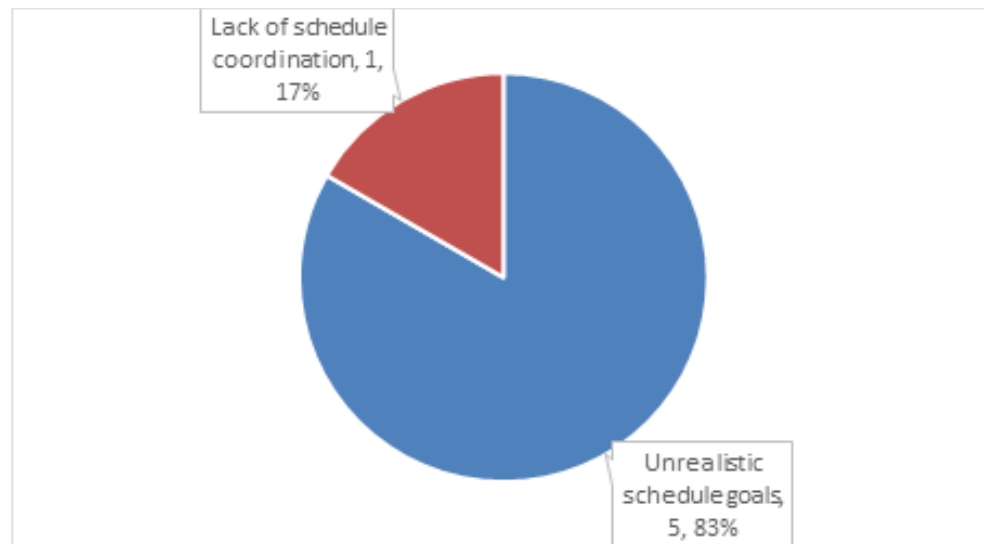
Examples of how “inadequate organizational learning systems” impacted several incidents in the study are:

- 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 spaceflight 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 [ref. 29].
- Apollo 1. An electrical fire occurred in an Apollo command module environmental control system (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% oxygen environment. The test incident report was classified and inaccessible to personnel without a security clearance [ref. 6].
- 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 the SSP or corrective actions proved to be ineffective [ref. 10].

Table J-10 in Appendix J contains a complete listing of the organizational learning causes identified in the study.

## 8.2.6 Inadequate Schedule Controls

**F-8.** 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 (see Figure 8.2-6).



**Figure 8.2-6. Breakdown of “Inadequate Schedule Controls”**

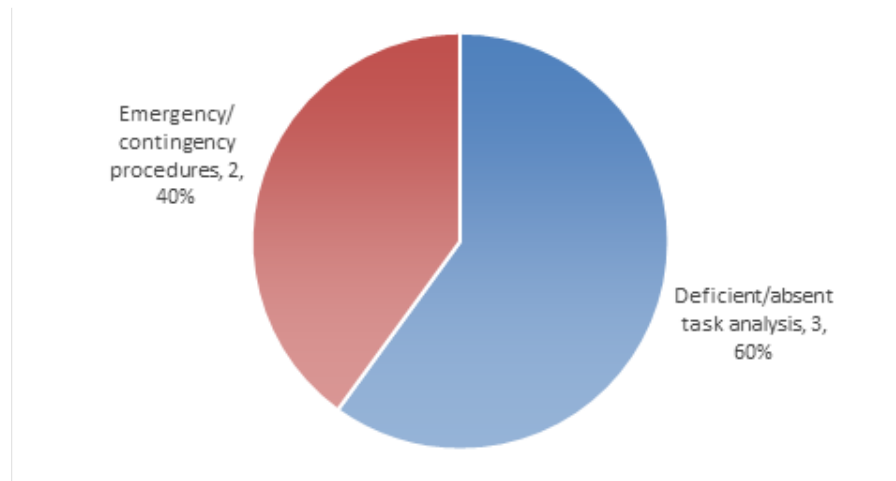
Examples of how “inadequate schedule controls” impacted several incidents in the study are:

- 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 approved and 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 [ref. 29].
- 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].

Table J-12 in Appendix J contains a complete listing of the schedule control causes identified in the study.

### 8.2.7 Inadequate Task Analysis and Design Processes

**F-9.** 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 task designs for emergency, contingency, or nonstandard operations (see Figure 8.2-7).



**Figure 8.2-7. Breakdown of “Inadequate Task Analysis and Design Processes”**

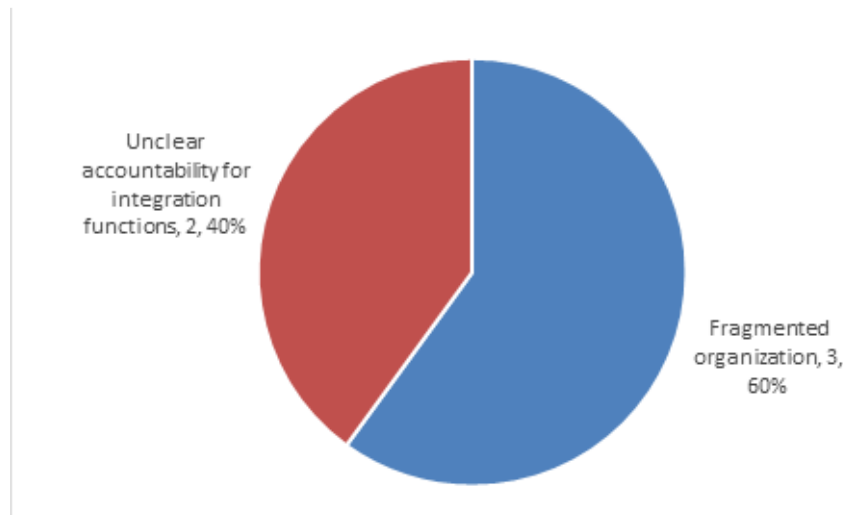
Examples of how “inadequate task analysis and design processes” impacted several incidents in the study are:

- Apollo 1. The astronauts requested that the emergency egress simulation be added to the end of the plugs out test because they were 3 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 [ref. 19].
- 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 [ref. 9].
- Ares 1-X. 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 [ref. 15].

Table J-14 in Appendix J contains a complete listing of the task analysis/design causes identified in the study.

## 8.2.8 Organizational Design Issues

**F-10.** 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, sometimes 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 (see Figure 8.2-8).



**Figure 8.2-8. Breakdown of “Organizational Design Issues”**

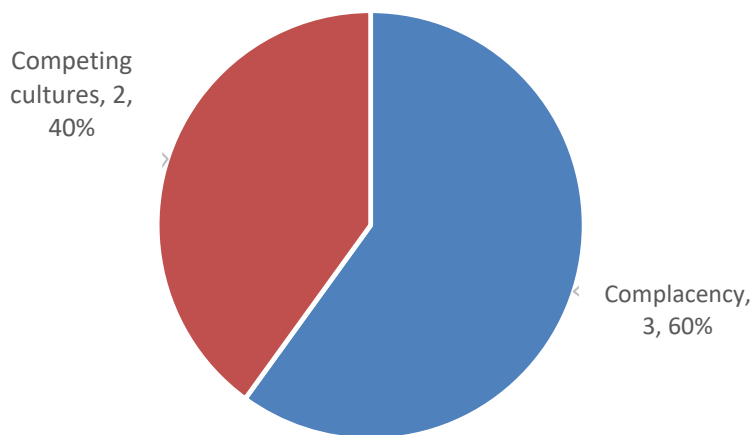
Examples of how “organizational design issues” impacted several incidents in the study are listed below.

- Apollo 1. North American Aviation’s (NAA’s) organization was too fragmented and un-integrated. 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” [refs. 6, 19].
- Skylab 1. No systems or chief engineer was designated for the meteoroid shield. At the time of the mishap, the systems engineering and technical discipline integration functions were sometimes given the label of “project engineer.” “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 1-X. The Ares 1-X 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 Ground Support Equipment (GSE) design) [ref 15].

Table J-16 in Appendix J contains a complete listing of the organizational design causes identified in the study.

### 8.2.9 Organizational Safety Culture Issues

**F-11.** 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 regarding centralized versus distributed command and control during ground tests and a research culture (see Figure 8.2-9).



**Figure 8.2-9. Breakdown of “Organizational Safety Culture Issues”**

Examples of how “organizational safety culture issues” impacted several incidents in the study are listed below.

- Ares 1-X. 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 1-X 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 first Ares 1-X parachute static strip test, which showed examples of behaviors demonstrating complacency, disengagement, and lack of discipline related to organizational safety culture [ref. 15].
- 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 [ref. 10].
- Scaled Composites. Scaled Composite’s culture seemed to be lulled into complacency regarding the documented hazards of N<sub>2</sub>O. 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 test stand trailer (TST) equipment test on July 26, 2007. This failure contributed to the serious injuries suffered by six employees working at the site” [ref. 29].

- SpaceShipTwo. Scaled Composites was proud of its research culture and roots. They would frequently “change things up” to see if the system worked. According to the Vice President/General Manager, they had a “history of building things,” and they relied on inputs from the pilots to identify and resolve ergonomic and human factor issues, despite a large body of evidence describing the pitfalls of relying exclusively on operators for those inputs and associated corrective actions [ref. 16].

Table J-18 in Appendix J contains a complete listing of the organizational safety culture causes identified in the study.

## **9.0 Confidence Building and Exploratory Analysis Activities**

Several additional activities were undertaken to build confidence in the recurring cause study results and to explore other aspects of recurring cause trends during flight tests and early operations phases of human spaceflight programs. These activities included a comparison to historical ground operations safety reports, a comparison to ASAP human spaceflight recommendations, a comparison to recurring causes during the late SSP operations phase, and a review of the mishap recurring cause analysis results by a cadre of human spaceflight subject matter experts (SMEs). These efforts are described in Sections 9.1 through 9.4.

### **9.1 Comparisons to Historical Ground Operations Safety Reports**

Four historical reports on causes of human spaceflight operations mishaps were reviewed. These reports explored the causes of mishaps during early and late Apollo program operations, and late SSP operations. Although the cause categories used in the analyses were different, similar underlying issues were identified.

*Manned Space Programs Accident/Incident Summaries* (1963-1969) [ref. 22]

Overview:

508 mishaps during the Apollo Program were reviewed. The mishaps occurred during the early-mid operations phases of the program.

Excerpt:

“The purpose of this project is to help prevent repetition of these errors and oversights in future programs. An epigram ascribed to Emerson says, ‘Learn from the mistakes of others; you’ll never live long enough to make them all yourself’ ” [ref. 22].

*Manned Space Programs Accident/Incident Summaries* (1970-1971) [ref. 23]

Overview:

Two hundred twenty-four additional Apollo Program mishaps were reviewed for a total of 732 events. Mishaps from the late operations phase were added to the mishaps in the previous study. The report broadly classified causes as hardware and software deficiencies, where software deficiencies include almost every type of failure that is not a hardware failure. The distribution for these 732 mishaps by cause type is shown in Figure 9.1-1.

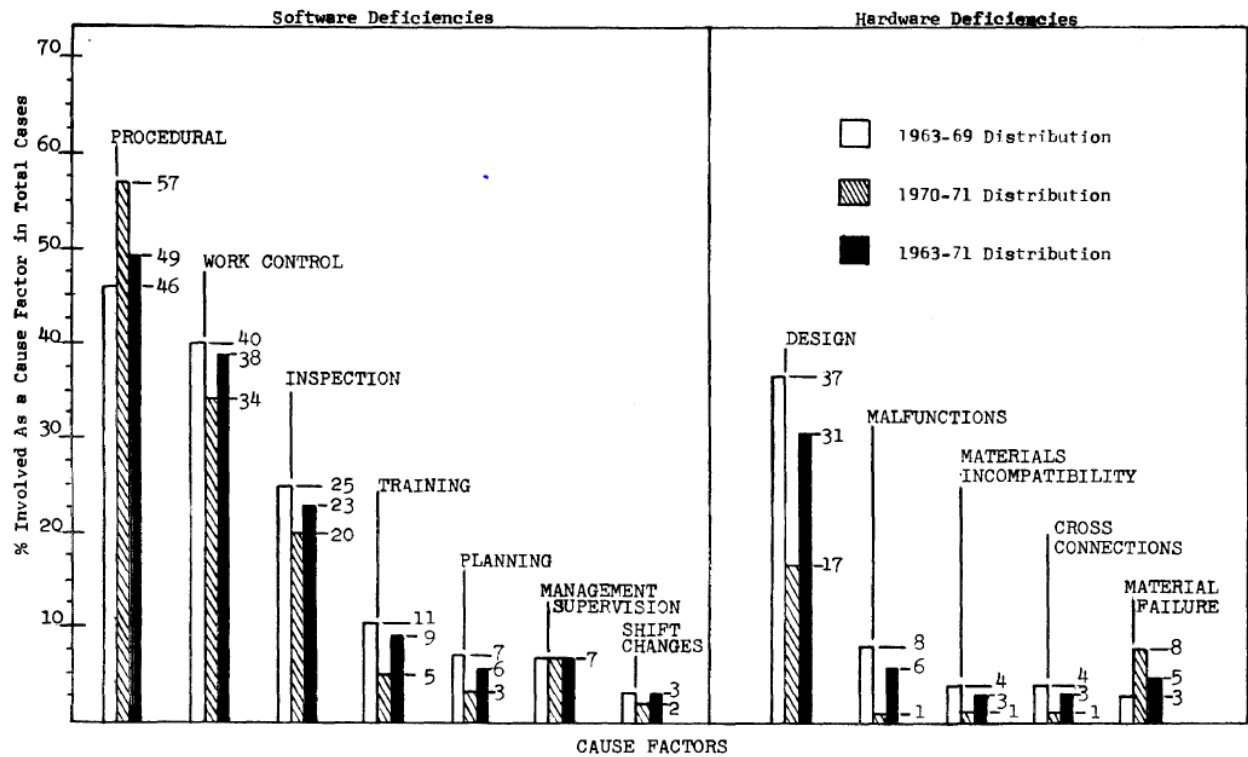


CHART 2 - DISTRIBUTION OF ACCIDENT/INCIDENTS BY CAUSES

Figure 9.1-1. Distribution of Mishap Causes during Apollo Operations [ref. 23]

Excerpt:

“For most effective use in future programs, the individual accidents/incidents recorded here must be interpreted by program specialists for application to potential hazards of the particular programs or systems involved” [ref. 23].

*Space Shuttle Productivity and Error Prevention Report* [ref. 24]

Overview:

Eighty-eight KSC SSP ground processing incidents from the early operations phase of SSP operations (January 1, 1981, to June 1, 1982) were evaluated.

The analysis examined 64 (of 88 total) mishaps precipitated directly by some human action (i.e., human errors). These mishaps were categorized into one of four human error types (i.e., procedural error, policy violations, inadvertent actions, and inadequate actions). Three “predisposing factors” were identified as primary conditions that contributed to the occurrence of these human errors. The predisposing factors were identified as document deficiencies (i.e., erroneously written work instructions), human-engineering deficiencies, and communications/coordination breakdowns. Examples of human engineering deficiencies included connectors that separated when bumped, work platforms that were crowded and/or did not provide rigid support, and “error-provocative” features (e.g., unclear labeling and configuration of controls, valves, and plugs).

Eighteen different contributing factors were identified, which were categorized into four main types:

1. Inadequate coordination (e.g., inadequate communications, inadequate scheduling, lack of mental preparation for tasks, and crisis orientation).
2. Poor job design (e.g., inadequate procedures, human engineering deficiencies, poor working conditions, insufficient technician input, insufficient warning information, and supervisor span of control too broad).
3. Inadequate training (e.g., unqualified personnel, lack of awareness of hazards/consequences, inadequate training content and scheduling, inadequate training requirements system).
4. Psychological factors (e.g., fear and negative emphasis, lack of positive incentives, frustration due to irregularities, and fatigue).

Another factor discussed was excessive time (schedule) pressure. “The pressure seems to be less a function of the overall schedule than it is a function of inadequate scheduling and coordination” [ref. 24].

Excerpts:

“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” [ref. 24].

“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” [ref. 24].

*Report of the Shuttle Processing Review Team* (i.e., the “Perry Committee” Report) [ref. 25]

Overview:

The Perry Committee reviewed summaries of all shuttle processing mishaps, incidents, and close calls that occurred between October 1990 and June 1993.

The focus of the report was a wide range of human factor issues, including team dynamics and communications. A joint NASA/contractor Shuttle Processing Human Factors Team was recommended. This recommendation was implemented, and the Human Factors Team became institutionalized and collected valuable mishap data during investigations through the end of the program.

Excerpts:

“The Shuttle Processing Review Team was...charged with the responsibility to review the circumstances, underlying causes, and corrective actions taken as a result of recent incidents and close calls during Shuttle Processing at KSC. The team was further tasked to determine if actions taken are considered sufficient to prevent problems from recurring” [ref. 25].

“The underlying causes for recent incidents and close calls during Shuttle Processing at KSC as determined through a review of documentation is attributable to human factors, equipment failures, and procedures. The predominant causes (66%) of all mishaps is human factors. For flight hardware incidents, human factors was responsible for 32% of the mishaps, and procedures caused 26% of the mishaps” [ref. 25].

#### Overall Summary:

The historical mishap reports were from the early and late operations phases of NASA’s Apollo Program and the SSP. The mishaps reviewed were primarily mishaps occurring during ground operations. Details of the mishaps were not provided. Although it was not possible to directly compare study results because of different methodologies and taxonomies, there were similarities in the various recurring cause types. All of the historical studies had the stated goal of identifying underlying or systemic causes of the safety issues to prevent recurrence. One study only analyzed mishaps precipitated directly by some human action (i.e., human errors). These mishaps were categorized into one of four human error types, so it was difficult to extract organizational and systemic issues. Another study tried to identify underlying causes, but the cause types were too broad (e.g., human factors, equipment failures, and procedures) to provide actionable results.

## 9.2 Comparison to ASAP Recommendations Analysis

The application of the dual role taxonomy to the eight mishaps in this study was performed primarily based on formal mishap investigation documents. Because of the level of detail available, an in-depth, “micro” analysis was possible. A disadvantage of this approach is the relatively small number of events from a statistical standpoint. In contrast, an analysis of 40 years of ASAP recommendations provided a complementary database for conducting a “macro” analysis. Unlike the mishap information, the dual role taxonomy was applied to the content of high-level recommendations from each report. The subject of the recommendations reflected the concerns of the ASAP members. What this data lacked in detail, it gained in quantity.

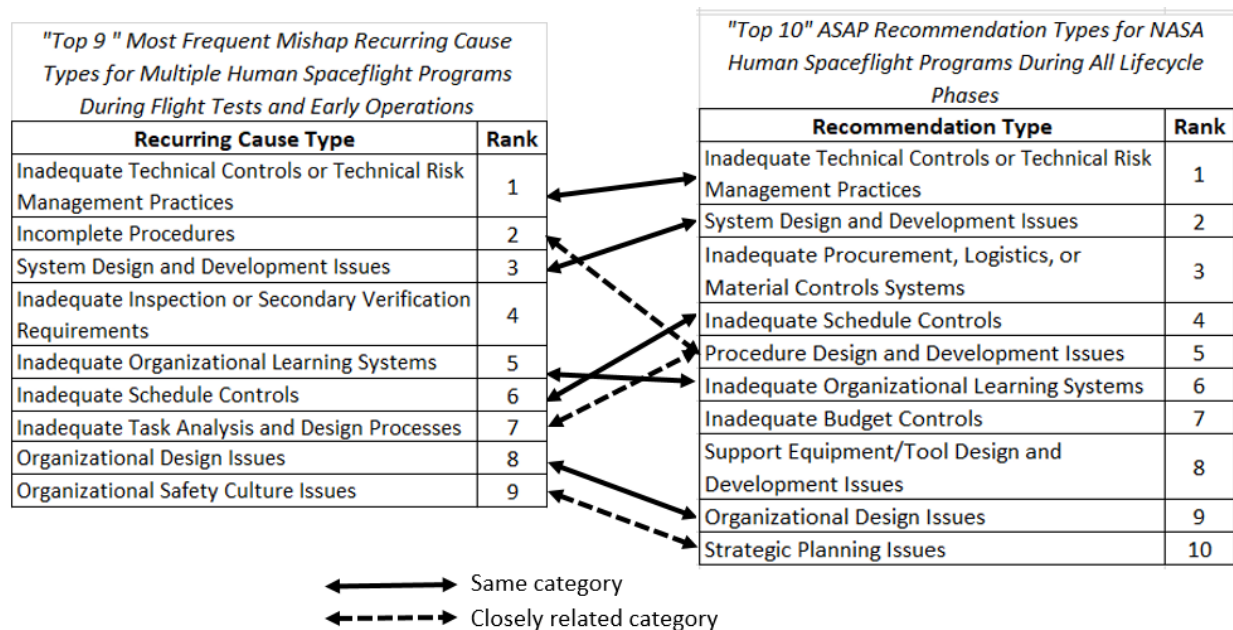
The ASAP, established by Congress after the Apollo 1 fire in January 1967, is a senior advisory committee that reports to NASA, the White House, and Congress. The NASA Administrator appoints the members, and the chair is selected from the members. Each member is appointed to a maximum 6-year term. The ASAP publishes an annual report that is available at <https://oiir.hq.nasa.gov/asap/reports.html>. The annual report has evolved over the years, but it has maintained a general format that includes new findings and recommendations, and tracks recommendations from earlier reports to closure. The recommendations in annual reports from 1972 through 2012 constituted the database for this macro analysis. While the recommendations did not pertain to specific mishaps, they did represent concerns and issues pertaining to a variety of aerospace topics and programs (e.g., SSP, International Space Station (ISS) Program, and aeronautics).

The ASAP recommendations database yielded 857 recommendations that were coded by topic; 40% that were less relevant or too few in number were omitted from further analysis (e.g., aeronautics, NASA Center-related achievements). The remaining 513 were primarily related to SSP (80%), although the recommendations were also directed at the Skylab Program (7%), Safety and Mission Assurance (SMA) (7%), Constellation Program and CCP (6%). Because the recommendation format changed from year to year, only the “year” and “recommendation” fields were used. Other information fields (e.g., NASA response, closure

rationale) were not used because they were not included consistently over the 40-year timeframe examined.

The 513 recommendations were categorized using the same dual role taxonomy used to categorize the causes of the individual mishaps. This categorization was performed independently from the other study team members by a researcher at NASA Ames Research Center. The taxonomy definitions and examples (see Appendix A) were provided to the researcher, but there was no formal or informal training. The “best fits” between the technical concerns being addressed by the recommendations and the definitions and examples in the taxonomy were selected. Because any given recommendation could be described by more than one cause category, the final analysis consisted of 1,066 recommendation codes (see Appendix K). The primary objective was to see how the “macro” and “micro” approaches would compare (i.e., how the ASAP recommendations analysis would compare with the mishap recurring cause analysis). In addition, since the ASAP data provided a sampling over 40 years, this comparison could potentially provide insight into shifts over time and/or topic.

Figure 9.2-1 shows the top nine mishap recurring causes compared with the top ten most frequent codes in the ASAP recommendations analysis. Although the mishap recurring cause and the ASAP recommendations analyses used extremely different approaches and independent data sets, there is good consistency with convergence on five organizational system cause types.



**Figure 9.2-1. Comparison of Most Frequent Mishap Recurring Cause Types to ASAP Recommendation Types**

It is worth noting that mishap recurring cause data focus on understanding why a mishap occurred. The mishap investigation board gathers detailed facts and performs numerous interviews and analyses. ASAP recommendations data focus at a high level from limited access to individuals, observations, and interviews to provide recommendations to NASA senior management pertaining to many programs across the Agency. Thus, it is not surprising that all of the most frequent ASAP recommendation types were concerned with organizational system

issues. However, seven of the top nine mishap recurring cause types were categorized as organizational system causes.

The five most frequent categories shared by the ASAP recommendation analysis and mishap recurring cause analysis were:

1. Inadequate technical controls or technical risk management practices.
2. System design and development issues.
3. Inadequate schedule controls.
4. Inadequate organizational learning systems.
5. Organizational design issues.

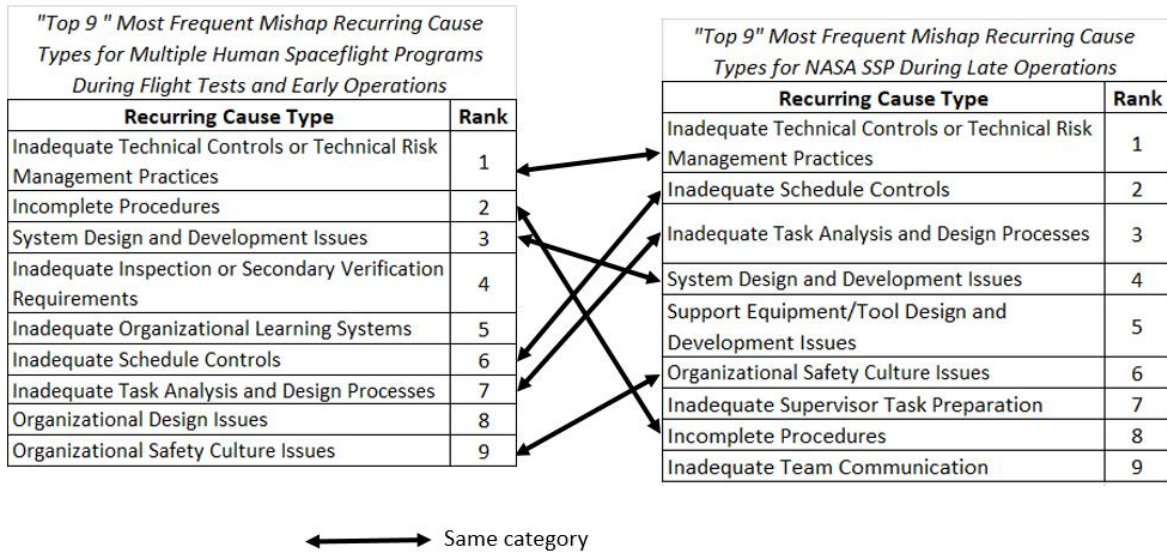
As applied by the independent analyst conducting the ASAP recommendations analysis, “inadequate task design and development processes” and “incomplete procedures” in the mishap recurring cause analysis top nine list were usually encompassed by “procedure design and development issues” in the ASAP recommendations analysis top ten list. “Organizational safety culture issues” in the mishap recurring cause analysis top nine list were closely related to “strategic planning issues” in the ASAP recommendations analysis top ten list. The remaining top nine mishap recurring cause category, “inadequate inspection or secondary verification requirements,” was a dual role cause, which was not expected to be the subject of high-level ASAP recommendations.

In summary, for the organizational system causes on which ASAP focused, there was agreement between the “micro” analysis of the eight mishaps in the recurring cause analysis study and the “macro” analysis of ASAP recommendations. However, the mishap recurring cause study included non-NASA mishaps (i.e., Russian and commercial suborbital providers) and only mishaps that occurred during early testing and operational phases. The ASAP recommendations analysis included all NASA human spaceflight programs during all lifecycle phases since the Apollo 1 fire which resulted in ASAP’s formation.

### **9.3 Comparison to Mishap Recurring Causes during Late Space Shuttle Operations**

In 2006, a similar mishap recurring cause study was initiated in the SSP. The goal of the study was to develop specific proactive initiatives to decrease the risks of major mishaps on the ground and in flight during Shuttle fly-out. The SSP was still recovering from the *Columbia* tragedy, which occurred on February 1, 2003. During this time period, systems were stretched to their limits: significant numbers of hardware and software changes, process changes, and workforce challenges were happening at the same time. The intent, through these data-driven proactive risk reduction actions, was to make SSP organizational systems and processes more robust to handle these changes and challenges.

Influence chain assessments were completed for over 60% (20 of 34) of Standing Accident Investigation Board (SAIB) investigations from February 2003 through May 2008. The results of the aggregate data analysis were used to formulate system-level risk reduction actions. These actions are summarized in Appendix M. The top nine most frequently recurring cause types for multiple human spaceflight programs during early ground and flight operations were compared with the top nine recurring cause types for NASA SSP during late ground operations in Figure 9.3-1.



**Figure 9.3-1. Comparison of Early Human Spaceflight and Late SSP Operations Mishap Recurring Cause Studies**

For this comparison of study results, the single factor determining the top nine causes and their rankings was the number of occurrences. In the late Shuttle operations study, several additional factors were used to develop and prioritize the final top nine list. Additional factors included extra consideration of recurring causes that were not being well-addressed by the existing investigation and corrective/preventive action processes, and consideration of emerging risk areas that warranted additional attention due to unique conditions associated with SSP fly-out.

Six recurring cause types are common to the two lists, as shown in Figure 9.3-1. Although the data set was limited and there were multiple human spaceflight programs in the early operations study, there appears to be a shift in some of the most significant systemic issues identified by the recurring causes. It is reasonable to expect that “inadequate inspection or secondary verification requirements” and “organization design issues” would eventually be worked out as additional years of operations were performed.

For design and development causes, the emphasis shifts from flight systems during early operations to ground systems/GSE as flight hardware modifications become cost-prohibitive later in the operations phase. “Inadequate supervisor task preparation” and “inadequate team communications” could be the result of strains on the workforce as the numbers of technicians and engineers were reduced during late SSP operations. SSP contractor personnel also provided matrixed support to the Constellation Program during late SSP operations, including ground processing of the hardware for the Ares 1-X test flight.

## 9.4 Human Spaceflight Experts Review

The assessment team solicited feedback on the initial study results during a video teleconference on October 9, 2014, with participants at JSC, MSFC, and KSC. The results reviewed did not include the data from the STS-1 SRB IOP mishap or the SpaceShipTwo mishap. The STS-1 SRB IOP mishap was added as a direct result of a suggestion made during this meeting. The SpaceShipTwo mishap occurred after the meeting. The human spaceflight experts were Bo Bejmuk, Wayne Hale, Gary Johnson, Mike Blythe, Nancy Currie-Gregg, and T. K. Mattingly from JSC; Jim Blair and Bob Ryan from MSFC; and Jay Honeycutt, Bob Lang, Charlie Mars, Gerry Schumann, Bob Sieck, Tip Talone, and John Tribe from KSC. The recurring cause analysis methodology and several of the confidence building activities were explained. The top nine most frequently recurring cause types were reviewed. The human spaceflight experts were in general agreement with the study results.

The experts also discussed two related themes. The first theme was the identification of additional adverse events or significant anomalies during NASA human spaceflight programs. Table 9.4-1 lists examples.

***Table 9.4-1. Examples of Undocumented Investigations of Human Spaceflight Adverse Events or Significant Anomalies***

<i>Examples</i>
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 Parachute Failure
Apollo 16 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 Reaction Control System (RCS) Control
Apollo-Soyuz Mission Command Module Crew Exposure to N <sub>2</sub> O <sub>4</sub>
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***

\* A NASA report exists but is not readily available.

\*\* "Near miss" used where no record of a NASA close-call investigation was found in NIMS going back to 1985.

\*\*\*NESC report available



Unfortunately, mishap investigation board reports do not exist for these events. Engineering investigations and troubleshooting were performed, but documentation was usually limited to PowerPoint presentations, such as those presented at Center pre-Flight Readiness Reviews (FRRs) and Agency FRR briefings. An exception was the STS-1 SRB IOP close call, which had an engineering report documenting the technical causes and corrective actions.

The second theme discussed by the human spaceflight experts was the importance of organizations to treat every human spaceflight mission as a “–1” mission (i.e., crewed test flight or inaugural mission). Mishaps depend on a specific situation and set of circumstances where the various conditions, barriers, controls, factors, and causes interact in complex ways. In different situations, it is possible that *Challenger* or *Columbia*-type tragedies could have occurred on STS-1. The Rogers Commission that investigated the *Challenger* tragedy concluded “that drive to declare the Shuttle operational had put enormous pressures on the system and stretched its resources to the limit” [ref. 32]. The Columbia Accident Investigation Board report identified the risks of declaring a human-rated space system “operational” when it was still in the developmental phase. “Throughout the history of the program, a gap has persisted between the rhetoric NASA has used to market the Space Shuttle and operational reality, leading to an enduring image of the Shuttle as capable of safely and routinely carrying out missions with little risk” [ref. 26].

## **10.0 Using the Mishap Recurring Cause Study Results**

The insights gained from the mishap recurring cause analysis can be used to assist human spaceflight organizations in developing effective mishap risk reduction strategies for the most significant systemic issues represented by the most frequently recurring cause types. The study results were presented during program management briefings, all-hands meetings, and a variety of Center and Agency lessons learned forums. The study results also provided the impetus for an Office of the Chief Engineer (OCE) sponsored knowledge-sharing forum, and the results have been reinforced in NESC and NSC activities designed to drive safety through engineering and technical excellence.

### **10.1 Developing Effective Mishap Risk Reduction Strategies**

The content of the various influence chains can be analyzed and used to develop effective and complementary mishap risk reduction initiatives. An example of an analysis of the common causes in the “inadequate schedule controls” influence chains is shown in Table 10.1-1. Two of the six occurrences of “inadequate schedule controls” (highlighted in blue) influence chains contained “organizational safety culture issues,” “high-level policy/guidance LTA,” “accepted team practices LTA,” “system-part reliability/usability LTA,” and “infrequent or unique task.” The other top nine recurring causes are highlighted in green. They included “organizational safety culture issues,” “system design and development issues,” and “inadequate inspection/secondary verification requirements.”

**Table 10.1-1. Inadequate Schedule Controls Influence Chain Analysis**

	Apol- lo-1	Soy- uz-1	Sky- lab -1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares -1X	Space- Ship-2
SL1 – Organizational Culture LTA	X							
SL3 – High Level Policy Guidance LTA		X						X
SL5 – Customer-Stakeholder Relationship Mgmt LTA							X	
ES3 – Schedule Controls LTA	X	X		X	X		X	X
DS2 – System-Part Design & Development LTA		X						
DS5 – Procedure Design & Development LTA				X				
DS7 – Organizational Design & Development LTA					X			
SV1 – Supervisor Task Preparation LTA							X	
SV2 – Supervision During Task LTA	X							
SV3 – Poor Supervisor Example or Excessive Risk Taking		X						
QC1 – Inspection-Surveillance-Audit Requirements LTA	X							
QC4 – Missed or Cursory Inspection-Surveillance-Audit								X
TT1 – Team Composition LTA								X
TT4 – Accepted Team Practices LTA	X				X			
OP4 – Unclear-Misunderstood Procedures				X				
MW3 – System-Part Reliability-Usability LTA		X						
MW5 – Infrequent or Unique Task				X	X			
IN2 – Cognitive Factors				X				
IN4 – Individual Experience & Skills LTA								
IN6 – Individual Assertiveness LTA							X	



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

A second example is the analysis of the content of the organizational safety culture influence chains, which is summarized in Table 10.1-2. “Organizational safety culture issues” (highlighted in blue) most frequently occurred with “accepted team practices LTA,” “inadequate schedule controls,” “inadequate organizational learning systems,” and “inadequate supervision during task.” The additional top nine recurring causes that were part of the organizational safety culture chains are highlighted in green. They were “inadequate schedule controls,” “inadequate organizational learning systems,” “system design and development issues,” “organizational design issues,” and “inadequate inspection/secondary verification requirements.”

**Table 10.1-2. Organizational Safety Culture Issue Influence Chain Analysis**

	Apol- lo-1	Soy- uz-1	Sky- lab -1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares -1X	Space- Ship-2
SL1 – Organizational Culture LTA	X			X		X	X	X
ES1 – Administrative Controls LTA							X	
ES3 – Schedule Controls LTA	X			X				
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA						X		X
DS2 – System-Part Design & Development LTA						X		
DS7 – Organizational Design & Development LTA				X				
TS1 – System Training LTA						X		
SV2 – Supervision During Task LTA	X						X	
QC1 – Inspection-Surveillance-Audit Requirements LTA	X							
TT1 – Team Composition LTA								X
TT4 – Accepted Team Practices	X			X			X	
MW3 – System-Part Reliability-Usability LTA						X		
MW5 – Infrequent or Unique Task				X				
IN4 – Individual Experience & Skills LTA	X							X
IN5 – Accepted Indiv Work Practices LTA							X	



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

Since the organizational safety culture influence chains involve six of the top nine mishap recurring causes, it is especially important to develop corrective and preventive actions from a broad organizational systems perspective, ensuring those actions complement and reinforce each other.

The influence chain analysis tables for each of the top nine mishap recurring cause types are contained in Appendix J.

## 10.2 Human Spaceflight Knowledge Sharing Forum

A Human Spaceflight Knowledge Sharing Forum was hosted by NASA's OCE and Office of the Chief Knowledge Officer in collaboration with the Human Exploration and Operations Mission Directorate on November 1-2, 2016. The forum was the result of a recommendation to address the findings of the study related to organizational learning systems (see Section 8.2.5). The study lead worked with the Agency's Chief Knowledge Officer (CKO) and his staff for over a year to develop the content, structure, and participant list for the meeting. The focus of the forum was system design and development, since the major NASA programs were at that point in their system life cycles at the time of the meeting. The results of the mishap recurring cause study were discussed, and the presentation slides are included in Appendix L.

The forum brought together human spaceflight experts from government, industry and academia to collaboratively identify and discuss applicable lessons from previous mission successes and failures. Forum participants included representatives from NASA centers, mission directorates and human spaceflight programs; NASA's Technical Authorities (TAs), including the OCE, the Office of Safety and Mission Assurance, and the Office of the Chief Health and Medical Officer; commercial contractors and partners; and academia. The forum was held on the campus of the

University of Alabama-Huntsville, near MSFC. Additional information is available at <https://appel.nasa.gov/2016/11/28/a-look-back-at-nasas-first-human-spaceflight-knowledge-sharing-forum/>.

### **10.3 NESC and NSC Activities**

Many NESC and NSC activities have helped current human spaceflight programs address the technical issues identified in this recurring cause study. Independent technical assessments frequently provide an opportunity to highlight a recurring cause issue. In some cases, the entire assessment is devoted to the issue. In other cases (see Appendix N), specific recommendations reinforce the importance of addressing the recurring cause. Examples are listed in Appendix N. The on-line NESC Academy videos (<https://nescacademy.nasa.gov/>) contain examples of lessons learned within the technical disciplines that reinforce the recurring causes in this study.

The NSC publishes System Failure Case Studies, Cases of Interest, and NASA Mishap Investigation Board Reports. In addition, the NSC runs the SMA Technical Excellence Program and performs Quality Audit, Assessment, and Reviews (QAARs).

### **11.0 Findings, Observations, and Recommendations**

The study findings embedded in Section 8 are listed together in Section 11.1. An observation is captured in Section 11.2. Joint NESC and NSC recommendations are listed in Section 11.3.

#### **11.1 Findings**

The overall mishap recurring cause analysis study results (findings) are:

- F-1.** 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.
- F-2.** Twenty-five cause types occurred at least twice (or recurred once). The top nine most frequently recurring cause types occurred at least five times in five separate mishaps. Seventy-five of the 117 (65%) organizational and dual role recurring causes are covered by the nine most frequently recurring cause types.

The specific study results (findings) corresponding to the top nine recurring causes are:

- F-3.** Sixteen occurrences of “inadequate technical controls or technical risk management practices” contributed to all eight (100%) of the incidents studied. Six of the 16 occurrences (37.5%) were inadequate safety reviews/analyses (e.g., inadequate hazard analyses or system safety analyses). Five of the 16 (31.3%) were due to technical issues not being sufficiently analyzed (e.g., inadequate failure modes and effects analyses (FMEA’s), process-FMEA’s, and quantitative risk assessments). Four of the 16 occurrences (25.0%) were inadequate readiness reviews. The remaining occurrence (6.2%) was a case where an aggregation of incremental technical risks was not performed.

- F-4.** 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).
- F-5.** 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.
- F-6.** 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 material safety and contamination. The remaining two of nine (22.2%) occurrences were attributable to basing inspection requirements on incorrect assumptions.
- F-7.** 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 were not shared, found, and/or heeded. Four of seven (57.1%) occurrences were internal lessons not learned, where “internal” refers to 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.
- F-8.** 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.
- F-9.** 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 task designs for emergency, contingency, or nonstandard operations.
- F-10.** 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, sometimes 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.

- F-11.** 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 regarding centralized versus distributed command and control during ground tests and a research culture.

## 11.2 Observations

The following observation was made during discussions with the group of human spaceflight SMEs:

- O-1.** 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.

## 11.3 Recommendations

The following joint NESC and NSC recommendations are directed to the OCE, OSMA, and Office of the Chief Knowledge Officer:

- R-1.** Encourage human spaceflight organizations to internalize the mishap recurring cause study results and determine whether additional mishap risk reduction actions are warranted. (*F-1 through F-11*)
- R-2.** Consider organizing a knowledge-sharing forum focused on ensuring safe and effective ground processing and mission operations. (*F-1 through F-11*)
- R-3.** 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). (*O-1*)

## 12.0 Acronyms and Nomenclature List

ASAP	Aerospace Safety Advisory Panel
ATD	anthropomorphic test device
CCP	Commercial Crew Program
CKO	Chief Knowledge Officer
CLV	Constellation Launch Vehicle
COTS	Commercial off the Shelf
DE	Design Engineering
DoD	Department of Defense
DPA	Destructive Physical Analysis
DS	Design Systems
ECS	Environmental Control System
EEE	Electrical, Electronic, and Electromechanical
EGS	Exploration Ground Systems
ES	Enabling Systems
ESD	Exploration Systems Development

EVA	Extravehicular Activity
FAA	Federal Aviation Administration
FMEA	Failure Modes and Effects Analysis
FRR	Fight Readiness Review
GSE	Ground Support Equipment
HLS	Human Landing System
HSIR	Human-System Integration Requirement
IN	Individuals
IOP	Ignition Over-Pressurization
IPT	Integrated Product Team
ISS	International Space Station
JSC	Johnson Space Center
KSC	Kennedy Space Center
LC	Launch Complex
LTA	Less than Adequate
MONOXCS	Mobile Nitrous Oxide Conditioning System
MPCV	Multi-Purpose Crew Vehicle
MS	Meteoroid Shield
MSDS	Material Safety Data Sheet
MSFC	Marshall Space Flight Center
MW	Material Resources & Work Environment
N <sub>2</sub> O	Nitrous Oxide
NAA	North American Aviation
NESC	NASA Engineering and Safety Center
NSC	NASA Safety Center
OCE	Office of the Chief Engineer
OP	Operational Procedure
OPF	Orbiter Processing Facility
OSHA	Occupational Safety and Health Administration
OWS	Orbital Workshop
QAAR	Quality Audit, Assessment, and Review
QC	Quality Control
POH	Pilot Operating Handbook
PRF	Parachute Refurbishment Facility
RCS	Reaction Control System
S&ID	Space and Information Systems Division
S&MA	Safety and Mission Assurance
SAIB	Standing Accident Investigation Board
SAS	Solar Array System
SE&I	Systems Engineering and Integration
SI	Support Information
SL	Senior Leadership
SLS	Space Launch System
SMA	Safety and Mission Assurance
SOCAR	Systems/Operations Compatibility Assessment Review
SRB	Solid Rocket Booster

SRBE	Solid Rocket Booster Element
SSA	System Safety Analysis
SSP	Space Shuttle Program
STS	Space Transportation System
SV	Supervision
TA	Technical Authority
TPS	Thermal Protection System
TS	Training Systems
TST	Test Stand Trailer
TT	Task Team
TWPB	Thin-walled Pressure Boundaries
WIO	Wind-induced Oscillations
USA	United Space Alliance

## 13.0 References

The documents listed below were referenced in the body of the report. Additional references were used to support the detailed analyses of individual mishaps, and these references are called out separately within the appendices.

1. Barth, T., Simpkins, P., Medina, J., and Blankmann-Alexander, D., “Model for Investigating Human Factors in an Organization,” *NASA Tech Briefs*, February 1998, pp. 78-80.
2. Barth, T., Human Factors Event Evaluation Model, John F. Kennedy Space Center Research and Technology Annual Report, pp. 12-13, 1996.
3. “Orion Multi-Purpose Crew Vehicle (MPCV) Human Systems Integration Requirements,” MPCV 70024, Rev. C, NASA Johnson Space Center, Houston, TX, January 2012.
4. Space Launch System (SLS) Human Systems Integration Requirements (HSIR), SLS-RQMT-161.
5. “NASA Spaceflight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health,” NASA-STD-3001, Volume 2, Revision B, September 9, 2019.
6. “Apollo 204 Accident Report,” Senate Report No. 956, January 1968.
7. Siddiqi, A. A., *Challenge to Apollo: The Soviet Union and the Space Race, 1945-1974*, NASA SP-2000-4408, 2000.
8. “Vladimir Komarov’s Tragic Flight aboard Soyuz-1,” January 19, 2019, URL: <http://russianspaceweb.com/soyuz1.html>, last accessed January 7, 2020.
9. “NASA Investigation Board Report on the Initial Flight Anomalies of Skylab 1 on May 14, 1973, NASA, July 13, 1973.
10. “National Aeronautics and Space Administration. LC 39A Mishap Investigation Board Final Report,” John F. Kennedy Space Center, 1981.
11. Ryan, R. S., Jones, J. H., Guest, S. H., Struck, H. G., Reinfurth, M. H., and Verderaime, V. S., “Propulsion System Ignition Overpressure for the Space Shuttle,” NASA TM-82458, December 1981.

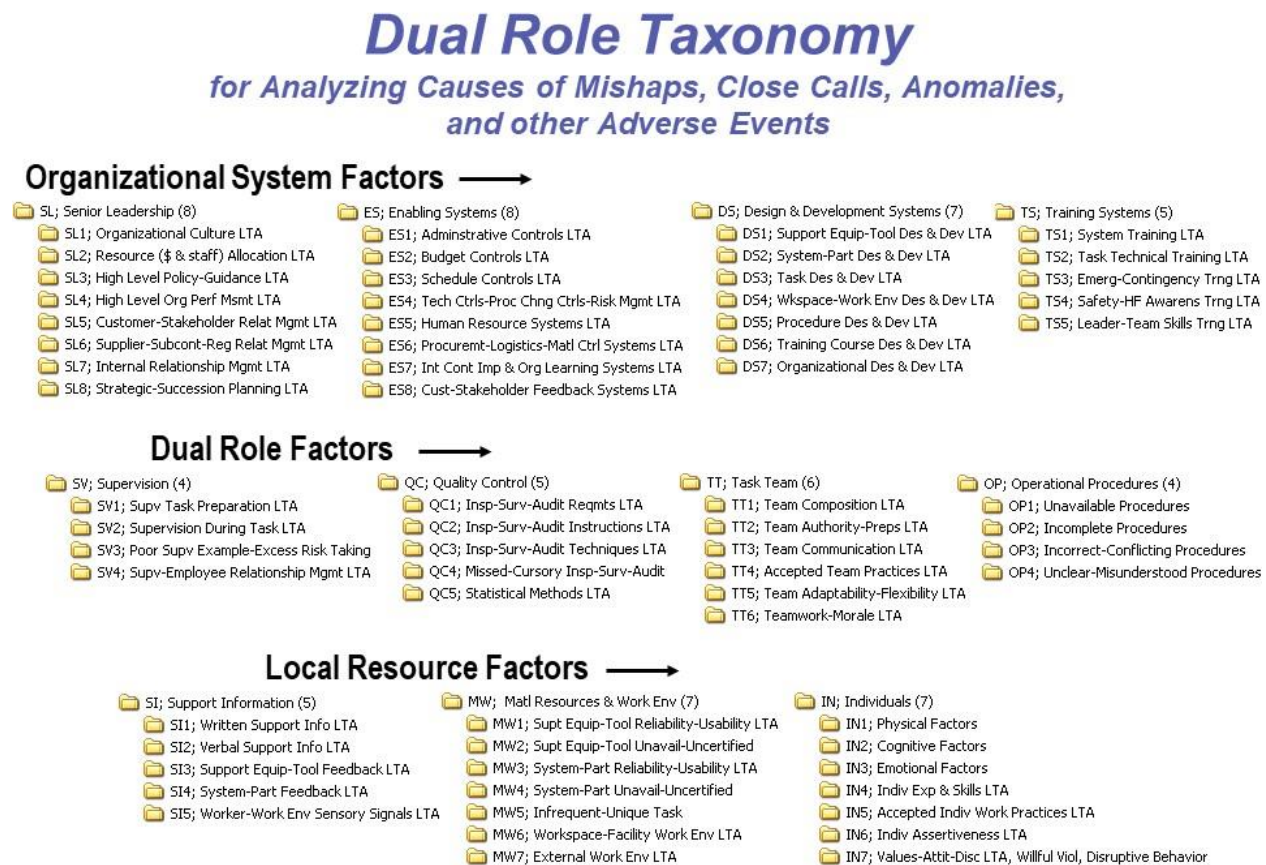


12. Lai, S., "Development of Space Shuttle Overpressure Environment and Correlation with Flight Data; Shuttle Performance Lessons Learned," NASA CR-2283, Part 1, pp. 259-281, March 1983.
13. "Human Spaceflights: STS-1, 1<sup>st</sup> Space Shuttle Mission, December 31, 2018, URL: <http://www.spacefacts.de/mission/english/sts-1.htm>, last accessed January 7, 2020.
14. "STS-1," December 31, 2020, URL: <https://en.wikipedia.org/wiki/STS-1>, last accessed January 7, 2020.
15. United Space Alliance, LLC, "Accident Investigation Board Report - SRBE Parachute Refurbishment Facility Strip Test Lost Time Injury," Flash Report Number 011757, September 5, 2007.
16. "In-Flight Breakup during Test Flight - Scaled Composites SpaceShipTwo," N339SS, Aerospace Accident Report NTSB/AAR-15/02, PB2015-105454, October 31, 2014.
17. Reason, J., *Managing the Risks of Organizational Accidents*, Ashgate Publishing Limited, Gower House, Hants, UK, 1997.
18. Barth, T., "Influence Map Methodology for Evaluating Systemic Safety Issues," University of Central Florida, August 2006.
19. "Report of Apollo 204 Review Board," NASA Historical Reference Collection, NASA History Office, NASA Headquarters, Washington, DC, April 5, 1967.
20. NESC Management Plan
21. NSC Implementation Plan
22. General Electric Company, "Manned Space Programs Accident/Incident Summaries (1963-1969)," NASA CR-120998, March 1970.
23. Cranston Research, Inc., "Manned Space Programs Accident/Incident Summaries (1970-1971)," NASA CR-120999, April 1972.
24. Anacapa Sciences, "Space Shuttle Productivity and Error Prevention," 1981.
25. "Report of the Shuttle Processing Review Team," NASA-TM-109728, June 30, 1993.
26. "Columbia Accident Investigation Board Report," NASA, US Government Printing Office, August 2003.
27. Petroski, H., *To Engineer is Human*, The Role of Failure in Successful Design," 1992.
28. Gawande, A., *Complications: A Surgeon's Notes on an Imperfect Science*, Picador, Henry Holt and Company, New York, NY, 2002.
29. State of California: Division of Occupational Safety and Health, "Inspection Report: 0950625, Inspection Number 310821103," 2008. Although Cal/OSHA can no longer provide the investigation records because the Agency only retains them for seven years, the websites provide a basis for this analysis: URL: [https://www.osha.gov/pls/imis/establishment.inspection\\_detail?id=310821103](https://www.osha.gov/pls/imis/establishment.inspection_detail?id=310821103), [https://www.bakersfield.com/news/scaled-composites-involved-in-mojave-airport-explosion/article\\_77d05184-4ebd-5c43-9c62-82d65040b0a8.html](https://www.bakersfield.com/news/scaled-composites-involved-in-mojave-airport-explosion/article_77d05184-4ebd-5c43-9c62-82d65040b0a8.html), and <https://apps.dtic.mil/dtic/tr/fulltext/u2/a489459.pdf>.

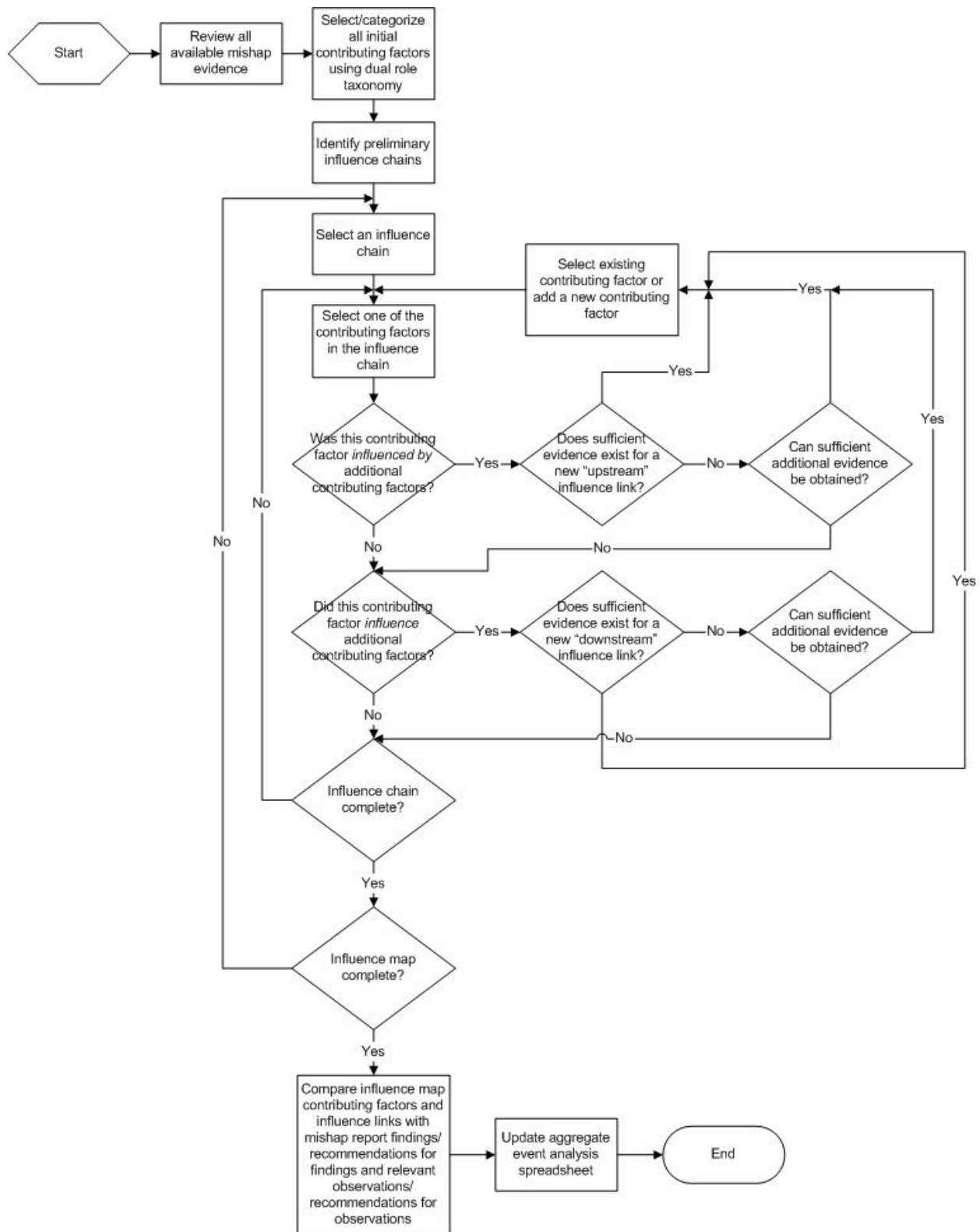
30. “NASA Academy of Program/Project & Engineering Leadership,” Recording of Masters Forum 18, [https://www.youtube.com/watch?v=t-jlwW7ppvA\\_](https://www.youtube.com/watch?v=t-jlwW7ppvA_).
31. Wilson, K., NTSB Senior Human Performance Investigator, quoted in Harwood, W., “SpaceShipTwo Mishap due to Pilot Error and Company Training Oversight,” July 28, 2015. URL: <http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-due-to-pilot-error-and-company-training-oversight/>.
32. “Rogers Commission Report on the Space Shuttle *Challenger* Accident,” June 6, 1986, URL: [https://spaceflight.nasa.gov/outreach/SignificantIncidents/assets/rogers\\_commission\\_report.pdf](https://spaceflight.nasa.gov/outreach/SignificantIncidents/assets/rogers_commission_report.pdf), last accessed January 23, 2020.

# Appendix A. Taxonomy of Causes/Factors in Mishaps, Close Calls, Anomalies, and other Adverse Events

Figure A-1 shows the entire set of causes/factors considered when assessing the causes of the mishaps studied. These factors included organizational system factors, local resource factors, and factors that were a combination of those two (i.e., dual role factors). Figure A-2 details the process used in evaluating these factors to arrive at a set of causes for each mishap. Many causes can manifest and contribute to mishaps in different ways. Detailed examples of potential subcategories and specific causes are listed in Table A-1.



**Figure A-1. Dual Role Taxonomy [ref. 18]**



**Figure A-2. Methodology for Single Event Analysis [ref. 18]**

**Table A-1. Detailed Dual Role Taxonomy Categories [ref. 18]**

Note: LTA = “less than adequate”

<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Examples</b>
<b>SL; Senior Leadership</b>	SL1; Organizational Culture LTA		Behavior valued and rewarded by management not consistent with long-term, ingrained beliefs
	SL2; Resource (\$ & staff) Allocation LTA		Inadequate resources - staff, funds, and equipment
	SL1; Organizational Culture LTA		Reporting culture LTA - reporting of concerns LTA
	SL1; Organizational Culture LTA		Just culture LTA - sense of fairness LTA
	SL1; Organizational Culture LTA		Flexible culture LTA - change to meet new demands LTA
	SL1; Organizational Culture LTA		Engaged culture LTA - not everyone is doing their part
	SL1; Organizational Culture LTA		Learning culture LTA - organizational learning from internal and external (to the organization) successes and mistakes LTA
	SL3; High Level Policy-Guidance LTA	Company policy LTA	Documents
	SL3; High Level Policy-Guidance LTA	Fail to Provide Guidance	
	SL3; High Level Policy-Guidance LTA	Inadequate Processes	Fail to Provide Oversight or Enforce Regulations
	SL3; High Level Policy-Guidance LTA	Reinf Policies-Unsafe Behav	
	SL4; High-Level Organizational Performance Measurement LTA	Inadequate Processes	Fail to Track Performance
	SL5; Customer-Stakeholder Relationship Management LTA		Program-level expectation management, impacts of HW/SW system mods
	SL6; Supplier-Subcontractor-Regulator Relationship Mgmt LTA		Environmental Protection Agency, OSHA, International Standards Organization
<b>ES; Enabling Systems</b>	SL7; Internal Relationship Management LTA		Poor relations among upper management, employees, and unions
	SL8; Strategic or Succession Planning LTA		Fail to invest in training and risk management. Organizational instability.
	ES1; Administrative Controls LTA		Poor document management practices. Standards and policies are unclear or contradictory and enforcement is inconsistent.
	ES2; Budget Controls LTA		Unrealistic budget (for labor, material, etc.)
	ES3; Schedule Controls LTA		Poor scheduling and unrealistic deadlines. Conflicted/uncoordinated resources - experts, labs, machinery. Real-time or near real-time changes.
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA	Document & Configuration Control	Documentss not up to date and current configuration not verified. Update procedure too long.
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA		Technical standards

Level 1	Level 2	Level 3	Examples
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA	Problem ID-Control	Problem reporting, analysis, and corrective actions slow to be implemented and inadequately assessed for effectiveness.
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA	Safety-Hazard-Risk Review	Unclear risk-acceptance criteria. Corrective actions slow to be implemented and inconsistently reviewed.
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA		Process creep, changing eng requirements, normalizing deviance, excessive waivers
	ES4; Technical Controls-Process Change Controls-Risk Mgmt LTA	Safety-Hazard-Risk Review	Effects of automation
	ES5; Human Resource Systems LTA	Rewards-Incentives	Incentives
	ES5; Human Resource Systems LTA	Employee Screen-Hire LTA	Poor recruiting, screening, and retention practices
	ES5; Human Resource Systems LTA	Oversight-Employee Relations	Inadequate employee relations audits and evaluations
<b>ES; Enabling Systems</b> (continued)	ES6; Procurement-Logistics-Material Control Systems LTA	Procurement Control	Poor procurement specifications, vendor selection, acceptance requirements, and change control.
	ES6; Procurement-Logistics-Material Control Systems LTA	Product-Material Control	Unclear product handling, packaging, inspection, and storage requirements. Unauthorized substitutions.
	ES7; Internal Continuous Improvement & Organizational Learning Systems LTA		Results of previous Incident investigations and corrective/preventive actions not implemented
	ES8; Customer-Stakeholder Feedback Systems LTA		Customer requirements not identified or addressed
<b>DS; Design Systems</b>	DS1; Support Equip-Tool Design & Development LTA		Critical errors in equipment/tool design - ex: material selection, display/control location and usability, and maintenance schedule/procedure. Poor documentation.
	DS2; System-Part Design & Development LTA		Inadequate design - material, weight, I/O compatibility. Unusable design - inaccessible, complex, unreliable, not robust, unserviceable. Poorly documented.
	DS2; System-Part Design & Development LTA	Non-Fault Tolerant Sys	Errors undetectable or unrecoverable
	DS3; Task Design & Development LTA		Unrecognized hazard. Operational task is overly complex/confusing, monotonous, or requires difficult communications.
	DS4; Workspace-Work Environment Design & Development LTA		Workspace has inadequate attention to comfort, safety, or standard practices.
	DS5; Procedure Design & Development LTA		Task is confusing, requires excessive references/look-ups, or complex
	DS6; Training Course Design & Development LTA		Inadequate/absent training/lesson content/lesson plan and insufficient testing. Poor records maintained.

Level 1	Level 2	Level 3	Examples
	DS7; Organizational Design & Development LTA		Unclear/overlapping responsibilities between organizations/departments
<b>TS; Training Systems</b>	TS1; System Training LTA		Insufficient training on flight and ground support systems - hardware and software
	TS2; Task Technical Training LTA		Inadequate initial & ongoing task training. Excessive workforce turnover. Poor performers not identified.
	TS3; Emergency or Contingency Training LTA		Abnormal Event/Emergency Procedure Training LTA
	TS4; Safety-Human Factors Awareness Training LTA		Orientation training LTA - reinforce safety culture, core values, and human factors
	TS5; Leadership and Team Skills Training LTA		Insufficient team training
<b>SV; Supervision</b>	SV1; Supervisor Task Preparation LTA		Poor task planning, worker selection, delegation, worker training, and resources acquisition.
	SV2; Supervision during Task LTA		Failure to track performance and coach employees (long-term). Improper performance not corrected. Excessive supervision provided.
	SV3; Poor Supervisor Example or Excessive Risk Taking		Supervisor accepting/encouraging unsafe practices
	SV4; Supervisor-Employee Relationship Management LTA		Poor employee/management relations
<b>QC; Quality Control</b>	QC1; Inspection-Surveillance-Audit Requirements LTA		Insufficient hardware or environment inspections. Insufficient quality controls.
	QC2; Inspection-Surveillance-Audit Instructions LTA		Unclear inspection-surveillance-audit instructions
	QC3; Inspection-Surveillance-Audit Techniques LTA		Inadequate or improper inspection techniques used.
	QC4; Missed or Cursory Inspection-Surveillance-Audit		Cursory inspection-surveillance-audit
	QC5; Statistical Methods LTA		Missing or improper statistical methods
<b>TT; Task Team</b>	TT1; Team Composition LTA		Too few or too many people. Inappropriate skill mix. Unclear boundaries.
	TT2; Team Authority or Preparation LTA	Team Authority LTA	Roles and responsibilities unclear.
	TT2; Team Authority or Preparation LTA	Team Preparation LTA	Inadequate task communication and prioritization. Poor shift-change processes.
	TT3; Team Communication LTA	Verbal comm between crew and team lead/supervisor	No Comm, Untimely Comm, Misunderstood Comm
	TT3; Team Communication LTA	Verbal communications between departments/work groups	Missing, unclear, or untimely communication between engineers and support groups/contractors
	TT3; Team Communication LTA	Verbal comm between different mgmt Levels	No Comm, Untimely Comm, Misunderstood Comm
	TT3; Team Communication LTA	Verbal comm between team lead/supv and management	No Communication, untimely or misunderstood Comm
	TT3; Team Communication LTA	Verbal communications between team members/peers	Missing, unclear, or untimely communication. Standard terminology and confirmation not used.

Level 1	Level 2	Level 3	Examples
	TT4; Accepted Team Practices LTA	Operational team behaviors LTA	Team shortcuts and adapting work procedures.
	TT4; Accepted Team Practices LTA	Peer pressure	Peer pressure
	TT4; Accepted Team Practices LTA	Safety team behavior LTA	Safety practices and PPE not used
	TT5; Team Adaptability-Flexibility LTA		Abnormal or emergency situations. Staffing changes.
	TT6; Teamwork-Morale LTA	Morale LTA	Low team morale
	TT6; Teamwork-Morale LTA	Teamwork LTA	Poor conflict resolution, cohesiveness, or commitment to the team/task.
<b>OP; Operational Procedure</b>	OP1; Unavailable Procedures		Documentation delayed, inaccessible, or unavailable.
	OP2; Incomplete Procedures		Situations not covered or use not required.
	OP3; Incorrect-Conflicting Procedures		Data/facts are wrong. Typos. Conflicting information.
	OP4; Unclear-Misunderstood Procedures		Too long/complicated or incomprehensible. Difficult to ID correct procedure.
<b>SI; Support Information</b>	SI1; Written Support Info LTA		Insufficient written instructions, signage, drawings, or notes.
	SI2; Verbal Support Info LTA		Disrupted, late, incomprehensible, or misunderstood verbal communication.
	SI3; Support Equip-Tool Feedback LTA		Inadequate/Incorrect Equip-Tool Feedback
	SI4 System-Part Feedback LTA		Inadequate/Incorrect System Feedback
	SI5; Worker or Work Environment Sensory Signals LTA		Inadequate visual, tactile, audio, or aroma cues.
<b>MW; Material Resources &amp; Work Environment</b>	MW1; Support Equip-Tool Reliability-Usability LTA	Support Equip-Tool Reliability LTA	Equipment unusable or failed during task.
	MW1; Support Equip-Tool Reliability-Usability LTA	Support Equip-Tool Usability/Ergonomics LTA	Equipment is inappropriate for task.
	MW2; Support Equip-Tool Unavailable-Uncertified	Support Equip-Tool Availability LTA	Equipment is unavailable or in use elsewhere.
	MW2; Support Equip-Tool Unavailable-Uncertified	Support Equip-Tool Certification/Calibration LTA	Equipment is uncalibrated, miscalibrated, uncertified, or expired.
	MW3; System-Part Reliability-Usability LTA	System-Part Reliability LTA	System/part is unusable or failed during test.
	MW3; System-Part Reliability-Usability LTA	System-Part Usability/Ergonomics LTA	System/part is inappropriate for task
	MW4; System-Part Unavailable-Uncertified	System-Part Availability LTA	Not enough usable parts available to do the job.
	MW4; System-Part Unavailable-Uncertified	System-Part Certification/Calibration LTA	System/parts are not certified/calibrated or have expired.
	MW5; Infrequent or Unique Task	Unique Task	Significant, non-routine change to task (needs to be a significant change so the overall task can be considered unique)
	MW5; Infrequent or Unique Task	Infrequent Task	Task not performed by the organization on a routine basis
	MW6; Workspace-Facility Work Env LTA	Workspace LTA	Tools are inaccessible. Poor lighting, inaccessibility, noisy, or unclear.



Level 1	Level 2	Level 3	Examples
	MW6; Workspace-Facility Work Env LTA	Facility Work Env LTA	Excessive acceleration/deceleration forces, temperature, humidity, or noise.
	MW7; External Work Env LTA	Poor Weather	Excessive rain, wind, lightning, fog, or other environmental stressors.
	MW7; External Work Env LTA	Time of Day	Poor night visibility
<b>IN; Individuals</b>	IN1; Physical Factors	Physical Health/Medical Illness	Effects of medicines, caffeine, cigarettes, obesity, pain, or illness. Loss of consciousness. Hypoxia or hyperventilation.
	IN1; Physical Factors	Physical fatigue/rest-sleep LTA	Long task duration, jet lag, stress, weight loss, blood donation, and shift rotation.
	IN1; Physical Factors	Physical/anthropometric limitations	Limited reaction time, vision, hearing, and strength.
	IN2; Cognitive Factors	Judgment-decision making LTA	Inappropriate decision, response, analysis, expectation, and habit.
	IN2; Cognitive Factors	Attention-situation awareness LTA	Distraction, interruption, boredom, fixation, and disorientation. Missed communication or inattention to feedback.
	IN2; Cognitive Factors	Memory lapse	Omitted step in procedure or checklist. Sequence error.
	IN2; Cognitive Factors	Cognitive limitations	Incompatible aptitude, intelligence, perception, or decision-making ability.
	IN3; Emotional Factors		Significant life changes or upsets. Panic, frustration, anxiety, and apprehension.
	IN4; Indiv Exp & Skills LTA	Technical knowledge LTA	Inadequate task knowledge or training
	IN4; Indiv Exp & Skills LTA	Individual skills-task proficiency LTA	Delayed response, poor technique, and lack of experience in task or emergency procedures.
	IN4; Indiv Exp & Skills LTA	Readiness - certification and qualification	Not qualified/certified or qualification expired.
	IN5; Accepted Individual Work Practices LTA	Bent rules/SOPs	Rules/SOPs not followed.
	IN5; Accepted Individual Work Practices LTA	Safety behaviors/PPE LTA	Improper PPE. Poor housekeeping.
	IN5; Accepted Individual Work Practices LTA	Skipped crosscheck or checklist	Improper or misused checkoff
	IN5; Accepted Individual Work Practices LTA	Substituted Equipment-Part-Tools	Improper or misused tools
	IN6; Indiv Assertiveness LTA		Failure to announce an identified problem. Overconfidence or lack of confidence.
	IN7; Values-Attit-Discipline LTA, Willful Violations, Disruptive Indiv Behavior	Disruptive individual behavior	Unprofessional attitude or poor work ethics. Alcohol or drug use. Excessive ego or poor interpersonal behavior.
	IN7; Values-Attit-Discipline LTA, Willful Violations, Disruptive Indiv Behavior	Values-Attitudes-Discipline LTA	Lack of safety awareness and unsafe or negative attitude.
	IN7; Values-Attit-Discipline LTA, Willful Violations, Disruptive Indiv Behavior	Willful violation	Sabotage and thrill seeking. Flagrant disregard for procedures or equipment limits.

## Appendix B. Apollo 1 Mishap Analysis

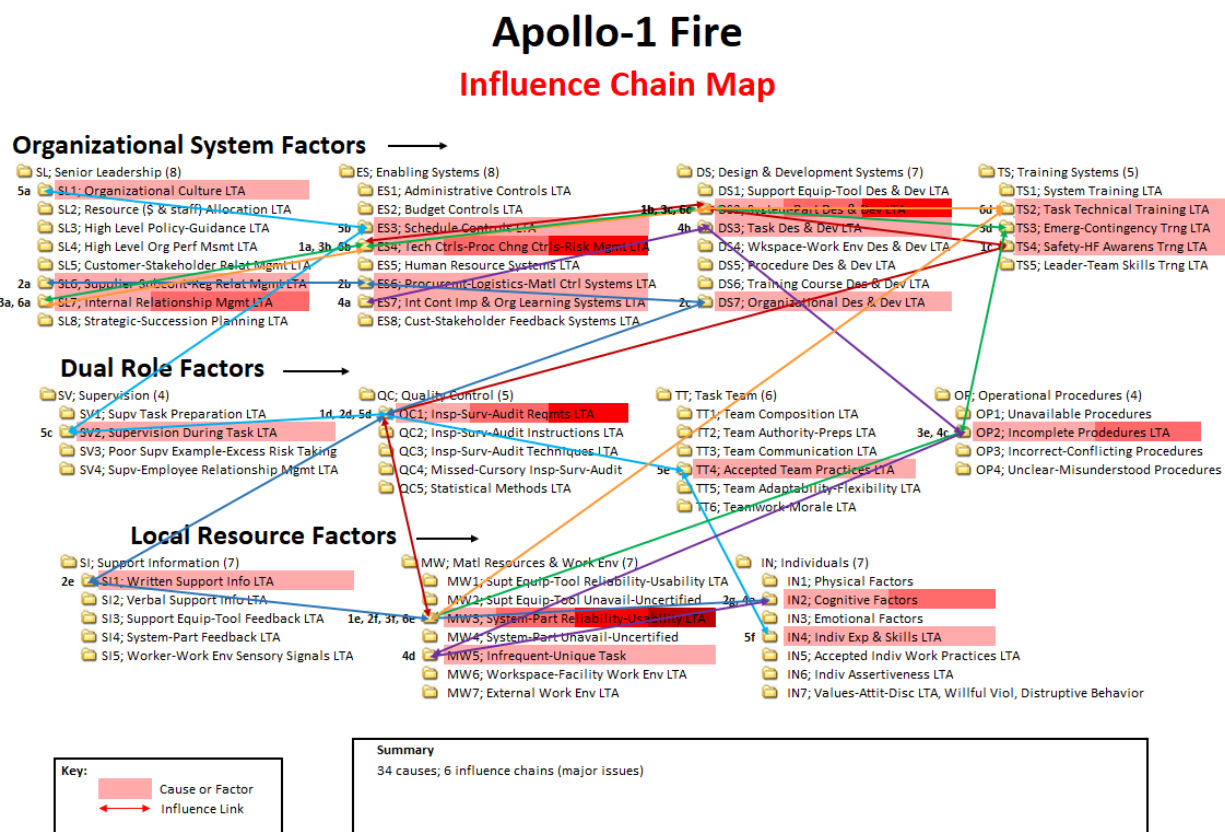
The probable cause of the Apollo 1 fire on January 27, 1967, was an electrical arc from a Teflon-coated wire located near the floor of the capsule. Interviews revealed a notable amount of carelessness when working around the delicate wire. Apollo operations were conducted in an environment of 100% oxygen pressurized to 16.7 psi, as had been done in Mercury and Gemini to save hundreds of pounds, yet the presence of combustibles in the cabin was not minimized. This put ground testing at a high likelihood of a fire if a spark was generated. The hatch was also not designed for emergency procedures, so it took nearly 5 minutes to open during the Apollo 1 emergency. The various influence chains for this incident are detailed in Table B-1 and displayed graphically in Figure B-1.

**Table B-1. Apollo 1 Mishap Influence Chain Summary**

#	Description of Cause	Type
	<b>Chain #1: Spark was caused by an electrical short in faulty wiring insulation.</b>	
1a	Risk Management. Teflon-coated wiring was selected for flight performance. The risk of wire abrasions due to vehicle ground processing and maintenance was not mitigated. The wiring was not protected by covers. The technicians requested trays to cover and protect the wiring and were told there was no time to design/build protective trays. They were told to use rubber mats instead to cover the wiring. Known risk that was ignored until after the fire. <i>See p. 27, Finding 1: NASA Apollo 204 Review Board</i> <i>See blog by technician.</i>	ES4
1b	System Part Design & Development. Teflon was specifically chosen for the wire coating due to its excellent insulation, chemical inertness and fire resistance. However, Teflon is soft and therefore susceptible to creep, or cold-flow deformation and abrasion. The Teflon coating had worn away during operations, exposing the electrical wiring.	DS2
1c	Safety/Human Factors Awareness Training. There was inadequate general workforce awareness regarding the fragile nature of the Teflon-coated wiring inside the command module.	TS4
1d	Inspection Requirements. Given the fragile nature of the Teflon-coated wiring, inadequate attention was given to the inspection of the wire bundles for evidence of insulation abrasion or deformation.	QC1
1e	System/Part Reliability-Usability. After the fire, special protective trays were designed and installed to limit the wiring exposure, protect the cables from physical damage, and reduce the risk of flame propagation.	MW3
	<b>Chain #2: Decision to use single gas design, 100% oxygen.</b>	
2a	Subcontractor Relationship Management. NASA over-ruled/directed NAA to use pure oxygen. <i>See p. 28, Finding 2: NASA Apollo 204 Review Board</i>	SL6
2b	Material Control Systems. Controls were LTA to mitigate the known fire risks of a pure oxygen environment by rigorously controlling/eliminating ignition sources and combustible materials inside the command module. There seemed to be a belief that 100% oxygen was not a hazard because there had not been any problems during the Mercury and Gemini programs. <i>See p. 32, Finding 11 - NASA Apollo 204 Review Board</i>	ES6
2c	Organizational Design. NAA was too fragmented, not integrated. Also, NASA's decentralization of R&QA functions and responsibilities decreased NASA's effectiveness in monitoring contractor R&QA activities.	DS7
2d	Inspection Reqrmts. Combustible materials were allowed inside vehicle.	QC1
2e	Written Support Information. Even though Dr. Roth's 1964 report warned against the use of nonmetallic materials in a pure oxygen environment, it appears this information was not widely shared to alert personnel to the dangers of having Velcro in the command module, as well as the flight suits made of nylon.	SI1
2f	System/Part Reliability-Usability. There were several sources of flammable materials in the command module: Velcro and its highly combustible adhesive, as well as the astronauts' nylon flight suits.	MW3
2g	Cognitive Factors. Unaware of the significance of the fire risks associated with pure oxygen environment.	IN2
	<b>Chain #3: Astronauts could not escape the fire - hatch redesigned to open inward.</b>	
3a	Internal Relationship Management. Perhaps to save face, in a seemingly knee-jerk reaction to the Mercury MR-4 Liberty Bell 7 event, NASA redesigned the hatch to open inward. NAA and the astronauts lobbied for an outward opening hatch, but NASA over-ruled them. <i>See p. 28, Finding 4 - NASA Apollo 204 Review Board</i>	SL7
3b	Risk Management/Technical Controls. The difficulty of opening the inward hatch in case of an emergency was not analyzed adequately. The increased pressure from the fire - in an already pressurized command module - made it impossible for the astronauts to open the hatch.	ES4

#	Description of Cause	Type
3c	System Design. The procedure planned for the emergency egress to occur in 90 seconds. Astronauts would open the interior hatch. The 2nd exterior hatch had 8 bolts that needed to be removed. A special tool was required to lift the 3rd hatch from the command module. The opening of the hatch was difficult and took too long to be executed in any emergency.	DS2
3d	Emerg/Contingency Training. There were inadequate emergency provisions for rescue or medical assistance. There were only 2 fire extinguishers located near the white room and not enough gas masks.	TS3
3e	Incomplete Procedures. There was no contingency procedure. <i>See blog by technician.</i>	OP2
3f	System/Part Usability. The inward opening hatch was not usable. After the fire, the hatch was redesigned back to an outward opening hatch.	MW3
	<b>Chain # 4: Procedure not marked as hazardous.</b>	
4a	Org. Learning Systems. NASA knew of recent accidents that had occurred in pure oxygen environments. NASA also had been briefed by experts about the hazards of working in 100% oxygen environments. Since the vehicle was not fueled, the plug-out test was considered non-hazardous. The procedure should have been marked hazardous because of the pure oxygen environment. <i>See p. 29, Finding 5: NASA Apollo 204 Review Board</i>	ES7
4b	Task Design. The astronauts requested the emergency egress simulation be added to the end of the plug-out test because they were 3 weeks from launch and had not practiced an emergency escape yet. The plug out test did not require all the hatches be closed and locked. Also, there was no consideration on how to handle troubleshooting - how long is it ok to keep flowing oxygen? All of the comm system problems prolonged the plug-out test, so oxygen was flowing continuously for approximately 4 hours. Also, the pressurization of the vehicle up to 16.7 psi could have been done in a separate test; it was not required for the plug out test.	DS3
4c	Incomplete Procedures. Adequate safety precautions were not established or observed for this test. Contingency preparations to permit escape or rescue of the crew from an internal command module fire were not made. <i>See p. 29, Finding 5: NASA Apollo 204 Review Board</i>	OP2
4d	Infrequent/Unique Task. This was the first launch simulation plug-out test for this mission.	MW5
4e	Cognitive Factors. The successes of Mercury and Gemini seemed to have lulled the Apollo team into complacency about the fire risks associated with a pure oxygen environment, in spite of several documented NASA cases of fires in pure oxygen environments and warning from researchers.	IN2
	<b>Chain 5: Poor workmanship and quality control, water/glycol leakage from ECS.</b>	
5a	Org. Culture. NASA noted NAA performance problems 13 months prior to the fire. <i>See "The Phillips Report" letter to NAA's President on Dec. 19, 1965 - pages 12 &amp; 13, and p. 31, Finding 10, NASA Apollo 204 Review Board</i>	SL1
5b	Schedule Controls. The command module was shipped to KSC with significant open work. "There is an inference that the design, qualification and fabrication process may not have been completed adequately prior to shipment to KSC." <i>See p. 3 "History of the Accident" <a href="http://history.nasa.gov/Apollo204/history.html">http://history.nasa.gov/Apollo204/history.html</a>. Gene Kranz, after the fire: "We were too gung ho about the schedule. We were not ready!" Deke Slayton: "We got in too much of a goddamned hurry."</i>	ES3
5c	Supervision during Task. Supervision during overtime shifts. <i>See "The Phillips Report" page 8: "Poor workmanship is evidenced by the continual high rates of rejection and Materials Review Board actions which result in rework that would not be necessary if the workmanship had been good. Recognizing that overtime shifts are necessary at this time, it is our view that strong and knowledgeable supervision of these overtime shifts is necessary. . ."</i>	SV2
5d	Inspection Requirements. The requirements for quality inspections were missing or deficient.	QC1
5e	Accepted Team Practices. Quality and workmanship issues. <i>See Thomas Barton Report. He was a quality inspector for NAA, and he communicated quality/workmanship problems to his supervisor, but nothing happened. He documented contamination issues, poor workmanship, people sleeping and drinking on the job, etc.</i>	TT4
5f	Individual Experience and Skills. This was a new program that required a very large workforce. Many of the workers were right out of high school, so their experience and skills were very limited. <i>Chris Kraft in his book stated, "I want you to know that the average age of my organization in 1969 was 26."</i>	IN4
	<b>Chain 6: Poor plumbing design on the ECS, design of the soldered joints in plumbing led to leakage of water/glycol.</b>	
6a	Internal Relationship Management. Astronauts were openly concerned with the large volume of open work and the overall reliability of the vehicle. The three astronauts posed for a crew picture with their heads bowed and their hands clasped as if in prayer because of their concerns with the vehicle's quality and integrity. <i>See p. 31, Finding 10, NASA Apollo 204 Review Board</i>	SL7
6b	Risk Management. Deputy Administrator Seamans wrote that NASA's single worst mistake in engineering judgment was not to run a fire test on the command module prior to the plug-out test. NASA almost scrubbed the block 1 spacecraft—all of them were scrubbed except spacecraft 012/Apollo 1.	ES4

#	Description of Cause	Type
6c	System Design and Development. Grissom was so frustrated by the many technical failures of the spacecraft during testing that he hung a lemon on the simulator.	DS2
6d	System Training. There were continual leakage problems with the ECS due to design issues. After the fire, workers were required to be trained and certified for soldering plumbing repair operations.	TS2
6e	System Reliability. Numerous hardware problems diminished the reliability of the command module's systems.	MW3
	<b>Summary: 34 causes, 6 chains</b>	



**Figure B-1. Apollo 1 Mishap Influence Chain Map**

## **Apollo 1 Mishap Analysis Notes**

### **Chain 1: Spark was caused by an electrical short in faulty wiring insulation**

See page 27, Finding 1: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

### **ES4 – Technical Controls/Risk Management LTA**

Teflon-coated wiring was selected for flight performance. The risk of wire abrasions due to vehicle ground processing and maintenance was not mitigated. The wiring was not protected by covers. The technicians requested trays to cover and protect the wiring and were told there was no time to design/build protective trays. They were told to use rubber mats instead to cover the wiring. The wire coating was a known risk that was not sufficiently mitigated until after the fire.

## **DS2 – System/Part Design & Development LTA**

“Teflon was specifically chosen for the wire coating due to its excellent insulation, chemical inertness and fire resistance. However, Teflon is soft and therefore susceptible to creep, or cold-flow deformation, and abrasion. The Teflon coating had worn away during operations, exposing the electrical wiring” (see NASA Safety Center’s System Failure Case Study, “Fire in the Cockpit”).

“The most probable initiator was an electrical arc in the sector between –Y and +Z spacecraft axes. The exact location best fitting the total available information is near the floor in the lower forward section of the left-hand equipment bay where ECS instrumentation power wiring leads into the area between the Environmental Control Unit (ECU) and the oxygen panel.” See page 28, “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

“This would place the origin to the left of the Command Pilot (Grissom), and considerably below the level of his couch.” See page 14, “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

NOTE: One theory hypothesizes that after being strapped in the capsule for 5.5 hours, and fed up with the persistent communication problems that kept delaying the test, Grissom may inadvertently have kicked a wire bundle that caused a spark. (See Apollo, John Saxon, page 8)

“Indications of Spacecraft Motion – A number of individual signals were received which are indicative of slight motions of the spacecraft within the last minute prior to the first fire report. These signals were of a random nature and are similar to signals that were obtained from the spacecraft during known crew movement. . . The nature of activity of the crew during this period could not be determined.” See page 19, “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

## **TS4 – Safety/Human Factors Awareness Training LTA**

There was an absence of general workforce awareness regarding the fragile nature of the Teflon-coated wiring inside the command module. As we learned with the SSP, workers had to be cautioned to avoid using wiring and plumbing lines as handholds and avoid stepping/leaning on them. Since cautions and warnings are a weak risk mitigation measure, physical covers were later added.

“Because of weight limitations, much of the wiring in the Apollo command module was insulated with thin-walled Teflon covered with a thin polyimide coating. This wire was extremely susceptible to damage.” (See page 21, “NASA’s Apollo Experience Report – Reliability and Quality Assurance,” 1973 – NASA Technical Note D-7438.)

“Initially, the wiring in the crew compartment was exposed and subject to possible damage during ground-based operations as well as during flight.” (See page 24, NASA’s Apollo Experience Report – Reliability and Quality Assurance, 1973 – NASA Technical Note D-7438.)

## **QC1 – Inspection Requirements LTA**

Given the issues the Teflon-coated wiring had with abrasions exposing conducting wires, inadequate attention was given to the inspection of the wire bundles for evidence of insulation abrasion or deformation.

### **MW3 – System/Part Reliability or Usability LTA**

After the fire, special protective trays were designed and installed to limit the wiring exposure, protect the cables from physical damage, and reduce the risk of flame propagation.

#### **Chain 2: Decision to use single gas design – 100% oxygen atmosphere and combustible materials in the command module in areas contiguous to possible ignition sources**

See page 28, Finding 2: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

### **SL6 – Supplier/Subcontractor/Regulator Relationship Management LTA**

When designing the Mercury spacecraft, NASA had considered using a nitrogen/oxygen mixture to reduce the fire risk near launch, but rejected it based on two considerations. First, nitrogen used with the in-flight pressure reduction carried the clear risk of decompression sickness (known as “the bends”). But the decision to eliminate the use of any gas but oxygen was crystallized when a serious accident occurred on April 21, 1960, in which McDonnell aircraft test pilot G. B. North passed out and was seriously injured when testing a Mercury cabin/spacesuit atmosphere system in a vacuum chamber. The problem was found to be nitrogen-rich (oxygen-poor) air leaking from the cabin into his spacesuit feed. North American Aviation had suggested using an oxygen/nitrogen mixture for Apollo, but NASA overruled this. The pure oxygen design also carried the benefit of saving weight, by eliminating the need for nitrogen tanks (<http://www.time.com/time/magazine/article/0,9171,840811,00.html#ixzz2HZqzn6HU>).

“In 1962, in the course of spaceflight simulations using human subjects, there had been two cases of fires breaking out, with nobody killed but with a few nasty injuries. North American’s design team knew of the fire hazard and had objected to the use of a pure oxygen atmosphere, but NASA had overruled them. (The intent of the 100% oxygen environment of the capsule was to reduce the weight of the vehicle by about 500 lbs.) Both Gemini and Mercury had used a pure oxygen atmosphere and there was precedent to believe that the risks were acceptable” (see page 2, “Setbacks,” [http://www.vectorsite.net/tamrc\\_21.html](http://www.vectorsite.net/tamrc_21.html)).

NASA directed NAA to use pure oxygen. “The single gas design (oxygen) was selected over a two gas design (oxygen and nitrogen) for mass considerations, complexity and reliability concerns, and crew vulnerability to the ‘bends’ (nitrogen bubbling in the body tissue during a rapid decompression event). Over 1,000 hours of flight time without incident had been previously logged with a 100% oxygen atmosphere, despite the threat of fire and physiological detriment.” (See NASA Safety Center’s System Failure Case Study, “Fire in the Cockpit.”)

After the fire, “the second major modification, (after the hatch redesign), was the change in the launch pad spacecraft cabin atmosphere for prelaunch testing from 100 percent oxygen to a mixture of 60 percent oxygen and 40 percent nitrogen to reduce support of any combustion.” (See “Apollo by the Numbers,” page 9.)

### **ES6 – Procurement/Logistics/Material Control Systems LTA**

Control practices were LTA to mitigate the known fire risks of pure oxygen environments by rigorously controlling/eliminating ignition sources and combustible materials. See Finding 11, page 32, “NASA Apollo 204 Review Board – History of the Accident,” <http://history.nasa.gov/Apollo204/history.html>.

“An examination of operating practices showed the following examples of problem areas: Discrepancies existed between NAA and NASA MSC specifications regarding inclusion and positioning of flammable materials...Problems of program management and relationships between Centers and with the contractor have led in some cases to insufficient response to changing program requirements.”

In 1964, Dr. Emmanuel Roth prepared a report for NASA on “The Selection of Space-Cabin Atmospheres.” “He warned that combustible items, including natural fabrics and most synthetics, would burn violently in the pure oxygen atmosphere of the command module. Even allegedly flame-proof materials would burn. He warned against the use of combustibles in the vehicle.” See *Predictions of Trouble* (<http://www.hq.nasa.gov/History/SP-4204/ch18-2.html>).

Also, prior to the Apollo 1 fire, there were several known fires that occurred in 100% oxygen environments that reinforced Dr. Roth’s warning to NASA:

- September 9, 1962 – A fire occurred in the Space Cabin Simulator at Brooks AFB in a chamber using 100% oxygen at 5 psi. The two occupants collapsed from smoke inhalation before being rescued.
- November 17, 1962 – A fire occurred at the Philadelphia Navy Laboratory in a chamber using 100% oxygen at 5 psi. There were four occupants in the chamber. The routine maintenance of replacing a burned-out light bulb caused their clothes to catch on fire. All suffered serious burns.
- April 28, 1966 – Another fire occurred at the Apollo Environmental Control System in Torrance, CA, as equipment was being tested under 100% oxygen and 5 psi.

In spite of these warnings, there were many sources of flammable materials in the command module. How did the design review process overlook so many combustible materials in the command module?

“The best way to guard against fire was to keep flammable materials out of the cabin. Hilliard W. Paige of General Electric had, as a matter of fact, warned Shea about the likelihood of spacecraft fires on the ground as recently as September 1966; and just three weeks before the accident, Medical Director Charles Berry had complained that it was certainly harder to eliminate hazardous materials from the Apollo spacecraft than it had been in either Mercury or Gemini...What was not fully understood by either North American or NASA was the importance of considering the fire potential of combustibles in a system of all materials taken together in the position which they would occupy in the spacecraft and in the environment of the spacecraft” (see <http://www.arlingtoncemetery.net/apollo.htm>).

## **DS7 – Organizational Design & Development LTA**

NAA was too fragmented – not integrated – over-manned. 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 S&ID organization (Space and Information systems Division) to contribute, in an integrated and effective manner, to the hard core requirements of the programs.”

(See *The Phillips Report*, letter to NAA’s President, Lee Atwood on December 19, 1965, by Major General Samuel C. Phillips, Apollo Program Director at NASA Headquarters.)

“I can see no way of improving future performance, and meeting commitments which NAA must meet if we are to achieve the national objectives of Apollo, except to improve the management and technical competence of your Space and Information systems Division. . . I had hoped that a letter such as this would not be necessary. However, I consider the present situation to be intolerable and can only conclude that drastic action is in the best national interest.”

(See *The Phillips Report*, letter to NAA’s President Lee Atwood on December 19, 1965, by George Mueller, Associate Administrator For Manned Space Flight.)

See: Apollo 1 “Phillips Report – Audit of North American Aviation,” December 1965, page 7:

“The most pronounced deficiencies observed in S&ID Engineering are:

- Fragmentation of the Engineering function throughout the S&ID organization, with the result that it is difficult to identify and place accountability for program-required Engineering outputs.
- Inadequate systems engineering job is being done from interpretation of NASA stated technical requirements through design release.
- Adequate visibility on intermediate progress on planned engineering releases is lacking. Late, incomplete, and incorrect engineering releases have caused significant hardware delivery schedule slippages as well as unnecessary program costs.
- The principles and procedures for configuration management, as agreed to between NAA and NASA, are not being adhered to by the engineering organizations.

How did these known organization problems continue to exist? NASA knew there were serious problems with NAA a full year prior to the accident. Where was the NASA oversight to ensure compliance with NASA’s requirements? How did the design review process overlook so many combustible materials in the command module?

(See page 2, f”NASA’s Apollo Experience Report – Reliability and Quality Assurance,” 1973 – NASA Technical Note D-7438):

“This decentralization of R&QA functions and responsibilities between these JSC elements resulted in differences regarding the establishment and interpretation of requirements, the degree of implementation, and the monitoring of contractor R&QA activities. . . . In 1968, all but two groups of the R&QA elements were reorganized into one central R&QA office responsible for all R&QA activities associated with all spacecraft hardware and providing appropriate support to



all program offices and JSC organizational elements...This centralization aided in establishing coordinated requirements and provided for the uniform interpretation and implementation of the R&QA tasks including the monitoring activities.”

### **QC1 – Inspection/Surveillance/Audit Requirements LTA**

Combustible materials were allowed inside vehicle.

### **SI1 – Written Support Information LTA**

Even though Dr. Roth’s 1964 report warned against the use of nonmetallic materials in a pure oxygen environment, it appears this information was not widely shared to alert personnel to the dangers of having abundant amounts of Velcro in the command module, as well as flight suits made of nylon.

### **MW3 – System/Part Reliability-Usability LTA**

There were several sources of flammable materials in the command module that were incompatible with a 100% oxygen environment – especially Velcro and the astronauts’ nylon flight suits. The astronauts entered the command module at 1:00 pm EST and the fire occurred at 6:31 pm EST. Everything in the command module had been saturated with oxygen for 5 ½ hours.

“From a materials standpoint, a significant experience of the Apollo Program is the use of nonmetallic materials (NMM) in the oxygen-rich spacecraft cabin atmosphere. The reliability tasks contained in the NASA handbook ‘Reliability Program Provisions for Aeronautical and Space Contractors’ included general requirements regarding materials but did not emphasize the importance of nonmetallic materials. At the start of the spacecraft design effort, the amount of data on the flammability of NMM in pure oxygen at 5 psia and the toxicity of NMM was limited.” (See pages 15 and 16, NASA’s Apollo Experience Report – Reliability and Quality Assurance, 1973 – NASA Technical Note D-7438.)

### **IN2 – Cognitive Factors**

In spite of Dr. Roth’s warning in 1964 against the use of combustible materials in a pure oxygen environment and the documented fires that occurred in 100% oxygen environments in 1962 and 1966, there seemed to be a belief that all was well with Apollo 1 because there had not been any major problems with the pure oxygen capsule environment during the Mercury and Gemini programs.

Frank Borman, a Gemini veteran who would go to the Moon on Apollo 8, served as the astronaut’s representative to the Apollo 1 accident investigation board. He made this point about the plugs out test’s status abundantly clear. “I don’t believe that any of us recognized that the test conditions for this test were hazardous,” he said on record. Without fuel in the launch vehicle and all the pyrotechnic bolts unarmed, no one imagined a fire could start, let alone thrive.

Borman identified what he considered the crux of the problem and the real reason, however indirect, behind the death of the crew. “We did not think,” he said, “and this is a failing on my part and on everyone associated with us; we did not recognize the fact that we had the three essentials, an ignition source, extensive fuel and, of course, we knew we had oxygen.” (See Apollo 1 Scientific American article.)

### **Chain 3: Astronauts could not escape the fire; hatch redesigned to open inward**

(See page 28, Finding 4: “NASA Apollo 204 Review Board – History of the Accident,” <http://history.nasa.gov/Apollo204/history.html>.)

#### **SL7 – Internal Relationship Management LTA**

Following Alan Shepard’s successful launch into space aboard the Freedom 7 on May 5, 1961, Gus Grissom became the second man in space on July 21, 1961, (Mercury-Redstone 4). Spacecraft 11 was nicknamed the Liberty Bell 7 and it had a new explosive hatch release. After splashdown, while waiting for the helicopter, Grissom stated that he heard a thud, which was the hatch detonating prematurely. Grissom escaped from the capsule, but the capsule took on too much water and The Liberty Bell 7 sank.

Perhaps to save face, in a seemingly knee-jerk reaction to the MR-4 Liberty Bell 7 event, NASA redesigned the hatch to open inward. NAA and the astronauts lobbied for an outward opening hatch, but NASA overruled them.

#### **ES4 – Technical Controls/Risk Management LTA**

The difficulty of opening the inward hatch in case of an emergency was not analyzed adequately. The increased pressure from the fire—in an already pressurized command module—made it impossible for the astronauts to open the hatch.

The command module had been pressurized to 16.7 lb psi for the test.

“With a slightly higher pressure inside the command module than outside, opening the inner hatch was impossible because of the resulting force on the hatch. The inability of the pressure relief system to cope with the pressure increase due to the fire made opening the inner hatch impossible until after cabin rupture.” (See page 6, “Apollo by the Numbers.”)

“Three hatches were installed on the command module. The outermost hatch, called the boost protective cover (BPC) hatch, was part of the cover which shielded the command module during launch and was jettisoned prior to orbital operation. The middle hatch was termed the ablative hatch and became the outer hatch when the BPC was jettisoned after launch. The inner hatch closed the pressure vessel wall of the command module and was the first hatch to be opened by the crew in an unaided crew egress.”

“The day of the fire, the outer BPC hatch was in place but not fully latched because of distortion in the BPC caused by wire bundles temporarily installed for the test. The middle hatch and inner hatch were in place and latched after crew ingress.”

“Although the BPC hatch was not fully latched, it was necessary to insert a specially-designed tool into the hatch to provide a hand-hold for lifting it from the command module. At this time the White Room was filling with dense, dark smoke from the command module interior and from secondary fires throughout level A-8.”

“The personnel who removed the BPC hatch could not remain in the White Room because of the smoke. They left the White Room and passed the tool required to open each hatch to other individuals. A total of five individuals took part in opening the three hatches and each made several trips into the White Room and out for breathable air.” (See pages 4 and 5, “Apollo by the Numbers.”)

## **DS2 – System/Part Design & Development LTA**

The procedure planned for the emergency egress to occur in 90 seconds: Astronauts to open interior hatch – second exterior hatch had eight bolts that needed to be removed – and a special tool was required to lift the third hatch from the command module.

The task of opening the hatch was difficult and took too long to be executed in any emergency. In reality, it took five personnel 5 minutes to remove all three hatches once the fire was announced.

## **TS3 – Emergency/Contingency Training LTA**

Inadequate Provisions for Rescue or Medical Assistance.

“While some personnel were able to locate and don operable gas masks, others were not. Some proceeded without masks, while others attempted without success to render masks operable. Even operable masks were unable to cope with the dense smoke present because they were designed for use in toxic rather than dense smoke atmospheres. Visibility in the White Room was virtually nonexistent” (see pages 4 and 5, “Apollo by the Numbers”).

“...it was concluded that all hatches were opened and the two outer hatches removed approximately five minutes after the report of the fire. Medical opinion, based on autopsy reports, concluded that chances of resuscitation decreased rapidly once consciousness was lost (about 15 to 30 seconds after the first suit failed) and that resuscitation was impossible by the time all three hatches were opened” (see pages 4 and 5, “Apollo by the Numbers”).

Personnel who opened the hatches unanimously stated that all hatches were open before any firefighters were seen on the level or in the White Room. It was estimated, based on tests, that 7 to 8 minutes were required to travel from the fire station to the launch complex and to ride the elevator from the ground to Level A-8.

Approximately 3 minutes after the firefighters arrived, three doctors entered the White Room and determined that the crew had not survived the heat, smoke, and thermal burns. The doctors were not equipped with breathing apparatus, and the command module still contained fumes and smoke (see pages 5 and 6, “Apollo by the Numbers”).

See page 29, Finding 5: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

- “Management continually monitor the safety of all test operations and assure the adequacy of emergency procedures.
- All emergency equipment (breathing apparatus, protective clothing, deluge systems, access arm, etc.) be reviewed for adequacy.
- Personnel training and practice for emergency procedures be given on a regular basis and reviewed prior to the conduct of a hazardous operation.
- Service structures and umbilical towers be modified to facilitate emergency operations.”

However, other important factors that must be considered for crew safety include control of ignition sources, control of the environment, fire-detection capability, and fire-extinguishment provisions. A systems engineering approach to fire safety must be established early in the development of space-flight programs” (see pages 15 and 16, “NASA Apollo Experience Report – Reliability and Quality Assurance,” 1973 – NASA Technical Note D-7438).

## **OP2 – Incomplete Procedures**

There was no formal contingency or emergency procedure for a fire on the ground during the test.

## **MW3 – System/Part Reliability or Usability LTA**

After the fire, the hatch was redesigned back to an outward opening hatch.

“The two-piece hatch was replaced by a single quick-operating, outward opening crew hatch made of aluminum and fiberglass. The new hatch could be opened from inside in 7 seconds and by a pad safety crew in 10 seconds. Ease of opening was enhanced by a gas-powered counterbalanced mechanism.” (See Apollo by the Numbers, page 9.)

## **Chain 4: Procedure not marked as hazardous because vehicle was not fueled**

See page 29, Finding 5: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

## **ES7 – Internal Continuous Improvement & Org. Learning Systems LTA**

Knowledge of previous accidents of pure oxygen environments – known hazards.

## **DS3 – Task Design & Development LTA**

Two tasks were scheduled to be worked in parallel to save time – increased pressure for demonstration countdown – should have done leak test separate – separate emergency egress simulation – oxygen had been flowing for approximately 4 hours. All of the problems they encountered with troubleshooting the communication system prolonged the planned plug-out test.

## **OP2 – Incomplete Procedures**

See page 29, Finding 5: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

“Adequate safety precautions were neither established nor observed for this test...Contingency preparations to permit escape or rescue of the crew from an internal command module fire were not made:

- No procedures for this type of emergency had been established either for the crew or for the spacecraft pad work team.
- The emergency equipment located in the White Room and on the spacecraft work levels was not designed for the smoke condition resulting from a fire of this nature.
- Emergency fire, rescue and medical teams were not in attendance.
- Both the spacecraft work levels and the umbilical tower access arm contain features such as steps, sliding doors and sharp turns in the egress paths which hinder emergency operations.”
- The January 27, 1967, launch simulation was a "plugs-out" test to determine whether the spacecraft would operate nominally on (simulated) internal power while detached from all cables and umbilicals. Passing this test was essential to making the February 21 launch date. The test was considered non-hazardous because the launch vehicle or the spacecraft was loaded with fuel or cryogenics, and all pyrotechnic systems were disabled.

- There was no procedure for a fire on the ground. With so many engineers on hand for every test, it was assumed that the astronauts would be safe so long as fire extinguishers were nearby. But, more importantly in the case of Apollo 1, is the plug-out test's status: it was not classified as dangerous.
- After the hatches were sealed, the air in the cabin was replaced with high-pressure (16.7 psia) pure oxygen.
- The board noted that the test planners had failed to identify the test as hazardous; the emergency equipment (such as gas masks) were inadequate to handle this type of fire; that fire, rescue, and medical teams were not in attendance; and that the spacecraft work and access areas contained many hindrances to emergency response such as steps, sliding doors, and sharp turns.

### **MW5 – Infrequent/Unique Task**

This was the first launch simulation plug-out test for this mission.

### **IN2 – Cognitive Factors**

The successes of Mercury and Gemini seemed to have lulled the Apollo team into complacency about the fire risks associated with a pure oxygen environment, in spite of several documented NASA cases of fires in pure oxygen environments and warnings from researchers.

### **Chain 5: Poor quality control and workmanship – water/glycol leakage from environmental control system**

See page 31, Finding 10: “NASA Apollo 204 Review Board – History of the Accident,” (<http://history.nasa.gov/Apollo204/history.html>).

### **SL1 – Organizational Culture LTA**

See *The Phillips Report*, Letter from George Mueller, Associate Administrator for Manned Space Flight to Lee Atwood, President of NAA, dated Dec. 19, 1965, pages 12 and 13:

“I can see no way of improving future performance, and meeting commitments which NAA must meet if we are to achieve the national objectives of Apollo, except to improve the management and technical competence of your Space and Information systems Division.

Take a hard look at the competence and effectiveness of individuals, especially in the upper echelons of the organization; move out those who are not really contributing, due either to the organization or to their own competence. . . I am convinced that there is no substitute for clear assignment of responsibility and accountability to individuals for delivering results.

I consider the present situation to be intolerable and can only conclude that drastic action is in the best national interest.”

### **ES3 – Schedule Controls LTA**

The first piloted Apollo mission was scheduled for launch on February 21, 1967. Three weeks before the launch, however, the Apollo 1 fire and the death of the prime crew on Friday January 27, 1967, put America's lunar landing program on hold for 18 months.

Quote from Gene Kranz, as he addressed his flight control team on the Monday morning following the Apollo 1 fire:

“...We were too gung ho about the schedule and we locked out all of the problems we saw each day in our work. Every element of the program was in trouble and so were we. The simulators were not working, Mission Control was behind in virtually every area, and the flight and test procedures changed daily. Nothing we did had any shelf life. Not one of us stood up and said, ‘Dammit, stop!’ I don’t know what Thompson’s committee will find as the cause, but I know what I find. We are the cause! We were not ready! We did not do our job. We were rolling the dice, hoping that things would come together by launch day, when in our hearts we knew it would take a miracle. We were pushing the schedule and betting that the Cape would stop before we did.”

“The biggest problem, however, was that the work schedule was just too aggressive. Deke Slayton called it ‘insane’ and put it simply: ‘We got in too much of a goddamned hurry.’ A lot of poor, hasty work was being put into the Moon project, and the margins for failure were painfully small.” (See *Setbacks Apollo and Soyuz*, page 3)

Cold war race to the moon – national pride, democracy, and the free world was at stake.

Helter-skelter work environment – aggressive schedule – continual design changes increased workload – fatigue working 12-hr days/60-hr weeks – Schedule delays were acknowledged as contributing factors to the design, manufacturing, and quality control process issues.

## **SV2 – Supervision During Task LTA**

See *The Phillips Report*, page 8:

“Poor workmanship is evidenced by the continual high rates of rejection and MRB actions which result in rework that would not be necessary if the workmanship had been good...Recognizing that overtime shifts are necessary at this time, it is our view that strong and knowledgeable supervision of these overtime shifts is necessary...NAA quality is not up to NASA required standards. This is evidenced by the large number of ‘correction’ E.O.’s and manufacturing discrepancies. This deficiency is further compounded by the large number of discrepancies that escape NAA inspectors but are detected by NASA inspectors.”

## **QC1 – Inspection/Surveillance/Audit Requirements LTA**

The requirements for quality inspections were missing or deficient.

## **IN4 – Individual Experience & Skills LTA**

This was a new program that required a very large workforce. Many of the workers were right out of high school, so their experience and skills were very limited.

In contrast, at the start-up of the SSP, the young workers had the “old Apollo guys” to mentor and train them.

## **TT4 – Accepted Team Practices LTA**

See *Thomas Barton Report*. He was a quality inspector for NAA, and he communicated quality/workmanship problems to his supervisor, but nothing happened. He documented contamination issues, poor workmanship, people sleeping and drinking on the job, etc.

**Chain 6: Issue of poor plumbing design and workmanship on the ECS – design of soldered joints in the plumbing that led to leakage of water/glycol which can corrode electrical connectors and its residue can contribute to the spread of fire – so much open work when command module was shipped to KSC**

See page 31, Finding 10: “NASA Apollo 204 Review Board – History of the Accident,” <http://history.nasa.gov/Apollo204/history.html>).

**SL7 – Internal Relationship Management LTA**

Astronauts were openly concerned with the large volume of open work and the overall reliability of the vehicle. The three astronauts posed for a crew picture with their heads bowed and their hands clasped as if in prayer because of their concerns with the vehicle's quality and integrity.

**ES4 – Technical Controls LTA**

James Webb, NASA Administrator, commented during his congressional testimony: ‘I wonder now why we ever planned to fly the Block 1 spacecraft at all. Why was it – all of them were scrubbed except this one, (Spacecraft 012/Apollo 1)?’ (The Block 1 design lacked the capability of docking with the Lunar Module.)

George Mueller, Associate Administrator for Manned Space Flight: “Well, it’s a good question. In fact if you go back, you’ll find that we almost scrubbed 012, and the reason we almost scrubbed it was that it wasn’t clear that we were going to gain enough in flying it to make it worthwhile finishing it up. I was on the side saying, ‘Well, I don’t think the forward program will be helped by the extra effort required to build this – get it built and furnished in a way that could fly – but what we ought to do is scrub it and do the next one right.’” However, Bob Gilruth and Joe Shea and the Houston people said, ‘No, we’ll learn an awful lot by moving this thing on through, even though it isn’t exactly the same configuration it clearly tests all of the equipment and all of the launch apparatus and so on, so we’ll get that out of the way – that in the long run, will save us time rather than lose us time.’” And I went along with them because it was a valid argument. We had an agreement, however, that if it was going to slip any more, more than another couple of months, that we would in fact bypass it. None of us, of course, had any idea that this would pose any danger to the crew. We all thought that the thing was perfectly safe. And in fact it had been through design certification reviews which supposedly picked up these things. And one of the things that was asked was, ‘Has this thing been examined for being fireproof?’ You’ll find in the record that there was a report prepared which said yes, it met all of the needs for fire resistance.” See pages 9 and 10, “Chapter 5” an interview with George Mueller (<http://www.apolloproject.com/sp-4223/b-ch5.htm>).

In his monograph *Project Apollo: The Tough Decisions*, Deputy Administrator Seamans wrote that NASA’s single worst mistake in engineering judgment was not to run a fire test on the command module prior to the plugs-out test. In the BBC documentary *NASA: Triumph and Tragedy*, Jim McDivitt said that NASA had no idea how a 100% oxygen atmosphere would influence burning. Similar remarks by other astronauts were expressed in the documentary *In the Shadow of the Moon* (see [http://en.wikipedia.org/wiki/Apollo\\_1](http://en.wikipedia.org/wiki/Apollo_1)).

## **TS2 – Task Technical Training LTA**

“Early in the Apollo Program, the fabrication and operations related to special processes, particularly the soldering operations, were of concern to NASA Headquarters. Because NASA as well as contractor personnel required training for these operations and techniques, soldering schools were established by NASA for the training and certification of contractor and supplier operator, inspectors, and instructors. In addition, NASA personnel were trained and certified, thereby enabling them to evaluate the contractor operations and techniques effectively.” (See “NASA Apollo Experience Report – Reliability and Quality Assurance,” 1973, NASA Technical Note TN D-7438, page 10.)

## **DS2 – System/Part Design & Development LTA**

Grissom was so frustrated by the many technical failures of the craft that he hung a lemon in the simulator. Also, the three astronauts posed for a crew picture with their heads bowed and their hands clasped together as if in prayer, because of their concerns with the spacecraft’s quality and integrity. The crew presented this parody of the crew portrait to the ASPO manager Joseph Shea on August 19, 1966, a week before the command module was shipped to Kennedy, with this inscription: “It isn’t that we don’t trust you Joe, but this time we’ve decided to go over your head” ([http://en.wikipedia.org/wiki/Apollo\\_1](http://en.wikipedia.org/wiki/Apollo_1)).

Vibration testing was not done on the flight-configured command module.

## **MW3 – System/Part Reliability or Usability LTA**

Four oxygen fires in the five years before the Apollo 1 accident were proof enough.

In fact, the decision to adopt a pure oxygen atmosphere for Apollo was vigorously debated by spacecraft manufacturers and government and academic clinicians before it was finalized by NASA as a weight-saving step. And as for object lessons, there was no shortage of them. NASA could also have taken warning from at least seven examples of oxygen-related fires in operational US testing facilities, four of which occurred between two years and nine months before the Apollo fire. Three involved unmanned tests of Apollo life support systems, at least one of which used pure oxygen at the planned cabin pressure of five pounds per square inch. The remaining four fire events took place during manned US Air Force and US Navy chamber tests in the late 1950s and 1962. Three of those were tests of cabin atmospheres planned for Mercury and Gemini, and their crews escaped with injuries ranging from smoke inhalation to first and second degree burns. The fourth, in early 1965, saw two Navy divers die in a fire in a chamber pressurized to 8.6 atmospheres. In this case, the pressure and gas combination was being investigated for use in deep ocean operations, not space flight. (These events—but not the Bondarenko fatality—and about 70 chamber fires since then are reviewed.)

That NASA failed to grasp the lessons of those fires is regrettable, but it was not unusual. Only four days after the Apollo fire, the Air Force lost two veterinary technicians in a pure oxygen chamber fire. Clearly, NASA’s own object lesson was lost on the Air Force as well. (See *The Space Review*, “Could the CIA have prevented the Apollo 1 Fire?” John Charles, January 29, 2007.)



## Appendix C. Soyuz 1 Mishap Analysis

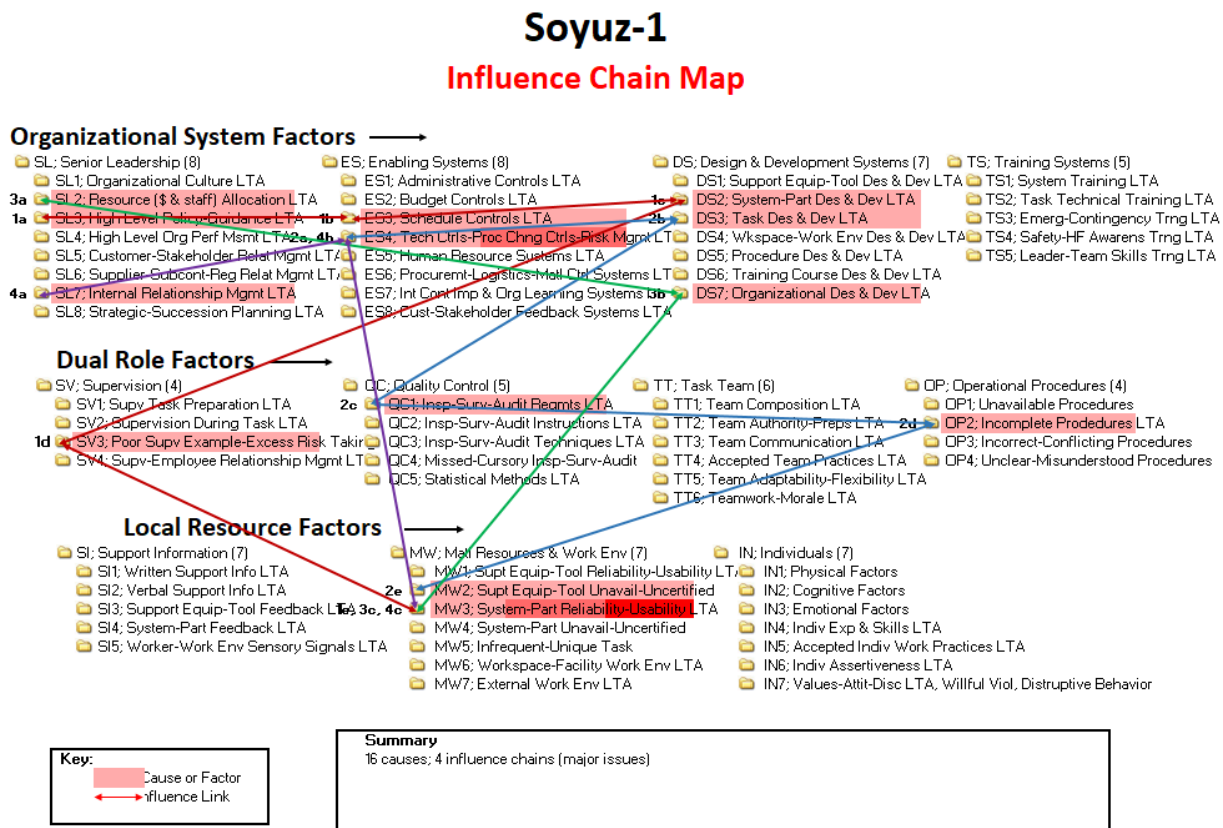
Pressured to regain the lead that Russia had lost in the “space race” and eager to launch the new Soyuz 1 spacecraft on the 50<sup>th</sup> anniversary of the Bolshevik Revolution, unusual risks were taken. In spite of more than 100 critical problems that had been identified by engineers and a series of test failures, the crewed vehicle was launched. The main and reserve parachutes failed during reentry on April 23, 1967, killing Soviet cosmonaut Vladimir Komarov and delaying the Soviet lunar program 18 months. The various influence chains for this incident are detailed in Table C-1 and displayed graphically in Figure C-1.

**Table C-1. Soyuz 1 Mishap Influence Chain Summary**

#	Description of Cause	Type
	<b>Chain #1 is about the Soviet's decision to launch the first manned Soyuz, in spite of three previous back-to-back failures with unmanned Soyuz launches.</b>	
1a	High Level Policy/Guidance. Political pressure and guidance - competition with U.S.  <i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 577: "The management of the Design Bureau knew that the vehicle had not been completely debugged: more time was needed to make it operational. But the Communist Party ordered the launch despite the fact that the preliminary launches had revealed faults in coordination, thermal control, and parachute systems. There was clearly much political pressure from Brezhnev and Ustinov to get the flight off the ground. It had been almost two years since a piloted Soviet spaceflight, while the Americans had flown ten Gemini missions. In addition, May Day, one of the most important holidays in Soviet culture, was imminent, and there was reason to believe that the Soyuz flight was timed to roughly coincide with the anniversary." (The 50th anniversary of the 1917 Bolshevik Revolution.)</i>	SL3
1b	Schedule Controls. Schedule pressure not managed properly.  <i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 573: "The pace at Tyura-Tam was intense."</i>	ES3
1c	System Design and Development. Inadequate testing of the spacecraft.  <i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 590: "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."</i>	DS2
1d	Poor Supervisor Example/Excessive Risk Taking. Inadequate pushback by supervisors on the intense schedule pressure.  <i>Excerpt from the Kamanin Diary: 1967 April 14, (10 days before the launch of Soyuz 1): "The cosmonauts are completely trained, ready for launch at any time with four hours' notice. Then Mishin calls Ustinov and tells him that their training is what is holding up the Soyuz 1 launch!"</i>	SV3
1e	System Reliability. Spacecraft reliability was LTA.  <i>From the point of view of the military quality assurance inspectors, there are 100 unresolved discrepancies on Soyuz 1 - "the spacecraft is a piece of shit."</i>	MW3
	<b>Chain #2 is about the failure of the primary parachute to deploy, which caused the backup system to malfunction.</b>	
2a	Risk Management. The failure mode of the primary parachute's malfunction of being stuck in the container, which caused a failure of the backup chute, was not accounted for in the design.  <i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 588: "Utkin's subcommission finished its work, which included some experimental analyses, by June 20 and emerged with the cause of the accident: a release failure of the container block of the primary parachute. The drag parachute itself was supposed to pull out the main parachute, but it did not do so because the latter had gotten jammed in the container. Under nominal circumstances, automated instruments on board the capsule would have detected an increase in velocity, discarded the primary drag and main parachutes, and activated the backup system. On Soyuz 1, once instruments detected the velocity increase, the capsule was unable to discard the primary chute because it was still stuck in the container. This meant that the primary drag chute was still deployed above the spacecraft. Once the single backup parachute was released, it was to have come out in the shape of a long, thin cylinder and then unfurl to its dome shape. In Komarov's case, the backup chute began to extend under the still attached drag parachute from the primary system, and it never filled with air."</i>	ES4

#	Description of Cause	Type
2b	<p>Task Design. The capsules used in the aircraft drop tests were covered with regular foam only. They did not go through the same thermal protective polymerization process that was used on the Soyuz capsules that were launched.</p> <p><i>Excerpt from <a href="http://www.russianspaceweb.com/soyuz1.html">http://www.russianspaceweb.com/soyuz1.html</a> - "After the investigative commission formally ended its work, another unofficial explanation for the parachute system failure had emerged. Boris Chertok, a key figure at OKB-1 design bureau laid out this scenario in his memoirs, and it also made it into the official history of the design bureau. According to the theory, the parachute container onboard Soyuz 1 could have been contaminated by a glue-like polymer-based thermal protection material, which is applied to the exterior of the reentry capsule. According to Chertok, first <u>unmanned</u> Soyuz capsules were placed inside a special autoclave to polymerize the thermal protective layer <u>without parachute containers</u>, whose production was behind schedule. By the time the reentry capsule of the Soyuz 1 went into the autoclave, parachute containers had been installed but their <u>covers were still unavailable</u>. As a result, Chertok hypothesized, a flight-ready parachute container on the Soyuz 1 could be protected with a <u>temporary cover</u> during the polymerization process, which could let glue-like substance to get inside." (This coating formed a rough surface, thus eventually preventing the parachute from deploying on Soyuz 1) This fatal flaw had never had a chance to manifest itself during aircraft drop tests, since the capsules used in those tests had been covered with regular foam and never had to go through the polymerization process.</i></p>	DS3
2c	<p>Inspection Requirements. No requirement to inspect the parachute container for contamination.</p> <p><i>Excerpt from: <a href="http://www.russianspaceweb.com/soyuz1.html">http://www.russianspaceweb.com/soyuz1.html</a> - After the loss of Soyuz 1, new regulations required the removal of the parachute containers from the reentry capsule, before its installation in the autoclave (for the polymerization process).</i></p>	QC1
2d	Incomplete Procedures. Procedure did not address the situation of parachute covers not being available.	OP2
2e	Support Equipment Unavailable. Parachute covers were unavailable.	MW2
<b>Chain #3 is about the Lack of Focus on the Soyuz Program</b>		
3a	<p>Resource Allocation. Resources were allocated among competing military and civilian space projects; manned spaceflight had low priority.</p> <p><i>Excerpt from Kamanin Diary: 1965 November 20 - Marshal Grechko convenes Soviet representatives to consider the issues raised by Gagarin's letter. The issues are:</i>  <i>(1) No program plan for manned flight.</i>  <i>(2) Manned flights have low priority. 30 four-stage rockets on robot missions to the moon, Mars, and Venus have been launched with virtually no scientific effect. The 8 rockets used for manned launches have had enormous impact, but this successful program has only had <u>one-quarter the allocation</u> of the unsuccessful unmanned planetary program.</i>  <i>(3) Not one new manned spacecraft has been developed in the last 5 years. Key subsystems - film and photographic equipment, spacesuits, parachutes, communication systems, and oxygen regeneration systems - have only begun preliminary tests in the last year." NOTE: 3 years later - 1968 December 26 - a year and a half after the Soyuz 1 fatality, the Soviets still had divided their attention/resources among 5 different space projects: the L1, L3, Soyuz, Soyuz VI, and Almaz. (Kamanin Diary)</i></p>	SL2
3b	<p>Organizational Design. The Soviets had multiple concurrent space projects, so their budget and resources were spread thin across these various programs. There was less emphasis on the manned programs.</p> <p><i>Excerpt from Kamanin Diary: 1965 September 8 - "Kamanin reviews a speech by President Johnson to the US Congress. From 1954-1965 the USA spent \$34 billion on space, \$26.4 billion of that in just the last four years. The Soviet Union has spent a fraction of that, but the main reason for being behind the U.S. is poor management and organization structure, in Kamanin's view."</i></p> <p><i>Excerpt from the Kamanin Diary: 1965 October 22 - Gagarin writes a letter to Brezhnev complaining of the poor organization of the Soviet space program. The letter specifically cites the multitude of space projects (5) and the de-emphasis of manned efforts.</i></p>	DS7
3c	<p>System Reliability. Parachute system was unreliable; two of seven drop tests failed.</p> <p><i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 569: "The engineers began the ground testing of the first flight model of the Soyuz spacecraft on May 12, 1966. There were many problems. Instead of the anticipated thirty days, it took four months to debug the ship. There were as many as 2,123 defects in the vehicle, significantly affecting the pace of the project. The official history of the design bureau states that the testing of the Soyuz spacecraft: Among the factors that the engineers had to face were problems with the parachute system. Serious defects were identified when two out of seven drop tests from the An-12 aircraft at Feodosiya failed. After one test on August 9, when the reserve parachute failed to open, Kamanin prophetically wrote in his diaries: One has to admit that the 7K-OK parachute system is worse than the parachute system of the Vostoks."</i></p>	MW3

#	Description of Cause	Type
	<b>Chain 4: Cosmonauts' Frustration with Vehicle Defects and being Ignored by the Hierarchy of the Ministry of Defense</b>	
4a	Internal Relationship Management. Cosmonauts' concerns were ignored by the Soviet's military hierarchy. Manned missions did not receive the same attention as the unmanned satellite programs.	SL7
4b	Risk Management/Technical Controls. There was no risk roll-up process to highlight the many defects and system test failures and make a solid case against the decision to launch. From the point of view of the military quality assurance inspectors, there are 100 unresolved discrepancies on Soyuz 1.	ES4
4c	System Reliability. The Soyuz 1 was an unreliable vehicle and was not ready to fly a manned mission.	MW3
	<b>Summary: 16 causes, 4 chains</b>	



**Figure C-1. Soyuz 1 Mishap Incident Influence Chain Map**

## **Soyuz 1 Mishap Analysis Notes**

### **Chain 1: Decision to launch**

#### **SL3 – High Level Policy/Guidance LTA**

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 570:

“The political pressure to return to flight was immense, as official TskBEM historians noted later...there was also pressure on the part of the government. Thus, Deputy Minister Litvinov personally daily in the morning carried out operative meetings in the 44<sup>th</sup> assembly shop...and signed a list of bonuses for accelerating work.”

Each of the first three unmanned Soyuz launches was a failure:

- November 28, 1966
- December 14, 1966
- February 7, 1967

In spite of these three failures, a decision was made to go ahead with the manned launch of Soyuz 1 with cosmonaut Vladimir Komarov, which was scheduled for April 23, 1967. The launch of Soyuz 2, with two cosmonauts on board, was to happen the next day to allow for an orbital rendezvous with Soyuz 1.

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 577:

“The management of the Design Bureau knew that the vehicle had not been completely debugged: more time was needed to make it operational. But the Communist Party ordered the launch despite the fact that the preliminary launches had revealed faults in coordination, thermal control, and parachute systems... There was clearly much political pressure from Brezhnev and Ustinov to get the flight off the ground. It had been almost two years since a piloted Soviet spaceflight, while the Americans had flown ten Gemini missions. In addition, May Day, one of the most important holidays in Soviet culture, was imminent, and there was reason to believe that the Soyuz flight was timed to roughly coincide with the anniversary” (i.e., the 50<sup>th</sup> anniversary of the 1917 Bolshevik Revolution).

Page 580 – “Just a week prior to the launch, on April 15, Air Force Lt. General Nikolay Kamanin wrote in his journal:

‘I am personally not fully confident that the whole program of flight will be completed successfully... In all previous flights we believed in success. Today there is not such confidence in victory’” (see <http://www.russianspaceweb.com/soyuz1.html>).

At least one Russian source names Dmitry Ustinov, a powerful member of the Soviet Politburo overseeing rocket industry, as the main force, hammering out deadline for the Soyuz 1 flight. Ustinov reportedly held numerous meetings on the issue and personally pressured Vasily Mishin, the head of the TsKBEM design bureau developing Soyuz, to fly on the eve of the Karlovy Vary summit. According to the source, Ustinov also threatened cosmonaut Vladimir Komarov, still skeptical about the Soyuz's readiness for flight, to “remove stars from his chest and shoulder straps,” unless he agrees to pilot the vehicle.

#### Last preparations

On the morning of April 14, 1967, a number of high-ranking space officials including Vasily Mishin and Boris Chertok flew to Baikonur to oversee final preparations for the first Soviet manned launch in more than two years. On the evening of the same day, at Site 2, Kerim Kerimov chaired a crowded meeting of the State Commission, which reviewed preflight processing of two Soyuz spacecraft and cleared them for fueling. Yurasov, who was in charge of prelaunch processing, reported on various aspects of the work. Next, Yurasov's associate Colonel Kirillov also spoke, pointing out hundreds of issues, which came up during tests. He concluded that vehicles are still “undercooked.” In response, Vasily Mishin went into rage and sharply told Kirillov that he “would teach him how to work.”

### **ES3 – Schedule Controls LTA**

Regarding the Soyuz schedule:

Excerpt from the book “Challenge to Apollo” by Asif A. Siddiqi, 2000, page 573: “The pace at Tyura-Tam was intense.”

### **DS2 – System/Part Design & Development LTA**

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 590:

“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. Although participants continue to deny that there was explicit pressure from Brezhnev, Ustinov, and Serbin to accomplish the flight as soon as possible, the implicit pressure had a much more imposing effect. It was not just a matter of Soviet prestige in space exploration, it was also the fact that perhaps many of the leading designers’ jobs were on the line. . . All told, the responsibility and guilt for the accident lay not on the conscience of any one person, but rather on a technological culture that considered high risks acceptable in the cause of satisfying political imperatives.”

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 573:

(Regarding the failure of the first unmanned Soyuz launch) “They found that the failures had nothing to do with design flaws but rather problems in assembling and testing that particular model on the ground.”

### **SV3 – Poor Supervisor Example or Excessive Risk Taking**

There was no pushback against the intense schedule.

### **MW3 – System/Part Reliability or Usability LTA**

Excerpt from the Kamanin Diary, April 14, 1967 - Huge blowup at Tyuratam:

“The cosmonauts are completely trained, ready for launch at any time with four hours’ notice. Then Mishin calls Ustinov and tells him that their training is what is holding up the Soyuz 1 launch! From the point of view of the military quality assurance inspectors, there are 100 unresolved discrepancies on Soyuz 1 - the spacecraft is a piece of shit.”

### **Chain 2: Failure of the primary parachute to deploy – which caused the backup system to malfunction**

### **ES4 – Technical Controls/Process Change Controls/Risk Management LTA**

The failure mode of the primary parachute’s malfunction of being stuck in the container, which caused a failure of the backup parachute, was not accounted for.

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 588:

“Utkin’s subcommission finished its work, which included some experimental analyses, by June 20 and emerged with the cause of the accident: a release failure of the container block of the primary parachute. . . The drag parachute itself was supposed to pull out the main parachute, but it did not do so because the latter had gotten jammed in the container. Under nominal circumstances, automated instruments on board the capsule would have detected an increase in velocity, discarded the primary drag and main parachutes, and activated the backup system.

On Soyuz -1, once instruments detected the velocity increase, the capsule was unable to discard the primary chute because it was still stuck in the container. This meant that the primary drag chute was still deployed above the spacecraft. Once the single backup parachute was released, it was to have come out in the shape of a long, thin cylinder and then unfurl to its dome shape. In Komarov's case, the backup chute began to extend under the still attached drag parachute from the primary system, and it never filled with air."

### **DS3 – Task Design & Development LTA**

The capsules used in the aircraft drop tests were covered with regular foam only. They did not go through the same thermal protective polymerization process that was used on the Soyuz capsules that were launched.

Excerpt from <http://www.russianspaceweb.com/soyuz1.html>:

"After the investigative commission formally ended its work, another unofficial explanation for the parachute system failure had emerged. Boris Chertok, a key figure at OKB-1 design bureau laid out this scenario in his memoirs, and it also made it into the official history of the design bureau.

According to the theory, the parachute container onboard Soyuz 1 could've been contaminated by a glue-like polymer-based thermal protection material, which is applied to the exterior of the reentry capsule. According to Chertok, first unmanned Soyuz capsules were placed inside a special autoclave to polymerize the thermal protective layer without parachute containers, whose production was behind schedule.

By the time the reentry capsule of the Soyuz 1 went into the autoclave, parachute containers had been installed but their covers were still unavailable. As a result, Chertok hypothesized, a flight-ready parachute container on the Soyuz 1 could be protected with a temporary cover during the polymerization process, which could let glue-like substance to get inside.

(This coating formed a rough surface, thus eventually preventing the parachute from deploying on Soyuz 1. See *Challenge to Apollo*, page 589.)

A fatal flaw had never had a chance to manifest itself during aircraft drop tests, since the capsules used in those tests had been covered with regular foam and never had to go through the polymerization process."

### **QC1 – Inspection/Surveillance/Audit Requirements LTA**

Excerpt from <http://www.russianspaceweb.com/soyuz1.html>:

"After the loss of Soyuz 1, new regulations required the removal of parachute containers from the reentry capsule, before its installation in the autoclave (for the polymerization process)."

### **OP2 – Incomplete Procedures**

Procedure did not address the situation of parachute covers not being available.

### **MW2 – Support Equipment/Tool Unavailable or Uncertified**

Parachute covers were unavailable.

### **Chain 3: Lack of focus on Soyuz Program**

#### **SL2 – Resource (Money and Staff) Allocation LTA**

Excerpt from the Kamanin Diary: October 22, 1965 - Gagarin writes a letter to Brezhnev:

“Gagarin has sent a letter to Brezhnev, complaining of the poor organization of the Soviet space program. The Kremlin has received it... reaction is awaited. The letter specifically cites the multitude of space projects and de-emphasis of manned efforts.”

#### **Text of Gagarin's Letter to Brezhnev:**

Central Committee of the Communist Party of the Soviet Union  
Comrade L.I. Brezhnev

Dear Leonid Il'ich!

We are writing to you to raise certain issues, which we consider very important for our state and for us.

Soviet achievements in space exploration are well-known, and there is no need to list all of our victories here. These victories have been achieved and will remain in history to be the pride of our nation forever. The people, the Party, and our leaders have always appropriately connected our achievements in space with our achievements in the construction of socialism. “Socialism is the best launching pad for space flights.” This catch phrase circled the entire world. Soviet people said these words with pride, the peoples of the socialist countries believed it was true, and hundreds of millions of people abroad learned the ABC of communism through our achievements in space. Such it was. We, cosmonauts, traveled abroad many times; a thousand times we witnessed how warmly multi-million crowds in various countries greeted Soviet achievements in space.

In the past year, however, the situation has changed. The USA have not only caught up with us, but even surpassed us in certain areas. The flights of space vehicles Ranger-7, Ranger-8, Mariner-4, Gemini-5, and others are serious achievements of American scientists.

This lagging behind of our homeland in space exploration is especially objectionable to us, cosmonauts, but it also damages the prestige of the Soviet Union and has a negative effect on the defense efforts of the countries from the socialist camp.

Why is the Soviet Union losing its leading position in space research? A common answer to this question answer is as follows: the USA have developed a very wide front of research in space; they allocate enormous funds for space research. In the past 5 years they spent more than 20 billion dollars, and in 1965 alone 7 billion dollars. This answer is basically correct. It is well known that the USA spend on space exploration much more than does the USSR.

But the matter is not only funding. The Soviet Union also allocates significant funds for space exploration. Unfortunately, in our country there are many defects in planning, organization, and management of this work. How can one speak about serious planning of space research if we do not have any plan for cosmonauts' flights? The month of October is coming to an end, there is a little time left before the end of the year 1965, but no one in Soviet Union knows whether there will be a manned space flight this year, what will be the task for that flight, and what duration. The same situation was characteristic of all the previous flights of the ship-satellites Vostok and

Voskhod. This creates totally abnormal conditions during cosmonauts' preparation for flight and precludes the possibility of preparing crews for flight without hassle ahead of time.

We know that in this country there are plans for developing space technology, we know decisions of the Central Committee of the CPSU and the government that include specific deadlines for the construction of spacecrafts. But we know also that many of these decisions are not being implemented at all, and most are being carried out with huge delays.

Manned space flights are becoming more and more complex and prolonged. The preparation of such flights takes a lot of time, requires special equipment, training spacecraft, and simulators, which are now being created with huge delay and with primitive methods. To put it briefly, we need a national plan of manned space flights which would include the flight task, the date, the composition of the crew, the duration of the flight, the deadline for the preparation of a spacecraft and a simulator, and many other important issues of flight preparation.

Up to now manned space flights have been carried out according to the plans of the USSR Academy of Sciences, while the direct management and technical support have been organized by representatives of the industry and the USSR Ministry of Defense. Items of military significance have been present in flight programs only to some degree, which can be explained by the fact that within the Ministry of Defense there is no organization that would unify the whole complex of questions of space exploration. Everybody is involved in space affairs - the Missile Forces, the Air Force, the Air Defense, the Navy, and other organizations. Such scattering of efforts and resources in space exploration interferes with work; a lot of time is spent on coordination of plans and decisions, and these decisions often reflect narrow departmental interests. The existing situation with the organization of space research contradicts the spirit of the decisions of the September Plenum of the Central Committee of the CPSU, and it must be changed.

In 1964 the chief of the Joint Staff, the Marshal of the Soviet Union Biriuzov created a special commission. This commission studied in detail the organization of work on space exploration and came to the conclusion that it was necessary to unify all space affairs under the command of the Air Force. The Marshal of Soviet Union, the General of the Army, and the Marshal of the Soviet Union supported this proposal. But after the tragic death of the Marshal of the Soviet Union this reasonable proposal was discarded and the Central Administration for Space Exploration (TsUKOS) was organized under the Missile Forces. The creation of this organization changed nothing, however. The narrow departmental approach, the scattering of resources, and the lack of coordination have persisted.

The Air Force leadership and we, cosmonauts, repeatedly addressed the Joint Staff, to the Minister of Defense, and to the Military-Industrial Commission with specific proposals on the construction of and the equipment for spacecrafts that would be capable of carrying out military tasks. As a rule, our proposals were not supported by the Missile Forces leadership. We received such replies as: "Vostok spacecraft do not have any military value, and it is inexpedient to order their construction" and "We will not order Voskhod spacecraft, for there are no funds."

- In 1961 we flew two Vostok spacecraft.
- In 1962 we flew two Vostok spacecraft.
- In 1963 we flew two Vostok spacecraft.
- In 1964 we flew one Voskhod spacecraft.



- In 1965 we flew one Voskhod spacecraft.

In 1965 the Americans launched three Gemini spacecraft, and they are planning to launch two more before the end of the year.

Why have not been enough ships built for our cosmonauts' flights? In any case, not because of the lack of funding. It happened because the leadership of the Missile Forces has more trust in automatic satellites, and it underestimates the role of human beings in space research. It is a shame that in our country, which was the first to send man into outer space, for four years the question has been debated whether man is needed on board a military spacecraft. In America this question has been resolved firmly and conclusively in favor of man. In this country, many still argue for automata. Only these considerations can explain why we build only 1-2 piloted ships in the same period as 30-40 automatic satellites are being produced. Many automatic satellites cost much more than a piloted ship, and many of them never reach their destination. The Vostok and the Voskhod piloted spacecraft have carried out a full program of scientific research and at the same time have produced a huge political effect for this country.

We do not intend to belittle the value of automatic spacecraft. But an infatuation with them would be, at the very least, harmful. Using the Vostok and the Voskhod spacecraft, it would have been possible to carry out a large complex of very important military research and to extend the duration of flights to 10-12 days. But we have no ships, nothing on which we could fly, nothing on which we could carry out a program of space research.

Besides what is stated above, there are also other defects in the organization of our flights - defects which we cannot remedy by ourselves. In our country there is no unified center for space flight control. During the flight every spacecraft has no communication with the command station in between the sixth and the thirteenth turn circuits of the day. At the testing range, there are bad conditions for training and resting of cosmonauts.

We also have other questions awaiting a resolution. Many questions could be resolved without appealing to the Central Committee of the CPSU. We repeatedly wrote to the Minister of Defense about these questions. We are aware of the petitions from the Air Force leadership to the Ministry of Defense and the government, but these petitions largely did not fulfill their purpose. Many times we met with the Minister of Defense, but unfortunately those were not business meetings. And today we have no confidence that the issues we raise can be resolved at the Ministry of Defense.

Dear Leonid Il'ich! We know how busy you are and nevertheless we ask you to familiarize yourself with our space affairs and needs.

The 50th anniversary of the Great October Revolution is approaching. We would like very much to achieve new big victories in space by the time of this great holiday.

We are deeply convinced that resolving the issue of unifying all military space affairs under the command of the Air Force, the thoughtful planning of space research, and the construction of spacecraft that would solve the problem of military application of piloted spacecraft would appreciably strengthen the defensive power of our homeland.

Pilots-cosmonauts of the USSR

- Yu. Gagarin
- A. Leonov

- P. Belyaev
- G. Titov
- A. Nikolaev
- V. Bykovsky

Excerpt from Kamanin Diary: November 1, 1965 - Soviets losing space race:

“Brezhnev has not yet had even one hour to glance at Gagarin's letter. Kamanin and the cosmonauts are frustrated - the country has the means - the rockets, the spacecraft designs - to be beating the Americans, but nothing is done due to zero planning, poor organization and management. Korolev still talks about flying a Voskhod in November, but the equipment for the artificial gravity experiment or the 3KD spacecraft for the EVA have been completed. Kamanin hears from Tsybin that Korolev is considering abandoning the Voskhod flights completely so that OKB-1 can concentrate on completing development of the Soyuz.”

Excerpt from Kamanin Diary, November 20, 1965 - Military-Technical Soviet of the Ministry of Defense:

“Marshal Grechko convenes the Soviet to consider the issues raised by Gagarin's letter. Representatives from the PVO, VVS, RVSN, and the NTK attend. Problems in the space program and the loss of the lead in the space race to the Americans are blamed on the Academy of Sciences and the design bureau and factories - none dare risk blaming poor management and support by the Ministry of Defense. The issues seen are:

- No program plan for manned flight.
- Manned flights have low priority. Keldysh and Korolev have launched 30 four-stage rockets on robot missions to the moon, Mars, and Venus, with virtually no publicity or scientific effect. The eight rockets used for manned launches have had enormous impact, but this successful program has only had one quarter the allocation of the spectacularly unsuccessful unmanned planetary program.
- Not one new manned spacecraft has been developed in the last five years. Key subsystems (e.g., film and photographic equipment, spacesuits, parachutes, communications systems, and oxygen regeneration systems) had only begun preliminary tests in the prior year.

There is no high-level support for moving space activities away from what Kamanin calls ‘the artillery people’ - it is known that Ustinov has made his career in building up the RVSN, and he is not about to criticize them.”

3 years later:

Excerpt from Kamanin Diary, December 26, 1968 - Heated arguments over technical approach of Soviet space systems:

“The Americans worked only on the Apollo spacecraft for the last two to three years, while the Soviets have divided their efforts on no less than five spacecraft types: the L1, L3, Soyuz, Soyuz VI, and Almaz. This is all Mishin's fault...”

## **DS7 – Organizational Design and Development LTA**

The Soviets had multiple concurrent space projects, so their budget and resources were spread thin across these various programs. There was less emphasis on the manned programs.

Excerpt from Kamanin Diary, September 8, 1965 - American versus Soviet programs:

Kamanin reviews a speech by President Johnson to the US Congress. From 1954 to 1965, the USA spent 34 billion dollars on space, \$ 26.4 billion of that in just the last four years. The Soviet Union has spent a fraction of that, but the main reason for being behind the US is poor management and organization structure, in Kamanin's view.

## **MW3 – System/Part Reliability or Usability LTA**

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 569:

“The engineers began the ground testing of the first flight model of the Soyuz spacecraft on May 12, 1966. There were many problems. Instead of the anticipated thirty days, it took four months to debug the ship. There were as many as 2,123 defects in the vehicle, significantly affecting the pace of the project. The official history of the design bureau states that the testing of the Soyuz spacecraft:

Among the factors that the engineers had to face were problems with the parachute system. Serious defects were identified when two out of seven drop tests from the An-12 aircraft at Feodosiya failed. After one test on August 9, when the reserve parachute failed to open, Kamanin prophetically wrote in his diaries:

*‘One has to admit that the 7K-OK parachute system is worse than the parachute system of the Vostoks.’”*

Excerpt from the Kamanin Diary – February 2, 1966, regarding the Voskhod parachute system:

“Smirnov again questions the chief designers about the reliability of the parachute systems developed by Tkachev. The VVS remains troubled as to the reliability of these systems.”

Excerpt from the book *Challenge to Apollo* by Asif A. Siddiqi, 2000, page 590:

“Two parachute testing failures following Soyuz 1 apparently sealed his fate. Tkachev was fired from his job in 1968, ending his role in designing the parachute systems for Vostok, Voskhod, Zenit, Soyuz, and many other Soviet spacecraft of the era.”

Excerpt from Kamanin Diary, May 15, 1967 - Soyuz parachute test results.

“In the first drop, the reserve parachute didn't open. In the second test, it did inflate, but only after a delay of twenty seconds. TsAGI studies show the drogue chute is creating an area of turbulence in the wake of the capsule, and the reserve chute is deploying right into that zone of chaotic air, preventing it from inflating. Tests on the parachute show that while it was designed to deploy with 1.8 tonnes of drag force from the drogue chute, it requires 3-4 tonnes of force to pull the packed parachute out of the container and allow parachute deployment. The parachute fails at 8 tonne load. The Soyuz parachute system is supposed to have a reliability of 95%...and this essential problem was unknown...”

Excerpt from Kamanin Diary: May 20, 1967 - LII Soyuz parachute findings:

“LII's recommended changes:

- Remove the reserve parachute and have a system of two main parachutes, with landing possible even if one of the main chutes does not deploy.
- Develop through extensive testing reliable inflation of the drogue chute.
- Add controls to allow manual parachute deployment by the crew, with appropriate cockpit instruments.
- Increase the jettison time of the heat shield from 60.7 seconds to 100 seconds after parachute deployment to allow the full interval for operation of the automatic landing system.”

#### **Chain 4: Cosmonauts’ frustration with vehicle defects and being ignored by the Ministry of Defense**

##### **SL7 – Internal Relationship Management LTA**

Cosmonauts’ concerns were ignored by the Soviet’s military hierarchy. Manned missions did not receive the same attention as the unmanned satellite programs.

##### **ES4 – Technical Controls/Risk Management LTA**

There was no risk roll-up process to highlight all the many defects and system test failures and make a case against the decision to launch.

##### **MW3 – System/Part Reliability or Usability**

The Soyuz 1 was an unreliable vehicle and should not have flown a manned mission (see <http://www.astronautix.com/articles/kamaries.htm>).

Excerpt from Kamanin Diary: Introduction:

“Nikolai Petrovich Kamanin headed the Soviet cosmonaut corps from 1960 to 1971. His diaries are a key documentary source for the history of the Soviet space program. They remained secret during the life of the Soviet Union. The first volume was only published in 1995, thirteen years after Kamanin's death. They portray a man engaged in a constant struggle with an indifferent hierarchy for an expansion of air force military operations into space. He blamed Soviet loss of the space race after 1966 to the unwillingness of Soviet engineers to let the cosmonauts actively control their spacecraft (as was the American practice). A good Communist and a bit of a martinet, he was scathing in his critiques of the unfocused Soviet leadership of the space program and especially the failings of Korolev's successor, Mishin.”

## Appendix D. Skylab 1 Mishap Analysis

A shield designed to protect the lab from micrometeoroids was damaged when it came loose during launch on May 14, 1973. It was not securely stowed during ground processing. This prevented the deployment of one of the solar panels and damaged an interstage adapter on the Saturn V launch vehicle. The various influence chains for this incident are detailed in Table D-1 and displayed graphically in Figure D-1.

**Table D-1. Skylab 1 Mishap Influence Chain Summary**

#	Description of Cause	Type
	<b>Chain #1: Aerodynamic loads during launch were not accounted for during the design of the MS. Design issues within the MS system.</b>	
1a	<p>Technical Controls: Failure to recognize the significance of the aerodynamic loads during launch on the MS during multiple design and milestone reviews.</p> <p><i>There was no shortage of reviews and yet, a major omission occurred throughout the process – consideration of aerodynamic loads on the meteoroid shield during the launch phase of the mission. Throughout the six-year period of progressive reviews and certifications . . . never did the matter of aerodynamic loads on the shield or aeroelastic interaction between the shield and its external pressure environment during launch receive the attention and understanding during the design and review process which in retrospect it deserved.[ref page 9-3]</i></p>	ES4
1b	<p>Organizational Design and Development. Absence of a designated project or chief engineer for the MS. Organizationally, the meteoroid shield 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. ((10 – 2) page 142)</p> <p>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. ((10 – 4), page 144)</p> <p>Today's organizations seldom include the old-fashioned "chief engineer" who, relatively devoid of administrative or managerial duties, brings his total experience and spends most of his time in the subtle integration of all elements of the system under his purview. Perhaps we should more actively seek and utilize these talented individuals in an engineering organization. (page 10-4)</p> <p>Positive steps must always be taken to assure that engineers become familiar with hardware, develop an intuitive understanding of computer-developed results, and make productive use of flight data in this learning process. The experienced "chief engineer," who can spend most of his time in the subtle integration of all elements of the system under his purview, free of administrative and managerial duties, can also be a major asset to an engineering organization. (page ix)</p>	DS7
1c	<p>Team Communication. Inadequate communication between discipline experts during the MS design.</p> <p><i>The venting analysis for the tunnel was predicated on a completely sealed aft end. The openings in the aft end of the tunnel thus resulted from a failure to communicate this critical design feature among aerodynamics, structural design, and manufacturing personnel. ((10 – 1), page 141)</i></p>	TT3
1d	System-Part Reliability/Usability LTA. The MS, as designed, built, and assembled, was not a reliable system.	MW3
	<b>Chain #2: The significance of the MS "tight to the tank" design requirement was not well understood by designers and ground crews (technicians, quality inspectors, ops engineers).</b>	
2a	<p>Technical Controls. It was a false presumption that the shield would be "tight to the tank" and "structurally integral with the S-IVB tank" as set forth in the design criteria.</p> <p><i>8. The failure to recognize many of these marginal design features through six years of analysis, design and test was due, in part, to a presumption that the meteoroid shield would be "tight to the tank" and "structurally integral with the S-IVB tank" as set forth in the design criteria.</i></p> <p><i>The most probable cause of the failure of the meteoroid shield was internal pressurization of its auxiliary tunnel. This internal pressurization acted to force the forward end of the tunnel and meteoroid shield away from the OWS and into the supersonic air stream. The resulting forces tore the meteoroid shield from the OWS. The pressurization of the auxiliary tunnel resulted from the admission of high pressure air into the tunnel through several openings in the aft end. These openings were: (1) an imperfect fit of the tunnel with the aft fairing; (2) an open boot seal between the tunnel and the tank surface; and (3) open stringers on the aft skirt under the tunnel. ((10 – 1), page 141)</i></p>	ES4
2b	System Training. The technicians, quality inspectors, and engineers were unaware of the lack of tight fit and its potential consequences to the mission.	TS1
2c	System-Part Feedback. There was no system feedback (such as a visual cue) to the technicians, quality inspectors, and engineers that a "tight fit" had not been achieved during rigging.	SI4

#	Description of Cause	Type
2d	Cognitive Factors. Those who processed the meteoroid shield were not aware of the need for the shield to be "tight to the tank" to achieve proper venting.	IN2
	<b>Chain #3: The MS rigging task design did not enable the ground crew to achieve the needed "tight fit." The rigging task could not meet what the design required.</b>	
3a	Task Design and Development LTA. The meteoroid shield was very difficult to rig to the tank. Some gaps undoubtedly existed between the forward and aft ends of the shield and the tank walls at the time of launch, which could have increased as the flight progressed due to the non-uniform growth of the tank.  <i>The major difficulty experienced with the meteoroid shield was in getting it stowed and rigged on the OWS. Handling such a large, lightweight structure proved difficult, requiring the coordinated action of a large group of technicians, and considerable adjustments to the assembly of the various panels were necessary in an effort to obtain a snug fit between the shield and the OWS wall. ((5-6) page 93)</i>	DS3
3b	Inspection Requirements LTA. Quality inspections were absent or inadequate; they did not identify the "tight fit" issue during ground processing.	QC1
3c	Incomplete/Unclear Procedures. The MS rigging procedures at KSC were based on the STA shield at MSFC, which was different from the flight MS in four significant aspects. These differences were not adequately accounted for in the KSC procedures, so troubleshooting and several additional tasks were needed to complete the MS rigging.  <i>The rigging procedure that was to be used at KSC was developed jointly by MSFC and MDAC using the STA at MSFC. The STA shield was, however, different from the flight MS in four significant aspects. On the flight MS: (1) the double butterfly hinges on the SAS 1 side of the main tunnel were bonded to the tension straps while on the STA they were present but unbonded; (2) the butterfly hinges on each side of the main tunnel were cut in the middle of a longitudinal joint and refitted to the adjacent panels at a slight angle as mentioned earlier. The longitudinal edges of the panels were also modified to suit the altered hinge line. This change to the flight MS at MDAC was necessary to accommodate the misalignment which occurred in the location of the tension straps on the OWS; (3) a longitudinal misplacement of the tension straps of 0.15 inch too high also resulted in some binding of the forward weather seal and torsion rods that had to be refitted at KSC; and (4) the trunnion bolts, nuts and washers were initially not lubricated on either the flight MS or the STA. This lack of lubrication caused difficulties in the final rigging of the shield at KSC, which was subsequently corrected by applying a solid film lubricant. ((5-7), page 94)</i>	OP2
3d	Infrequent/Unique Task. This was a "one-of" task that had not been performed during the Apollo missions.	MW5
	<b>Chain #4: Inadequate understanding/modeling/analysis of system interfaces; cross-system issues.</b>	
4a	Risk Management. Inadequate fault trees/failure modes and effects analysis. As a consequence of the meteoroid shield break-up and loss, there was 1) a failure of full deployment of the SAS-2 wing and 2) a failure of the S-II interstage adapter to separate in flight. The effect of one system failure had consequences for the proper functioning of other related systems.  <i>SAS-2 wing An analysis of the impingement forces on the wing was made and compared to the force required to produce the observed vehicle motion. This comparison provides a reasonable fit for the first 50 to 60 degrees of wing rotation as shown in figure 3-13. At 593.4 seconds the wing imparted momentum to the vehicle, probably by hitting and breaking the 90 degree fully deployed stops and at 593.9 imparted a final kick as it tore completely free at the hinge link. In-orbit photographs show clearly the hinge separation plane and the various wires which were torn loose at the interface ((3-4 p. 37) As a consequence of the meteoroid shield failure at approximately 63 seconds, the SAS-2 wing was unlatched and partially deployed as evidenced by minor variations in the main solar array system electrical voltages and SAS-2 temperatures. Full deployment was prevented due to the aerodynamic forces and accelerations during the remainder of powered flight. (Readings, page 186) S-II interstage adapter separation...the increasing temperatures after the time of normal S-II interstage separation are indicative of an abnormal condition. More detailed investigation based on performance evaluation and axial acceleration time history revealed that the interstage had not been jettisoned; however, due to the vehicle performance characteristics and performance margin, the desired orbit was achieved. (Readings.. page 108-187) A review of the history of manufacturing, acceptance, checkout, qualification and flight environment revealed no basic cause for failure. The most probable cause is secondary damage as a result of the meteoroid shield failure, attributed to falling debris as evidenced by the various shock and acoustic disturbances occurring in the 63-second time period.</i>	ES4
4b	System Part Design and Development LTA. Inadequate testing and verification of system interfaces. In addition to considering the MS as a system, the consideration of the MS as a part of other systems was not fully appreciated, increasing the brittleness of the OWS system.  <i>No deployment tests were conducted under vacuum conditions, which is quite acceptable in view of the low rate of motion of the deployment. Vibration, acoustic, and flutter tests were specifically omitted in the test specifications because of the design requirement that the shield be "tight to the tank." This design requirement</i>	DS2

#	Description of Cause	Type
	<p>and pervading philosophy of design and development also served to omit all aerodynamic tests of the meteoroid shield.</p> <p>12. Given the basic view that the meteoroid shield was to be completely in contact with and perform as structurally integral with the S-IVB tank, the testing emphasis on ordnance performance and shield deployment was appropriate. ((10-3) page 143)</p> <p>The redundant mode of ordnance operation of all prior Saturn flights in which both ends of the linear shaped charge are fired at once from a single command would probably have prevented the failure, depending on the extent of damage experienced by the linear shaped charge. (Readings in Systems Engineering, page 186)</p>	
4c	<p>Accepted Team Practices. In spite of 6 years of analysis, design and testing, there was a failure to recognize other marginal aspects of the design of the meteoroid shield which, when taken together, could also result in failure during launch. Engineers were not familiar with the subtle integration and interface issues of all elements of the system.</p> <p>Finding 11. No evidence was found to indicate that the design, development and testing of the meteoroid shield were compromised by limitations of funds or time. The quality of workmanship applied to the MS was adequate for its intended purpose.</p> <p>Finding 13. Engineering and management personnel on Skylab, on the part of both contractor and government, were available from the prior Saturn development and were highly experienced and adequate in number. ((10-3) page 143)</p>	TT4
4d	System-Part Reliability/Usability LTA. The MS, as designed, built, and assembled was not a reliable system.	MW3
	<b>Summary: 16 causes, 4 chains</b>	

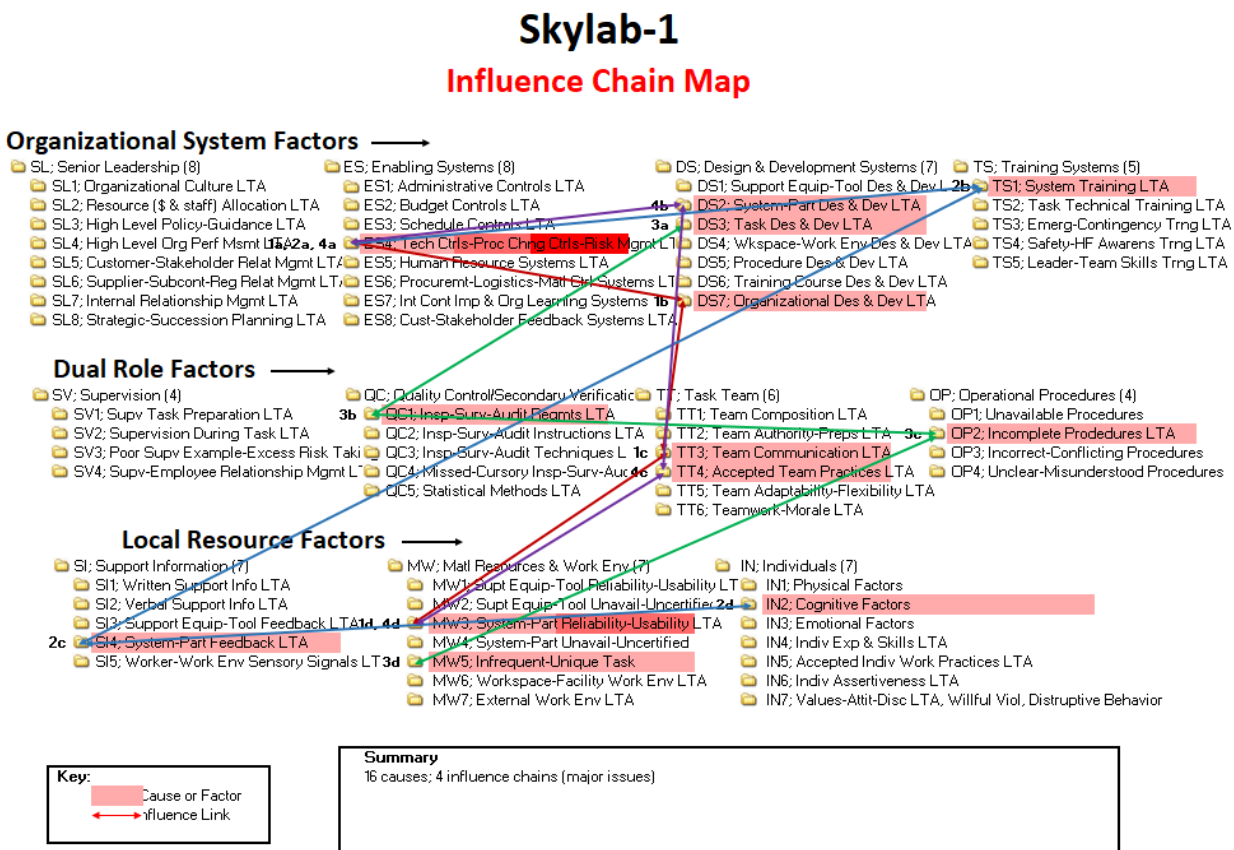


Figure D-1. Skylab 1 Mishap Incident Influence Chain Map

## **Skylab 1 Mishap**

### **Analysis Notes**

**Chain 1 Issue: Aerodynamic loads during launch were not accounted for during design of the MS; design issues within the MS system**

#### **ES4 – Technical Controls LTA**

Failure to recognize the significance of the aerodynamic loads during launch on the MS during multiple design and milestone reviews.

The internal pressurization of the meteoroid shield's auxiliary tunnel acted to force the forward end of the meteoroid shield away from the shell of the workshop and into the supersonic air stream. The pressurization of the auxiliary tunnel was due to the existence of several openings in the aft region of the tunnel.

There were no shortage of reviews...and yet, a major omission occurred throughout the process – consideration of aerodynamic loads on the meteoroid shield during the launch phase of the mission. Throughout the six-year period of progressive reviews and certifications...never did the matter of aerodynamic loads on the shield or aeroelastic interaction between the shield and its external pressure environment during launch receive the attention and understanding during the design and review process which in retrospect it deserved. (page 9-3)

#### **DS7 – Organizational Design and Development**

Absence of a designated project or systems engineer for the MS.

Organizationally, the meteoroid shield 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. ((10 – 2) page 142)

Complex, multidisciplinary 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. ((10 – 4), page 144)

View of the meteoroid shield as a piece of structure, rather than as a complex system involving several different technical disciplines. Complex, multidisciplinary 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.

Absence of sound engineering judgment and alert engineering leadership regarding the significance of the aerodynamic loads on the meteoroid.

#### **TT3 – Team Communication LTA**

Inadequate communication between discipline experts during the MS design.

The venting analysis for the tunnel was predicated on a completely sealed aft end. The openings in the aft end of the tunnel thus resulted from a failure to communicate this critical design feature among aerodynamics, structural design, and manufacturing personnel. ((10 – 1), page 141)

Failure of communication among aerodynamics, structural design, and manufacturing personnel. Failure to communicate within the project the critical nature of its proper venting.



### **MW3 – System/Part Reliability or Usability LTA**

The MS, as designed, built, and assembled, was not a reliable system.

**Chain 2 Issue: The significance of MS “tight to the tank” design requirement was not well understood by designers and ground crews (technicians, quality inspectors, operations engineers)**

### **ES4 – Technical Controls LTA**

It was a false presumption that the shield would be “tight to the tank” and “structurally integral with the S-IVB tank” as set forth in the design criteria.

8. The failure to recognize many of these marginal design features through six years of analysis, design and test was due, in part, to a presumption that the meteoroid shield would be “tight to the tank” and “structurally integral with the S-IVB tank” as set forth in the design criteria.

The most probable cause of the failure of the meteoroid shield was internal pressurization of its auxiliary tunnel. This internal pressurization acted to force the forward end of the tunnel and meteoroid shield away from the OWS and into the supersonic air stream. The resulting forces tore the meteoroid shield from the OWS...The pressurization of the auxiliary tunnel resulted from the admission of high-pressure air into the tunnel through several openings in the aft end. These openings were: (1) an imperfect fit of the tunnel with the aft fairing; (2) an open boot seal between the tunnel and the tank surface; and (3) open stringers on the aft skirt under the tunnel. ((10 – 1), page 141)

There followed a submittal of design criteria for the MS by MSFC stating, among other things, that it “shall be designed as a structurally integrated part of stage 209 capable of withstanding the dynamic forces imposed during the orbital workshop mission” and that “the weight of the bumper system shall be a primary design consideration.” Protection from meteoroid penetration with a probability of 0.9950 of no penetration for a 12-month mission was also specified. ((5 – 1), page 88)

### **TS1 – System Training LTA**

The technicians, quality inspectors, and engineers were unaware of the lack of tight fit and its potential consequences to the mission.

### **SI4 – System/Part Feedback LTA**

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.

### **IN2 – Cognitive Factors**

Those who processed the meteorite shield were not aware of the need for the shield to be “tight to the tank” to achieve proper venting.

Since there was not a project/chief engineer who was familiar with the hardware and hardware processing environment, and since the design review process did not emphasize how essential it was for the shield to be “tight to the tank” nor the critical nature of the venting, how else could the team members obtained this necessary information?

**Chain 3 Issue: The MS rigging task design did not enable the ground crew to achieve the needed tight fit; the rigging task could not meet what the design required**

### **DS3 – Task Design and Development LTA**

The meteoroid shield was very difficult to rig to the tank. Some gaps undoubtedly existed between the forward and aft ends of the shield and the tank walls at the time of launch, which could have increased as the flight progressed due to the non-uniform growth of the tank. The major difficulty experienced with the meteoroid shield was in getting it stowed and rigged on the OWS. Handling such a large, lightweight structure proved difficult, requiring the coordinated action of a large group of technicians, and considerable adjustments to the assembly of the various panels were necessary in an effort to obtain a snug fit between the shield and the OWS wall. ((5 – 6), page 93)

In practice, the meteoroid shield was a large, flexible, limp system that proved difficult to rig to the tank and to obtain the close fit that was presumed by the design. Given the realities of ground processing, the MS design did not allow the rigging to meet design requirements.

Note: This disconnect between the design's intent and the difficulty of rigging the hardware is similar to the STS-95 incident when the drag-chute door fell off. The drag chute door was incredibly difficult to rig, and as it turned out, the shear pins holding the door on were not strong enough for the design environment.

### **QC1 – Inspection Requirements LTA**

Quality inspections were absent or inadequate; they did not identify the “tight fit” issue during ground processing.

### **OP2 - Incomplete Procedures**

The MS rigging procedures at KSC were based on the STA shield at MSFC, which was different from the flight MS in four significant aspects. These differences were not adequately accounted for in the KSC procedures, so troubleshooting and several additional tasks were needed to complete the MS rigging.

The rigging procedure that was to be used at KSC was developed jointly by MSFC and MDAC using the STA at MSFC. The STA shield was, however, different from the flight MS in four significant aspects. On the flight MS: (1) the double butterfly hinges on the SAS 1 side of the main tunnel were bonded to the tension straps while on the STA they were present but unbonded; (2) the butterfly hinges on each side of the main tunnel were cut in the middle of a longitudinal joint and refitted to the adjacent panels at a slight angle as mentioned earlier. The longitudinal edges of the panels were also modified to suit the altered hinge line. This change to the flight MS at MDAC was necessary to accommodate the misalignment which occurred in the location of the tension straps on the OWS; (3) a longitudinal misplacement of the tension straps of 0.15 inch too high also resulted in some binding of the forward weather seal and torsion rods that had to be refitted at KSC; and (4) the trunnion bolts, nuts and washers were initially not lubricated on either the flight MS or the STA. This lack of lubrication caused difficulties in the final rigging of the shield at KSC, which was subsequently corrected by applying a solid film lubricant. ((5 – 7), page 94)

## **MW5 – Infrequent/Unique Task**

This was a “one-of” task that had not been performed during the Apollo missions.

### **Chain 4 Issue: Inadequate understanding/modeling/analysis of system interfaces and cross-system issues**

#### **ES4. Technical Controls/Risk Management LTA**

Inadequate fault trees/failure modes and effects analysis.

- The proximity of the MS forward reinforcing angle to the air stream.
- The existence of gaps between the OWS and the forward ends of the MS.
- The light spring force of the auxiliary tunnel frames.
- The aerodynamic crushing loads on the auxiliary tunnel frames in flight.
- The action of the torsion-bar actuated swing links applying an outward radial force to the MS.
- The inherent longitudinal flexibility of the shield assembly.
- The non-uniform expansion of the OWS tank when pressurized.
- The inherent difficulty in rigging for flight and associated uncertain tension loads in the shield. ((10 – 1, 2) pages 141-142)

Fault tree modeling. As a consequence of the meteoroid shield breakup and loss, there was 1) a failure of full deployment of the SAS-2 wing and 2) a failure of the S-II interstage adapter to separate in flight. The effect of one system failure has consequences for the proper functioning of other related systems.

When considering the MS as a system among other systems in the OWS, a consideration of one system failure should be considered with respect to its effect on others.

#### **SAS-2 Wing**

An analysis of the impingement forces on the wing was made and compared with the force required to produce the observed vehicle motion. This comparison provides a reasonable fit for the first 50 to 60 degrees of wing rotation as shown in figure 3-13. At 593.4 seconds, the wing imparted momentum to the vehicle, probably by hitting and breaking the 90 degree fully deployed stops and at 593.9 imparted a final kick as it tore completely free at the hinge link. In-orbit photographs show clearly the hinge separation plane and the various wires which were torn loose at the interface ((3 - 4 p. 37)

As a consequence of the meteoroid shield failure at approximately 63 seconds, the SAS-2 wing was unlatched and partially deployed as evidenced by minor variations in the main solar array system electrical voltages and SAS-2 temperatures. Full deployment was prevented due to the aerodynamic forces and accelerations during the remainder of powered flight. (Readings, page 186)

#### **S-II Interstage Adapter Separation**

...the increasing temperatures after the time of normal S-II interstage separation are indicative of an abnormal condition. More detailed investigation based on performance evaluation and axial acceleration time history revealed that the interstage had not been jettisoned; however, due to the

vehicle performance characteristics and performance margin, the desired orbit was achieved. (Readings, page 108-187)

- Primary ordnance command was properly issued.
- Backup command was issued, but exploding bridge wire circuit discharge indicated an open circuit consistent with separation.

A review of the history of manufacturing, acceptance, checkout, qualification and flight environment revealed no basic cause for failure. The most probable cause is secondary damage as a result of the meteoroid shield failure, attributed to falling debris as evidenced by the various shock and acoustic disturbances occurring in the 63-second time period.

The redundant mode of ordnance operation of all prior Saturn flights in which both ends of the linear shaped charge are fired at once from a single command would probably have prevented the failure, depending on the extent of damage experienced by the linear shaped charge. (Readings in Systems Engineering, page 186)

## **DS2 – System/Part Design and Development LTA**

Inadequate testing and verification of system interfaces. In addition to considering the MS as a system, the consideration of the MS as a part of other systems was not fully appreciated, increasing the brittleness of the OWS system.

No deployment tests were conducted under vacuum conditions, which is quite acceptable in view of the low rate of motion of the deployment. Vibration, acoustic and flutter tests were specifically omitted in the test specifications because of the design requirement that the shield be “tight to the tank.” This design requirement and pervading philosophy of design and development also served to omit all aerodynamic tests of the meteoroid shield.

12. Given the basic view that the meteoroid shield was to be completely in contact with and perform as structurally integral with the S-IVB tank, the testing emphasis on ordnance performance and shield deployment was appropriate. ((10 – 3) page 143)

## **TT4 – Accepted Team Practices LTA**

In spite of 6 years of analysis, design and testing, there was a failure to recognize other marginal aspects of the design of the meteoroid shield which, when taken together, could also result in failure during launch.

Engineers (must) become familiar with the hardware...chief engineer...spent most of his time in the subtle integration of all elements of the system.

NOTE: On the other hand, there was no indication that time, resources, workmanship, or inexperienced workforce were contributing factors (e.g., SL2, ES2, ES3, IN4, IN5).

11. No evidence was found to indicate that the design, development and testing of the meteoroid shield were compromised by limitations of funds or time. The quality of workmanship applied to the MS was adequate for its intended purpose.

13. Engineering and management personnel on Skylab, on the part of both contractor and government, were available from the prior Saturn development and were highly experienced and adequate in number. ((10 – 3) page 143)

### **MW3 – System/Part Reliability or Usability LTA**

The MS, as designed, built, and assembled was not a reliable system.

Mishap Consequences and Recovery: The micrometeoroid shield and solar panel on one side of the OWS had been lost during ascent. The other OWS solar panel was stuck and did not deploy as planned.

With the loss of an OWS solar panel, Skylab would not have enough electrical energy to conduct its mission. The station was also heating up rapidly (temperatures approached 190 F at one point). The lost micro-meteoroid shield also provided protection from solar heating. Sans this protection, internal temperatures could rise high enough to destroy food, medical supplies, film and other perishables and render the OWS uninhabitable...NASA engineers quickly went to work developing fixes for Skylab's problems. A mechanism was invented to free the stuck solar panel. A parasol of gold-plated flexible material, deployed from an OWS scientific airlock, was then fashioned and tested on the ground. This material would cover the exposed portion of the OWS and provide the needed thermal shielding.

On Friday, 25 May 1973, the Skylab 2 crew and their Apollo Command and Service Module (CSM) were rocketed into orbit by a Saturn IB launch vehicle...The first order of business was to try to free the stuck solar panel...The crew had to fix it or go home. With great difficulty, they did so and were finally able to dock with Skylab. The objective now was to enter Skylab and deploy the parasol thermal shield.

Kerwin and Weitz sported gas masks and cautiously entered Skylab. The temperature inside of the OWS was 130 deg F. Fortunately, the air was found to be of good quality and the pair went to work deploying the thermal shield through a scientific airlock. The deployment was successful and the temperature started to slowly fall.

It would not be until Thursday, 07 June 1973, that the stuck solar panel finally would be freed. (See Saving Skylab, J. Terry White, May, 24, 2010)

## Appendix E. STS-1 Oxygen Deficiency Mishap Analysis

More than 500 deviations were made to the standard procedures to accommodate the activities happening in parallel during a simulated countdown on the launch pad. One of those activities was a nitrogen purge that was not labeled hazardous on the integrated schedule, with minimal review by the safety officers. At the end of the countdown test on March 19, 1981, technicians were allowed in the purged area. Three technicians were killed by asphyxiation. Emergency personnel were unable to travel through the narrow passages to get to the area of concern. The various influence chains for this incident are detailed in Table E-1 and are displayed graphically in Figure E-1.

**Table E-1. STS-1 Oxygen Deficiency Mishap Influence Chain Summary**

#	Description of Cause	Type
	<b>Chain #1 is about the S0017 Deviation 13-20 (extension of GN<sub>2</sub> purge for a special leak test) not being identified as hazardous and being added at the last minute</b>	
1a	<p>Schedule Controls LTA</p> <p>OMI S0017 Launch Countdown Demonstration Test - Dry was conducted during the period from March 17 through March 19, 1981. In the preplanning for this test activity, Deviation 13-20 was written to accommodate the special test. (page 2a5) Dev. 13-20 was written on March 16th. The deviation did not identify the fact that the GN<sub>2</sub> purge would have to be extended to accomplish the test. The deviation was inserted just prior to the GN<sub>2</sub> to air transfer (p. 2a-5). During the performance of the FRR, which was conducted 2/20/81, there was an indication of a GN<sub>2</sub> intrusion into the crew compartment. Since GN<sub>2</sub> was provided during S0017, a special leak test was planned to be conducted as a tack-on to that procedure. (Question: If they knew they needed a special leak test in mid-February, why was the deviation written the day before S0017 began? Because of schedule pressure and workload?)</p> <p>See page 1d-10 for deviation processing timeline. See Chain #2 re: 500 deviations.</p> <p>Dev not on the integrated schedule as a hazard. Last minute, opportunistic scheduling (similar to NLGD mishap when the forward RCS was off, and they could manually lower the orbiter in the Orbiter Processing Facility (OPF))</p>	ES3
1b	<p>Procedure Design &amp; Development LTA</p> <p>Deviation was tacked on for convenience. In total, the procedure had 500 deviations (p. 1d-11). Review copies did not have all deviations.</p> <p>The deviation was written and inserted for accomplishment into the procedure just prior to termination of the GN<sub>2</sub> purge following T-O. This was a point where the special test could be conducted utilizing the GN<sub>2</sub> purge still in progress and would utilize a crew in the cockpit to obtain in the necessary air samples. (page 2a5) (page 1d-11) Deviation 13-74 was also; inserted into OMI S0017 and this procedure had 500 deviations.</p>	DS5
1c	<p>Unclear Procedures</p> <p>Since the fact that additional GN<sub>2</sub> purge time would be required for the special leak test was not identified in the deviation, the deviation was processed as though the test was to take place during the already planned GN<sub>2</sub> purge hazardous period. As a result, the deviation was not processed through the contractor or NASA Safety. (p. 2a-5) The deviation was written in such a manner that it...did not identify the fact that the GN<sub>2</sub> purge would have to be extended to accomplish the test. (page 2a5) The author of the deviation failed to identify the requirement to extend the GN<sub>2</sub> purge air beyond the originally planned termination of the GN<sub>2</sub> purge following T-O.</p> <p>The deviation was written on the 16th of March following discussions pertaining to the special test between KSC and JSC. The deviation was written in such a manner that it specified the detailed steps of the functions to be performed but did not discuss nor identify the fact that the GN<sub>2</sub> purge would have to be extended to accomplish the test. The CDT procedure reflected a GN<sub>2</sub> to air transfer and the deviation was inserted just prior to that point. Since the fact that additional GN<sub>2</sub> purge time was not identified in the deviation, the deviation was processed as though this activity was to take place in the course of the existing planned GN<sub>2</sub> purge hazardous period. The deviation was not processed through contractor or NASA Safety. (page 2a5) (page 2a-6) The procedure included steps for clearing the areas, but specific steps for area securing were not included.</p>	OP4
1d	<p>Infrequent/Unique Task</p> <p>The deviation was written to troubleshoot a leak into the crew cabin during a January test.</p> <p>The deviation was discussed at the pretest briefing on the 17th of March; however, the discussion addressed only the activities required to perform the test and no mention was made that it would be necessary to extend the GN<sub>2</sub> purge. Consequently, the extension of that hazardous period was not identified and was not carried forward in the integrated schedule, nor was it brought to anyone's attention as a matter of course in the pretest briefing. (See copy of dev page 1h-5)</p>	MW5

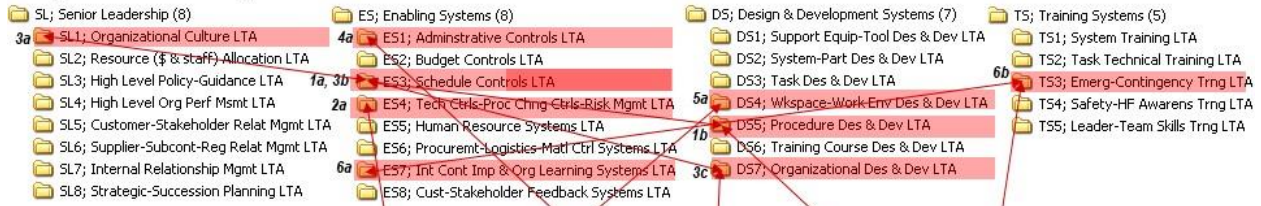
#	Description of Cause	Type
1e	<p>Cognitive Factors</p> <p>Technicians and NTDs (everyone except the RI systems engineer) apparently didn't know the GN<sub>2</sub> purge was going on, and it was a hazardous (oxygen deficient) environment. When the aft monitor got the word, he removed the access sign because there was nothing to clue him in that he needed to do a sniff check. (page 2a-5/6) The deviation was discussed at the pretest briefing on the 17th of March; however, the discussion addressed only the activities required to perform the 2a-5 test and no mention was made that it would be necessary to extend the GN<sub>2</sub> purge. Consequently, the extension of that hazardous period was not identified and was not carried forward in the integrated schedule, nor was it brought to anyone's attention as a matter of course in the pretest briefing.</p>	IN2
	<b>Chain #2 is about the safety controls and procedures</b>	
2a	<p>Technical Controls/Process Change Controls/ Risk Management LTA</p> <p>The dev was not processed through contractor or NASA safety. Processed as a normal dev, not a hazardous dev. Since the dev was not labeled as hazardous, safety did not review, and an access control sign was used. Who was ensuring that the deviations were labeled correctly, especially when there were 500 deviations? Went through multiple reviews, and they all missed it.</p> <p>GP 1098B specifies and establishes the safety policy and procedures required during prelaunch and launch and landing operations. This document supplements KMI 1710.1C and KHB 1710.2A and specifically covers the SSP landing facility, the OPF, the VAB, and Pads A and B. The document contains the Safety operating procedures related to LC 39 specifically, and addresses specific safety requirements and instructions such as: Orbiter mate to the external tank, Orbiter mate and demate with the carrier aircraft, and inspection and sampling hazardous fluids systems inside the Orbiter. As a result of the above review, KMI 5310.9 which deals with hazard analysis was also reviewed. It requires a specific hazard be identified by Design Hazard Analysis (DHA) or an Operational Hazard Analysis (OHA). The Design Hazard Analysis, SAA 09GS05-001 H03, identifies the hazard of inadvertent release of GN<sub>2</sub> into the ECS room and is addressed in the Rockwell International (RIC) OHA, hazard No. 23H03-SAA09GS05-001. The Design Hazard Analysis, SAA09GS05-001 H04, identifies the hazard of inadvertent release of GN<sub>2</sub> into the ECS conditioned air subsystem and is addressed in the RIC OHA, hazard No. 23H04-SAA09GS05-001. All four of these analyses require certain controls including sniff checks of areas receiving a deliberate GN<sub>2</sub> purge prior to personnel entry. OMI S0017 was not added to the list of effected procedures in the GHA's or OHA's, nor were the O<sub>2</sub> sniff check requirements included in the released procedure.</p> <p>In general, the document revealed most Safety requirements were adequately identified. Existing KSC Safety documents, however, do not specifically address low oxygen atmosphere other than for tank entry (KHB 1710.2A (V2), 2g-60 SFOP-4), manhole entry (KHB 1710.2A (V2), SFOP-31), and KHB 1710.2A, Volume 1, on hazards associated with helium and nitrogen pressure systems. The KSC documents do not address areas where GN<sub>2</sub> is deliberately delivered, nor does it specify procedure for personnel entry into those areas. In addition, there is no specific definition for confined spaces and no related safety procedures for entry into confined spaces. The intent of the DHA and OHA's was not met in OMI S0017 nor were these documents updated when OMI S0017 became one of the procedures that contained a deliberate GN<sub>2</sub> purge activity. (Page 2g-60)</p>	ES4
2b	<p>Missed Inspections.</p> <p>No atmosphere checks or verification of an air purge before aft reentry. Normally areas exposed to GN<sub>2</sub> would have been purged with air and checked with a hand held O<sub>2</sub> meter for a breathable atmosphere before allowing entry." (Page 2g-81)</p>	QC1
2c	<p>Incomplete Procedures</p> <p>Atmosphere checks or air purge verifications were not in the safety procedure.</p>	OP2
2d	<p>Sensory Signals LTA</p> <p>Support information</p>	SI5
2e	<p>Cognitive Factors</p> <p>Safety personnel.</p>	IN2
	<b>Chain #3 is about the underlying organizational issues</b>	
3a	<p>Org. Culture LTA</p> <p>Emerging, competing cultures two different worlds, two different operations philosophies.</p>	SL1
3b	<p>Schedule Controls LTA</p> <p>Schedule pressure, shop schedule being followed versus the integrated schedule. Shop schedule showed the deviation as being hazardous, but the integrated schedule did not.</p>	ES3
3c	<p>Org. Design and Development LTA</p> <p>Firing room chain of command; firing room control versus control at the pad...centralized versus localized control of integrated operations.</p>	DS7
3d	<p>Accepted Team Practices LTA</p> <p>Excessive use of test time to redline deviations and procedures. Schedule motivation of allowing side work to be carried out in parallel with hazardous operations.</p>	TT4
3e	<p>Infrequent/Unique Task</p> <p>New task (S0017) - it was all new to them at the time.</p>	MW5

#	Description of Cause	Type
	<b>Chain #4 is about the communications breakdown</b>	
4a	Admin Controls LTA Hazardous badging bypassed since the pad was going to be cleared. Access control.	ES1
4b	Team Communication LTA Communication between the FR and the field. Once the astrovan left, people dropped their guard and opened the pad. Inadequate turnover briefings. PA announcement to clear the pad. Finding the locked areas, going back and forth to open the areas. Pad leader completely left out of the loop.  (page 2a-10) - The Rockwell detailed schedule showed work initiation in the aft compartment while the orbiter was still under the hazardous activity reflected in the integrated schedule for the same period of time. - (page 1d-16) Earlier at 0700, at a daily RI working meeting, the RI technician supervisor was told that the controlled area would be open at approximately 0900. He conveyed this to his technicians, including those that were to enter the aft compartment. - Personnel involved in work in the aft compartment proceeded in that direction once they heard the first pad open announcement. Some were stopped and diverted because controls were still being maintained, and then later obtained access to that area. The first one of these was the aft access.  (page 2a-11) The people in the firing room were not aware that this activity was taking place and that people were in fact entering the aft compartment to do work. There was no coordination between personnel at the pad, as far as this entry was concerned, and the personnel in the firing room who were still in a test configuration. The pad leader who normally is aware of work activity, was not involved in dispatching the crew to do work in the aft compartment nor was he aware that this activity was in fact being initiated. As far as he was concerned the aft compartment was still closed off and there was no work activity scheduled for that area.	TT3
4c	Incomplete Procedures No steps in the procedure to open the pad after S0017 was complete.	OP2
4d	Written Support Info. LTA The sign that at aft area access (50-1 door) was an area access sign (Fig 1j-9, page 1j-11). The aft access control monitor attempted to reach the aft fuselage, but it was initially locked out. When he returned, it was unlocked, so he proceeded to his station and removed the Rockwell access monitor access sign at ramp level 130-RSS. If it had been a hazard sign, only KSC safety would have been allowed to remove it.	SI1
4e	Emotional Factors People were "spring loaded" to get into the area; hysteria associated with the first flight, relaxation of test team discipline after the astronauts left.	IN3
	<b>Chain #5 is about the absence of an oxygen deficiency monitoring system and availability of portable air sources</b>	
5a	Workspace/Work Environment Design LTA No staged portable air packs in the aft.	DS4
5b	System Feedback LTA No oxygen deficiency monitoring system in the aft.	SI4
5c	Support Equipment Availability LTA The air packs were in lockers on the platforms rather than in the aft.	MW6
	<b>Chain #6 is about the failure to learn from earlier mishaps and warning signs</b>	
6a	Organizational Learning Systems LTA (1) "In April 1967, during the Congressional hearings of the Apollo 204 accident, Congress requested for the record correspondence from the Safety Office, Kennedy Space Center, pertaining to timely submittals of operational checkout procedures for review. The response from KSC Safety was not favorable. A workable solution had not been established to assure the receipt of procedures in a timely manner. The review and processing of 5T5-1 procedures also has experienced difficulties in timeliness in submission to Safety for review. For additional information refer to Report of the Apollo 204 Review Board Appendix G, Part 2, Page G34, G35." (2) Similar incident on January 16, 1981.	ES7
6b	Emergency/Contingency Training LTA Personnel training and practice for emergency procedures had been completed in the form of an emergency dry run some months earlier, but nothing was ever formally documented. Practice for emergency procedures is not given on a regular basis, and a review of these practices is not conducted prior to the hazardous operation scheduled. The design of the tri-fold platform at the end of the ramp on the 130-foot level of the RSS, which provides access to the 50-1 door, does not facilitate easy egress with incapacitated personnel during an emergency operation. (page 2g-88)	TS3
6c	Incomplete Procedures OMI S0017, contingency procedures.	OP2
6d	Cognitive Factors Lack of awareness of the GN <sub>2</sub> purge hazard.	IN2
	<b>Summary: 27 Causes, 6 Chains</b>	



# STS-1 Orbiter Aft Compartment Mishap Influence Chain Map

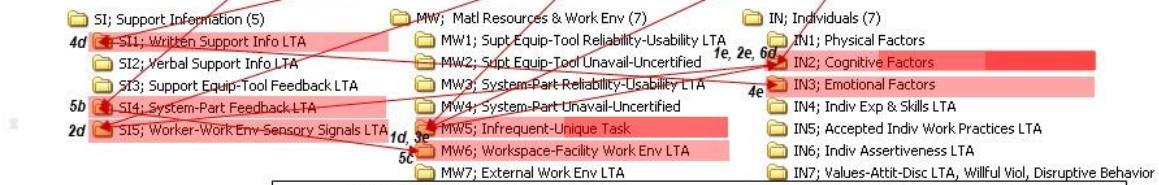
## Organizational System Factors →



## Dual Role Factors →



## Local Resource Factors →



**Key:**  
Cause or Factor  
Influence Link

### SUMMARY

27 causes and factors; 6 influence chains (major issues)

1. Last-minute dev not ID'd as hazardous
2. Inadequate safety controls/procedures
3. Underlying organizational issues
4. Communications breakdown
5. Limited portable air bottles, no O2 deficiency monitoring
6. Previous warning signs not heeded, and lessons not learned

Figure E-1. STS-1 Oxygen Deficiency Mishap Influence Chain Map

## STS-1 Oxygen Deficiency Mishap Analysis Notes

All notes from the analysis are contained in Table E-1.

## Appendix F. STS-1 SRB IOP Close Call Analysis

A significantly low estimate of the SRB ignition IOP resulted in nearly catastrophic damage to the orbiter during STS-1 on March 19, 1981. The prelaunch modeling was conducted using Tomahawk missile motors, but the SRBs have much higher ignition pressures. The pressure wave buckled a strut that supported an RCS oxidizer tank and overextended the body flap used during reentry. Had the oxidizer tank ruptured, the vehicle would have been destroyed and the crew would have been killed. The various influence chains for this incident are detailed in Table F-1 and are displayed graphically in Figure F-1.

*Table F-1. STS-1 SRB IOP Close Call Influence Chain Summary*

#	Description of Cause	Type
	<b>Chain #1 is about using Tomahawk ignition transients for preflight conditions that were very different from SRB; the 6.4% scale model tests conducted did not simulate the structural loads during SRB ignition events well.</b>	
1a	<p>Resource Allocation LTA During this time period, several concerns were raised: 1. The effects of Pc' Pc rise rate, and other motor parameters. 2. The proper scaling functions. 3. The variability in data.</p> <p>As a result of these concerns, a comprehensive analytical and experimental effort was proposed by MSFC in May 1976 to systematically evaluate these key parameters. This proposal was not funded, since the overpressure environments were not impacting the SSP element interface loads, which were the loads driven by the liftoff event at this stage of program development. It should be pointed out that whatever the current problems are, all activities are focused on that area; this emphasis results in overlooking other key areas. (See NASA TM 82458, page 5)</p>	SL2
1b	<p>Technical Controls LTA During the 1975 timeframe, the inter-element interfaces and their element backup structure were extremely sensitive to small parameter changes, such as SRM thrust mismatch, rise rate, and misalignment, and forced a costly redesign of this structure. Since the overpressure environment did not have a major influence on these loads, it was inadvertently assumed to be insignificant to all the SSP subelements.</p> <p>The Loads Panel, under the guidance of JSC, convened all known people with overpressure experience and initiated a study of suppression techniques.</p> <p>Methods considered were hard covers over holes in the MLP, water injection, baffles in MLP, and soft covers over holes in MLP. Again, questions were raised concerning the understanding of the key parameters in the overpressure phenomenon and scaling uncertainties. In May 1978, before these suppression concepts could be evaluated, an error was found in the liftoff loads simulation in how the overpressure phasing with the liftoff twang was considered. Eliminating this error again showed overpressure to be a small contributor to vehicle loads, as well as the Orbiter heat shield and the SRB thermal curtain. This removed the urgency on the design of suppression devices, and this effort was dropped. In retrospect, this large sensitivity to small changes should have been a key concern, and should have been given a more in-depth consideration. (See NASA TM 82458, page 5)</p>	ES4
1c	<p>System/Part Design and Development LTA SRB Ignition is a powerful driver in liftoff environments. System Integration, responsible for liftoff environment definition, accepted the Tomahawk ignition test as a sufficient simulation of SRB ignition IOP – Did not fully appreciate the effect of the differences between the SRB and the Tomahawk ignition characteristics (See Space Shuttle STS-1 Close Calls, Bejmuk, page 7)</p> <p>Pre STS-1 IOP environments were based on sub-scale testing of 6.4% models (Tomahawk solid propellant rocket) conducted at MSFC). These data were scaled to full scale and applied to the lift off simulations for structural sizing analyses.</p> <p>An IOP Wave Committee was formed to, among other assignments; determine why the IOP environment was under predicted. Several root causes were identified. Two of these were: 1) the 6.4% scale model tests conducted did not simulate the SRB ignition events well, 4) the structural math model did not adequately reflect the Space Shuttle Vehicle. (See NASA LLIS)</p>	DS2

#	Description of Cause	Type
1d	System/Part Reliability or Usability LTA The initial launch of the SSP (STS-1) experienced flight hardware damage and excessive control surface excitation attributed to the SRB IOP transient (buckling of a support strut of an Orbiter RCS oxidizer tank and the dynamic response measured on the body flap, elevons, and rudders that far exceeded predicted values).	MW3
	<b>Chain #2 is about focusing on overpressure wave amplitude and not adequately considering wave frequency and its effects on the structural response of the vehicle.</b>	
2a	Organizational Learning Systems LTA Incomplete lesson learned. SRB IOP was a known phenomenon and considered in the design; however, although the amplitude was generally predicted, its frequency characteristics were less well defined, and there was no adequate determination of the AP forcing function or the structural response of the vehicle to this function. Therefore, the correct response was not predicted. (See NASA TM 82458, page 1)	ES7
2b	System/Part Design and Development LTA  Liquid and solid rocket motor propulsion systems create an overpressure wave during ignition, caused by the accelerating gas particles pushing against or displacing the air contained in the launch pad or launch facility and by the afterburning of the fuel-rich gases. This wave behaves as a blast or shock wave characterized by a positive triangular-shaped first pulse and a negative half sine wave second pulse. The pulse travels up the space vehicle and has the potential of overloading individual elements or exciting overall vehicle dynamics. The latter effect results from the phasing difference of the wave from one side of the vehicle to the other. This overpressure phasing, or delta-P environment, because of its frequency content as well as amplitude, becomes a design driver for certain panels (e.g., thermal shields) and payloads for the SSP. (See NASA TM 82458, Abstract)  As the SSP moved toward final verification, it was decided to run some additional tests to obtain better overpressure characteristics. These tests were run without firing the Space Shuttle Main Engines to remove the extraneous noise from the data. There were differing opinions on how to treat overpressure and analyze the data from the tests. The issue was settled at this time by running loads and again showing the interface loads to not be sensitive to overpressure environments. In retrospect, the amplitudes of the overpressure were fairly accurately predicted by Guest as seen in Figure 4. However, no attempt was made to adjust the overpressure frequency for Pc rise rate effects: this meant that the frequency was under predicted by about 40 percent: 4 Hz from model test data versus 6 Hz from STS-I full-scale data. (See NASA TM 82458, Abstract, page 6)  An IOP Wave Committee was formed to, among other assignments; determine why the IOP environment was under predicted. Several root causes were identified. One of these was: 3) the physics of IOP wave development was not well understood. (See LLIS)	DS2
2c	Statistical Methods LTA An IOP Wave Committee was formed to, among other assignments; determine why the IOP environment was under predicted. Several root causes were identified. One of these was: 2) the analysis of the IOP data was flawed with excessive "smoothing" which alter the basic characteristics of the IOP waves. The excessive smoothing of the 6.4% test data prior to STS-1 not only reduced the amplitudes of the IOP, it also altered the frequency characteristics of the IOP waves. (See LLIS)  One final review was made of the overpressure environment by the Williams committee in April 1980. This group also raised concerns over the data analysis methods and overpressure levels. As a result, loads were reassessed and an additional factor of two (increase) was placed on the amplitude (Titan experience). Again, no load exceedances (interfaces) were found; and the issue was closed. See NASA TM82458, Abstract, page 7)	QC5
2d	System/Part Reliability or Usability LTA The dynamic response of the Orbiter to the SRB IOP was greater than expected. (See LLIS)  SRB IOP measured at the vehicle exceeded the 3-sigma liftoff design environment. Accelerations measured on the wing, body flap, vertical tail, and crew cabin exceeded predictions during the liftoff transient. Support struts for the Orbiter's RCS oxidizer tank buckled. Post flight analysis revealed that water spray designed to suppress SRB IOP was not directed at the source of IOP; the source of IOP was believed to be at the plume deflector. STS-1 data analysis showed the primary source located immediately below the nozzle exit plane. (See Space Shuttle STS-1 Close Calls, Bejmuk, page 3) <b>Summary: 8 Causes, 2 Chains</b>	MW3

# STS-1 SRB IOP Close Call

## Influence Chain Map

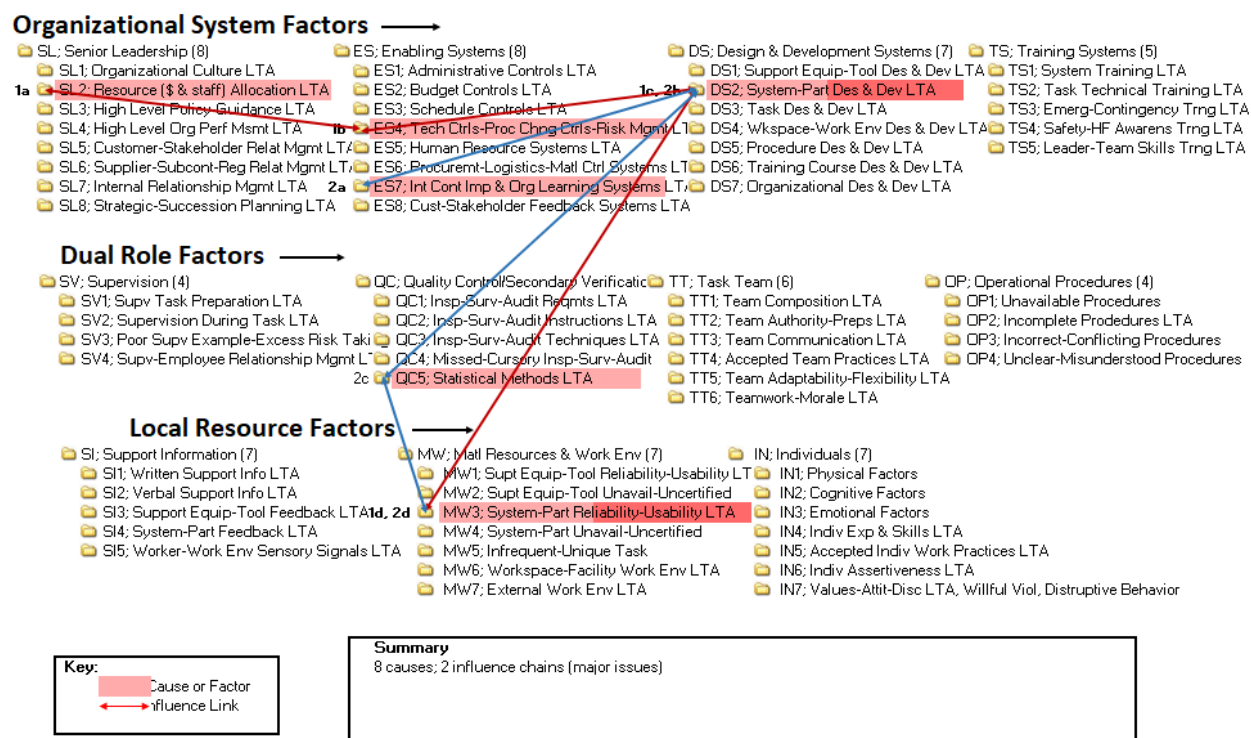


Figure F-1. STS-1 SRB IOP Close Call Influence Chain Map

## STS-1 Close Call Analysis Notes

All notes from the analysis are contained in Table F-1.

## Appendix G. Scaled Composites Mishap Analysis

Ground operations of SpaceShipOne included a steel tank carrying approximately 10,000 lb of N<sub>2</sub>O. On July 26, 2007, while testing in the desert at ~105 °F, the N<sub>2</sub>O exploded, killing three ground crew members and injuring three others. The ground crew had not been informed that N<sub>2</sub>O, above 96.8 °F, becomes a supercritical fluid and is much easier to ignite. Furthermore, the N<sub>2</sub>O was being transferred into a composite tank. N<sub>2</sub>O decomposes most composite materials and produces a vapor that is also explosive.

**Table G-1. Scaled Composites Mishap Influence Chain Summary**

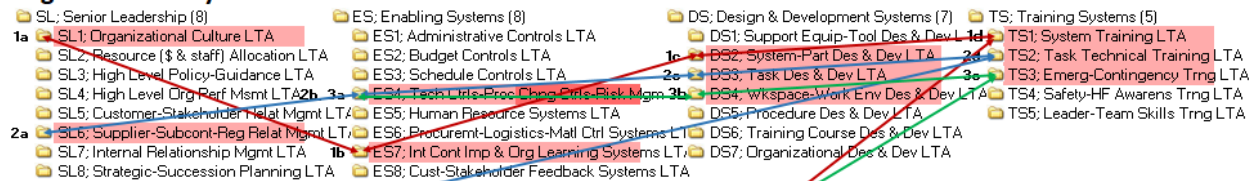
#	Description of Cause	Type
	<b>Chain #1: Deficient Tank Design for N<sub>2</sub>O Storage</b>	
1a	Org. Culture LTA. Scaled Composites' culture seemed to be lulled into complacency regarding the documented hazards of N <sub>2</sub> O.	SL1
1b	Org. Learning Systems LTA. Failure to learn from previous OSHA citations. There was a serious lack of engineering controls to abate the documented hazards of N <sub>2</sub> O storage and handling. It is not clear to what extent the hazards of N <sub>2</sub> O were understood by the test team, even though the hazards of N <sub>2</sub> O were well documented in industry.	ES7
1c	System Design LTA. The tank's design included several materials that were incompatible with N <sub>2</sub> O and the tank did not have a burst disc, to protect against rapid over-pressurization.	DS2
1d	System Training LTA. Not only did the test team appear to have a lack of knowledge about the hazards of N <sub>2</sub> O in general, it also seems they did not understand the critical importance of the tank design, maintenance and inspection, to prevent an explosion.	TS1
1e	System-Part Reliability LTA. The TST tank was constructed from composite materials that did not have a metal tank liner.	MW3
	<b>Chain #2: Deficient Hazardous Task Design</b>	
2a	Regulator Relationship Management LTA. In spite of OSHA having a federal policy for process safety management regarding the storage and handling of highly hazardous chemicals, it does not appear that Scaled Composites had a policy that addressed the documented hazards of N <sub>2</sub> O. It would seem there was a lack of due-diligence in researching the hazards of using N <sub>2</sub> O.  <i>Cal OSHA Report - Finding 1 - Item 001 "General Violation, \$280.00 penalty: The employer failed to provide procedures for identifying and evaluating work place hazards, unsafe conditions, and other work endangerment associated with the use of the chemical compound N<sub>2</sub>O and/or the TST propulsion equipment apparatus."</i>	SL6
2b	Risk Management LTA. It appears that an operational hazard analysis was not performed.  <i>Cal OSHA Report - Finding 2 - Item 001 "Serious Violation, \$18,000 penalty: The employer failed to provide for correcting the unhealthy or unsafe conditions, and other work practices and procedures associated with the use of N<sub>2</sub>O chemical compound . . . this failure contributed to the serious injuries suffered by six employees."</i>	ES4
2c	Task Design LTA. The test was done at the hottest part of the day. N <sub>2</sub> O had been in the tank overnight and all day. The test was conducted at an un-shaded, open-air site on a hot desert day in July at 2:20 p.m.	DS3
2d	System Training LTA. The N <sub>2</sub> O can be hot in one place in the tank and quite cold in another place in the same tank. (Unless the tank had a stirring mechanism, it is difficult to know the mean temperature of the N <sub>2</sub> O in either tank.)  <i>Cal OSHA Report - Finding 1 - Item 002 "General Violation, \$280 penalty: The employer failed to provide training and instruction for the supervisors prior to a catastrophic incident, to insure the supervisors familiarized themselves with the safety and health hazards of the N<sub>2</sub>O chemical compound..."Also Finding 3 - Item 001 "Serious Violation, \$6,750 penalty: The employer failed to provide employees working at a remote testing facility effective information and training of the health and physical hazards associated with the use of the N<sub>2</sub>O chemical compound..."</i>	TS2
2e	Supervisor Task Preparation LTA. Non-essential personnel were allowed in close proximity to the test site. Eleven people gathered at the chain-link fence to watch the test.  <i>Cal OSHA Report - Finding 1 - Issue 3, "General Violation, \$560 penalty: The employer failed to monitor the work environment and ensure that employees were not exposed in excess of the N<sub>2</sub>O permissible exposure limit of 50 ppm."</i>	SV1
2f	Incomplete Procedures (no warnings). MSDS documents, in their most basic form from N <sub>2</sub> O suppliers, caution against pressure shock. There were no warnings in the work instructions about the dangers of pressure shock. There was not a designated hazard control area.	OP2

#	Description of Cause	Type
2g	Infrequent Task. One seemingly small change to a task can increase the hazard level significantly. The propulsion engineers were experimenting with a new valve on the oxidizer tank for SpaceShipTwo. The test was simply to open the valve, let the N <sub>2</sub> O escape: a cold flow test that had been done before.	MW5
	<b>Chain #3: Deficient Work Environment Design</b>	
3a	Technical Controls/Risk Management LTA. There was no evidence of a blast danger area computation, or even consideration of a blast danger area control zone for the N <sub>2</sub> O test site.	ES4
3b	Work Environment/Workspace Design LTA. With the exception of an earthen berm approximately 430 feet from the testing site, there was no containment barrier surrounding the test site in case of an explosion. The test site was in the open air, without any shade, enclosed by a chain-link fence.	DS4
3c	Emergency-Contingency Training LTA.	TS3
3d	Task Team Composition LTA. Emergency response personnel were not on site.	TT1
3e	Incomplete Procedures. There was no written contingency or emergency procedure.	OP2
3f	External Work Environment LTA. There was no evidence of operational hazard controls to minimize or mitigate the dangers associated with using/storing N <sub>2</sub> O. A hot desert environment is probably the worst possible place for N <sub>2</sub> O rocket-motor testing.	MW7
	<b>Summary: 18 causes, 3 chains</b>	

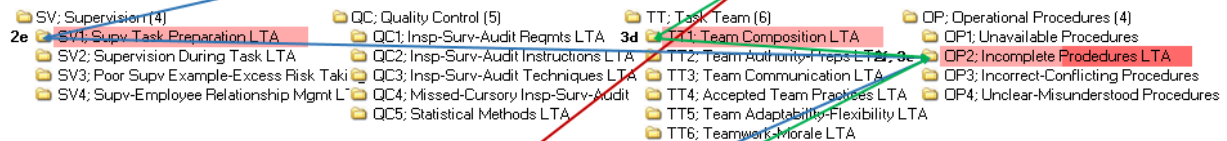
## Scaled Composites Ground Facility Explosion

### Influence Chain Map

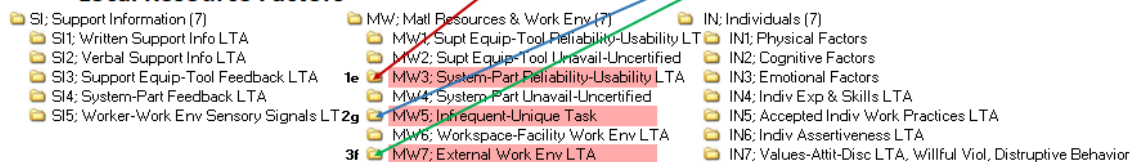
#### Organizational System Factors



#### Dual Role Factors



#### Local Resource Factors



**Key:**  
 Cause or Factor  
 Influence Link

**Summary**  
 18 causes; 3 influence chains (major issues)

Figure G-1. Scaled Composites Mishap Influence Chain Map

## **Scaled Composites Mishap Analysis Notes**

July 26, 2007 – Mojave, CA

There was a N<sub>2</sub>O explosion during propellant flow testing. This was a “cold flow” test intended to study oxidizer flow into a “balance chamber” without rocket motor ignition. An unknown quantity of N<sub>2</sub>O was being transferred to the test stand trailer (TST) tank, as part of the testing apparatus. Three seconds into the test, there was an explosion.

“The propulsion engineers from Scaled were experimenting with a new valve on the oxidizer tank for SpaceShipTwo, a two-meter sphere of carbon fiber designed to hold 5,500kg of liquid N<sub>2</sub>O under 800 atmospheres of pressure. The test was simply to open the valve, let the N<sub>2</sub>O escape: a ‘cold flow’ test that Scaled engineers had done before.” (See <http://www.wired.co.uk/magazine/archive/2013/03/features/up?page=all>)

The Mobile N<sub>2</sub>O Conditioning System (MONOXCS) tank was mounted on a flatbed trailer inside the test site perimeter. The MONOXCS tank was used as the storage tank for the N<sub>2</sub>O used in the test. Also, a mobile test stand, the TST, was located in the center of the site which housed the propulsion system article that was under test.

There were 17 people present, six of whom retreated to a mobile control unit behind an earthen berm approximately 430 feet from the testing site. The remaining eleven people gathered at a chain-link fence in close proximity to the testing rig to watch the experiment.

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings> based on the Cal OSHA report:

“The test was conducted at an open-air and unshaded facility containing a testing rig and various support and ancillary equipment, surrounded by a chain-link fence. It was conducted at approximately 2:20 pm. The ambient temperature is reported as 105+ degrees F. The records show that the ambient recorded temperature at the nearby Mojave Airport peaked at 115 degrees F on that date.

There was a holding tank on site containing more than 10,000 lb of N<sub>2</sub>O, which had been filled the previous night.

Some unknown quantity of the N<sub>2</sub>O was transferred to the TST tank, which composed part of the testing apparatus. A tank was filled the night before. It is not clear which tank this refers to, but we suspect this would be a transfer from the holding (MONOXCS) tank to the TST tank. There is no clear indication of how much N<sub>2</sub>O was in the test apparatus before the testing commenced.”

### **Chain 1: Apparent lack of knowledge about known hazards of N<sub>2</sub>O storage and high pressure vessels as it pertains to tank design**

#### **SL1 – Organizational Culture LTA**

Scaled Composite’s culture seemed to be lulled into complacency regarding the documented hazards of N<sub>2</sub>O.

#### **ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA**

Failure to learn from previous OSHA citations.

Note: Item # 25 on the Cal OSHA form, “Previous Citation History” is marked “Yes.” There is no attached citation history.

There was a serious lack of engineering controls to abate the documented hazards of N<sub>2</sub>O storage and handling. It is not clear to what extent the hazards of N<sub>2</sub>O were understood by the test team, even though the hazards of N<sub>2</sub>O are well documented.

## **DS2 – System/Part Design & Development LTA (for the N<sub>2</sub>O tank design)**

The tank's design included several materials that were incompatible with N<sub>2</sub>O. The TST tank was constructed from composite materials and did not have a metal tank liner. The tank also did not have a burst disc, to protect against rapid over-pressurization. ("Nitrous oxide systems sold to the racing community for use in car engines all have over-pressure protection built in. This has long been considered a basic safety requirement." (Reference: Knights Arrow article)

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings/>

"Experiments that have been conducted show that N<sub>2</sub>O (which is a very powerful solvent) can dissolve the hydrocarbon binders in a composite material. This hydro-carbon, when present in the gas at the top of the tank, will greatly reduce the energy required to initiate a detonation event. It has also been suggested that friction caused by vibration of a composite dip-tube flange (retained by steel bolts) was the ignition source. This may well be the case. There may also have been other material incompatibilities in the system, in valves, other ancillary equipment, or in the balance chamber.

It may also be the case that ignition was the result of compression shock of super-critical N<sub>2</sub>O. This phenomenon has been described in literature dating back to 1937 and is well known amongst those with expertise in the handling, production, and use of N<sub>2</sub>O.

With either source of ignition, both materials incompatibility and high temperature would have contributed to the detonation event."

### **Corrective Actions:**

Excerpt from: <http://www.spaceref.com/news/viewpr.html?pid=26119> which quotes the Scaled Composites website from a letter written August 1, 2008:

"Scaled has implemented a variety of improvements to enhance the safety of the N<sub>2</sub>O hybrid rocket motor:

- Conduct increased compatibility testing between N<sub>2</sub>O and any materials that contact it in the tank and eliminate incompatible materials in the flow path.
- Revise cleaning procedures to further minimize the risk of contaminants in the system.
- Replace the composite liner in the N<sub>2</sub>O tank with a metal tank liner.
- Dilute N<sub>2</sub>O vapor in the tank with nitrogen or another inert gas to decrease its volatility and/or act as a pressurant.
- Design additional safety systems for the N<sub>2</sub>O tank to minimize the danger due to tank overpressure; for example, a burst disk feature; and increase the amount of testing during the development program to demonstrate that these design changes, and any improvements to system components, prevent the sequence of events that led to the accident."



## **TS1 – System Training LTA**

Not only did the team appear to have a lack of knowledge regarding the hazards of N<sub>2</sub>O in general, it also seems they did not understand the critical importance of the tank design, maintenance, and inspection in preventing an explosion.

## **MW3 – System/Part Reliability-Usability LTA**

The TST tank was constructed from composite materials that did not have a metal tank liner.

Monitor/measure/inspect/test – mechanical integrity of all rocket motor equipment such as: vessels, containers, hoses, piping, plumbing, connections, fixtures, valves, etc. Monitoring also should ensure all equipment used to transfer propellants, fuels, and oxidizers is free from contaminants.

## **Chain 2: Deficient Hazardous Task Design**

### **SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA**

In spite of OSHA having a federal policy for process safety management regarding the storage and handling of highly hazardous chemicals, it does not appear that Scaled Composites had a policy that addressed the documented hazards of N<sub>2</sub>O.

Excerpt from a Scaled Composites' press release subsequent to the accident (see <http://spaceref.com/news/viewpr.html?pid=26119>):

“It should go without saying that we were completely surprised by this accident, as we had conducted numerous tests, without incident, on similar systems including the SpaceShipOne rocket motor. The body of knowledge about nitrous oxide (N<sub>2</sub>O) used as a rocket motor oxidizer did not indicate to us even the possibility of such an event.”

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings>:

“This would seem to indicate either a lack of due-diligence in researching the hazards surrounding N<sub>2</sub>O (negligence) or a willful disregard of the truth. In the light of the above, one would be cavalier to advertise Nitrous Oxide and its use in rocketry as ‘safe’ or ‘benign.’

Consider then, the current advertising claim on the Virgin Galactic website:

Hybrid motors offer both simplicity and safety. This is the type of motor that SpaceShipTwo will employ and that was used by SpaceShipOne. The oxidizer is nitrous oxide and the fuel a rubber compound; both benign, stable as well as containing none of the toxins found in solid rocket motors.”

Finding 1 – Item 001 – Cal OSHA Report: “General Violation, (\$280.00 penalty): “The employer failed to provide procedures for identifying and evaluating workplace hazards, unsafe conditions, and other work endangerment associated with the use of the chemical compound nitrous oxide and/or the ‘TST’ propulsion equipment apparatus.”

### **ES4 – Technical Controls/Process Change Controls/Risk Management LTA**

It appears that an operational hazard analysis was not performed, per the requirements for OSHA's Process Safety Management Program.

Finding 2 – Item 001 – Cal OSHA Report: “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.”

### **DS3 – Task Design & Development LTA**

Why was the test being conducted at the hottest part of the day? N<sub>2</sub>O had been in the tank overnight and all day. The test was conducted at an un-shaded, open-air site on a hot desert day in July at 2:20 p.m.

Excerpts from: <http://knightsarrow.com/rockets/scaled-composites-findings>:

“It is reasonable to assume that the N<sub>2</sub>O could have reached a temperature quite close to the actual air temperature.”

“N<sub>2</sub>O in a closed system on a hot day will gain temperature very quickly...The critical point of N<sub>2</sub>O is 96.8 °F. At that point, N<sub>2</sub>O becomes a super-critical fluid, regardless of the pressure it is subjected to. Beyond that point, as temperatures increase, pressure increases at a high rate. Super-critical N<sub>2</sub>O is very susceptible to pressure-shock which will result in a very high velocity detonation during which temperatures can exceed 5,000 °F.”

“The test appears to have been conducted on a concrete pad. If the ambient temperature (in the shade) was 110 °F, the temperature a few feet above the concrete pad would probably have been in excess of 140 °F.”

### **TS2 – Task Technical Training LTA**

Finding 1 – Item 002 – Cal OSHA Report:

“General Violation, (\$280.00 penalty): The employer failed to provide training and instruction for the supervisors prior to a catastrophic incident, to ensure the supervisors familiarized themselves with the safety and health hazards of the nitrous oxide chemical compound used for the test and which employees under their immediate direction and control to which employees were exposed.”

Did the test team know about N<sub>2</sub>O characteristics? That N<sub>2</sub>O can be hot in one place in the tank and quite cold in another place in the same tank? (Unless the tank had a stirring mechanism, it is difficult to know the mean temperature of the N<sub>2</sub>O in either tank.) Excerpt from <http://knightsarrow.com/rockets/scaled-composites-findings>

Finding 3 – Item 001 – Cal OSHA Report:

“Serious Violation, (\$6,750.00 penalty): The employer failed to provide employees working at a remote testing facility effective information and training of the health and physical hazards associated with the use of the nitrous oxide chemical compound the workers were exposed to while in the course of a TST equipment apparatus test.”

### **SV1 – Supervisor Task Preparation LTA**

Nonessential personnel were allowed in close proximity to the test site. Eleven people gathered at the chain-link fence to watch the test.

### Finding 1 – Issue 3 – Cal OSHA Report:

“General Violation (\$560.00 penalty): The employer failed to monitor the work environment during a test on 07/26/2007, and ensure that employees were not exposed in excess of the nitrous oxide permissible exposure limit of 50 parts per million.”

#### **OP2 – Incomplete Procedures**

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings>:

“MSDS documents, in their most basic form from N<sub>2</sub>O suppliers, caution against pressure shock.”

There was no designated hazard control clear area. Workers were allowed to stand behind a chain link fence to watch the test, in close proximity to the N<sub>2</sub>O tank.

#### **MW5 – Infrequent / Unique Task**

One seemingly small change to a task can increase the hazard level significantly.

“The propulsion engineers from Scaled were experimenting with a new valve on the oxidizer tank for SpaceShipTwo, a two-metre sphere of carbon fiber designed to hold 5,500 kg of liquid N<sub>2</sub>O under 800 atmospheres of pressure. The test was simply to open the valve, let the N<sub>2</sub>O escape: a ‘cold flow’ test that scaled engineers had done before.” (See <http://www.wired.co.uk/magazine/archive/2013/03/features/up?page=all>)

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings>:

“Even if the N<sub>2</sub>O in the tank had not gone critical, it is likely that N<sub>2</sub>O in valves and lines could have. This would elevate the pressure in the system to 1,000’s psig. It is also possible that the temperature inside the balance chamber could have been at or above ambient before the test commenced. This could have resulted in the formation of super-critical fluid inside the chamber as flow was started, creating a possible detonation source. Opening a valve to allow flow into a highly constricted chamber could, once the valve opens fully, cause a pressure shock in the balance chamber which would be transmitted to the TST tank resulting in the detonation of all gaseous N<sub>2</sub>O in the system.”

### **Chain 3: Deficient Workspace/Work Environment Design**

#### **ES4 – Technical Controls LTA**

There was no evidence of a blast danger area computation, or even consideration of a blast danger area control zone for the N<sub>2</sub>O test site.

#### **DS4 – Workspace/Work Environment Design & Development LTA**

With the exception of an earthen berm approximately 430 feet from the testing site, there was no containment barrier surrounding the test site in case of an explosion. The test site was in the open air, without any shade, enclosed by a chain-link fence.

#### **TS3 – Emergency/Contingency Training LTA**

Emergency response was not on site.

#### **TT1 – Team Composition LTA**

Emergency response personnel were not on site.

## **OP2 – Incomplete Procedures**

There was no written contingency/emergency procedure.

## **MW7 – External Work Environment LTA**

There was no evidence of operational hazard controls to minimize or mitigate the dangers associated with using/storing N<sub>2</sub>O.

Excerpt from: <http://knightsarrow.com/rockets/scaled-composites-findings>:

“We understand why so many rockets are tested at Mojave; because you can. It is a place where lesser safety standards are tolerated to allow experimental stuff to make it to reality. A hot desert environment is probably the worst possible place for N<sub>2</sub>O rocket-motor testing. This is one field where being cold is good and being hot is not.”

## Appendix H. Ares 1-X Mishap Analysis

On September 5, 2007, the Ares 1-X recovery parachute risers were being tested in a refurbishment facility. There was a rush to complete the testing so the parachute system could meet the schedule. The new test strategy being used was a deviation from a standard SSP test procedure. The load on the risers was to be generated by a large winch and transferred to the riser through steel rods. At some point during the test, one of the steel rods separated from the risers and was pulled back toward the operator, striking him at high energy across the legs. A 5-day lost-time injury resulted. Thirty-one causes were identified by the study team.

*Table H-1. Ares 1-X Mishap Influence Chain Summary*

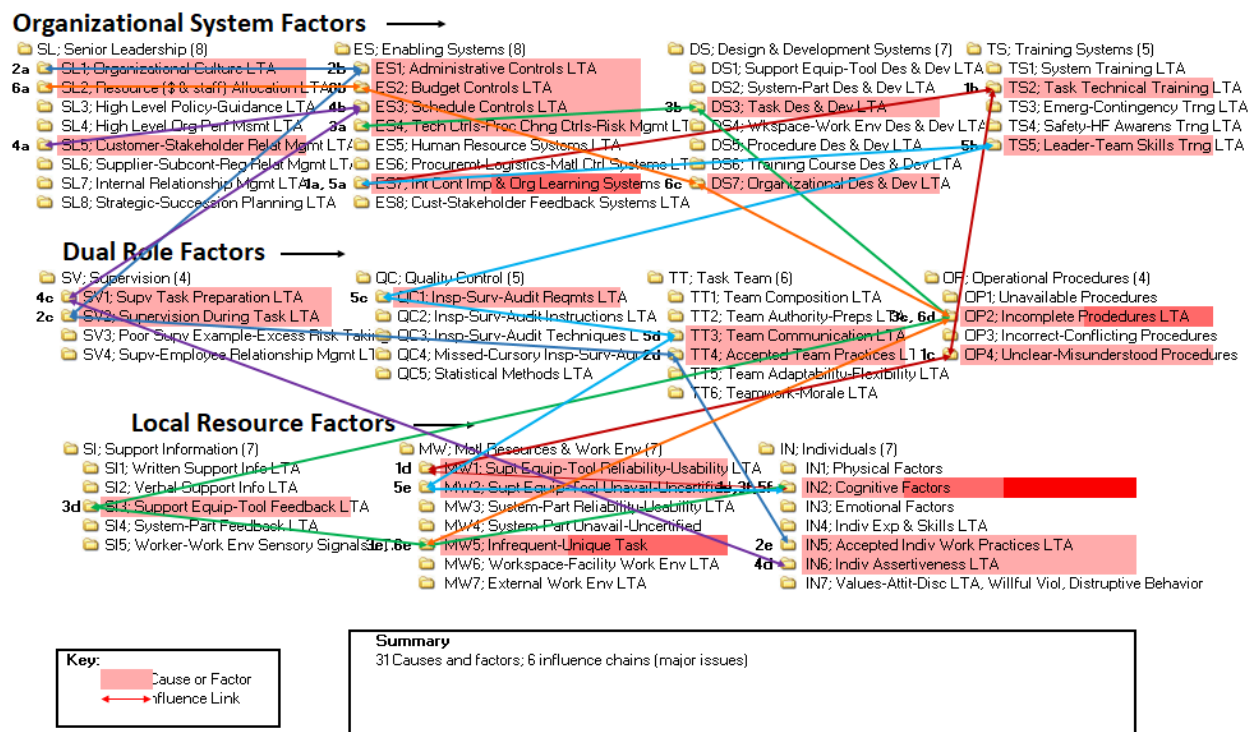
#	Description of Cause	Type
	<b>Chain #1: Use of Nylon Rope - Not Understanding Hazards of Stored Energy</b>	
1a	Organizational Learning Systems LTA. Nine months prior to this lost time injury event, on 12/10/2006, during SRBE retrieval ship operations following the launch of STS-116, a ship's member lost a portion of his toe when the frustum they were securing unexpectedly rose approximately 3 inches from the wooden decking and immediately returned to the deck, trapping the left foot/toes of the team member. Nylon straps were used to secure the frustum. The nylon straps stretched and allowed the load (frustum) to shift, during a crane movement and pivoting of the power block.  Finding 2-A recommended a "First Time Test Review" for all new test setups. The corrective action was incomplete as the First Time Test Review was applied only to that one task, not the PRF globally. Corrective action closure was not recognized as inadequate when verified.  A recommended corrective action was to share the lessons learned of the stored energy hazard inherent in using nylon ropes/straps. Also, in 2002, the PRF incurred a mishap involving a tensile tester.	ES7
1b	Task Technical Training LTA. There is no documented evidence that the stored energy hazard of using nylon ropes/straps was disseminated throughout the SRBE organization after the 2006 mishap, to increase awareness of this hazard and mitigate the risk of using nylon ropes/straps in operations. Likewise, formal training on the capstan winch was not provided. Operation of the capstan winch was by "word of mouth." (See Independent Review Report, page 8)	TS2
1c	Unclear Procedures. The SAA on the capstan winch states that a 7200-lb rope should be used, (9/16 inch diameter). Instead, the riggers used a 3600-lb rope, (3/8-inch diameter nylon dock rope), to connect the capstan winch to the parachute riser lines. The SAIB report does not state why this size nylon rope was chosen - the presumption is that it was an "off-the-shelf" handy material - perhaps it already was attached to the capstan winch. The procedure did not identify what type/size rope to use to connect the parachute risers to the capstan winch.	OP4
1d	Support Equipment Reliability LTA. Riggers used a nylon 3/8-inch diameter rope to connect the capstan winch to the parachute risers.	MW1
1e	Cognitive Factors. No one on the test team questioned the use of the nylon rope. There were no precautions taken in the test setup that would indicate that the team was aware of the stored energy hazard inherent in using a rope that stretches.	IN2
	<b>Chain #2: PRF Culture - Lack of Test Team Rigor</b>	
2a	Organizational Culture LTA. Two very serious injuries occurred in December 2006 during two retrieval operations, (post-launch of STS-116), which questioned the safety culture and leadership of the SRBE organization. A video recording was being made of this first Ares 1-X parachute static strip test. The video recording would be sent to the Marshall Space Flight Center. Inappropriate music was played during the static strip test. This was one example of less than desired test team rigor at the PRF.  (See <u>SAIB Report</u> , page 35, Observation 2: "Board noted lack of rigor in implementing the first time test of new Ares test.")	SL1
2b	Administrative Controls LTA. Because it was the first Ares 1-X static strip test, there were numerous spectators. An operational control area for this hazardous operation was not established, to separate the observers from the operation - especially around the deployment area of the risers. As a result, essential test team personnel were not the only people in the operational area. The PRF Manager was not part of the test team. Since there was no barrier to stop him, the PRF Manager entered into the operational area just as the test began so he could communicate with the test engineer via cell phone.	ES1

#	Description of Cause	Type
2c	Supervision During Task LTA. The PRF Manager did not stop the inappropriate music that was playing, nor did he ensure that the spectators were standing away from the deployment area of the parachute riser lines. The PRF Manager was not a member of the test team and did not participate in any test setup briefing. As the test began, he became involved with the test by agreeing to communicate with the test engineer via cell phone. Shortly after the test began, the PRF Manager positioned himself next to the capstan winch on the west side, to help keep the capstan steady as it was moving back and forth and bumping the table in front of the capstan. This position placed him directly in line with the tensioned nylon rope that was attached between the capstan and the parachute risers. (See SAIB report, pages 15 and 47)	SV2
2d	Accepted Team Practices LTA. Prior to the start of the test on Sept. 5th, before the test engineer arrived, one of the parachute riggers decided to insert 2 stainless steel rods into the riser lines, to help ensure an even pull and smooth deployment. This deviation to the procedure and the potential risks of using the 2 rods were not discussed with the test team as a group, nor was the deviation recorded in the procedure. (The SAIB Report does not indicate whether or not the Quality inspector was aware of the procedural deviation.) A pretest walkdown was not performed prior to the start of the static strip test on Sept. 5th to verify the correct test setup configuration. A capstan winch tie-down floor strap had been loosened the previous day, to avoid a potential trip hazard, when the test was discontinued. The tie-down floor strap was not tightened prior to the start of the test on Sept 5th. The test engineer did not perform the role of a task team leader. A pre-task briefing was not conducted. When the parachute rigger independently inserted the two metal rods into the riser lines, the test engineer did not stop and discuss this action with anyone else on the team. The test engineer did not annotate this deviation in the procedure. The test engineer did not turn off the inappropriate music, nor did he establish a clear area to separate the spectators from the operational area.	TT4
2e	Accepted Individual Work Practices LTA. The rigger and the test engineer did not document the deviation to the procedure when the 2 metal rods were inserted into the riser lines.	IN5
<b>Chain #3: Absent First Time Test Analysis and Readiness Review</b>		
3a	Technical Controls/Risk Management LTA. There was no contractual requirement to do a first time test readiness review or perform a loads analysis. Those assigned to the Ares 1-X task did not perceive the Constellation Launch Vehicle (CLV) work as being "new" but rather an extension of well-practiced SSP-type tasks. Even though the Ares 1-X parachute riser lines were approximately 4x longer than the riser lines on the orbiter's drag chute, there was no requirement for engineering to perform a first-time GSE Design Engineering (DE) load's analysis of the test setup, or an Integrated Product Team (IPT) readiness review, for the initial Area 1X parachute static strip test. (See SAIB Report, page 32 - Finding 3: "Parachute riggers did not know actual loads being applied to test rig because Engineering did not perform a load analysis for strip test.")	ES4
3b	Task Design LTA. The first time Ares 1-X strip test setup was "non-standard" with many new components being used such as a forklift, a capstan winch, nylon break ties, and a nylon towline. The use of a 3/8 inch nylon towline to pull out the parachute created a dangerous amount of stored energy.	DS3
3c	Incomplete Procedures. The task was not identified as hazardous, nor did it contain instructions to rope off a control area. Because the task was not identified as hazardous a safety person was not required to be present during the static strip test and was not in the facility at the time of the injury. (See SAIB Report, page 30 - Finding 1: "Two non-load rated stainless steel rods tied at mid-point became overloaded, bent and escaped riser loops." Also page 31 - Finding 2: "Task was not identified as hazardous in WAD. Use of nylon towline to pull out parachute created dangerous amount of stored energy." Also, page 33 - Finding 4: "Tying towline to stainless steel rod mid-point permitted the escape of the rods when the rods bent.")	OP2
3d	Support Equipment Feedback LTA. There was no means of measuring the load that was being applied to the riser lines as they were being pulled from the chute's container.	SI3
3e	Infrequent/Unique Task. This was the first Ares 1-X Parachute static strip test.	MW5
3f	Cognitive Factors. The test team did not know the loads being applied to the test rig. The team failed to recognize the off-nominal configuration as a risk, (the insertion of the 2 stainless steel rods into the riser lines). Lack of engineering mindset rigor to "expect the unexpected" especially for a first time task. (See SAIB Report, page 32 - Finding 3: "Parachute riggers did not know actual loads being applied to test rig because Engineering did not perform a load analysis for strip test.")	IN2
<b>Chain #4: USA's New Role as a Subcontractor to ATK in a DDT&amp;E environment</b>		
4a	Customer/Stakeholder Relationship Management LTA. In spite of USA incurring a lost-time injury, ATK gave kudos to USA for meeting the Yuma, AZ, drop test schedule which reinforced USA's belief that they could not challenge the schedule and fortified their "must do" mindset. USA's letter contract with ATK left many of the requirements undefined and negotiable. The Ares 1-X work was bid at one level of "bare bones" requirements/expectations and then later USA faced greater customer expectations from the SSP.	SL5

#	Description of Cause	Type
4b	Schedule Controls LTA. Schedule pressure contributed to a focus on the completion of the static strip test rather than the test itself. There was a delay in obtaining a DOT certified container for shipping the parachute to AZ, yet the scheduled date for the AZ drop test was not slipped to the right. Immediately after the static strip test was completed at KSC, the parachute was being delivered to Yuma, AZ for the first Ares 1-X parachute drop test which was scheduled the next week. On Sept. 4th, the procedure was written, approved by Quality and Safety, released and worked. A same day turnaround on releasing a procedure begs the question of how much attention was given to the content of the procedure. Interviews with PRF personnel and comments in the SAIB report reflect the "insane" and "aggressive" Ares 1-X schedule.	ES3
4c	Supervisor Task Preparation LTA. Rush to put procedure together, release it and work it the same day. Poor task planning.	SV1
4d	Individual Assertiveness LTA. No one was willing to push back against an aggressive schedule. Sixty hour workweeks were common as workers juggled both SSP and Ares 1-X responsibilities.	IN6
<b>Chain # 5: Absent Test Team Leader and Task Team Best Practices</b>		
5a	Organizational Learning Systems LTA. Nine months prior to this lost time injury event, on 12/10/2006, during SRBE retrieval ship operations following the launch of STS-116, the ship's crew experienced two significant lost time injuries. Both incidents reflected deficient task team leader behaviors as well as task team behaviors.	ES7
5b	Leadership/Team Skills Training LTA. Both of the STS-116 post-launch retrieval ship injuries, along with this PRF injury, reflect a lack of task team roles and responsibilities as well as a lack of task team leader skills. While Ground Ops organization trained and reinforced both task team and task team leader skills, the SRBE did not. The SRBE reported to Marshall SFC and responded to a different set of expectations from those of Ground Ops and their NASA KSC and JSC SSP counterparts.	TS5
5c	Inspection Requirements LTA. The insertion of the rods was a definite deviation from the written procedure - and unless the quality rep wasn't paying any attention at all, he would have seen the rods inserted through the two riser end loops, prior to the start of the test. Unlike SSP operations, the SRBE did not have a requirement for real-time "pen and ink" annotations in the procedure, to authorize deviations from the released floor procedure.	QC1
5d	Team Communication LTA. Three people separately questioned the rigger about the adequacy of the rods and voiced concerns about the rods bending and coming loose, (USA Test Engineer, USA capstan winch operator, and a NASA Ares Observer), and all 3 deferred to the judgment and experience of the parachute rigger. None of these separate concerns were discussed with the entire team. (See SAIB Report, page 33 - Finding 5: "Three individuals questioned the Parachute Rigger regarding the adequacy of rigging with stainless steel rods prior to test start, but the concern was not brought to the attention of the entire team and the test continued.")	TT3
5e	Support Equipment Uncertified. Prior to the start of the test on Sept. 5th, before the test engineer arrived, one of the parachute riggers decided to insert 2 stainless steel rods into the riser lines, to help ensure an even pull and smooth deployment. Normally these rods are used to secure end loops and dispersion bridles during parachute washing on the "defoul" deck. These non-rated metal rods never had been used before in any other parachute rigging configuration.	MW2
5f	Cognitive Factors. An engineering loads analysis had not been performed and the test team erroneously believed they knew the approximate load required to break the nylon ties. The test team underestimated all loads. (See p. 32 SAIB Report - Finding 3) Also, the team did not have an awareness of the stored energy risk of using nylon rope to pull the parachute out of its container. (See SAIB Report, page 32 - Finding 3: "Parachute riggers did not know actual loads being applied to test rig because Engineering did not perform a load analysis for strip test.")	IN2
<b>Chain #6: New Business Risks - Same Resources for Two Programs</b>		
6a	Resource Allocation LTA. Aggressive pursuit of opportunity for new business created a strain on resources reflected in a "must do" mindset. The Ares 1-X schedule was set outside of USA and there was a reluctance to challenge the "aggressive" schedule, for fear of losing an opportunity to preserve jobs with Ares work after the SSP retirement, which was slated for 2010. Working 2 programs with 1 set of resources led to overtime and work time deviations, and was noted as a "weakness" in an award fee write-up by NASA. (See USA Independent Review Report, page 13)	SL2
6b	Budget Controls LTA. Basis of Estimate (BOE) forecasting was done on incomplete requirements. USA's "letter" contract with ATK left many of the requirements undefined and negotiable. The ATK requirements were increasing (scope creep) without an adjustment to resources. Staffing level was adjusted downward if not deemed competitive. (See USA Independent Review Report, pages 13-14)	ES2
6c	Organizational Design LTA. The Ares 1-X 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 on the IPT was at the IPT lead's discretion. In some cases a necessary discipline may be missed, (e.g., Safety or SGE design), or a "devil's advocate" role. How are the risks associated with a DDT&E environment identified, elevated, discussed, resolved, and documented, (i.e., a closed loop process)? (See USA Independent Review Report, pages 15-17)	DS7
6d	Incomplete Procedures. The work order did not specify a detailed test setup for attaching the load line to the risers. Consequently, the riggers used a 3/8 inch nylon rope. The fact that the work order was written, approved by Quality and Safety, released and worked all in the same day could be a reason why the work order did not specify a detailed test setup for attaching the load line to the risers.	OP2

#	Description of Cause	Type
6e	Unique Task. This was the first Ares 1-X parachute static strip test.	MW5
<b>Summary: 31 causes, 6 chains</b>		

## Ares-1X PRF Injury Influence Chain Map



**Figure H-1. Ares 1-X Mishap Influence Chain Map**

### Ares 1-X Mishap Analysis Notes

During the first time parachute static strip test for the Ares 1-X (Constellation Program), an employee standing next to the capstan winch was struck across both thighs by a two-foot long, 3/8-inch diameter stainless steel rod. The rod, which was inserted into the riser lines just prior to the start of the test, was propelled approximately 50 feet by a sudden release of stored energy in the nylon rope that was attached to the parachute riser lines and the capstan winch. The rope was being used in the retraction of the parachute from its container. The injury resulted in 5 days of lost time from work.

Note: Ares 1-X launched October 28, 2009 @ 11:30 a.m. with an original launch date scheduled for April 15, 2009.



## **Chain 1: Use of nylon rope – not understanding the hazards of stored energy**

### **ES7 – Internal Continuous Improvement and Organizational Learning Systems LTA**

Nine months prior to this lost time injury event, on December 10, 2006, during SRBE retrieval ship operations following the launch of STS-116, a ship's member lost a portion of his toe when the frustum they were securing unexpectedly rose approximately 3 inches from the wooden decking and immediately returned to the deck, trapping the left foot/toes of the team member. Nylon straps were used to secure the frustum. The nylon straps stretched and allowed the load (frustum) to shift, during a crane movement and pivoting of the power block. A recommended corrective action was to share the lessons learned of the stored energy hazard inherent in using nylon ropes/straps.

Also, in 2002, the PRF incurred a mishap involving a tensile tester. Finding 2-A recommended a "First Time Test Review" for all new test setups. The corrective action was incomplete as the First Time Test Review was applied only to that one task, not the PRF globally. Corrective action closure was not recognized as inadequate when verified.

### **TS2 – Task Technical Training LTA**

There is no documented evidence that the stored energy hazard of using nylon ropes/straps was disseminated throughout the SRBE organization after the 2006 mishap, to increase awareness of this hazard and mitigate the risk of using nylon ropes/straps in operations.

Likewise, formal training on the capstan winch was not provided. Operation of the capstan winch was by "word of mouth." (See Independent Review Report, page 8)

### **OP4 – Unclear/Misunderstood Procedures**

The SAA on the capstan winch states that a 7200-lb rope should be used, (9/16-inch diameter). Instead, the riggers used a 3600-lb rope, (3/8-inch diameter nylon dock rope), to connect the capstan winch to the parachute riser lines. [The SAIB report does not state why this size nylon rope was chosen; the presumption is that it was an "off-the-shelf" handy material, perhaps already attached to the capstan winch.

The level of detail was LTA. The procedure did not identify what type/size rope to use to connect the parachute risers to the capstan winch.

### **MW1 – Support Equipment/Tool Reliability Usability LTA**

Riggers used a nylon 3/8-inch diameter rope to connect the capstan winch to the parachute risers.

### **IN2 – Cognitive Factors**

No one on the test team questioned the use of the nylon rope. There were no precautions taken in the test setup that would indicate that the team was aware of the stored energy hazard inherent in using a rope that stretches.

## **Chain 2: PRF Culture – lack of test team rigor and an absent “what can go wrong?” mindset with a first time task – undocumented deviation to the procedure**

### **SL1 – Organizational Culture LTA**

Two very serious injuries occurred in December 2006 during two SRB retrieval operations (post launch of STS-116), which questioned the safety culture and leadership of the SRBE organization.

Operations that occur in isolation tend to have a greater risk of behaviors that deviate from safety standards that are the norm in other “fishbowl” facilities, (e.g. the heavily trafficked OPF high-bays vs. the remote PRF, HMF, NSLD, etc.) At KSC, these isolated facilities often have less safety surveillance and independent monitoring than the other more integrated facilities, which can contribute to culture drift.

A video recording was being made of this first Ares-1X parachute static strip test. The video recording would be sent to the Marshall Space Flight Center. (See SAIB Report, page 35, Observation 2: “Board noted lack of rigor in implementing the first time test of new Ares test.”)

### **ES1 – Administrative Controls LTA**

Because it was the first Ares 1-X static strip test, there were numerous spectators. An operational control area for this hazardous operation was not established, to separate the observers from the operation, especially around the deployment area of the risers. As a result, essential test team personnel were not the only people in the operational area.

The PRF Manager was not part of the test team. Since there was no barrier to stop him, the PRF Manager entered into the operational area just as the test began so he could communicate with the test engineer via cell phone. Approximately 5 minutes after the test began, as the tension tightened on the rope, the capstan winch began to move back and forth and contact the last table. The PRF Manager moved to the west side of the capstan winch. His intention was to help steady the capstan winch. His position placed him in the trajectory path of the stainless steel rod. He was struck by one of the metal rods, which was catapulted approximately 50 feet from the end of the deployed riser lines towards the capstan winch.

### **SV2 – Poor Supervision During Task**

The PRF Manager did not stop the inappropriate music that was playing, nor did he ensure that the spectators were standing away from the deployment area of the parachute riser lines.

The PRF Manager was not a member of the test team and did not participate in any test setup briefing. As the test began, he became involved with the test by agreeing to communicate with the test engineer via cell phone. The Test Engineer was standing on one side of the parachute container and holding the container’s curtain open to allow the parachute to come freely out of its pack. The rigger who had inserted the two rods was standing on the other side of the parachute container, also holding open the curtain.

Shortly after the test began, the PRF manager positioned himself next to the capstan winch on the west side, to help keep the capstan steady as it was moving back and forth and bumping the table in front of the capstan. This position placed him directly in line with the tensioned nylon rope that was attached between the capstan and the parachute risers. Approximately 5 minutes into the test, when the stainless steel rod/nylon towline was deployed within approximately 50 feet of the capstan, the metal rods bent and disconnected from the riser lines. The rope that

was tied around the rods recoiled and the stored energy in the nylon towline propelled the rods toward the capstan winch. He was struck across both thighs by one of the rods and was transported to the hospital and incurred a lost time injury (5 days). (See SAIB Report, pages 15 and 47)

#### **TT4 – Accepted Team Practices LTA**

The rope used in the test was 3600 lb. The capstan SAA calls for a 7200 lb rope to be used with the capstan. (See SAIB Report, page 45)

Prior to the start of the test on September 5th, before the test engineer arrived, one of the parachute riggers decided to insert two stainless steel rods into the riser lines, to help ensure an even pull, smooth deployment. This deviation to the procedure and the potential risks of using the two rods were not discussed with the test team as a group, nor was this deviation recorded in the procedure. (The SAIB Report does not indicate whether or not the Quality Inspector was aware of the procedural deviation.)

A pretask briefing was not conducted. The test engineer did not perform the role of a task team leader. The test engineer did not conduct a pretask briefing. A clear area was not established to separate the spectators from the operational area.

A pretest walk down was not performed prior to the start of the static strip test on September 5<sup>th</sup> to verify the correct test setup configuration. The previous day, after the parachute pack had been lifted and installed into the parachute container, a decision was made to stop and continue with the test the next morning. (The SAIB Report does not explain why this postponement decision was made.)

To avoid a potential trip hazard, a capstan winch tie-down floor strap was loosened when the test was discontinued on September 4<sup>th</sup>. The next morning, the tie-down strap was not resecured prior to the test initiation. Shortly after the test began, the capstan winch was seen to contact repeatedly the last parachute table in a jerking motion. Since the hoist straps had not been secured properly to the floor hoist, the nylon rope and risers had been acting as rubber bands, storing and releasing energy during the test while the capstan was jerking back and forth. The test was temporarily halted to allow for the adjustment of the capstan winch and hoist straps. As the test resumed, the PRF Manager positioned himself immediately to the west of the capstan winch to help steady it. The capstan operator was positioned on the east side of the winch.

#### **IN5 – Accepted Individual Work Practices LTA**

The rigger or the test engineer did not document the deviation to the procedure when the two metal rods were inserted into the riser lines.

### **Chain 3: Absent first time test analysis and readiness review**

#### **ES4 – Technical Controls/Risk Management LTA**

There was no contractual requirement to do a first time test readiness review or perform a loads analysis.

Those assigned to the Ares 1-X task did not perceive the Constellation Launch Vehicle (CLV) work as being “new” but rather an extension of well-practiced SSP-type tasks. Even though the Ares 1-X parachute riser lines were approximately 4 times longer than the riser lines on the orbiter’s drag chute, there was no requirement for engineering to perform a first-time GSE DE

load's analysis of the test setup, or an Integrated Product Team (IPT) readiness review, for the initial Ares 1-X parachute static strip test.

NOTE: The length of the riser lines to be deployed from the Ares 1-X chute was over 200-feet long. The riser lines deployed for the SSP SRB pilot chute (9 feet) and main drag chute (40 feet) are a combined 49 feet.

The purpose of the static strip test was to verify the chute bag and riser lines would deploy in an orderly manner, as well as confirm the packing and tying methods were acceptable. The static strip test was the final task prior to the shipment of the parachute to Yuma, AZ, for the first Ares 1-X drop test.

### **DS3 – Task Design & Development LTA**

The first time Ares 1-X strip test setup was “non-standard” with many new components being used such as a forklift, a capstan winch, nylon break ties, and a nylon towline. A forklift was used to raise and position the parachute container and position the pack at the south end of the packing tables. Because the length of riser lines to be pulled out was over 200 feet long, and the nylon break ties securing them into the parachute had to be overcome, a capstan winch was used to pull the parachute from its container. The use of a 3/8-inch nylon towline to pull out the parachute created a dangerous amount of stored energy.

### **OP2 – Incomplete Procedures**

The work order did not specify a detailed test setup for attaching the load line to the risers. Consequently, the riggers used a 3/8 inch nylon rope. Additionally, one of the riggers independently decided to insert two, non-load certified, off-the-shelf, 3/8-inch stainless steel rods into the riser lines.

(See SAIB Report, pages 18 and 22, “Data Analysis.” and page 30, Finding 1: “Two non-load rated stainless steel rods tied at mid-point became overloaded, bent and escaped riser loops. Stretched nylon towline catapulted rods across room, one rod striking employee across both thighs, causing Lost Time Injury.” Also, SAIB Report, page 33, Finding 4: “Tying towline to stainless steel rod mid-point permitted the escape of the rods when the rods bent.”)

The task was not identified as hazardous, nor did it contain instructions to rope off a control area. (See SAIB Report, page 31, Finding 2: “Task was not identified as hazardous in WAD. Use of nylon towline to pull out parachute created dangerous amount of stored energy.”)

Because the task was not identified as hazardous, a safety person was not required to be present during the static strip test and was not in the facility at the time of the injury.

### **SI3 – Support Equipment/Tool Feedback LTA**

There was no means of measuring the load that was being applied to the riser lines as they were being pulled from the parachute's container.

### **MW5 – Infrequent/Unique Task**

This was the first Ares 1-X parachute static strip test.

### **IN2 – Cognitive Factors**

Team's failure to recognize the off-nominal configuration (use of the two metal rods) as a risk. Lack of engineering mindset rigor to “expect the unexpected” especially for a first time task.

An engineering loads analysis had not been performed and the test team erroneously believed they knew the approximate load required to break the nylon ties. The test team underestimated all loads. (See SAIB Report, page 32 – Finding 3: “Parachute Riggers did not know actual loads being applied to test rig because Engineering did not perform a load analysis for Strip Test.”)

The test team did not know the loads being applied to the test rig. They assumed the force needed to break the nylon ties that secured the riser lines in the parachute bag and allow the chute to deploy was between 250 and 300 lb. A post-incident test revealed the range of break force to be between 349 and 446 lb. (See SAIB Report, page 44)

**Chain 4: The CLV’s “new business” Design/Develop/Test/Evaluate (DDT&E) environment had USA as a subcontractor to ATK, (sub versus prime work environment), which created a tenuous relationship with ATK**

The USA SRBE workers had a “must do” mindset to keep ATK happy and hopefully be awarded more CLV work and preserve jobs, as the SSP SRB work was being retired. USA had less influence on schedule and requirements and was reluctant to challenge ATK’s aggressive schedule, for fear of losing potential future work. The “Can Do” SSP motto morphed into the “Must Do” motto as it related to Ares 1-X work. (See Independent Review Report)

**SL5 – Customer/Stakeholder Relationship Management LTA**

In spite of USA incurring a lost-time injury, ATK gave kudos to USA for meeting the Yuma, AZ, drop test schedule, which reinforced USA’s belief that they could not challenge the schedule and fortified their “must do” mindset.

USA’s “letter” contract with ATK left many of the requirements undefined and negotiable. The Ares 1-X work was bid on one level of “bare bones” requirements/expectations and then later USA faced greater customer expectations from Marshall SFC and ATK, (e.g., configuration control, safety, and quality similar to that of the SSP).

**ES3 – Schedule Controls LTA**

Schedule pressure contributed to a focus on the completion of the static strip test rather than the test itself. There was a delay in obtaining a DOT certified container for shipping the parachute to Arizona, yet the scheduled date for the Arizona drop test was not slipped to the right. Immediately after the static strip test was completed at KSC, the parachute was being delivered to Yuma, AZ, for the first Ares 1-X parachute drop test, which was scheduled the following week.

On September 4<sup>th</sup>, the procedure was written, approved by Quality and Safety, released and worked. A same day turnaround on releasing a procedure begs the question of how much attention was given to the content of the procedure. On September 4<sup>th</sup>, the parachute was lifted and installed into the parachute container. The pack was then secured to the container, rotated to a horizontal position, and then placed on dunnage. At this point, a decision was made to stop and continue with the test the next morning.

Interviews with PRF personnel and comments in the SAIB Report reflect the “insane” and “aggressive” Ares 1-X schedule.

**SV1 – Supervisor Task Preparation LTA**

Rush to put procedure together and work it the same day. Poor task planning.

## **IN6 – Individual Assertiveness LTA**

No one was willing to push back against an aggressive schedule. Sixty-hour work weeks were common as workers juggled SSP and Ares 1-X responsibilities.

## **Chain 5: Absent task team leader and task team best practices**

### **ES7 – Internal Continuous Improvement & Org. Learning Systems LTA**

Nine months prior to this lost time injury event, on December 10, 2006, during SRBE *Freedom Star's* retrieval ship operations following the launch of STS-116, a ship's member lost a portion of his toe when the frustum they were securing unexpectedly rose approximately 3 inches from the wooden decking and immediately returned to the deck, trapping the left foot/toes of the team member. SRB recovery operations were suspended that day to transport the injured to medical treatment. Recovery operations resumed the next day. A second crew member received an abdominal lost time injury when the tow wire escaped the tow chute and struck him. The mishap reports for both of these injuries indicated deficient task team leader behaviors as well as teaming behaviors.

### **TS5 – Leader/Team Skills Training LTA**

Both of the STS-116 post-launch retrieval ship injuries, along with this PRF injury, reflect a lack of task team roles and responsibilities as well as a lack of task team leader skills. It should be noted that while the Ground Operations organization trained and reinforced both task team and task team leader skills, the SRBE did not. The SRBE reported to Marshall SFC and responded to a different set of expectations from those of Ground Operations and their NASA KSC and JSC SSP counterparts.

NOTE: Many Ground Operations OPF and pad workers were loaned to the SRBE to help with their workload. A consistent comment from the Ground Operations workers is that the SRBE folks did not follow task team and task team leader best practices to the same degree that was the norm in Ground Operations.

### **QC1 – Inspection and Secondary Verification Requirements LTA**

The insertion of the rods was a definite deviation from the written procedure, and unless the quality representative wasn't paying any attention at all, he would have seen the rods inserted through the two riser end loops prior to the start of the test.

Unlike SSP operations, the SRBE did not have a requirement for real-time "pen and ink" annotations in the procedure to authorize deviations from the authorized procedure.

### **TT3 – Team Communication LTA**

Three people separately questioned the rigger regarding the adequacy of the rods and voiced concerns about the rods bending and coming loose (USA Test Engineer/Task Team Leader, USA capstan winch operator, and a NASA observer), and all three deferred to the judgment and experience of the parachute rigger.

The NASA observer, an experienced parachute rigger, later said that he felt uncomfortable with the stability of the rod configuration, but deferred to the USA team whose task it was. "I should have said something to stop the test from proceeding." (See SAIB Report, page 14 and 15, and page 33, Finding 5: "Three individuals questioned the Parachute Rigger regarding the adequacy

of rigging with stainless steel rods prior to test start, but the concern was not brought to the attention of the entire test team and the test continued.”)

It is not clear from the SAIB report whether the quality representative was aware of the rigger’s real-time deviation from the written procedure with the insertion of the two stainless steel rods through the two riser end loops. The report does not identify the quality representative as questioning the rigger about the insertion of the two rods.

## **MW2 – Support Equipment/Tool Uncertified**

Prior to the start of the strip test, before the test engineer arrived, two parachute riggers were connecting the capstan winch to the ends of the parachute risers. One of the riggers had a concern about being able to achieve an even pull on the parachute lines while protecting the Teflon buffers inside the loops at the ends of the risers. These Teflon buffers were hard to get approval to replace. As a solution to his concern, the parachute rigger independently decided to use a pair of two-foot long, 3/8-inch diameter stainless steel rods. Each of the two rods was inserted through two riser end loops, one above the other and parallel to each other. The nylon towline from the capstan winch was tied around the midpoint of the rods between the riser end loops. (See SAIB report, page 14)

NOTE: Normally these rods are used to secure end loops and dispersion bridles during parachute washing on the “defoul” deck. These non-rated metal rods never had been used before in any other parachute rigging configuration.

## **IN2 – Cognitive Factors**

An engineering loads analysis had not been performed and the test team erroneously believed they knew the approximate load required to break the nylon ties. The test team underestimated all loads. (See SAIB Report, page 32, Finding 3: “Parachute riggers did not know actual loads being applied to test rig because Engineering did not perform a load analysis for Strip Test.”)

The test team did not know the loads being applied to the test rig. They assumed the force needed to break the nylon ties that secured the riser lines in the parachute bag and allow the chute to deploy was between 250 and 300 lb. A post-incident test revealed the range of break force to be between 349 and 446 lb. (See SAIB Report, page 44)

Also, the team did not have an awareness of the stored energy risk of using nylon rope to pull the parachute out of its container.

## **Chain 6: New business risks – using same SSP resources for Ares 1-X Program – more work than people**

### **SL2 – Resource Allocation (Budget and Staff) LTA**

Aggressive pursuit of opportunity for new business created a strain on resources – “must do” mindset. The Ares 1-X schedule was set outside of USA, and there was a reluctance to challenge the “aggressive” schedule for fear of losing an opportunity to preserve jobs with Ares work after the SSP retirement, which was slated for 2010.

Working two programs with one set of resources led to overtime and work time deviations. The following note is an excerpt from a “weakness” that was noted in the SRBE Award Fee:

“Staffing levels in Electrical Design Engineering continue to be of concern. With the number of failure investigations, and tiger teams that continue to be on-going, coupled with the loss of personnel to the Ares Program, personnel are being pushed to their breaking point to keep up with the workload. Level IV commitments also are being broken due to the unreasonable amount of work in the queue for the personnel available to perform that work.” (See Independent Review Report, page 13)

One SRBE Safety and one Quality employee simultaneously were supporting all of the CLV IPTs, along with their other SRBE duties. (See Independent Review Report, page 13)

## **ES2 – Budget Controls LTA**

Basis of Estimate (BOE) forecasting was done on incomplete requirements. USA’s “letter” contract with ATK left many of the requirements undefined and negotiable. The Ares 1-X work was bid on one level of “bare bones” requirements/expectations and then later USA faced greater customer expectations from Marshall SFC and ATK, (e.g., configuration control, safety, and quality similar to that of the SSP).

The Ares 1-X requirements were increasing without an adjustment to resources. Staffing level was adjusted downward if not competitive. “Severe scope creep,” some organizations were not asked to review additional requirements from other USA organizations, which could impact workload without adding resources. For example, one SRBE Safety and one Quality employee simultaneously were supporting all CLV IPTs, along with other SRBE duties.

Support organization input to BOE was inconsistent.

(See Independent Review Report, pages 13 and 14))

## **DS7 – Organization Design LTA**

The Ares 1-X 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 on the IPT was at the IPT lead’s discretion. In some cases, a necessary discipline may be missed (e.g., Safety or GSE design), or a “devil’s advocate” role. (See Independent Review Report, pages 15–17)

What was different between being a lead on a SSP and being an IPT lead for a DDT&E project? How are the risks associated with a DDT&E environment identified, elevated, discussed, resolved, and documented, (i.e., a closed loop process)?

Define: How is risk (other than cost and schedule) identified?

Assign: Who is responsible for identifying and mitigating the risk or elevating it?

Train: What training should be required to focus IPT and management on emerging risks associated with a DDT&E environment? The DDT&E environment is “learn as you go” and hazards may not be identified yet. Rules for SSP are different for Ares 1-X.

Organize: Does the IPT structure give enough visibility to management? What are the processes and tools for identifying and assessing risk? (Suggest using the Ground Operations Risk Assessment (GORA) process.)

Monitor: How is SRBE measuring the success or failure of Ares 1-X work?



CLV work was not identified as “new” enough to be different from existing work. CLV work was viewed merely as an extension of existing SRBE work.

Missing SRBE operational definition of “First Time Article” or “First Time Test Plan.”

Missing “First Time” policy requiring a first time review.

### **OP2 – Incomplete Procedures**

Procedure was missing a detailed test setup.

The fact that the work order was written, approved by Quality and Safety, released, and worked all in the same day seems to indicate schedule pressure. This could be a reason why the work order did not specify a detailed test setup for attaching the load line to the risers.

### **MW5 – Infrequent/Unique Task**

This was the first Ares 1-X parachute static strip test.

## Appendix I. SpaceShipTwo Mishap Analysis

Large flaps on the trailing edge of the wings of the Virgin Galactic SpaceShipTwo launch vehicle are deployed on approach to landing to increase drag and reduce speed. During boost phase, the aerodynamic loads on the flaps and the booms attached to them are more powerful than the actuators can control, so the assembly is held in the low-drag position with locking pins. Once the spacecraft reaches Mach 1.4, the locking mechanism can be safely disengaged. On October 31, 2014, the copilot unlocked the flaps prematurely, and the tail assembly was destroyed. As a result, the spacecraft was lost, and the copilot was killed. The pilot was injured but survived. Thirty causes were identified by the study team.

**Table I-1. SpaceShipTwo Mishap Influence Chain Summary**

#	Description of Cause	Type
	<b>Chain #1: Task Design Issue:</b> <b>Although the copilot made the required 0.8 Mach callout at the correct point in the flight, he incorrectly unlocked the feather immediately afterward instead of waiting until SpaceShipTwo reached the required speed of 1.4 Mach. [ref. 16, Finding #1]</b>	
1a	Technical Controls, Risk Management Systems LTA PF04 Flight Readiness Reviews – Scaled Composites held three flight readiness reviews (FRR's) prior to PF04: a FRR, a Delta FRR and an Executive FRR. The FRR was held on October 3, 2014, the Delta FRR was held on October 27, 2014, and the Executive FRR was held on October 29, 2014. According to those in attendance at the FRRs, there was no discussion of the feather system. A review of the FRR action items revealed several item related to the feather system, but no items were found related to the pilot's use of the feather system. The FRRs were 3 missed opportunities to discuss the catastrophic hazard of unlocking the feather system too early.	ES4
1b	Task Design & Development LTA The copilot was experiencing high workload as a result of recalling tasks from memory while performing under time pressure and with high vibration and high G force loads that he had not recently experienced, which increased the opportunity for errors. (Ref. 16 Finding #3) Validation of the "reasonableness" of the task did not include some important human factors considerations. Scaled Composites could also have considered a procedure to unlock the feather during a less critical flight phase and still mitigate the hazard resulting from an unfeathered reentry. Note: Regarding the 0.8 Mach callout by the copilot: "This and other tasks during the boost phase of flight were memorized due to the dynamic nature of this phase. The purpose of the copilot's 0.8 Mach callout was to alert the pilot that a transonic 'bobble' would be occurring as the vehicle accelerated through the transonic region and became supersonic." "Because of the dynamic nature of the boost phase, the copilot memorized his three tasks to be accomplished during that phase: calling out 0.8 Mach, calling out the pitch trim position in degrees as the pilot trimmed the horizontal stabilizers, and unlocking the feather at 1.4 Mach. In addition to recalling these tasks from memory, each of the tasks needed to be accomplished in a limited time frame. During a simulator run on October 27, 2014, the copilot unlocked the feather after 1.4 Mach (after he received a caution message on the MFD); this situation was debriefed afterward."	DS3
1c	Incomplete Procedures 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 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. If Scaled Composites had incorporated a pilot flying/pilot monitoring challenge and response protocol for the unlocking task (given the safety consequences if the task were performed incorrectly), the task would have been redundant because both pilots would have been included in the recognition and response decision-making of the task. Also, there was "no warning, caution, or limitation in the SpaceShipTwo POH that specified the risk of unlocking the feather before 1.4 Mach." "There was no warning, caution, or limitation in the SpaceShipTwo pilot operating handbook or on the PF-04 (powered flight No. 4) test card that specified this risk." (Quote by NTSB Senior Human Performance Investigator Katherine Wilson in the following article: <a href="http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/">http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/</a> ) The NTSB's review of the SpaceShipTwo emergency procedures did not find a warning stating that uncommanded feather movement during transonic flight would also be catastrophic.	OP2

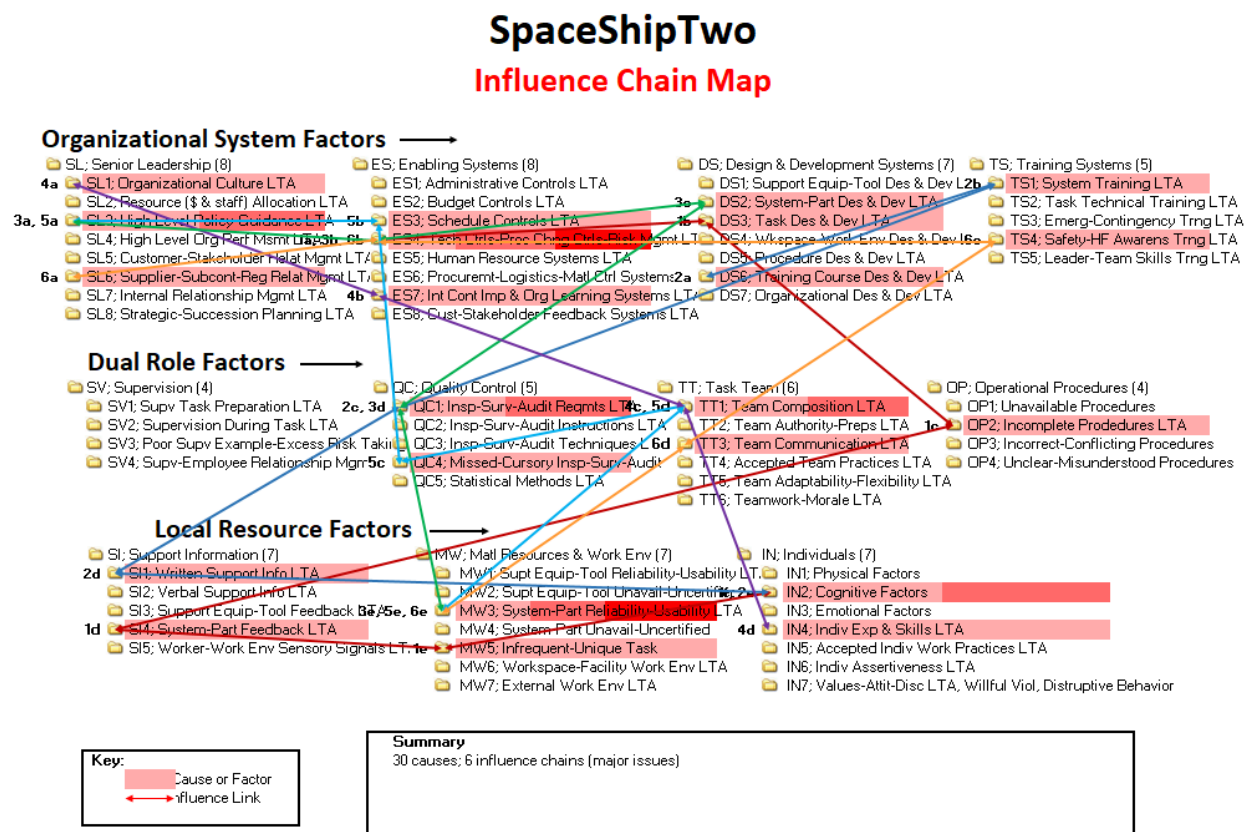
#	Description of Cause	Type
1d	<p>System-Part Feedback LTA</p> <p>The SpaceShipTwo feather system provided no warning annunciator on the multifunctional display (MFD) to prompt pilot action when it was appropriate to unlock the feather.</p> <p>NOTE: Scaled Composites...programmed the MFD to provide pilots with an aural and a visual annunciation if the feather was not unlocked by 1.5 Mach to ensure the feather would be unlocked by 1.8 Mach. In addition, if the feather was not unlocked by 1.5 Mach, a light would illuminate on the caution annunciator panels in front of the pilot and copilot.</p> <p>Also, Scaled Composites engineers were concerned about damaging the feather if it were locked before being fully retracted during the glide phase, so they programmed the MFD to provide pilots with an "OK TO LOCK" annunciation.</p>	SI4
1e	<p>Infrequent-Unique Task</p> <p>"Time pressure has been shown to increase the rate at which an individual must process information, which can lead to cognitive overload. To compensate for time pressure, there is often a tradeoff of speed versus accuracy") During a simulator run on October 27, 2014, the copilot unlocked the feather after 1.4 Mach (after he received a caution message on the MFD); this situation was debriefed afterward." [So perhaps because he experienced unlocking the feather after 1.4 Mach in the simulator 4 days before the powered flight, maybe mentally he was a bit spring-loaded to unlock the feather?]</p> <p>Copilot was experiencing high vibration and high G force loads that he had not recently experienced. "The lack of recent experience with powered flight vibration and loads could increase the copilots' stress and thus his workload, during a critical phase of flight." (Quote from Katherine Wilson, NTSB Senior Human Performance Investigator in the following article: <a href="http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/">http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/</a>)</p> <p>Note: Debated with IN4 since this was only the copilot's second powered test flight and his first attempt to unlock the feather system. His first powered test flight occurred on April 2013 for PF01 and he was the copilot. NOTE: The feather was not unlocked during PF01.</p> <p>Decided against IN4 based on following quote from NTSB board member Robert Sumwalt:</p> <p>"Quoting interviews with other Scaled Composites test pilots, Sumwalt said Alsbury was 'as professional a copilot as you could have and was 100 percent prepared for the mission . . . No one was better at procedures than him.' And I think that really puts it in perspective, this was somebody who was really a professional, trying to do it the right way and yet the error occurred." <a href="http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/">http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/</a></p>	MW5
1f	<p>Cognitive Factors. No one on the test team questioned the use of the nylon rope. There were no precautions taken in the test setup that would indicate that the team was aware of the stored energy hazard inherent in using a rope that stretches.</p>	IN2
	<p><b>Chain #2: Training Issue:</b></p> <p><b>Scaled Composites did not ensure that the accident pilots and other SpaceShipTwo test pilots adequately understood the risks of unlocking the feather early. [ref. 16, Finding #8]</b></p>	
2a	<p>Training Course Design and Development LTA</p> <p>Scaled Composites relied exclusively on the lowest mitigation strategy (training) to mitigate the catastrophic hazard associated with unlocking of the feather prematurely.</p> <p>Because uncommanded feather operation was classified as a catastrophic hazard, Scaled Composites performed a Fault Tree Analysis (FTA) to identify and analyze potential failure conditions. Scaled Composites' (FTA) assumed that the flight crew would be properly trained through simulator sessions . . . These assumptions relied on the flight crew to correctly operate the feather system during every flight.</p> <p>According to the Tier1B program manager, there was a small window in which they counted on the pilot "to do the right thing" so they did not build any safeguards into the system.</p> <p>The SpaceShipTwo simulator did not model uncommanded feather deployment with the feather unlocked. As a result, if a pilot were to unlock the feather early in the simulator, the pilot would not receive direct feedback regarding the catastrophic results of that action during a flight.</p>	DS6
2b	<p>System Training LTA</p> <p>Pilots did not train in the simulator with flight suits, helmets, oxygen masks, parachutes, or gloves. Because Scaled Composites did not require test pilots to train in their flight gear, human factor limitations in the cockpit might not have been apparent until flight.</p> <p>Some aspects of the SpaceShipTwo operating environment were difficult to model in the fixed-base (no motion) simulator, including the high G forces and vibration during flight. As a result of the lack of motion in the SpaceShipTwo simulator, pilots were unfamiliar with the vibration and loads to be expected during powered flight.</p> <p>NOTE: After the accident, Virgin Galactic added vibration to its fixed-base simulator, but the simulator still cannot model G loads.</p>	TS1
2c	<p>Inspection/Surveillance/Audit (Validation) Requirements LTA</p> <p>Scaled Composites did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Although the unlocking task was directly associated with a catastrophic hazard, Scaled Composites did not evaluate this task to determine a specific training protocol that would measurably and reliably reduce the possibility that the task would be performed incorrectly.</p> <p>Validation is the process that ensures that the implemented safety measure (i.e., training) is right.</p> <p>Scaled Composites' assumptions regarding pilot performance were not rigorously verified and validated...</p>	QC1

#	Description of Cause	Type
2d	Written Support Information LTA The NTSB could find only two written references involving the accident pilots (an email from 2010 and a presentation slide from the April 2011 FRR that addressed the excessive tail loads during the transonic region and the inability of the feather actuators to hold the feather in place under such loads. These references did not acknowledge the catastrophic risk of unlocking the feather before 1.4 Mach. Although some evidence indicated that SpaceShipTwo pilots were made aware that the feather should not be unlocked before the designated Mach speed, there was insufficient evidence to determine whether the pilots fully understood the potential consequences of unlocking the feather early.	SI1
2e	Cognitive Factors There is insufficient evidence to determine whether the pilots fully understood the potential consequences of unlocking the feather early.	IN2
	<b>Chain # 3 – Failure to Design System Against Human Error: Scaled Composites' System Safety Analysis (SSA) process did not consider human error as a potential cause of an uncommanded feather extension on the SpaceShipTwo vehicle. (ref. 16)</b>	
3a	High Level Policy/Guidance LTA Lack of human factors guidance for commercial space operators...Because commercial space flight is an emerging industry, no guidance currently exists specifically for commercial space operators that advises them to, among other things, obtain human factors expertise, consider human error in hazard analyses, ensure that hazard analyses avoid or adequately mitigate single-point failures, and ensure that flight crews are aware of known catastrophic hazards that could result from a single human error.	SL3
3b	Technical Controls/Risk Management LTA Scaled Composites' 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, Finding #6] By not considering human error as a potential cause of uncommanded feather extension on the SpaceShipTwo vehicle, Scaled Composites missed opportunities to identify the design and/or operational requirements that could have mitigated the consequences of human error during a high workload phase of flight. (ref. 16, Finding #7) The SSA did not adhere to Advisory Circular (AC) 437.55-1, "Hazard Analysis for the Launch or Reentry of a Reusable Suborbital Rocket Under an Experimental Permit," which the FAA/AST issued in April 2007. The AC stated that a hazard analysis must address human errors, including "decision errors, such as using flight controls at the wrong time" and skill-based errors, such as improperly following a procedure." Scaled Composites stated that the SSA process for SpaceShipTwo met the requirements of 14 CFR 437.55 because (1) "the design of the vehicles is such that mission assurance results in the protection of public health and safety, and property," (2) "the approach is similar to [the approach provided in] AC 437-55," and (3) "the approach is derived from industry practice for certificated aircraft, which have higher standards than experimental aircraft." Scaled Composites' SSA included a functional hazard assessment (FHA) and a fault tree analysis (FTA). There was no Process Failure Modes and Effects Analysis (PFMEA) or similar detailed task analysis that included pilot error.	ES4
3c	System/Part Design & Development LTA The SpaceShipTwo feather system was not error tolerant. (Design Out, Guard Against, Warn, Train, or Accept Risk) The SpaceShipTwo feather system had no design barrier that prevented a crewmember from erroneously unlocking the feather during the transonic region, and the system provided no warning annunciator on the MFD to prompt pilot action when it was appropriate to unlock the feather. (The transonic region was described as occurring between 0.9 and 1.1 Mach) According to the SpaceShipTwo program manager, no safeguards were built into the feather system design because Scaled Composites counted on the pilot "to do the right thing" and dealing with redundancies was "complex." The NTSB notes that Scaled Composites considered design mitigations for other aspects of the feather system. For example...Scaled Composites...programmed the MFD to provide pilots with an aural and a visual annunciation if the feather was not unlocked by 1.5 Mach to ensure the feather would be unlocked by 1.8 Mach... NOTE: Design considerations for the SpaceShipTwo feather system could have included, but would not have been limited to, a mechanical lock for the handle or a "wait to unlock" or an "ok to unlock" annunciation during the boost phase.	DS2
3d	Inspection/Surveillance/Audit (Validation) Requirements LTA Scaled Composites did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Validation is the process that ensures that the implemented safety measure is right. Specifically, AC 23.1309-1D stated, "for the purposes of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and found to be reasonable.	QC1

#	Description of Cause	Type
3e	System Reliability LTA Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.	MW3
	<b>Chain # 4 – Failure to Apply Human Factors Principles and Capabilities: Scaled Composites did not take advantage of human factors engineering specialists, documented human system integration design guidance, or many years of lessons from commercial and DoD aviation, as well as NASA</b>	
4a	Organizational Culture LTA Scaled Composites' management, test pilots, and engineers did not fully consider the risk of human error because of the flawed assumption that test pilots would operate the vehicle correctly during every flight. Also, Scaled Composites had not informed FAA/AST personnel that early unlocking of the feather could be catastrophic, which provided further evidence of Scaled Composites' expectation that a pilot would perform as trained and not unlock the feather early. Scaled Composites did not have a dedicated human factors expert on staff. According to the vice president/general manager of Scaled Composites, they had a "history of building things" and relied on input from the pilots to identify and resolve ergonomic and human factor issues. He said Scaled Composites did not need to hire an outside human factors company because they did that internally. They were a research company and would "change things up" to see if it worked.	SL1
4b	Organizational Learning Systems LTA 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 aviation (DoD and commercial), 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.	ES7
4c	Team Composition LTA Critical evaluations of a commercial space system design should be performed as early as possible as part of a comprehensive SSA process—beginning with the concept development phase and continuing throughout the design and development phases—using a multifunctional team approach that includes human factors experts, test pilots, and design engineers. Scaled Composites did not have a dedicated human factors expert on staff.	TT1
4d	Individual Experience and Skills LTA Scaled Composites relied on input from the pilots to identify and resolve ergonomic and human factor issues.	IN4
	<b>Chain # 5 – FAA's Deficient Evaluation of SpaceShipTwo's Experimental Permit Application: The FAA Office of Commercial Space Transportation's evaluations of Scaled Composites' initial and first renewal of the SpaceShipTwo experimental permit application were deficient because the evaluations failed to recognize that Scaled Composites' hazard analysis did not meet regulatory requirements to identify hazards caused by human error. (ref. 16, Finding #10)</b>	
5a	High-Level Policy/Guidance LTA The lack of direct communication between FAA Office of Commercial Space Transportation technical staff and Scaled Composites technical staff...the lack of a defined line between public safety and mission safety assurance interfered with the FAA's ability to thoroughly evaluate the SpaceShipTwo experimental permit application. (ref. 16, Finding #11) FAA/AST technical staff members stated that, during the permit evaluation process, their questions to Scaled Composites that did not directly relate to public safety were "filtered" or "scrubbed." One FAA/AST evaluator noted that, because these questions were filtered, the technical information received in response was "so washed out, it's not even what we asked for in the beginning." Further, FAA/AST engineers with significant expertise in space operations (from their previous experience at NASA with the SSP and International Space Station programs) expressed frustration that their questions to experimental permit applicants were reviewed and significantly edited by FAA/AST management and Operations Integration Division staff members who had limited knowledge about space flight. An FAA/AST engineer stated, "what really exacerbates the pressure on us, or the time constraints, is the fact that...the technical data that we need to do the evaluation isn't always there...[but] we had to press forward in the majority of the cases." An FAA/AST evaluator added that there was "a lot of pressure, political pressure" to issue experimental permits, even when FAA/AST evaluators were uncomfortable with an application, which diminished AST's safety culture.	SL3
5b	Schedule Controls LTA The pressure to approve experimental permit applications within a 120-day review period interfered with the FAA's ability to thoroughly evaluate the SpaceShipTwo experimental permit application. [ref. 16, Finding #11]	ES3

#	Description of Cause	Type
5c	<p>Cursory Inspection/Audit</p> <p>An FAA/AST analyst was required to perform a thorough evaluation of Scaled Composites' hazard analysis to ensure that it clearly documented how compliance was shown for each of the hazard analysis requirements of 14 CFR 437.55(a). During a post-accident interview, the analyst who evaluated Scaled Composites' applications for the SpaceShipTwo original permit and first renewal of the permit stated that Scaled Composites' analysis had addressed human error. He recalled that software and human errors were represented in the fault trees. However, the analyst did not document his rationale for accepting Scaled Composites' method for addressing the section 437.55(a) human error requirements. If this information had been documented in the analyst's evaluation report, FAA/AST management and system safety analysts (who would later evaluate the hazard analysis for subsequent permit renewals) would have better understood the reasons for the FAA/AST's acceptance of the method that Scaled Composites used to comply with the human error hazard analysis requirements.</p> <p>Note: Reference 16 does not give any information regarding the experience/skill of the FAA/AST analyst who evaluated Scaled Composites' hazard analysis, or any information regarding the FAA/AST analyst's workload or time constraint, if any, to complete the evaluation within the 120-day review period.</p>	QC4
5d	<p>Team Composition LTA</p> <p>According to the FAA's Licensing and Evaluation Division (AST) manager, there was no one in the division with a degree in human factors, however, there were two pilots on his staff that were familiar with human factors concepts.</p>	TT1
5e	<p>System Reliability LTA</p> <p>Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.</p>	MW3
	<p><b>Chain #6 – Unrequested Hazard Analysis Waiver Issue:</b></p> <p><b>The FAA Office of Commercial Space Transportation (AST) did not ensure that Scaled Composites was in compliance with the mitigations cited in the waiver from regulatory requirements or determine whether those mitigations would adequately address human errors with catastrophic consequences. [ref. 16, Finding #12]</b></p>	
6a	<p>Regulator Relationship Management LTA</p> <p>Limited interactions between the FAA/AST and applicants during the experimental permit evaluation process. The dividing line between the questions that the FAA/AST needs to ask to determine the risk to the public and those to assess mission objectives is not always apparent because certain aspects of a vehicle's design and operation could impact both public safety and mission safety assurance. Thus, more extensive interactions between FAA/AST technical staff and prospective experimental permit applicants during permit evaluations would help to perform this work more effectively in the future.</p> <p>Scaled Composites had not informed FAA/AST personnel that early unlocking of the feather could be catastrophic, which provided further evidence of Scaled Composites' expectation that a pilot would perform as trained and not unlock the feather early.</p> <p>According to interviews with FAA AST personnel, some were aware that unlocking the feather during the transonic phase could lead to a catastrophic failure; however, that specific issue was not looked at because while "the team might have discussed it, but it wasn't one of those items, because of the limitations we have on the permit, that we really looked at that particular issue." Asked if there was any discussion about Scaled Composites mitigating the risk of this catastrophic failure, one AST 200 staff member said, "Well, there was no, that I know of, no legal requirement that they need to mitigate that risk."</p>	SL6
6b	<p>Technical Controls/Risk Management LTA</p> <p>Scaled Composites did not request the waiver or have an opportunity to comment on the waiver before it was issued.</p> <p>Scaled Composites did not have an "opportunity to comment on or correct the areas of noncompliance before the waiver was issued. In addition, the FAA/AST did not consult with Scaled Composites technical staff as part of the waiver evaluation process.</p> <p>According to an April 2015 FAA memo in response to an NTSB request for information as part of the accident investigation, the FAA/AST did not ask Scaled Composites to modify its hazard analysis because the areas of noncompliance raised no public safety issues. The memo also indicated that, after reassessing Scaled Composites' hazard analysis, the FAA/AST recognized that a waiver was "procedurally" necessary because Scaled Composite's approach did not meet all of the requirements of the regulation.</p>	ES4
6c	<p>Safety/Human Factors Awareness Training LTA</p> <p>The NTSB believes that the FAA/AST should only waive regulatory requirements for identifying hazards caused by human error under very limited circumstances and should ensure that an applicant seeking a waiver has sufficiently justified the basis for the waiver.</p> <p>The NTSB is concerned about the FAA/AST's lack of awareness regarding whether Scaled Composites was in compliance with the mitigations discussed in the waiver from the software and human error hazard analysis requirements of 14 CFR 437.55(a). Some of the inspectors who were interviewed were unfamiliar with the details of the waiver, and all of the interviewed inspectors thought that Scaled Composites complied with the waiver for each powered flight. The NTSB concludes that the FAA/AST did not ensure that Scaled Composites was in compliance with the mitigations cited in the waiver from regulatory requirements or determine whether those mitigations would adequately address human errors with catastrophic consequences.</p>	TS4

#	Description of Cause	Type
6d	Team Communication LTA The lack of direct communication between FAA Office of Commercial Space Transportation technical staff and Scaled Composites technical staff interfered with the FAA's ability to thoroughly evaluate the SpaceShipTwo experimental permit application. [ref. 16, Finding #11]	TT3
6e	System Reliability or Usability LTA Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.	MW3
	<b>Summary: 30 causes, 6 chains</b>	



**Figure I-1. SpaceShipTwo Mishap Influence Chain Map**

## SpaceShipTwo Mishap Analysis Notes

Note: When applying the influence chain map model to an organizational system, the system boundaries need to be defined. For this analysis to be consistent with reference 16, the “organization” includes both Scaled Composites and the FAA.

### Chain # 1 – Task Design Issue

Although the copilot made the required 0.8 Mach callout at the correct point in the flight, he incorrectly unlocked the feather immediately afterward instead of waiting until SpaceShipTwo reached the required speed of 1.4 Mach (ref. 16, Finding #1).

### Influence Chain #1 Summary:

- **ES4** – Technical Controls, Risk Management Systems LTA ->
- **DS3** – Task Design & Development LTA ->

- **OP2** – Incomplete Procedures ->
- **SI4** – System-Part Feedback LTA ->
- **MW5** – Infrequent – Unique Task ->
- **IN2** – Cognitive Factors

#### **ES4 – Technical Controls, Risk Management Systems LTA**

PF04 Flight Readiness Reviews – Scaled Composites held three flight readiness reviews (FRR's) prior to PF04: a FRR, a Delta FRR, and an Executive FRR. The FRR was held on October 3, 2014, the Delta FRR was held on October 27, 2014, and the Executive FRR was held on October 29, 2014. According to those in attendance at the FRRs, there was no discussion of the feather system...A review of the FRR action items revealed several item related to the feather system, but no items were found related to the pilot's use of the feather system. The FRRs were three missed opportunities to discuss the catastrophic hazard of unlocking the feather system too early.

#### **DS3 – Task Design & Development LTA**

The copilot was experiencing high workload as a result of recalling tasks from memory while performing under time pressure and with high vibration and high G force loads that he had not recently experienced, which increased the opportunity for errors (ref. 16, Finding #3).

Validation of the “reasonableness” of the task did not include some important human factors considerations.

Scaled Composites could also have considered a procedure to unlock the feather during a less critical flight phase and still mitigate the hazard resulting from an unfeathered reentry.

Note: Regarding the 0.8 Mach callout by the copilot, “This and other tasks during the boost phase of flight were memorized due to the dynamic nature of this phase. The purpose of the copilot's 0.8 Mach callout was to alert the pilot that a transonic ‘bobble’ would be occurring as the vehicle accelerated through the transonic region and became supersonic.”

“Because of the dynamic nature of the boost phase, the copilot memorized his three tasks to be accomplished during that phase: calling out 0.8 Mach, calling out the pitch trim position in degrees as the pilot trimmed the horizontal stabilizers, and unlocking the feather at 1.4 Mach. In addition to recalling these tasks from memory, each of the tasks needed to be accomplished in a limited time frame. During a simulator run on October 27, 2014, the copilot unlocked the feather after 1.4 Mach (after he received a caution message on the MFD); this situation was debriefed afterward.”

#### **OP2 – Incomplete Procedures**

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 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.

If Scaled Composites had incorporated a pilot flying/pilot monitoring challenge and response protocol for the unlocking task (given the safety consequences if the task were performed incorrectly), the task would have been redundant because both pilots would have been included in the recognition and response decision-making of the task.



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.”

“There was no warning, caution, or limitation in the SpaceShipTwo pilot operating handbook or on the PF-04 (powered flight No. 4) test card that specified this risk” (ref. 31).

The NTSB’s review of the SpaceShipTwo emergency procedures did not find a warning stating that uncommanded feather movement during transonic flight would also be catastrophic.

#### **SI4 – System/Part Feedback LTA**

The SpaceShipTwo feather system provided no warning annunciator on the multifunctional display (MFD) to prompt pilot action when it was appropriate to unlock the feather.

NOTE: Scaled Composites...programmed the MFD to provide pilots with an aural and a visual annunciation if the feather was not unlocked by 1.5 Mach to ensure the feather would be unlocked by 1.8 Mach. In addition, if the feather was not unlocked by 1.5 Mach, a light would illuminate on the caution annunciator panels in front of the pilot and copilot.

Also, Scaled Composites engineers were concerned about damaging the feather if it were locked before being fully retracted during the glide phase, so they programmed the MFD to provide pilots with an “OK TO LOCK” annunciation.

#### **MW5 – Infrequent or Unique Task**

This was the fourth powered test flight of SpaceShipTwo. The feather was not unlocked during PF01.

#### **IN2 – Cognitive Factors**

“Time pressure has been shown to increase the rate at which an individual must process information, which can lead to cognitive overload. To compensate for time pressure, there is often a tradeoff of speed versus accuracy...”)

During a simulator run on October 27, 2014, the copilot unlocked the feather after 1.4 Mach (after he received a caution message on the MFD); this situation was debriefed afterward.” Copilot was experiencing high vibration and high G force loads that he had not recently experienced. “The lack of recent experience with powered flight vibration and loads could increase the copilot’s stress and thus his workload, during a critical phase of flight” (ref. 31).

Note: Considered “Individual Experience and Skills LTA” since this was only the copilot’s second powered test flight and his first attempt to unlock the feather system. His first powered test flight occurred on April 2013 for PF01 and he was the copilot. The feather was not unlocked during PF01. Decided against this cause category based on following quote from NTSB board member Robert Sumwalt:

“Quoting interviews with other Scaled Composites test pilots, Sumwalt said Alsbury was ‘as professional a copilot as you could have and was 100 percent prepared for the mission...No one was better at procedures than him.’ And I think that really puts it in perspective, this was somebody who was really a professional, trying to do it the right way and yet the error occurred” (ref. 31).

## **Chain # 2 – Training Issue**

Scaled Composites did not ensure that the accident pilots and other SpaceShipTwo test pilots adequately understood the risks of unlocking the feather early (ref. 16, Finding #8).

### **Influence Chain #2 Summary:**

- **DS6** – Training Course Design and Development LTA ->
- **TS1** – System Training LTA ->
- **QC1** – Inspection/Surveillance/Audit (Validation) Requirements LTA ->
- **SI1** – Written Support Information LTA ->
- **IN2** – Cognitive Factors

### **DS6 – Training Course Design and Development LTA**

Scaled Composites relied exclusively on the lowest mitigation strategy (training) to mitigate the catastrophic hazard associated with unlocking of the feather prematurely.

Because uncommanded feather operation was classified as a catastrophic hazard, Scaled Composites performed a Fault Tree Analysis (FTA) to identify and analyze potential failure conditions. Scaled Composites' FTA assumed that the flight crew would be properly trained through simulator sessions... These assumptions relied on the flight crew to correctly operate the feather system during every flight.

According to the Tier1B program manager, there was a small window in which they counted on the pilot "to do the right thing," so they did not build any safeguards into the system.

The SpaceShipTwo simulator did not model uncommanded feather deployment with the feather unlocked. As a result, if a pilot were to unlock the feather early in the simulator, the pilot would not receive direct feedback regarding the catastrophic results of that action during flight.

### **TS1 – System Training LTA**

Pilots did not train in the simulator with flight suits, helmets, oxygen masks, parachutes, or gloves. Because Scaled Composites did not require test pilots to train in their flight gear, human factor limitations in the cockpit might not have been apparent until flight.

Some aspects of the SpaceShipTwo operating environment were difficult to model in the fixed-base (no motion) simulator, including the high G forces and vibration during flight. As a result of the lack of motion in the SpaceShipTwo simulator, pilots were unfamiliar with the vibration and loads to be expected during powered flight.

Note: After the accident, Virgin Galactic added vibration to its fixed-base simulator, but the simulator still could not model G loads.

### **QC1 – Inspection/Surveillance/Audit (Validation) Requirements LTA**

Scaled Composites did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Although the unlocking task was directly associated with a catastrophic hazard, Scaled Composites did not evaluate this task to determine a specific training protocol that would measurably and reliably reduce the possibility that the task would be performed incorrectly.

Validation is the process that ensures that the implemented safety measure (i.e., training) is right. Scaled Composites' assumptions regarding pilot performance were not rigorously verified and validated.

### **SI1 – Written Support Information LTA**

The NTSB could find only two written references involving the accident pilots (an email from 2010 and a presentation slide from the April 2011 Feather Flight Readiness Review [FRR]) that addressed the excessive tail loads during the transonic region and the inability of the feather actuators to hold the feather in place under such loads. The references did not acknowledge the catastrophic risk of unlocking the feather before 1.4 Mach. Although some evidence indicated that SpaceShipTwo pilots were made aware that the feather should not be unlocked before the designated Mach speed, there was insufficient evidence to determine whether the pilots fully understood the potential consequences of unlocking the feather early.

### **IN2 – Cognitive Factors**

There is insufficient evidence to determine whether the pilots fully understood the potential consequences of unlocking the feather early.

### **Chain # 3 – Failure to Design System against Human Error**

Scaled Composites' System Safety Analysis (SSA) process did not consider human error as a potential cause of an uncommanded feather extension on the SpaceShipTwo vehicle.

#### **Influence Chain #3 Summary:**

- **SL3** – High Level Policy/Guidance LTA ->
- **ES4** – Technical Controls / Risk Management LTA ->
- **DS2** – System Part Design & Development LTA ->
- **QC1** – Inspection/Surveillance/Audit (Validation) Requirements LTA ->
- **MW3** – System Reliability LTA

Note: This chain most directly maps to the NTSB probable cause statement:

“Scaled Composites’ failure to consider and protect against the possibility that a single human error could result in a catastrophic hazard to the SpaceShipTwo vehicle. This failure set the stage for the copilot’s premature unlocking of the feather system as a result of time pressure and vibration and loads that he had not recently experienced, which led to uncommanded feather extension and the subsequent aerodynamic overload and in-flight breakup of the vehicle.”

### **SL3 – High Level Policy/Guidance LTA**

Lack of human factors guidance for commercial space operators...Because commercial space flight is an emerging industry, no guidance currently exists specifically for commercial space operators that advises them to, among other things, obtain human factors expertise, consider human error in hazard analyses, ensure that hazard analyses avoid or adequately mitigate single-point failures, and ensure that flight crews are aware of known catastrophic hazards that could result from a single human error.

## **ES4 – Technical Controls/Risk Management LTA**

Scaled Composites' 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, Finding #6).

By not considering human error as a potential cause of uncommanded feather extension on the SpaceShipTwo vehicle, Scaled Composites missed opportunities to identify the design and/or operational requirements that could have mitigated the consequences of human error during a high workload phase of flight (ref. 16, Finding #7).

The SSA did not adhere to Advisory Circular (AC) 437.55-1, "Hazard Analysis for the Launch or Reentry of a Reusable Suborbital Rocket under an Experimental Permit," which the FAA/AST issued in April 2007. The AC stated that a hazard analysis must address human errors, including "decision errors, such as using flight controls at the wrong time" and skill-based errors, such as improperly following a procedure." Scaled Composites stated that the SSA process for SpaceShipTwo met the requirements of 14 CFR 437.55 because (1) "the design of the vehicles is such that mission assurance results in the protection of public health and safety, and property," (2) "the approach is similar to [the approach provided in] AC 437-55," and (3) "the approach is derived from industry practice for certificated aircraft, which have higher standards than experimental aircraft."

Scaled Composites' SSA included a functional hazard assessment (FHA) and a fault tree analysis (FTA). There was no Process Failure Modes and Effects Analysis (PFMEA) or similar detailed task analysis that included pilot error.

## **DS2 – System/Part Design & Development LTA**

The SpaceShipTwo feather system was not error tolerant. The SpaceShipTwo feather system had no design barrier that prevented a crewmember from erroneously unlocking the feather during the transonic region, and the system provided no warning annunciator on the MFD to prompt pilot action when it was appropriate to unlock the feather. (The transonic region was described as occurring between 0.9 and 1.1 Mach)

According to the SpaceShipTwo Program Manager, no safeguards were built into the feather system design because Scaled Composites counted on the pilot "to do the right thing" and dealing with redundancies was "complex."

The NTSB notes that Scaled Composites considered design mitigations for other aspects of the feather system. For example, Scaled Composites programmed the MFD to provide pilots with an aural and a visual annunciation if the feather was not unlocked by 1.5 Mach to ensure the feather would be unlocked by 1.8 Mach.

Note: Design considerations for the SpaceShipTwo feather system could have included, but would not have been limited to, a mechanical lock for the handle or a "wait to unlock" or an "ok to unlock" annunciation during the boost phase.

## **QC1 – Inspection/Surveillance/Audit (Validation) Requirements LTA**

Scaled Composites did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Validation is the process that ensures that the implemented safety measure is right.

Specifically, AC 23.1309-1D stated, “for the purposes of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and found to be reasonable.”

## **MW3 – System Reliability LTA**

Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.

## **Chain # 4 – Failure to Apply Human Factors Principles and Capabilities**

Scaled Composites did not take advantage of human factors engineering specialists, documented human system integration design guidance, or many years of lessons from commercial and DoD aviation, as well as NASA.

### **Influence Chain #4 Summary:**

- **SL1** – Organizational Culture ->
- **ES7** – Organizational Learning Systems LTA ->
- **TT1** – Team Composition LTA ->
- **IN4** – Individual Experience and Skills LTA

### **SL1 – Organizational Culture**

Scaled Composites’ management, test pilots, and engineers did not fully consider the risk of human error because of the flawed assumption that test pilots would operate the vehicle correctly during every flight. Also, Scaled Composites had not informed FAA/AST personnel that early unlocking of the feather could be catastrophic, which provided further evidence of Scaled Composites’ expectation that a pilot would perform as trained and not unlock the feather early.

Scaled Composites did not have a dedicated human factors expert on staff. According to the vice president/general manager of Scaled Composites, they had a “history of building things” and relied on input from the pilots to identify and resolve ergonomic and human factor issues. He said Scaled Composites did not need to hire an outside human factors company because they did that internally. They were a research company and would “change things up” to see if it worked.

### **ES7 – Organizational Learning Systems LTA**

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 aviation (DoD and commercial), 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.

### **TT1 – Team Composition LTA**

Critical evaluations of a commercial space system design should be performed as early as possible as part of a comprehensive SSA process—beginning with the concept development

phase and continuing throughout the design and development phases—using a multifunctional team approach that includes human factors experts, test pilots, and design engineers.

Scaled Composites did not have a dedicated human factors expert on staff.

#### **IN4 – Individual Experience and Skills LTA**

Scaled Composites relied on input from the pilots to identify and resolve ergonomic and human factor issues.

#### **Chain # 5 – FAA’s Deficient Evaluation of SpaceShipTwo’s Experimental Permit Application**

The FAA Office of Commercial Space Transportation’s evaluations of Scaled Composites’ initial and first renewal of the SpaceShipTwo experimental permit application were deficient because the evaluations failed to recognize that Scaled Composites’ hazard analysis did not meet regulatory requirements to identify hazards caused by human error [ref. 16, Finding #10].

Human factors-applicable regulations can be found in 14 CFR 437 Experimental Permits and 14 CFR 460 Human Space Flight Requirements.

14 CFR 437.55 (a) Hazard Analysis stated, in part:

This hazard analysis must –

- (1) Identify and describe hazards, including but not limited to each of those that result from
  - (i.) Component, subsystem, or system failures or faults;
  - (ii.) Software errors;
  - (iii.) Environmental conditions;
  - (iv.) Human errors;
  - (v.) Design inadequacies; or
  - (vi.) Procedural deficiencies.

The FAA/AST approved the initial and first renewal of the SpaceShipTwo experimental permit without recognizing that the SpaceShipTwo hazard analysis did not identify single flight crew tasks that, if performed incorrectly or at a wrong time, could result in a catastrophic hazard.

#### **Influence Chain #5 Summary:**

- **SL3** – High-Level Policy/Guidance LTA ->
- **ES3** – Schedule Controls LTA ->
- **QC4** – cursory Inspection/Audit
- **TT1** – Team Composition LTA ->
- **MW3** – System Reliability LTA

#### **SL3 – High-Level Policy/Guidance LTA**

The lack of direct communication between FAA Office of Commercial Space Transportation technical staff and Scaled Composites technical staff, the lack of a defined line between public safety and mission safety assurance interfered with the FAA’s ability to thoroughly evaluate the SpaceShipTwo experimental permit application (ref. 16, Finding #11).

FAA/AST technical staff members stated that, during the permit evaluation process, their questions to Scaled Composites that did not directly relate to public safety were “filtered” or “scrubbed.” One FAA/AST evaluator noted that, because these questions were filtered, the technical information received in response was “so washed out, it’s not even what we asked for in the beginning.” Further, FAA/AST engineers with significant expertise in space operations (from their previous experience at NASA with the SSP and International Space Station Program) expressed frustration that their questions to experimental permit applicants were reviewed and significantly edited by FAA/AST management and Operations Integration Division staff members who had limited knowledge about space flight...An FAA/AST engineer stated, “what really exacerbates the pressure on us, or the time constraints, is the fact that...the technical data that we need to do the evaluation isn’t always there...[but] we had to press forward in the majority of the cases.” An FAA/AST evaluator added that there was “a lot of pressure, political pressure” to issue experimental permits, even when FAA/AST evaluators were uncomfortable with an application, which diminished AST’s safety culture.

### **ES3 – Schedule Controls LTA**

...the pressure to approve experimental permit applications within a 120-day review period...interfered with the FAA’s ability to thoroughly evaluate the SpaceShipTwo experimental permit application (ref. 16, Finding #11).

### **QC4 – Cursory Inspection/Audit**

An FAA/AST analyst was required to perform a thorough evaluation of Scaled Composites’ hazard analysis to ensure that it clearly documented how compliance was shown for each of the hazard analysis requirements of 14 CFR 437.55(a). During a post-accident interview, the analyst who evaluated Scaled Composites’ applications for the SpaceShipTwo original permit and first renewal of the permit stated that Scaled Composites’ analysis had addressed human error. He recalled that software and human errors were represented in the fault trees. However, the analyst did not document his rationale for accepting Scaled Composites’ method for addressing the section 437.55(a) human error requirements. If this information had been documented in the analyst’s evaluation report, FAA/AST management and system safety analysts (who would later evaluate the hazard analysis for subsequent permit renewals) would have better understood the reasons for the FAA/AST’s acceptance of the method that Scaled Composites used to comply with the human error hazard analysis requirements.

Note: Reference 16 does not give any information regarding the experience/skill of the FAA/AST analyst who evaluated Scaled Composites’ hazard analysis, or any information regarding the FAA/AST analyst’s workload or time constraint, if any, to complete the evaluation within the 120-day review period.

### **TT1 – Team Composition LTA**

According to the FAA’s Licensing and Evaluation Division (AST) manager, there was no one in the division with a degree in human factors; however, there were two pilots on his staff that were familiar with human factors concepts.

### **MW3 – System Reliability LTA**

Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.

## **Chain #6 – Unrequested Hazard Analysis Waiver Issue**

The FAA Office of Commercial Space Transportation (AST) did not ensure that Scaled Composites was in compliance with the mitigations cited in the waiver from regulatory requirements or determine whether those mitigations would adequately address human errors with catastrophic consequences (ref. 16, Finding #12).

The FAA issued an experimental permit to Scaled Composites on May 23, 2012, which was granted renewal on May 22, 2013. On July 18, 2013, the FAA published a notice of waiver, “Waiver of 14 CFR 437.29 and 437.55(a) for Scaled Composites, LLC,” which waived them of the need to comply with regulations 437.29 and 437.55(a). A renewal of the permit and waiver was granted again on May 21, 2014.

After the FAA/AST granted the first renewal of the SpaceShipTwo experimental permit, the FAA/AST formed a team to conduct another review of Scaled Composites’ hazard analysis because of questions that an FAA/AST system safety engineer raised. The review determined that the hazard analysis did not meet the minimum regulatory requirements. (Specifically, Scaled Composites’ hazard analysis did not clearly establish the relationship between each of the requirements of the regulation, the assumptions made, the resulting method used to show compliance, and any mitigation used. As a result, on July 9, 2013, the FAA/AST issued a waiver for the software and human error hazard analysis requirements of sections 437.29 and 437.55(a) for the first renewal of Scaled Composites’ experimental permit. The FAA’s notice of waiver stated that, although Scaled Composites’ experimental permit application did not identify software or human errors, the mitigations that Scaled Composites had in place (aircraft and spacecraft design redundancy, flight and maintenance procedures, and ground and flight training) would prevent hazards resulting from such errors.

### **Influence Chain #6 Summary:**

- **SL6** – Regulator Relationship Mgmt LTA ->
- **ES4** – Technical Controls/Risk Mgmt LTA ->
- **TS4** – Safety/Human Factors Awareness ->
- **TT3** – Team Communication LTA ->
- **MW3** – System Reliability LTA

### **SL6 – Regulator Relationship Mgmt LTA**

Limited interactions between the FAA/AST and applicants during the experimental permit evaluation process. The dividing line between the questions that the FAA/AST needs to ask to determine the risk to the public and those to assess mission objectives is not always apparent because certain aspects of a vehicle’s design and operation could impact both public safety and mission safety assurance. Thus, more extensive interactions between FAA/AST technical staff and prospective experimental permit applicants during permit evaluations would help to perform this work more effectively in the future.

Scaled Composites had not informed FAA/AST personnel that early unlocking of the feather could be catastrophic, which provided further evidence of Scaled Composites’ expectation that a pilot would perform as trained and not unlock the feather early.



According to interviews with FAA AST personnel, some were aware that unlocking the feather during the transonic phase could lead to a catastrophic failure; however, that specific issue was not looked at because while “the team might have discussed it, but it wasn’t one of those items, because of the limitations we have on the permit, that we really looked at that particular issue.” Asked if there was any discussion about Scaled Composites mitigating the risk of this catastrophic failure, one AST 200 staff member said, “Well, there was no, that I know of, no legal requirement that they need to mitigate that risk.”

#### **ES4 – Technical Controls/Risk Mgmt LTA**

Scaled Composites did not have an “opportunity to comment on or correct the areas of noncompliance before the waiver was issued. In addition, the FAA/AST did not consult with Scaled Composites technical staff as part of the waiver evaluation process.

According to an April 2015 FAA memo in response to an NTSB request for information as part of the accident investigation, the FAA/AST did not ask Scaled Composites to modify its hazard analysis because the areas of noncompliance raised no public safety issues. The memo also indicated that, after reassessing Scaled Composites’ hazard analysis, the FAA/AST recognized that a waiver was “procedurally” necessary because Scaled Composites’ approach did not meet all of the requirements of the regulation.

#### **TS4 – Safety/Human Factors Awareness**

“The NTSB believes that the FAA/AST should only waive regulatory requirements for identifying hazards caused by human error under very limited circumstances and should ensure that an applicant seeking a waiver has sufficiently justified the basis for the waiver.

The NTSB is concerned about the FAA/AST’s lack of awareness regarding whether Scaled Composites was in compliance with the mitigations discussed in the waiver from the software and human error hazard analysis requirements of 14 CFR 437.55(a). Some of the inspectors who were interviewed were unfamiliar with the details of the waiver, and all of the interviewed inspectors thought that Scaled Composites complied with the waiver for each powered flight. The NTSB concludes that the FAA/AST did not ensure that Scaled Composites was in compliance with the mitigations cited in the waiver from regulatory requirements or determine whether those mitigations would adequately address human errors with catastrophic consequences.” (ref. 16)

#### **TT3 – Team Communication LTA**

The lack of direct communication between FAA Office of Commercial Space Transportation technical staff and Scaled Composites technical staff...interfered with the FAA’s ability to thoroughly evaluate the SpaceShipTwo experimental permit application [ref. 16, Finding #11].

#### **MW3 – System Reliability LTA**

Due to inadequate design considerations of the pilot-system interface, the feather system design was not reliable.

Note: The following two NTSB findings do not seem to describe direct contributors to the mishap. They would likely be listed as observations if NASA MIB terminology was used by the NTSB:

- The experimental permit pre-application consultation process would be more effective if it were to begin during a commercial space vehicle's design phase so concerns can be resolved before a commercial space vehicle is developed and manufactured and potential catastrophic hazards resulting from human error can be identified early (ref. 16, Finding #13).
- The effectiveness of the FAA Office of Commercial Space Transportation's inspection process would be improved if inspectors were assigned to commercial space operators rather than individual commercial space launch operations because the inspectors could become more familiar with the operators' training and procedures and could identify ways to enhance safety (ref. 16, Finding #14).

## Appendix J. Aggregate Data Analysis

The causes involved in the eight analyzed incidents are listed in Table J-1. The organizational and dual organizational/local factors that occurred a minimum of five times and in at least five of the eight incidents have been highlighted.

***Table J-1. Number of Causes for All Categories***

<b>Cause Type</b>	<b># of HSF-1 Events</b>	<b>Total</b>
SL1 Organizational Culture LTA	5	5
SL2	3	3
SL3	2	3
SL4	0	0
SL5	1	1
SL6	3	3
SL7	2	3
SL8	0	0
ES1	2	2
ES2	1	1
ES3 Schedule Controls LTA	5	6
ES4 Technical Controls/Technical Risk Management LTA	8	16
ES5	0	0
ES6	1	1
ES7 Organizational Learning Systems LTA	6	7
ES8	0	0
DS1	0	0
DS2 System/Part Design & Development LTA	6	10
DS3 Task Design & Development LTA	5	5
DS4	2	2
DS5	1	1
DS6	1	1
DS7 Organizational Design LTA	5	5
TS1	3	3
TS2	3	3
TS3	3	3
TS4	2	2
TS5	1	1
SV1	2	2

<b>Cause Type</b>	<b># of HSF-1 Events</b>	<b>Total</b>
SV2	2	2
SV3	1	1
SV4	0	0
<b>QC1 Inspection/Secondary Verification Requirements LTA</b>	<b>6</b>	<b>9</b>
QC2	0	0
QC3	0	0
QC4	1	1
QC5	1	1
TT1	2	3
TT2	0	0
TT3	4	4
TT4	4	4
TT5	0	0
TT6	0	0
OP1	0	0
<b>OP2 Incomplete Procedures</b>	<b>7</b>	<b>12</b>
OP3	0	0
OP4	2	2
SI1	3	3
SI2	0	0
SI3	1	1
SI4	3	3
SI5	1	1
MW1	1	1
MW2	2	2
MW3	6	15
MW4	0	0
MW5	6	8
MW6	1	1
MW7	1	1
IN1	0	0
IN2	5	11
IN3	1	1
IN4	2	2
IN5	1	1
IN6	1	1
IN7	0	0

**Table J-2. “Inadequate Technical Controls/Technical Risk Management” Summary Table**

<b>Event</b>	<b>Tech Controls/Risk Mgmt LTA: Technical Issue Not Sufficiently Analyzed</b>	<b>Tech Controls/Risk Mgmt LTA: Safety Issue Not Sufficiently Analyzed</b>	<b>Tech Controls/Risk Mgmt LTA: Aggregation of Technical Risks Not Performed</b>	<b>Tech Controls/Risk Mgmt LTA: Readiness Reviews LTA</b>
Apollo 1	Tech Controls LTA. The difficulty of opening the inward hatch in case of an emergency was not analyzed adequately. The increased pressure from the fire - in an already pressurized Command Module - made it impossible for the astronauts to open the hatch.	Tech controls LTA. Teflon coated wiring was selected for flight performance. The risk of wire abrasions due to vehicle ground processing and maintenance was not mitigated. The wiring was not protected by covers. The technicians requested trays to cover and protect the wiring and were told there was no time to design/build protective trays. They were told to use rubber mats instead to cover the wiring. Known risk that was ignored until after the fire. <i>See p. 27, Finding 1: NASA Apollo 204 Review Board</i>		Tech Controls LTA. (Reviews not adequate). Deputy Administrator Seamans wrote that NASA's single worst mistake in engineering judgment was not to run a fire test on the Command Module prior to the plug-out test. NASA almost scrubbed the block 1 spacecraft - all of them were scrubbed except spacecraft 012/Apollo 1.

Soyuz 1	<p>Tech Controls LTA The failure mode of the primary parachute's malfunction of being stuck in the container, which caused a failure of the backup chute, was not accounted for in the design.</p> <p><i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 588: "Utkin's subcommission finished its work, which included some experimental analyses, by June 20 and emerged with the cause of the accident: a release failure of the container block of the primary parachute. .</i></p>		<p>Technical Controls LTA. There was no risk roll-up process to highlight all the many defects and system test failures and make a solid case against the decision to launch. From the point of view of the military quality assurance inspectors, there were 100 unresolved discrepancies on Soyuz-1</p>	
Skylab 1	<p>Tech Controls LTA. As a consequence of the meteoroid shield break-up and loss, there was 1) a failure of full deployment of the SAS-2 wing and 2) a failure of the S-II interstage adapter to separate in flight. The effect of one system failure had consequences for the proper functioning of other related systems.</p>	<p>Technical Controls. It was a false presumption that the shield would be "tight to the tank" and "structurally integral with the S-IVB tank" as set forth in the design criteria; therefore no safety review.</p> <p><i>The most probable cause of the failure of the meteoroid shield was internal pressurization of its auxiliary tunnel. This internal pressurization acted to force the forward end of the tunnel and meteoroid shield away from the OWS and into the supersonic air stream. The resulting forces tore</i></p>		<p>Technical Controls: Failure to recognize the significance of the aerodynamic loads during launch on the MS during multiple design and milestone reviews. <i>There was no shortage of reviews and yet, a major omission occurred throughout the process – consideration of aerodynamic loads on the meteoroid shield during the launch phase of the mission. Throughout the six-year period of progressive reviews and certifications . . . never did the matter of aerodynamic loads on the shield or aeroelastic interaction between the shield and its external pressure environment during launch receive</i></p>

		<p><i>the meteoroid shield from the OWS...The pressurization of the auxiliary tunnel resulted from the admission of high pressure air into the tunnel through several openings in the aft end. These openings were: (1) an imperfect fit of the tunnel with the aft fairing; (2) an open boot seal between the tunnel and the tank surface; and (3) open stringers on the aft skirt under the tunnel. ((10 – 1), p. 141)</i></p>		<p><i>the attention and understanding during the design and review process which in retrospect it deserved. (See page 9-3)</i></p>
STS-1 Oxygen Deficiency		<p>Technical Controls LTA. The dev was not processed through contractor or NASA safety. Processed as a normal dev, not a hazardous dev. Since the dev was not labeled as hazardous, safety did not review and an access control sign was used. No one was ensuring that the devs were labeled correctly, especially when there were 500 devs.</p>		

STS-1 SRB IOP	During the 1975 timeframe, the inter-element interfaces and their element backup structure were extremely sensitive to small parameter changes, such as SRM thrust mismatch, rise rate, and misalignment, and forced a costly redesign of this structure. Since the overpressure environment did not have a major influence on these loads, it was inadvertently assumed to be insignificant to all the Shuttle subelements.			
Scaled Composites		Tech Controls LTA. It appears that an operational hazard analysis was not performed. <i>Cal OSHA Report - Finding 2 - Item 001 "Serious Violation, \$18,000 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 . . . this failure contributed to the serious injuries suffered by six employees."</i>		
		Technical Controls/Risk Management. There was no evidence of a blast danger area computation, or		



		even consideration of a blast danger area control zone for the N2O test site.		
Ares 1-X				Technical Controls/Risk Management. There was no contractual requirement to do a first time test readiness review or perform a loads analysis. Those assigned to the Ares 1X task did not perceive the Constellation Launch Vehicle (CLV) work as being "new" but rather an extension of well-practiced Shuttle-type tasks. Even though the Ares 1X parachute riser lines were approximately 4x longer than the riser lines on the Shuttle's drag chute, there was no requirement for engineering to perform a first-time GSE DE load's analysis of the test set-up, or an Integrated Product Team (IPT) readiness review, for the initial Area 1X parachute static strip test.
SpaceShipTwo	Technical Controls/Risk Mgmt LTA Scaled did not request the waiver or have an opportunity to comment on the waiver before it was issued...(NTSB, p. 51) Scaled did not have an "opportunity to comment on or correct the areas of noncompliance before the waiver was issued. In addition, the FAA/AST did not consult with Scaled technical staff as part of	Technical Controls / Risk Management LTA Scaled Composites' 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. (NTSB Finding #6, p. 67) By not considering human error as a		Technical Controls LTA PF04 Flight Readiness Reviews – Scaled Composites held three flight readiness reviews (FRR's) prior to PF04 – a FRR, a Delta FRR and an Executive FRR. The FRR was held on October 3, 2014, the Delta FRR was held on October 27, 2014, and the Executive FRR was held on October 29, 2014. According to those in attendance at the FRRs, there was <u>no discussion of the feather system</u> . . . A review of the FRR action items revealed several item related to the feather system but no items were found related to the pilot's use of the feather system. (NTSB

	the waiver evaluation process...(NTSB , p. 53	potential cause of uncommanded feather extension on the SS2 vehicle, Scaled Composites missed opportunities to identify the design and/or operational requirements that could have mitigated the consequences of human error during a high workload phase of flight. (NTSB Finding #7, p. 67)		Human Performance Report, p. 23) The FRRs were 3 missed opportunities to discuss the catastrophic hazard of unlocking the feather system too early.
--	---	---	--	---

**Table J-3. “Inadequate Technical Controls/Technical Risk Management” Influence Chain Analysis**

	Apollo 1			Soyuz 1			Skylab -1			STS-1 Oxygen Deficiency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two		
SL2 - Resource (\$ & staff) Allocation LTA											X					
SL3 – High Level Policy Guidance LTA															X	
SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA												X				X
SL7 – Internal Relationship Management LTA		X			X											
ES4 – Technical Controls-Process Change Controls-Risk Management LTA	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DS2 – System-Part Design & Development LTA	X		X					X			X				X	
DS3 – Task Design & Development LTA		X		X								X		X	X	
DS4 – Workspace-Work Env Design & Dev LTA												X				
DS7 – Organizational Design & Development LTA						X										
TS1 – System Training LTA							X									
TS2 – Task Technical Training LTA			X									X				
TS3 – Emergency or Contingency Training LTA		X										X				
TS4 – Safety-HF Awareness Training LTA	X															X
SV1 – Supervisor Task Preparation LTA												X				
QC1 – Inspection-Surveillance-Audit Requirements LTA	X	X		X					X						X	
QC4 – Missed or Cursory Inspection-Surveillance-Audit																
TT1 – Team Composition LTA												X				
TT3 – Team Communication LTA						X										X
TT4 – Accepted Team Practices LTA							X									
OP2 – Incomplete Procedures		X		X					X			X	X	X	X	
SI3 – Support Equip-Tool Feedback LTA													X			
SI4 – System-Part Feedback LTA						X								X		
SI5 – Worker or Work Env Sensory Signals LTA									X							
MW2 – Support Equip-Tool Unavailable-Uncertified				X												
MW3 – System-Part Reliability-Usability LTA	X	X	X		X	X	X			X					X	X
MW5 – Infrequent or Unique Task											X				X	
MW7 – External Work Environment LTA												X				
IN2 – Cognitive Factors						X			X				X	X		



Focus of this influence  
chain analysis



Other top nine recurring cause  
type

**Table J-4. “Incomplete Procedures” Summary Table**

Event	Incomplete Procedures: Situation Not Covered	Incomplete Procedures: Missing Steps
Apollo 1	Incomplete Procedures. Adequate safety precautions were neither established nor observed for this test. Contingency preparations to permit escape or rescue of the crew from an internal Command Module fire were not made. <i>See p. 29, Finding 5: NASA Apollo 204 Review Board</i>	
	Incomplete Procedures. There was no contingency procedure. <i>See blog by technician.</i>	
Soyuz 1	Incomplete Procedures. Procedure did not address the situation of parachute covers not being available.	
Skylab 1		<p>Incomplete/Unclear Procedures. The MS rigging procedures at KSC were based on the STA shield at MSFC, which was different from the flight MS in four significant aspects. These differences were not adequately accounted for in the KSC procedures, so troubleshooting and several additional tasks were needed to complete the MS rigging.</p> <p><i>The rigging procedure that was to be used at KSC was developed jointly by MSFC and MDAC using the STA at MSFC. The STA shield was, however, different from the flight MS in four significant aspects. On the flight MS: (1) the double butterfly hinges on the SAS 1 side of the main tunnel were bonded to the tension straps while on the STA they were present but unbonded; (2) the butterfly hinges on each side of the main tunnel were cut in the middle of a longitudinal joint and refitted to the adjacent panels at a slight angle as mentioned earlier. The longitudinal edges of the panels were also modified to suit the altered hinge line. This change to the flight MS at MDAC was necessary to accommodate the misalignment which occurred in the location of the tension straps on the OWS; (3) a longitudinal misplacement of the tension straps of 0.15 inch too high also resulted in some binding of the forward weather seal and torsion rods that had to be refitted at KSC; and (4) the trunnion bolts, nuts and washers were initially not lubricated on either the flight MS or the STA. This lack of lubrication caused difficulties in the final rigging of the shield at KSC, which was subsequently corrected by applying a solid film lubricant. ((5-7), page 94)</i></p> <p><i>Missing steps (to account for differences in flight MS from the STA shield)</i></p>

Event	Incomplete Procedures: Situation Not Covered	Incomplete Procedures: Missing Steps
STS-1 Oxygen Deficiency		<p>Incomplete Procedures - atmosphere checks or air purge verifications were not in the safety procedure.</p> <p><i>SF1. Additionally, the Access Control procedure, POP 0-204, does not routinely require verification of a safe environment prior to personnel entry of previously closed out compartments. The GP 1098A, referenced by POP 0-204 for enforcement, did contain a requirement for verification of an air purge prior to personnel entry into the Orbiter with toxic propellants on board. The Orbiter had toxic propellants on board but the verification of an air purge was not performed.</i></p> <p>SF1-R2. The KSC Safety documents should be revised and Safety operating procedures developed to adequately describe the requirements and procedures to close out and re-open work areas exposed to inert gases.</p> <p>PF1-R1. Procedures with hazardous operations should contain steps for closing and reopening the affected areas. For procedures involving hazardous environment such steps could include, but not be limited to, environmental sniff checks, placement or removal of barriers and hazard warning signs, use of warning lights, placement of standby emergency personnel, and the establishment of security check points</p> <p><i>Missing steps (to satisfy hazardous constraints)</i></p>
		<p>Incomplete Procedures - no steps in the procedure to open the pad after S0017 was complete.</p> <p><i>PF1. The test procedure in progress did not contain adequate steps for clearing the vehicle/pad complex for hazardous operations or for partially or completely reopening the vehicle/pad complex for resumption of scheduled normal work. A very significant step not included in the test procedure was the posting of the hazardous area of the Orbiter interior with a hazard warning sign. An "access control" sign was used, which could be and was removed without Safety concurrence.</i></p> <p>PF1-R1. Procedures with hazardous operations should contain steps for closing and reopening the affected areas. For procedures involving hazardous environment~ such steps could include, but not be limited to, environmental sniff checks, placement or removal of barriers and hazard warning signs, use of warning lights, placement of standby emergency personnel, and the establishment of security</p>

Event	Incomplete Procedures: Situation Not Covered	Incomplete Procedures: Missing Steps
		check points. <i>Missing steps (to satisfy hazardous constraints)</i>
		Incomplete Procedures - OMI S0017, contingency procedures  <i>CF4. The OMRSD for the ECS System requires that O2 atmosphere checks be conducted prior to personnel re-entry into areas that have been exposed to GN2. The atmosphere checks subsequent to GN2 purge for the Orbiter compartments were not included in OMIs S0017 or VI122.</i>  CF4-R1. All OMIs should be reviewed to insure that OMRSD hazardous constraints have been included.  <i>Missing steps (to satisfy hazardous constraints)</i>
STS-1 SRB IOP		
Scaled Composites	Incomplete Procedures. There was no written contingency or emergency procedure.  <i>Situation not covered</i>	Incomplete Procedures (no warnings). MSDS documents, in their most basic form from N2O suppliers, caution against pressure shock. There were no warnings in the work instructions about the dangers of pressure shock. There was not a designated hazard control area.  <i>Missing cautions/warnings</i>
Ares 1-X		Incomplete Procedures. The work order did not specify a detailed test set-up for attaching the load line to the risers. Consequently, the riggers used a 3/8 inch nylon rope. The fact that the work order was written, approved by Quality and Safety, released and worked all in the same day could be a reason why the work order did not specify a detailed test set-up for attaching the load line to the risers.  <i>Missing steps (test setup)</i>
		Incomplete Procedures. The task was not identified as hazardous, nor did it contain instructions to rope off a control area. Because the task was not identified as hazardous a safety person was not required to be present during the static strip test and was not in the facility at the time of the injury.  <i>See page 30 of SAIB Report - Finding 1: "Two non-load rated stainless steel rods tied at mid-point became overloaded, bent and escaped riser loops." Also page 31 - Finding 2: "Task was not identified as hazardous in WAD. Use of nylon towline to pull out parachute created dangerous amount of stored energy." Also, page 33 - Finding 4: "Tying towline to stainless steel rod mid-point</i>

Event	Incomplete Procedures: Situation Not Covered	Incomplete Procedures: Missing Steps
		<p><i>permitted the escape of the rods when the rods bent."</i></p> <p><i>Missing steps (to satisfy hazardous constraints)</i></p>
SpaceShipTwo		<p>Incomplete Procedures</p> <p>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 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. (NTSB Human Performance Report, p. 21)</p> <p>If Scaled had incorporated a pilot flying/pilot monitoring challenge and response protocol for the unlocking task (given the safety consequences if the task were performed incorrectly), the task would have been redundant because both pilots would have been included in the recognition and response decision-making of the task. (NTSB p. 43)</p> <p>Also, there was "no warning, caution, or limitation in the SS2 pilot operating handbook (POH) that specified the risk of unlocking the feather before 1.4 Mach." (NTSB p. 39)</p> <p>"There was no warning, caution, or limitation in the SS2 pilot operating handbook or on the PF-04 (powered flight No. 4) test card that specified this risk." (Quote by NTSB Senior Human Performance Investigator Katherine Wilson in the following article:  <a href="http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/">http://spaceflightnow.com/2015/07/28/spaceshiptwo-mishap-dut-to-pilot-error-and-company-training-oversight/</a>)</p> <p>The NTSB's review of the SS2 emergency procedures did not find a warning stating that uncommanded feather movement during transonic flight would also be catastrophic. (NTSB, p. 39)</p>

**Table J-5. “Incomplete Procedures” Influence Chain Analysis**

	Apol- lo 1	Soy- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two
SL2 - Resource (\$ & staff) Allocation LTA							X	
SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA						X		
SL7 – Internal Relationship Management LTA	X							
ES1 – Administrative Controls LTA				X				
ES2 – Budget Controls LTA							X	
ES4 – Technical Controls-Process Change Controls-Risk Management LTA	X	X		X		X	X	X
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA		X			X			
DS3 – Task Design & Development LTA	X	X	X			X	X	X
DS4 – Workspace-Work Environment Design & Dev LTA							X	
DS7 – Organizational Design & Development LTA								X
TS2 – Task Technical Training LTA						X		
TS3 – Emergency/Contingency Training LTA	X				X	X		
SV1 – Supervisor Task Preparation LTA						X		
QC1 – Inspection-Surveillance-Audit Requirements LTA		X	X	X				
TT1 – Team Composition LTA							X	
TT3 – Team Communication LTA				X				
OP2 – Incomplete Procedures	X	X	X	X	X	X	X	X
SI1 – Written Support Information LTA				X				
SI3 – Support Equipment-Tool Feedback LTA							X	
SI4 – System-Part Feedback LTA								X
SI5 – Worker or Work Environment Sensory Signals LTA				X				
MW2 – Support Equip-Tool Unavailable-Uncertified		X						
MW3 – System-Part Reliability-Usability LTA	X							
MW5 – Infrequent or Unique Task		X	X			X	X	X
MW7 – External Work Environment LTA						X		
IN2 – Cognitive Factors		X		X	X		X	X
IN3 – Emotional Factors				X				



Focus of this influence  
chain analysis



Other top nine recurring  
cause type



**Table J-6. “Inadequate Inspection/Secondary Verification Requirements” Summary Table**

Event	Quality Inspection/Secondary Verification Requirements LTA: Missing or Deficient Requirements	Quality Inspection/Secondary Verification Requirements LTA: Incorrect Assumptions
Apollo 1	Inspection Reqmts. Given the fragile nature of the Teflon coated wiring, inadequate attention was given to the inspection of the wire bundles for evidence of insulation abrasion or deformation.	
	Inspection Requirements. The requirements for quality inspections were either missing or deficient.	
	Inspection Reqmts. Combustible materials were allowed inside vehicle. No requirements for inspection.	
Soyuz 1	Inspection Requirements. No requirement to inspect the parachute container for contamination. <i>Excerpt from:</i> <a href="http://www.russianspaceweb.com/soyuz1.html">http://www.russianspaceweb.com/soyuz1.html</a> - <i>After the loss of Soyuz-1, new regulations required the removal of the parachute containers from the reentry capsule, before its installation in the autoclave (for the polymerization process).</i>	
Skylab 1	Inspection Requirements LTA. Quality inspections were either absent or inadequate; they did not identify the “tight fit” issue during ground processing.	
STS-1 Oxygen Deficiency	Inspection Requirements LTA - applicable safety documents did not have sufficient requirements for atmosphere checks or verification of an air purge before aft reentry.  <i>Normally areas exposed to GN2 would have been purged with air and checked with a hand held O2 meter for a breathable atmosphere before allowing entry.” (2g-81)</i>  <i>SF1. The KSC Safety documents (KMI I710.IC, KHB I710.2A, and GP 1098A) do not contain requirements and/or procedures for closing or opening work areas exposed to an inert gas environment.</i>  SF1-R1. Access control policy and practice should be implemented to insure a safe environment before allowing entry into the Orbiter or other similar flight hardware and facility/equipment compartments.	

Event	Quality Inspection/Secondary Verification Requirements LTA: Missing or Deficient Requirements	Quality Inspection/Secondary Verification Requirements LTA: Incorrect Assumptions
STS-1 SRB IOP		
Scaled Composites		
Ares 1-X		Inspection Requirements. The insertion of the rods was a definite deviation from the written procedure - and unless the quality rep wasn't paying any attention at all, he would have seen the rods inserted through the two riser end loops, prior to the start of the test. Unlike Shuttle operations, the SRBE did not have a requirement for real-time "pen and ink" annotations in the procedure, to authorize deviations from the released floor procedure.
SpaceShipTwo	Inspection/Surveillance/Audit (Validation) Requirements LTA Scaled did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Validation is the process that ensures that the implemented safety measure is right. Specifically, AC 23.1309-1D stated, "for the purposes of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and found to be reasonable. (NTSB, p. 41)	Inspection/Surveillance/Audit (Validation) Requirements LTA Scaled did not perform task-specific validation measures consistent with those in AC 23.1309-ID. Although the unlocking task was directly associated with a catastrophic hazard, Scaled did not evaluate this task to determine a specific training protocol that would measurably and reliably reduce the possibility that the task would be performed incorrectly. (NTSB, p. 42) Validation is the process that ensures that the implemented safety measure (i.e., training) is right. Scaled Composite's assumptions regarding pilot performance were not rigorously verified and validated . . . (NTSB, p. 43)

**Table J-7. “Inadequate Inspection/Secondary Verification Requirements” Influence Chain Analysis**

	Apollo - 1		So y- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two	
SL1 – Organizational Culture LTA			X							
SL3 – High Level Policy Guidance LTA										X
SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA		X								
ES3 – Schedule Controls LTA			X							
ES4 – Technical Controls-Process Change Controls-Risk Management LTA	X			X	X					X
ES6 – Procurement-Logistics-Material Control Sys LTA		X								
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA										X
DS2 – System-Part Design & Development LTA	X							X		
DS3 – Task Design & Development LTA			X	X						
DS6 – Training Course Design & Development LTA									X	
DS7 – Organizational Design & Development LTA		X								
TS1 – System Training LTA									X	
TS4 – Safety-Human Factors Awareness Training LTA	X									
TS5 – Leadership and Team Skills Training LTA								X		
SV2 – Supervision During Task LTA			X							
QC1 – Inspection-Surveillance-Audit Requirements LTA	X	X	X	X	X			X	X	X
TT3 – Team Communication LTA								X		
TT4 – Accepted Team Practices LTA			X							
OP2 – Incomplete Procedures			X	X	X					
SI1 – Written Support Information LTA		X							X	
SI5 – Worker or Work Environment Sensory Signals LTA					X					
MW2 – Support Equipment-Tool Unavailable-Uncertified			X					X		
MW3 – System-Part Reliability-Usability LTA	X	X								X
MW5 – Infrequent or Unique Task				X						
IN2 – Cognitive Factors		X			X			X	X	
IN4 – Individual Experience & Skills LTA			X							



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

**Table J-8. "Inadequate Schedule Controls" Summary Table**

Event	Schedule Controls LTA: Overly Aggressive or Unrealistic Schedules	Schedule Controls LTA: Schedule Communication/Coordination
Apollo 1	<p>Schedule Controls. The Command Module was shipped to KSC with much open work. "There is an inference that the design, qualification and fabrication process may not have been completed adequately prior to shipment to KSC."</p> <p>See p. 3 "History of the Accident" <a href="http://history.nasa.gov/Apollo204/history.html">http://history.nasa.gov/Apollo204/history.html</a>).  Gene Kranz - after the fire: "We were too gung ho about the schedule . . . We were not ready!"  Deke Slayton: "We got in too much of a goddamned hurry."</p>	
Soyuz 1	<p>Schedule Controls. Schedule pressure not managed properly.</p> <p>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 573: "The pace at Tyura-Tam was intense."</p>	
Skylab 1		
STS-1 Oxygen Deficiency	<p>Schedule controls - schedule pressure, shop schedule being followed versus the integrated schedule. Shop schedule showed the dev as being hazardous, but the integrated schedule did not.</p> <p>SF3. Schedule motivation created a practice of allowing side work to be approved and carried out in parallel with hazardous operations. This practice, even when subjected to special Safety controls, increased risk and susceptibility to accident. One example was an incident recorded on January 16, 1981, involving personnel who were doing side work inside the LOX TSM while GN2 was flowing per OMI and who had to evacuate when an 8-inch GN2 duct failed. Another incident earlier on the day of the accident involved two LPAC monitors performing a side task who were exposed to HPU exhaust products without Scott Air Paks fully donned.</p> <p>SF3-R1. 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.</p>	<p>Schedule Controls LTA. OMI S0017 Launch Countdown Demonstration Test was conducted during the period from March 17 through March 19, 1981. In the pre-planning for this test activity deviation #13-20 was written to accommodate the special test. (page 2a5) Dev. 13-20 was written on March 16th. The dev. did not identify the fact that the GN2 purge would have to be extended to accomplish the test. The dev. was inserted just prior to the GN2 to air transfer (p. 2a-5). During the performance of the FRR, which was conducted 2/20/81, there was an indication of a GN2 intrusion into the crew compartment. Since GN2 was provided during S0017, a special leak test was planned to be conducted as a tack-on to that procedure.</p> <p>See p. 1d-10 for dev. processing timeline.  See Chain #2 re: 500 devs.  Dev not on the integrated schedule as a hazard. Last minute, opportunistic scheduling.</p> <p>CF3. The Orbiter Daily Schedule reflected work to be accomplished in the Orbiter aft section at a time when the integrated schedule showed the Orbiter was under test with a hazardous operation indicated.</p> <p>CF3-R1. Element work schedules should reflect with high fidelity the Shuttle Operations (VO) integrated test schedule timeline to prevent planning of incompatible stand-alone work.</p> <p>SF2-R2. An operational constraint on deviation traffic should be implemented such as providing a hard cutoff point at or prior to the pre-test briefing on all but mandatory</p>

Event	Schedule Controls LTA: Overly Aggressive or Unrealistic Schedules	Schedule Controls LTA: Schedule Communication/Coordination
		<i>deviations to a procedure. All significant deviations released prior to the cutoff point should be reviewed at the pre-test briefing and the subsequent mandatory deviations reviewed prior to initiation of test or at an appropriate test point prior to execution. SF2-R3. Changes to hazardous tests which extend the duration of the hazardous operation should be identified, timed, and reflected in the schedule.</i>
STS-1 SRP IOP		
Scaled Composites		
Ares 1-X	Schedule Controls. Schedule pressure contributed to a focus on the completion of the static strip test rather than the test itself. There was a delay in obtaining a DOT certified container for shipping the parachute to AZ, yet the scheduled date for the AZ drop test was not slipped to the right. Immediately after the static strip test was completed at KSC, the parachute was being delivered to Yuma, AZ for the first Ares 1X parachute drop test which was scheduled the next week. On Sept. 4th, the procedure was written, approved by Quality and Safety, released and worked. Interviews with PRF personnel and comments in the SAIB report reflect the "insane" and "aggressive" Ares 1X schedule.	
SpaceShipTwo	Schedule Controls LTA ...the pressure to approve experimental permit applications within a 120-day review period... interfered with the FAA's ability to thoroughly evaluate the SS2 experimental permit application. (NTSB Finding #11, p. 68)	

**Table J-9. “Inadequate Schedule Controls” Influence Chain Analysis**

	Apol- lo 1	Soy- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency		STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two
SL1 – Organizational Culture LTA	X								
SL3 – High Level Policy Guidance LTA		X							X
SL5 – Customer-Stakeholder Relationship Mgmt LTA								X	
ES3 – Schedule Controls LTA	X	X		X	X			X	X
DS2 – System-Part Design & Development LTA		X							
DS5 – Procedure Design & Development LTA				X					
DS7 – Organizational Design & Dev LTA					X				
SV1 – Supervisor Task Preparation LTA								X	
SV2 – Supervision During Task LTA	X								
SV3 – Poor Supervisor Example or Excessive Risk Taking		X							
QC1 – Inspection-Surveillance-Audit Requirements LTA	X								
QC4 – Missed or Cursory Inspection-Surveillance-Audit									X
TT1 – Team Composition LTA									X
TT4 – Accepted Team Practices LTA	X				X				
OP4 – Unclear-Misunderstood Procedures				X					
MW3 – System-Part Reliability-Usability LTA		X							
MW5 – Infrequent or Unique Task				X	X				
IN2 – Cognitive Factors				X					
IN4 – Individual Experience & Skills LTA									
IN6 – Individual Assertiveness LTA								X	



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

**Table J-10. "Inadequate Organizational Learning Systems" Summary Table**

<b>Event</b>	<b>Organizational Learning Systems LTA: Internal Lesson Not Learned</b>	<b>Organizational Learning Systems LTA: External Lesson Not Learned</b>
Apollo 1		Org. Learning Systems. NASA knew of recent accidents that had occurred in pure oxygen environments. NASA also had been briefed by experts about the hazards of working in 100% oxygen environments. Since the vehicle was not fueled, the plug-out test was considered non-hazardous. The procedure should have been marked hazardous because of the pure oxygen environment. <i>See p. 29, Finding 5: NASA Apollo 204 Review Board</i>
Soyuz 1		
Skylab 1		
STS-1 Oxygen Deficiency	<p>Organizational learning systems LTA.</p> <p>(1) "In April 1967, during the Congressional hearings of the Apollo 204 accident, Congress requested for the record correspondence from the Safety Office, Kennedy Space Center, pertaining to timely submittals of operational checkout procedures for review. The response from KSC Safety was not favorable. A workable solution had not been established to assure the receipt of procedures in a timely manner. The review and processing of STS-1 procedures also has experienced difficulties in timeliness in submission to Safety for review. For additional information refer to Report of the Apollo 204 Review Board Appendix G, Part 2, Page G34, G35."</p> <p>(2) Similar incident on January 16, 1981.</p> <p><i>SF3. Schedule motivation created a practice of allowing side work to be approved and carried out in parallel with hazardous operations. This practice, even when subjected to special Safety controls, increased risk and susceptibility to accident. One example was an incident recorded on January 16, 1981, involving personnel who were doing side work inside the LOX TSM while GN2 was flowing per OMI and who had to evacuate when an 8-inch GN2 duct failed. Another incident earlier on the day of the accident involved two LPAC monitors performing a side task who were exposed to HPU exhaust products without Scott Air Paks fully donned.</i></p>	

Event	Organizational Learning Systems LTA: Internal Lesson Not Learned	Organizational Learning Systems LTA: External Lesson Not Learned
STS-1 SRP IOP	<p>Partial lesson learned. Solid rocket motor ignition overpressure was a known phenomenon and considered in the design; however, although the amplitude was generally predicted, its frequency characteristics were less well defined, and there was no adequate determination of either the AP forcing function or the structural response of the vehicle to this function. Therefore, the correct response was not predicted.</p> <p>Ref. NASA TM82458 p1</p>	
Scaled Composites		<p>Org Learning Systems. It was not clear to what extent the hazards of N2O were understood by the test team, even though the hazards of N2O were well documented in industry. Failure to learn from previous OSHA citations. There was a serious lack of engineering controls to abate the documented hazards of N2O storage and handling.</p>
Ares 1-X	<p>Organizational Learning Systems. Stored energy. Nine months prior to this lost time injury event, on 12/10/2006, during Solid Rocket Booster Element (SRBE) retrieval ship operations following the launch of STS-116, a ship's member lost a portion of his toe when the frustum they were securing unexpectedly rose approximately 3 inches from the wooden decking and immediately returned to the deck, trapping the left foot/toes of the team member. Nylon straps were used to secure the frustum. The nylon straps stretched and allowed the load (frustum) to shift, during a crane movement and pivoting of the power block. A recommended corrective action was to share the lessons learned of the stored energy hazard inherent in using nylon ropes/straps. Also, in 2002, the PRF incurred a mishap involving a tensile tester.</p>	
	<p>Organizational Learning Systems. Task team leadership. During Solid Rocket Booster Element (SRBE) retrieval ship operations following the launch of STS-116, the ship's crew experienced 2 significant lost time injuries. Both incidents reflected deficient task team leader behaviors as well as task team behaviors; these lessons were not incorporated in the PRF.</p>	



<b>Event</b>	<b>Organizational Learning Systems LTA: Internal Lesson Not Learned</b>	<b>Organizational Learning Systems LTA: External Lesson Not Learned</b>
SpaceShipTwo		Organizational Learning Systems LTA 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 aviation (DOD and commercial), 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.

**Table J-11. “Inadequate Organizational Learning Systems” Influence Chain Analysis**

	Apol- lo 1	Soy- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two
SL1 – Organizational Culture LTA						X		X
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA	X			X	X	X	X	X
DS2 – System-Part Design & Development LTA					X	X		
DS3 – Task Design & Development LTA	X							
TS1 – System Training LTA						X		
TS2 – Task Technical Training LTA							X	
TS3 – Emergency or Contingency Training LTA				X				
TS5 – Leadership and Team Skills Training LTA							X	
QC1 – Inspection-Surveillance-Audit Requirements LTA							X	
QC5 – Statistical Methods LTA					X			
TT1 – Team Composition LTA								X
TT3 – Team Communication LTA							X	
OP2 – Incomplete Procedures	X			X				
OP4 – Unclear-Misunderstood Procedures							X	
MW1 – Support Equip-Tool Reliability-Usability LTA							X	
MW2 – Support Equipment-Tool Unavailable-Uncertified							X	
MW3 – System-Part Reliability-Usability LTA					X	X		
MW5 – Infrequent or Unique Task	X							
IN2 – Cognitive Factors	X			X			X	X
IN4 – Individual Exp & Skills LTA								X



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

**Table J-12. “System Design and Development Issues” Summary Table**

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
Apollo 1	System Design and Development. Grissom was so frustrated by the many technical failures of the spacecraft during testing that he hung a lemon on the simulator.	System Design. The procedure planned for the emergency egress to occur in 90 seconds. Astronauts would open the interior hatch. The 2nd exterior hatch had 8 bolts that needed to be removed. A special tool was required to lift the 3rd hatch from the command module. The actual opening of the hatch was difficult and took too long to be executed in any emergency.		System Part Design & Development. Teflon was specifically chosen for the wire coating due to its excellent insulation, chemical inertness and fire resistance. However, Teflon is soft and therefore susceptible to creep, or cold-flow deformation and abrasion. The Teflon coating had worn away during operations, exposing the electrical wiring.
Soyuz 1	System Design and Dev. Inadequate testing of the spacecraft.  <i>Excerpt from the book "Challenge to Apollo" by Asif A. Siddiqi, page 590: "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."</i>			
	System Design. The capsules used in the aircraft drop tests were covered with regular foam only. They did not go through the same thermal protective polymerization process that was used on the Soyuz capsules that were launched.  <i>Excerpt from <a href="http://www.russianspaceweb.com/soyuz1.html">http://www.russianspaceweb.com/soyuz1.html</a> - "After the investigative commission formally ended its work, another unofficial</i>			

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
	<p><i>explanation for the parachute system failure had emerged. Boris Chertok, a key figure at OKB-1 design bureau laid out this scenario in his memoirs, and it also made it into the official history of the design bureau. According to the theory, the parachute container onboard Soyuz-1 could have been contaminated by a glue-like polymer-based thermal protection material, which is applied to the exterior of the re-entry capsule. According to Chertok, first unmanned Soyuz capsules were placed inside a special autoclave to polymerize the thermal protective layer <u>without parachute containers</u>, whose production was behind schedule. By the time the re-entry capsule of the Soyuz-1 went into the autoclave, parachute containers had been installed but their <u>covers were still unavailable</u>. As a result, Chertok hypothesized, a flight-ready parachute container on the Soyuz-1 could be protected with a <u>temporary cover</u> during the polymerization process, which could let glue-like substance to get inside." (This coating formed a rough surface, thus eventually preventing the parachute from deploying on Soyuz-1) This fatal flaw had never had a chance to manifest itself during aircraft drop tests, since the capsules used in those tests had been covered with regular foam and never had to go through the polymerization process.</i></p>			

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
Skylab 1	<p>System Part Design and Development LTA. Inadequate testing and verification of system interfaces. In addition to considering the MS as a system, the consideration of the MS as a part of other systems was not fully appreciated, increasing the brittleness of the OWS system.</p> <p><i>No deployment tests were conducted under vacuum conditions, which is quite acceptable in view of the low rate of motion of the deployment. Vibration, acoustic, and flutter tests were specifically omitted in the test specifications because of the design requirement that the shield be "tight to the tank." This design requirement and pervading philosophy of design and development also served to omit all aerodynamic tests of the meteoroid shield.</i></p> <p><i>12. Given the basic view that the meteoroid shield was to be completely in contact with and perform as structurally integral with the S-IVB tank, the testing emphasis on ordnance performance and shield deployment was appropriate. ((10 – 3) page 143)</i></p> <p><i>The redundant mode of ordnance operation of all prior Saturn flights in which both ends of the linear shaped charge are fired at once from a single command would probably have prevented the failure, depending on the extent of damage experienced by the linear shaped charge. (Readings in Systems Engineering, page 186)</i></p>			
STS-1 Oxygen Deficiency				
STS-1 SRB IOP	<p>Liquid and solid rocket motor propulsion systems create an overpressure wave during ignition, caused by the accelerating gas particles pushing against or displacing the air contained in the launch pad or launch facility and by the afterburning of the fuel-rich gases. This wave behaves as a blast or shock wave characterized by a positive triangular-shaped first pulse and a negative half sine wave second pulse. The pulse travels up the space vehicle and has the potential of either overloading individual elements or exciting overall</p>		<p>SRB Ignition is a powerful driver in liftoff environments. System Integration, responsible for liftoff environment definition, accepted the Tomahawk ignition test as a</p>	

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
	<p>vehicle dynamics. The latter effect results from the phasing difference of the wave from one side of the vehicle to the other. This overpressure phasing, or delta-P environment, because of its frequency content as well as amplitude, becomes a design driver for certain panels (e.g., thermal shields) and payloads for the Space Shuttle. Ref. NASA TM82458 abstract</p> <p>As the Shuttle moved toward final verification, it was decided to run some additional tests to obtain better overpressure characteristics. These tests were run without firing the SSME's to remove the extraneous noise from the data. There were differing opinions on how to treat overpressure and analyze the data from the tests. The issue was settled at this time by running loads and again showing the interface loads to not be sensitive to overpressure environments. In retrospect, the amplitudes of the overpressure were fairly accurately predicted by Guest as seen in Figure 4. However, no attempt was made to adjust the overpressure frequency for Pc rise rate effects: this meant that the frequency was under predicted by about 40 percent: 4 Hz from model test data versus 6 Hz from STS-I full-scale data. Ref. NASA TM82458 abstract p6</p> <p>An IOP Wave Committee was formed to, among other assignments; determine why the IOP environment was under predicted. Several root causes were identified: 3) the physics of IOP wave development was not well understood Ref LLIS</p>		<p>sufficient simulation of SRB ignition IOP – Did not fully appreciate the effect of the differences between the SRB and the Tomahawk ignition characteristics Ref Space Shuttle STS-1 Close Calls, Bejmuk, p7</p> <p>Pre STS-1 IOP environments were based on sub-scale testing of 6.4% models (Tomahawk solid propellant rocket) conducted at MSFC. These data were scaled to full scale and applied to the lift off simulations for structural sizing analyses.</p> <p>An IOP Wave Committee was formed to, among other assignments; determine why the IOP environment was under predicted. Several root causes were identified: 1) the 6.4% scale model tests conducted did not simulate the SRB ignition events well, 4) the structural math model did not adequately</p>	

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
			reflect the Space Shuttle Vehicle. Ref: NASA LLIS	
Scaled Composites				System Design. The tank's design included several materials that were incompatible with N2O and the tank did not have a burst disc to protect against rapid over-pressurization.
Ares 1-X				
SpaceShip Two		System Part Design & Development LTA The SS2 feather system was not error tolerant. (Design Out, Guard Against, Warn, Train, or Accept Risk) The SS2 feather system had no design barrier that prevented a crewmember from erroneously unlocking the feather during the transonic region, and the system provided no warning annunciator on the MFD to prompt pilot action when it was appropriate to unlock the feather. (NTSB p. 43) (The transonic region was described as		

Event	System Design & Dev. LTA: Testing Issues (Insufficient Testing, TLYF - FLYT Violations)	System Design & Dev. LTA: Human-System Integration Issues	System Design & Dev LTA: Modeling and Simulation Issues	System Design & Dev LTA: Material Selection Issues
		<p>occurring between 0.9 and 1.1 Mach) According to the SS2 program manager, no safeguards were built into the feather system design because Scaled counted on the pilot "to do the right thing" and dealing with redundancies was "complex." (NTSB p. 43) The NTSB notes that Scaled considered design mitigations for other aspects of the feather system. For example, ..Scaled Composites programmed the MFD to provide pilots with an aural and a visual annunciation if the feather was not unlocked by 1.5 Mach to ensure the feather would be unlocked by 1.8 Mach...(NTSB, p. 43) NOTE: Design considerations for the SS2 feather system could have included, but would not have been limited to, a mechanical lock for the handle or a "wait to unlock" or an "ok to unlock" annunciation during the boost phase. (NTSB, p. 44)</p>		



**Table J-13. “System Design and Development Issues” Influence Chain Analysis**

	Apollo - 1			Soy-uz 1	Sky-lab 1		STS-1 Oxygen Deficiency	STS-1 SRB IOP	Scaled Composites	Ares 1-X	Space-Ship Two
SL1 – Organizational Culture LTA									X		
SL2 - Resource (\$ & staff) Allocation LTA								X			
SL3 – High Level Policy Guidance LTA				X							X
SL7 – Internal Relationship Management LTA		X	X								
ES3 – Schedule Controls LTA				X							
ES4 – Technical Controls-Process Change Controls-Risk Management LTA	X	X	X		X	X		X			
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA									X	X	X
DS2 – System-Part Design & Development LTA	X	X	X	X	X	X		X	X	X	X
TS1 – System Training LTA									X		
TS2 – Task Technical Training LTA			X								
TS3 – Emergency or Contingency Training LTA		X									
TS4 – Safety-Human Factors Awareness Training LTA	X										
SV3 – Poor Supervisor Example or Excessive Risk Taking				X							
QC1 – Inspection-Surveillance-Audit Req'ments LTA	X				X						X
QC5 – Statistical Methods LTA								X			
TT4 – Accepted Team Practices						X					
OP2 – Incomplete Procedures		X			X						
MW3 – System-Part Reliability-Usability LTA	X	X	X	X		X		X	X	X	X



Focus of this influence chain analysis



Other top nine recurring cause type

**Table J-14. "Inadequate Task Analysis and Design Processes" Summary Table**

Event	Task Design and Analysis LTA: Inadequate Design of Emergency/Troubleshooting/ Nonstandard Tasks	Task Design and Analysis LTA: Task Analysis LTA
Apollo 1	Task Design. The astronauts requested the emergency egress simulation be added to the end of the plug-out test because they were 3 weeks from launch and had not practiced an emergency escape yet. The plug out test did not require all the hatches be closed and locked. Also, there was no consideration on how to handle troubleshooting - how long is it ok to keep flowing oxygen? All of the comm system problems prolonged the plug-out test, so that oxygen was flowing continuously for approximately 4 hours. Also, the pressurization of the vehicle up to 16.7 psi could have been done in a separate test; it was not required for the plug out test.	
Soyuz 1		
Skylab 1		Task Design and Development LTA. The meteoroid shield was very difficult to rig to the tank. Some gaps undoubtedly existed between the forward and aft ends of the shield and the tank walls at the time of launch, which could have increased as the flight progressed due to the non-uniform growth of the tank. <i>The major difficulty experienced with the meteoroid shield was in getting it stowed and rigged on the OWS. Handling such a large, lightweight structure proved difficult, requiring the coordinated action of a large group of technicians, and considerable adjustments to the assembly of the various panels were necessary in an effort to obtain a snug fit between the shield and the OWS wall. ((5-6) p. 93)</i>
STS-1 Oxygen Deficiency		
STS-1 SRB IOP		
Scaled Composite s		Task Design. The test was done at the hottest part of the day. N2O had been in the tank overnight and all day. The test was conducted at an un-shaded, open-air site on a hot desert day in July at 2:20 p.m.
Ares 1-X	Task Design. The first time Ares IX strip test set-up was "non-standard" with many new components being used such as a forklift, a capstan winch, nylon break ties, and a nylon towline. The use of a 3/8 inch nylon towline to pull out the parachute created a dangerous amount of stored energy.	

Event	Task Design and Analysis LTA: Inadequate Design of Emergency/Troubleshooting/ Nonstandard Tasks	Task Design and Analysis LTA: Task Analysis LTA
SpaceShip Two Mishap During Test Flight		<p>Task Design &amp; Development LTA</p> <p>The copilot was experiencing high workload as a result of recalling tasks from memory while performing under time pressure and with high vibration and high G force loads that he had not recently experienced, which increased the opportunity for errors. (NTSB Finding #3, p. 67)</p> <p>Validation of the “reasonableness” of the task did not include some important human factors considerations.</p> <p>Scaled could also have considered a procedure to unlock the feather during a less critical flight phase and still mitigate the hazard resulting from an unfeathered reentry. (NTSB, p. 44)</p> <p>NOTE: Regarding the 0.8 Mach callout by the copilot: “This and other tasks during the boost phase of flight were memorized due to the dynamic nature of this phase. The purpose of the copilot’s 0.8 Mach callout was to alert the pilot that a transonic ‘bobble’ would be occurring as the vehicle accelerated through the transonic region and became supersonic.” (NTSB, p. 9)</p> <p>“Because of the dynamic nature of the boost phase, the copilot memorized his three tasks to be accomplished during that phase: calling out 0.8 Mach, calling out the pitch trim position in degrees as the pilot trimmed the horizontal stabilizers, and unlocking the feather at 1.4 Mach. In addition to recalling these tasks from memory, each of the tasks needed to be accomplished in a limited time frame. . . .</p> <p>During a simulator run on October 27, 2014, the copilot unlocked the feather after 1.4 Mach (after he received a caution message on the MFD); this situation was debriefed afterward.” (NTSB, p. 15)</p>

**Table J-15. “Inadequate Task Analysis and Design Processes” Influence Chain Analysis**

	Apollo 1		Soy-uz 1	Sky-lab 1	STS-1 Oxygen Deficiency	STS-1 SRB IOP	Scaled Composites	Ares 1-X	Space-ship Two
SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA	X						X		
SL7 – Internal Relationship Management LTA									
ES4 – Technical Controls-Process Change Controls-Risk Management LTA	X		X				X	X	X
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA		X							
DS3 – Task Design & Development LTA	X	X	X	X			X	X	X
TS2 – Task Technical Training LTA							X		
TS3 – Emergency/Contingency Training LTA	X								
SV1 – Supervisor Task Preparation LTA							X		
QC1 – Inspection-Surveillance-Audit Requirements LTA			X	X					
OP2 – Incomplete Procedures	X	X	X	X			X	X	X
SI3 – Support Equip-Tool Feedback LTA								X	
SI4 – System-Part Feedback LTA									X
MW2 – Support Equip-Tool Unavailable-Uncertified			X						
MW3 – System-Part Reliability-Usability LTA	X								
MW5 – Infrequent or Unique Task		X		X			X	X	X
IN2 – Cognitive Factors		X						X	X



Focus of this influence chain analysis



Other top nine recurring cause type

**Table J-16. “Organizational Design Issues” Summary Table**

Event	Organizational Design LTA: Fragmented Org Structure/Competing Projects	Organizational Design LTA: Unclear Accountability for Integration
Apollo 1	Organizational Design. NAA was too fragmented, not integrated. Also, NASA's decentralization of R&QA functions and responsibilities decreased NASA's effectiveness in monitoring contractor R&QA activities.	
Soyuz 1	<p>Organizational Design. The Soviets had multiple concurrent space projects, so their budget and resources were spread thin across these various programs. There was less emphasis on the manned programs.</p> <p><i>Excerpt from Kamanin Diary: 1965 September 8 - "Kamanin reviews a speech by President Johnson to the US Congress. From 1954-1965 the USA spent \$34 billion on space, \$26.4 billion of that in just the last four years. The Soviet Union has spent a fraction of that, but the main reason for being behind the U.S. is poor management and organization structure, in Kamanin's view."</i></p> <p><i>Excerpt from the Kamanin Diary: 1965 October 22 - Gagarin writes a letter to Brezhnev complaining of the poor organization of the Soviet space program. The letter specifically cites the multitude of space projects (5) and the de-emphasis of manned efforts.</i></p>	
Skylab 1		<p>Organizational Design and Development. Absence of a designated project or systems engineer for the MS.</p> <p><i>Organizationally, the meteoroid shield 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. ((10 – 2) page 142)</i></p> <p>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. ((10 – 4), page 144)</p>

Event	Organizational Design LTA: Fragmented Org Structure/Competing Projects	Organizational Design LTA: Unclear Accountability for Integration
STS-1 Oxygen Deficiency		<p>Org Design and development. FR chain of command. FR control vs control at the pad...centralized vs localized control of integrated operations.</p> <p>PF2-R4. The test conductor or his agent (pad leader) should be aware of the initiation of hardware hands-on work.</p> <p><i>O24. Between the NASA/Contractor Safety personnel, there is a significant pool of Safety resources available. The organizational barriers that presently exist tend to preclude effective utilization of this Safety "team."</i></p> <p>O24-R1. The utilization of Safety personnel (NASA/Contractor) should be reviewed to ensure an effective consolidation of Safety resources during test operations.</p>
STS-1 SRB IOP		
Scaled Composites		
Ares 1-X	<p>Organizational Design. 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 on the IPT was at the IPT lead's discretion. In some cases a necessary discipline may be missed, (e.g., Safety or SGE design), or a "devil's advocate" role. How are the risks associated with a DDT&amp;E environment identified, elevated, discussed, resolved, and documented, (i.e., a closed loop process)?</p> <p><i>See p. 15-17, USA Independent Review Report.</i></p>	
SpaceShipTwo		

**Table J-17. “Organizational Design Issues” Influence Chain Analysis**

	Apol- lo 1	Soy- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two
SL1 – Organizational Culture LTA				X				
SL2 - Resource (\$ & staff) Allocation LTA		X					X	
SL6 – Supplier-Subcontractor-Regulator Relationship Management LTA	X							
ES2 – Budget Controls LTA							X	
ES3 – Schedule Controls LTA				X				
ES4 – Technical Controls-Process Change Controls-Risk Management LTA			X					
ES6 – Procurement-Logistics-Material Control Sys LTA	X							
DS7 – Organizational Design & Development LTA	X	X	X	X			X	
QC1 – Inspection-Surveillance-Audit Requirements LTA	X							
TT3 – Team Communication LTA			X					
TT4 – Accepted Team Practices				X				
OP2 – Incomplete Procedures							X	
SI1 – Written Support Information LTA	X							
MW3 – System-Part Reliability-Usability LTA	X	X	X					
MW5 – Infrequent or Unique Task				X			X	
IN2 – Cognitive Factors	X							



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

**Table J-18. “Organizational Safety Culture Issues” Summary Table**

Event	Organizational Safety Culture LTA: Org. complacency regarding known, documented safety issues – learning culture needs improvement	Organizational Safety Culture LTA: Competing cultures
Apollo 1	Org. Culture. NASA noted NAA performance problems 13 months prior to the fire. <i>See "The Phillips Report" letter to NAA's President on Dec. 19, 1965 - pages 12 &amp; 13, and p. 31, Finding 10, NASA Apollo 204 Review Board</i>	
Soyuz 1		
Skylab 1		
STS-1 Oxygen Deficiency		Org Culture. Emerging, competing cultures...2 different worlds, 2 different ops philosophies.
STS-1 SRB IOP		
Scaled Composites	Org Culture. Scaled Composites' culture seemed to be lulled into complacency regarding the documented hazards of N2O.	
Ares 1-X	Org. Culture. Two very serious injuries occurred in December 2006 during two retrieval operations, (post-launch of STS-116), which questioned the safety culture and leadership of the SRBE organization. A video recording was being made of this first Ares 1X parachute static strip test. The video recording would be sent to the Marshall Space Flight Center. Strip tease music was played during the static strip test. <i>(See p. 35 SAIB Report, Observation 2: "Board noted lack of rigor in implementing the first time test of new Ares test.")</i>	



Event	Organizational Safety Culture LTA: Org. complacency regarding known, documented safety issues – learning culture needs improvement	Organizational Safety Culture LTA: Competing cultures
SpaceShipTwo		<p>Organizational Culture</p> <p>Scaled Composites did not have a dedicated human factors expert on staff. According to the vice president/general manager of Scaled Composites, they had a “history of building things” and relied on input from the pilots to identify and resolve ergonomic and human factor issues. He said Scaled Composites did not need to hire an outside human factors company because they did that internally. They were a research company and would “change things up” to see if it worked. (NTSB, Human Performance Report, p. 17)</p> <p>Scaled Composite’s management, test pilots, and engineers did not fully consider the risk of human error because of the flawed assumption that test pilots would operate the vehicle correctly during every flight. Also, Scaled Composites had not informed FAA/AST personnel that early unlocking of the feather could be catastrophic, which provided further evidence of Scaled Composite’s expectation that a pilot would perform as trained and not unlock the feather early. (NTSB, p. 45)</p>

**Table J-19. “Organizational Safety Culture Issues” Influence Chain Analysis**

	Apol- lo 1	Soy- uz 1	Sky- lab 1	STS-1 Oxygen Defi- ciency	STS-1 SRB IOP	Scaled Com- posites	Ares 1-X	Space- Ship Two
SL1 – Organizational Culture LTA	X			X		X	X	X
ES1 – Administrative Controls LTA							X	
ES3 – Schedule Controls LTA	X			X				
ES7 – Internal Continuous Improvement & Organizational Learning Systems LTA						X		X
DS2 – System-Part Design & Development LTA						X		
DS7 – Organizational Design & Development LTA				X				
TS1 – System Training LTA						X		
SV2 – Supervision During Task LTA	X						X	
QC1 – Inspection-Surveillance-Audit Requirements LTA	X							
TT1 – Team Composition LTA								X
TT4 – Accepted Team Practices	X			X			X	
MW3 – System-Part Reliability-Usability LTA						X		
MW5 – Infrequent or Unique Task				X				
IN4 – Individual Experience & Skills LTA	X							X
IN5 – Accepted Individual Work Practices LTA							X	



Focus of this influence  
chain analysis



Other top nine recurring  
cause type

## Appendix K. Examples of ASAP Recommendations for Human Spaceflight Programs

Following the Apollo 1 fire in January 1967, Congress established the ASAP to identify concerns and issues pertaining to a variety of aerospace topics and programs. These concerns and recommendations are reported annually to NASA and Congress. 513 recommendations were categorized using the same taxonomy used to categorize the causes of the individual mishaps. This categorization was performed independently from the other study team members by a researcher at NASA Ames Research Center. The taxonomy definitions and examples in were provided to the researcher, but there was no formal or informal training. The “best fits” between the technical concerns being addressed by the recommendation and the definitions and examples in the taxonomy were selected. The ASAP findings from 1972–1981 are presented in Table K-1 as examples.

*Table K-1. ASAP Recommendations*

Year	Conclusions/Recommendations
1972	The large extension of man’s role in space afforded by Skylab presents many new challenges to the various echelons of program management. Among these new elements of manned space flight are the extended mission duration, the absence of continuous contact with the ground, the first-of-a-kind nature of the hardware and mission, the very complexity and scope of the equipment, and the need for flexibility of response to unforeseen limitations or opportunities during the mission. To date, program management has been able, within the limits of available experience and knowledge, to respond to these new challenges and resolve the many new problems and requirements that have been encountered.
1972	The technical management system for design and fabrication of the modules appears adequate based on our review of contractors and the results of the design certification and module acceptance reviews.
1972	The traditional system safety and reliability functions were augmented with a number of special working groups. They considered such areas as critical mechanisms, electric circuit malfunctions, and microbial and contamination control. The Panel is satisfied with the comprehensiveness of this risk assessment effort. Apollo experience was used in the systematic identification and evaluation of Skylab efforts. Finally, while there are flammable materials on board, the risk associated with them has been evaluated by management. This risk has been minimized by isolating flammable materials from ignition sources and propagation paths. This is a prudent and reasonable approach.
1972	Cluster integration and the compatibility of the systems with operating requirements have been under review by numerous working groups, inter-Center panels, and Systems/Operations Compatibility Assessment Review (SOCAR). The system of review was generally satisfactory. However, the full effectiveness of system integration can be better evaluated after KSC testing.
1972	Since the Skylab CSM’s are a modification of the very successful Apollo CSM’s and the contractor appears to be maintaining the technical management systems and skills, the Panel has a high degree of confidence in the capability of the CSM to do its assigned job. Past Apollo anomalies have been evaluated for their impact on Skylab.
1972	In the Panel’s opinion the launch vehicle stages have received the necessary attention during storage. The system for post storage checkout and review appear comprehensive. Modifications made to the stages do not impact crew safety. While launch teams for the Saturn V are present from Apollo, the development of new teams with appropriate skills for the S-IB will require continuing management attention.

Year	Conclusions/Recommendations
1972	Checkout and launch preparations of the cluster will be more extensive than those for Apollo because of the complexity of the modules and the number of interfaces involved. Module systems will be integrated into the cluster configuration for testing. Many of these interfaces will be functionally integrated for the first time. Experiments and other stowage items still have to be fitted aboard the modules. Problems will undoubtedly occur. Therefore, senior program management will need to closely monitor the system for the resolution of these problems to assure that risk assessment is accomplished at the appropriate level of management. Based on the Apollo learning curve, the operation of ground support equipment will again have to be carefully planned and controlled to avoid overexcitation of flight systems during test activities.
1972	To obtain a confidence factor in qualifications by similarity, VI the Panel requests a review of those problem areas encountered during checkout at KSC, where the item had been previously qualified by similarity rather than testing.
1972	The extensive checkout and launch preparations of the cluster are to be completed within a tight schedule having a minimum of "unscheduled time" available for additional work. Therefore, senior program management must control additional work and be prepared to respond promptly to early indications of problems. Among those factors warranting particular management attention are (1) a high change rate in January and February, (2) the amount of overtime necessary, and (3) the unexpected events or problems experienced in checkout.
1972	<p>The Skylab Program provides more opportunities for experiments and astronaut activities than can be accommodated during the available mission time. This must be accepted by all to assure realistic expectation of mission activities and results. Priorities will have to be maintained and timelines carefully planned accordingly. Adequate time must be provided for crew rest and personal requirements. While the detailed mission planning and control of timelines typical of Apollo must be developed as work planning tools, the conduct of the mission will require a greater flexibility of response to accommodate unforeseen limitations or unexpected opportunities.</p> <p>Additional scientific opportunities will undoubtedly be discovered in flight. Housekeeping and experiment tasks may take more time in orbit than planned. This will require that the initial timeline not be fully committed. Also, it will require a management system to revise priorities and timelines during the mission. The flow of information to mission controllers, the assembly and display of this information to mission managers, and procedures for near-real-time evaluation and operational decisions are areas requiring management's attention in the period ahead.</p>
1972	A number of significant open items and concerns noted by the Panel are highlighted as areas for further attention. The pace of the Skylab program and the normal problem solving process will to some extent have already closed or provided planned closures for a good many of the items noted. However, further test and checkout experience may indicate that, in fact, some may not have been successfully closed.
1973	There is ample evidence that the system developed by Skylab management for the resolution of anomalies and the retention of skilled personnel has been highly effective in meeting real-time resolution of day-to-day mission problems.
1973	Skylab operations have confirmed man's value in maintaining onboard equipment and in their ability to take corrective action inside and outside the space vehicle.
1973	The possibility of human errors, particularly during test and checkout, is inherently ever-present in programs as complex as Apollo and Skylab. Experience in these programs has shown that the ability to respond in an adequate and timely fashion to such errors is a result of detailed contingency planning, personnel training and sureness in the management decision-making process.
1973	Qualification and validation test planning and execution to meet program requirements without compromising safety, reliability and performance differed from the Apollo concept in that Skylab incorporated verification by similarity and/or analysis wherever possible. Program results are evidence that this system worked very well.

Year	Conclusions/Recommendations
1973	Skylab management systems for configuration control, interface engineering and control, weight control and documentation in general were streamlined to reduce redundancy and manpower without losing controls and visibility.
1973	Contamination control was of vital importance to the long duration operation of experiments (internal and external) and the health of the crew. The Skylab system has been highly effective in understanding contamination problems and resolving them. Skylab mission data indicate that there were no unusual problems resulting from contamination sources, but that constant monitoring is valuable to assure continued contamination-free operation.
1973	Control Moment Gyro failed early in the final Skylab mission phase. The cause of the problem appeared to be a lack of bearing lubrication or bearing instability. Control Moment Gyro #2 showed similar, but to a smaller magnitude, the same symptoms as CMG #1. Bearing temperature increases and wheel current increases were observed. CMG #1 was shut down and the Orbital Cluster was stabilized using CMG #2 and #3.
1973	The contamination problem associated with close-tolerance hardware manifested itself in such items as the Service Module reaction control system Quad B positive yaw engine oxidizer valve on Command and Service Module 117 during the second manned visit. As a result of analysis, it appears that there is a need for all checkout personnel to exercise extreme care during vehicle checkout to prevent entry of contamination to assure that valves are not actuated without system pressurization, and to assure the cleanliness of the loaded propellants. This is particularly true of valves with Teflon or Teflon-like seats in which particles can be imbedded.
1973	The Panel was impressed by the thoroughness of the Skylab 1 Investigation Board report on the meteoroid shield failure which occurred on May 14, 1973. The Panel agreed with the many suggestions made to improve the management system to preclude, insofar as possible, similar problems in the future. Of particular interest were the observations that "A major emphasis on status, on design details, or on documentation can detract from a productive examination of "how does it work" or "what do you think" and the utilization of "The experienced 'chief engineer' who can spend most of his time in the subtle integration of all elements of the system under his purview, free of administrative and managerial duties, can also be a major asset to an engineering organization."
1973	The Panel, after reviewing the Skylab 1 Investigation Board Report, endorses the Board's recommendations for application to current and planned programs.
1973	The SOCAR team indicated that there is a deficiency in the contamination data capability because no measurement of the composition of the Skylab environment is available. Knowing the contaminates composition would serve a threefold purpose: combined with the quartz crystal microbalance output it would help establish "go-no-go" criteria for experiments in real time; it would provide a basis for a correction factor to experiment data affected by the environment; and it would enable a more direct determination of the sources of contamination. The proposed mass spectrometer noted in the previous listing is suggested for this purpose.
1973	Treated cardboard has been placed in many stowage containers to alleviate the launch environment. These large quantities of cardboard are then discarded. The manner in which this is to be accomplished still appears to be unresolved. A secondary problem attendant to this material is the problem of shedding when the material is handled. Obviously this is not just a hardware concern but also an operations concern since the crew interfaces with this material.
1973	Concern exists (re: the fire extinguishers) that during prelaunch storage as well as during zero-g storage in orbit the yield of foam may degrade to an unacceptable level.
1973	With respect to the Service Module, thermal control tests were conducted to assure adequacy of current paint system as a result of paint blisters observed during CSM 112 EVA on Apollo.
1973	The CSM electrical power system nonpropulsive vents used to vent the hydrogen and the oxygen were discussed, and it appears that only the hydrogen vent was tested to assure adequacy. The oxygen vent was assumed to work on the basis of similarity. One could question the validity of such an assumption since the working fluids are different.

Year	Conclusions/Recommendations
1973	The question of how long the crew can use the cluster if the ECS fails is one that must be answered in contingency planning.
1973	The operational acceptability of the oxygen consumption analysis at 5 psig appears to be somewhat of a problem.
1973	The posture of documentation and acceptability of the small hardware elements of M487 are not known by the Panel at this time.
1973	The following documentation needs to be updated: Skylab biomedical failure mode and effects analysis (FMEA) for the hardware; the mission level FMEA; the operational data book (ODB).
1973	Among the items still open with regard to the EREP are: discrepancies on S192, S193, S194 requiring rework at the vendors; ESE and functional interface verification for S192 and 193 at KSC; Flight filters and descants for S190B qualification and delivery.
1973	The habitation area configuration during periods of leakage control is the normal manned orbital configuration (i.e., OWS/AM hatch open, and pneumatic and solenoid vent port plugs installed). There was a proposal to leave the solenoid vent port unplugged. A change to the specification permitting habitation area pressures below 02 psia during launch and a common bulkhead delta P larger than 7.5 psi were being considered.
1973	With regard to the ATM deployment mechanism MDAC-East was to establish, through analysis and test, the minimum margin for deployment when one or both trunnion bearings are jammed or "frozen." Test were initiated to verify the analysis.
1973	One of the questions for the Phase III review is whether moisture can or has seeped in (point where Solar Array System attaches to the OWS structure in the folded position) and could, when frozen, impact the deployment mechanism.
1974	Generally, the management system is adequate for the current state of development.
1974	Systems integration management needs to strengthen its "check and balance" capability.
1974	The management system for avionics hardware and software should be reviewed by senior program management to assure it is adequate for the indicated complexity of the program.
1974	It is important that senior program management review both the scope and results of safety analyses to reinforce early resolution of risks. Similarly, attention should also be given to the scope and results of technical management audits to assure that such systems as described to the Panel are being applied properly. Two examples are Configuration Management and Material Control.
1974	The development of the Orbiter system is proceeding as scheduled. Manufacturing procedures appear comparable to those used on prior spacecraft programs.
1974	The design and quality control for the doors, Thermal Protection System penetrations and thermal seals should be closely monitored by management to assure that the reliability necessary to satisfy safety will be achieved.
1974	The procedures, instructions, and training requirements for installation and quality control of the Thermal Protection System components should be reviewed by program management to assure the aero/thermodynamic requirements are met.
1974	Free fall deployment of landing gear may introduce safety problems. Therefore the use of a positive system for rapid extension of landing gear should be considered.
1974	The major challenges of significance for crew safety on the Space Shuttle Main Engine are materials behavior under severe environments, weld integrity, POCO suppression and engine controller performance and reliability. Therefore, the results of the test program will be critical to developing confidence in these areas.
1974	The major challenges on the External Tank of safety significance are thermal insulation, ice formation, the use of Teflon electrical wire insulation in the liquid oxygen tank and provisions for control of reentry.
1974	The SRB is in an early stage of development. Critical areas must be monitored closely for the earliest possible detection and resolution of problems to assure that trade-offs provide for the maximum Shuttle system safety. Such areas include recovery and reuse of the booster.

Year	Conclusions/Recommendations
1974	The program in assuring the cost effectiveness of its requirements for ground support equipment needs to assure safety receives appropriate attention.
1974	The program is in the period of defining the detailed requirements and plans for major development and flight testing. Plans for ground testing appear adequate. Safety-related testing should be monitored to insure it is carried through as planned. The interactions between the Orbiter, External Tank and SRB, including separation dynamics are complex. Analyses based on ground testing should be thorough enough to maximize confidence in safe development flights.
1974	More information is needed on the risks of Approach and Landing Testing in comparison with the value of information which would be obtained in such flights.
1974	The role of man-in-the-loop, especially during landing, rollout and braking, needs reexamination as the program reaches the point where avionics capability and limitations are better known.
1974	Contingency analyses especially for aborts, ditching, landing accidents, and range safety should be completed early enough to assure design solution rather than operational workarounds.
1975	There is no margin in the schedule to accommodate major perturbations.
1975	Senior management will need to monitor the ability to meet minimum requirements where there are further reductions or changes in the major test program.
1975	Senior management will need to monitor the realism of plans and schedules for the remaining tests where there are significant problems so that decisions can be made early rather than under schedule pressure.
1975	An area that warrants review now is the data required from ALT to support a flight readiness decision on the first orbital flights and therefore the current mission planning to obtain these data.
1975	An area that warrants review now is the aggregate risk inherent in the "first flight" plan to assure it remains at an acceptable level.
1975	The basis for confidence that the structural capability of the 747 tail section will not be overloaded during tailcone off flights and that vibrations will not exceed crew tolerance.
1975	The test requirements and plans to give confidence that landing gear will deploy and lock as required.
1975	An area that warrants re-review now is the plan to have adequate GSE at the proper place to support the ALT program.
1975	The flight software requirements warrant review so there is an identical flight profile for autoland and manual modes.
1975	An area that warrants review now is the provision to allow the crew to adjust the gain of the control system.
1975	Give attention to the effectiveness of recent changes in the avionics management approach and the need for a software expert in the Technical Assessment Office as an independent advisor and check and balance.
1975	The management system to assure that contingency abort analyses are given the proper priority now so that changes, particularly in the software, are being made while there is still the capability for changes.
1975	Give attention to the total or integrated management plan to assure SRB reliability.
1975	The selection of a material and its methods of application for the external insulation, so that the program gets the flight performance it needs.
1975	Safeguards to protect auxiliary power unit with sea water exposure.
1975	Follow closely the provisions to assure that TPS installation procedures and tools will maintain the required gap and step between tiles and to avoid the problem of an early tripping of the boundary layer.
1975	Follow closely the provision to adequately protect vehicle openings during entry with insulation while assuring this insulation will not obstruct the operation of doors.
1975	The staff of engineers in the systems engineering office may need to be increased. Management regularly should review the staffing of the systems engineering office to assure that its capability is appropriate for its responsibilities.



Year	Conclusions/Recommendations
1975	Most of the directives have to do with responsibilities for monitoring and evaluating Space Shuttle progress rather than specifying how the daily work gets done or how the daily integration decisions are made. Some do not clearly define responsibilities.
1975	Work on this (system engineering) plan has been delayed further. If the plan is not to be available in a timely fashion, the management will have to assure that the basic need that required such a document is met in another way.
1975	Newly established chief engineer at MSFC for the Main Propulsion System was not a member of the Systems Integration Review Panel (SIR) at JSC. The panel believes that he should have direct participation and membership in the Systems Integration Review Panel activities, as well as be a part of the approval cycle for Level I1 and I11 documents.
1975	1. The Panel favors the role of identifying problems so the assessment groups can cover more areas of the program. 2. The Panel suggests that priority be given to safety issues rather than non-safety issues that may seem more pressing.
1975	SRB or External Tank separation
1975	Suggested that input and output devices and mechanisms be reviewed to doubly assure no "hard-overs" can exist.
1975	Adequacy of test and APU system design should be reviewed.
1975	Loss of pressure in the cabin appears to be a singular and important hazard. There are two cabin air supply systems and three fuel cells which provide cabin air pressure and conditioning. The system must operate for the entire mission and total failure would be fatal. It is suggested that a concentrated review take place meeting once again the strong confirmation that there is a remote enough risk to take. A third air supply system might be feasible and valuable.
1975	Reevaluate total system.
1975	"Destruct" decisions for operational flight are needed.
1975	A similar detail review should be made of the crossover capability which exists on the control system to maintain hydraulic pressure in the event of APU failure with a specific focus on the adequacy of maintaining hydraulic pressure in the main engine control valve system. If an MU shuts down there will be an automatic shutdown of that engine being served.
1975	"Comprehensive review of integrating groups operations should be conducted regularly to insure responsiveness to program needs."
1976	In the lifting body flights, the pilots were substantially assisted by calls from the control room where a pilot was available showing the actual location of the vehicle as compared with the planned locations. The Panel is very impressed by both the simplicity and effectiveness of this "modified GCA" in assisting the busy pilot on these short flights. For ALT it is understood that such a plot is planned at Mission Control JSC. It appears prudent to maintain the same plot at DFRC as a backup in the event of the highly unlikely but still possible loss of voice communications between Houston and Edwards. The Panel wonders what penalty the ALT would encounter by including this already available backup system.
1976	The closest actual experiences to the ALT flights are those that were gained during the lifting body and earlier rocket aircraft flights. We should not overlook any opportunity to use this background wherever appropriate. For example, it is suggested that lifting body pilots be requested to fly the STA and Orbiter simulators and provide comments on their flight experiences. Similarly, it may be useful to have a general critique of ALT mission plans by a group of experienced personnel who have not been involved to date. This group might include such people as Chuck Yeager, Bob White, Bob Rushworth and lifting body engineers of AFFTC.
1976	The Panel suggests that crew training might be enhanced by the use of additional existing simulators with capabilities different from simulators now being used. For example, the Air Force simulator (AFFTC Engineering Simulators) at Edwards AFB has proved very valuable for lifting body training. The Air Force simulator is not as comprehensive as other such training devices, but changes in aerodynamic values are easy to accomplish and should be useful in pilot training. Also, interaction between Air Force and NASA personnel would be enhanced.



Year	Conclusions/Recommendations
1976	Experience in lifting body simulator training and missions show that pilots are able to accomplish tasks at a higher rate in the simulator than in actual flights. Use of "fast time" simulators for training is one way of insuring that the pilot is not overburdened in flight. It is recommended that the use of such a simulator be given further consideration.
1976	The Panel acknowledges the massive and dedicated effort applied to the avionics system during last year and can only recommend the continued use of the simulators and Orbiter 101 to build up the testing experience the extent of which is the only real verifier of a hardware-software system.
1976	If the modified actuator system is not installed in time for the regularly scheduled integrated tests, a special thorough end to end integrated test of the hydraulic system should be required for certification of flightworthiness for ALT.
1976	Parasitic uses of the main hydraulic power systems are not considered to be acceptable in most modern aircraft practice without careful attention to isolation systems, and should be minimized or eliminated if possible by provision of special power systems before the first free flight of the Orbiter (ALT). It would appear that there are reasonably simple solutions for all such individual systems (brakes, nose wheel steering, etc.). It is possible that on ALT the reservoir can handle the largest expected leak.
1976	The APU's are on a very tight schedule but their thorough certification must not be short circuited. Further, the Panel suggests serious consideration of a backup source of hydraulic power and added fuel capacity so that starting and stopping of the APUs in active ALT flights are not necessary.
1976	Orbiter software presently limits control surface movement rate to 200 per second. The Panel recommends that changes in software be considered to permit an increased rate of movement. Experience in the X-15, X-24, YF 16 and B-1 graphically illustrated that flight control problems can result from restrictive rate limits. It is understood that hydraulic system capacity may become a limiting factor for control surface. If simulation with higher rate control surface movement suggests any kind of capacity restraints on the control of the Orbiter an increase of capacity should be considered along with other hydraulic systems modifications now being contemplated.
1976	Ejection seat tests (sled tests) should be completed for velocities up to launch speeds before the first manned flight of the Orbiter 101 on the 747.
1976	The landing gear system is critical and system ground tests are essential to confidence in the time and certainty of drop. The Panel feels that nose gear shimmy is as critical as extension. Nose gear shimmy will be checked at the contractor and NASA's Langley Research Center before free flight. The program feels a more pressing concern is the completion of the qualification test with static loads and the test of the nose gear door thruster on the simulator. The Panel recommendation is that management review the requirements and results of the certification program.
1976	The Panel has consistently emphasized that a "tail fairing Off" flight is one of the most persuasive reasons for the ALT program. This test should not be scrubbed for the reason of further need for the 101 vehicle. It should only be scrubbed if it is determined that buffet levels on the 747 are too high for safety and no alternative method of running the test can be devised.
1976	The Panel is particularly concerned that the concept of parallel or tandem multiple chamber pistons for elevon actuation be seriously considered for incorporation in the planned modification of the control system. If adoption of such a revised control system should be elected, the design and development program would need to be started immediately.
1976	The rudder speed brake actuation system deserves a thorough review for vulnerability to single point failure. For instance, a failure in one of the motors used to position the rudder speed brake could cause an overload on an adjacent motor causing the failure of all the motors in a zipper fashion.
1976	Increasing the APU fuel capacity on Orbiter 102 should be seriously considered.

Year	Conclusions/Recommendations
1976	The concept of hydraulic control of the main engines needs a critical review both for the effect on the hydraulic system and to ascertain that the operation of the main engines is not subject to shut down due to "service" system failures when the engine itself is still operable. Inherent in such a reassessment should be a review of the desirability and potential methods for isolating the engine control system after the main engines have fulfilled their function.
1976	The Panel would recommend that the new computer development with the double density memory system be closely monitored so as to assure the maximum compatibility with the present hardware and software. This will ensure a backlog of experience from ALT to aid in the verification of the software programs for the new computer.
1976	Currently there is very little experience to predict the behavior of the thermal protection system in hypersonic flow and therefore the system cannot be certified by similarity or analysis. Among the areas that are particularly unpredictable are: <ul style="list-style-type: none"> <li>a. The gap configurations in width, its direction with regard to the surface flow.</li> <li>b. The steps between tile and its tripping influence on the boundary layer into turbulence.</li> <li>c. Flow in door seal cavities and gaps.</li> </ul>
1976	The HRSI insulated umbilical doors are exposed to the flight environment on ascent. After separation the doors will be closed. There is no inspection mode or access planned to assure a proper closure. Consideration should be given to an on orbit inspection and repair of the TPS and particularly the umbilical door seals to assure a safe reentry.
1976	The currently developed engineering criteria for TPS coating erosion and inspection method should include access feasibility studies.
1976	The integrity of the aluminum structure after any flight depends on the cooling efficiency of the GSE equipment after landing and the novel design of cooling ducts to prevent the orbiter structure from excessive temperatures. The design and implementation of such a cooling duct system has not yet been certified by a total system test and should be.
1976	It appears that, as a result of a good reliability history, the maintenance of cabin atmosphere integrity has been based on a "two engine" concept. This has the practical result that any failure will cause the termination of a mission in order to protect the crew from a subsequent single failure. This suggests that systems which must last through the total time of a mission probably should be augmented so that such single failures do not force mission termination for safety.
1976	The flash evaporator used to supplement radiator cooling is of the "fail safe" variety like the environmental system where a single failure will abort the mission in order to maintain safety should be considered to ensure that such system failures will not abort extensive missions in the name of safety.
1976	The SRM, as in other areas of the SRB total assembly, are affected by the system aerothermodynamic loads. These latest data must be factored into the analysis and test as soon as practical to assure proper margins are maintained in the structures and other critical areas.
1976	The nozzle bearing boot, although it has passed some tests, is not out of the woods as yet. Ensuring that maximum material temperatures are not exceeded during the firing time and that no splits or openings occur allowing hot gas. There are concerns with regard to flow inside the bearing.
1976	The Auxiliary Power Unit has experienced some "under performance" tests which require a reexamination and review to define the manner in which the performance and reliability of these important units can be upgraded.
1976	The use of the RDX linear shaped charge to sever the aft end of the SRM nozzle is a concern from the viewpoint of premature ignition. The temperatures and their duration would suggest that this item might be classed as a Category 1 hazard and treated accordingly.

Year	Conclusions/Recommendations
1976	The data returned from the first Orbital Flight Test mission, the first time the total SRB system will be tested as part of a total Shuttle system, will be crucial in defining the margins the SRB makes available to the total system. Since the SRB's must work each and every time, the flight test instrumentation, its location, etc. must be thoughtfully considered. Where transducers are placed into bosses they must be fail-safe. In other words the DFI must not be thought of as simply an "add-on" subsystem.
1976	Consideration should be given to contingency planning or success assurance. The spray-on insulation is not expected to be machined over. What then would be done with an application that is too thick for the spec because of a breakdown of a spray gun or blockage of the nozzles.
1976	Additional management control should be considered for the ET-Orbiter interface. There is no plan for a mock-up or separation test with a complete hi-fidelity mock-up. Another concern that needs additional assessment is the possible damage to the Tank caused by the separation dynamic impact loads and subsequent endangering of the Orbiter.
1976	Additional effort to determine the adequacy of the present ET/SRB attachment struts may be warranted if present struts do not attenuate pyro separation impact loads. There are no shock absorption devices on the ET-side of the interface.
1976	The Panel recognizes the accomplishments of both senior program and Safety, Reliability and Quality Assurance management and their continuing efforts to define and determine aggregate risk in a manner most useful to senior management. The current system provides a great deal of risk information, but the challenge is to assure it is a useful tool for the decision-makers on the Shuttle program. Mission hazard analyses were made on prior manned space missions to show those safety concerns which would constrain a mission until resolved. In this way they were providing the aggregate risk based on the best available information which was examined from objective and subjective viewpoints. The ALT project safety assessment report has essentially done this as noted by this statement "The JSC Safety Division considers the aggregate risk acceptable, based on the assessment of safety concerns to date, considering the accepted risks and the actions being accomplished to resolve open items." Perhaps what is needed are detailed presentations to management by project and sub-system engineers as well as safety, reliability and quality assurance engineers so that statements made in mission safety analyses allows management to selectively review the background for specific Shuttle flights.
1976	As noted the technical assessment group at JSC is off to a good start and shows that it can make a significant contribution to risk management. Since their continued effectiveness now depends upon the level of support and direct interest by senior program management the Panel makes a point of recommending such personal attention.
1976	The effectiveness of configuration management depends upon the implementation of the system as described to the Panel. Therefore, the Panel recommends that audits of the operation of the system continue to be brought to management's attention during this period of development testing, checkout to assure the "as-built" and "as-tested" reflects the "as-designed" systems. This applies to both hardware and software.
1976	The Panel agrees with the program investigation that the quality of small electronic parts in the Shuttle is adequate, and would suggest that in the procurement of this class of parts that reliance be placed on the performance specification rather than brand name.
1979	It is important to set a realistic schedule that will allow the orderly completion of the work to prepare the STS-1 for flight. For instance, all manufacturing should be completed before stacking, and it is imperative that all testing be finished with adequate time for analysis and evaluation before flight.
1979	Start the necessary main engine design for 109 percent rated operations.
1979	Start an alternate APU design and plan for early replacement of present APUs.
1979	Continue thermal protection material development and system design looking to simplification and elimination of present fragility.
1979	Investigate the assertion of ground control of reentry in an emergency.
1979	Investigate the widening of flight control and center of gravity margins.

Year	Conclusions/Recommendations
1979	Review the redundancy philosophy for major systems, particularly in light of first flight experience.
1979	Review black box inventory for state of the art improvements that should be utilized.
1979	NASA should take the lead in getting high reliability users of materials to solve the problem of the inadequacy of industrial material supplies.
1979	NASA should formalize an improvement program similar to that followed by transport manufacturers following introduction of a new model transport airplane. Elements of such a program have been suggested throughout this report. Recommendations 2, 3, 4, 7 and 8 contain such improvement candidates, and comments under System Safety Improvements for the Shuttle Operational Mode contain similar proposals.
1980	Pioneering programs such as the Shuttle must be conservatively defined and adequately funded at the start and throughout life in order to insure a timely and satisfactory conclusion with a minimum of risk and maximum cost effectiveness.
1980	Sufficient time must be scheduled between flights of the initial test series to analyze data and implement the changes indicated to upgrade the safety for each subsequent critical test.
1980	Ensure that the eventual operational organization is involved in the definition of any "product improvement" program for the operational Shuttle.
1980	Define early and implement those long-term developments necessary for the operational Shuttle; for instance, uprated engines for more demanding missions.
1980	Develop and implement a more effective method of assuring quality control, particularly with respect to routine as well as new and unusual materials.
1981	To achieve true operating safety, regularity, and minimum practical cost, the organization of efforts between the R&D community and any transportation service organization should be clearly separated. The transportation service organization should assume responsibilities analogous to commercial airline managements. This includes marketing of its services to government agencies, and to commercial as well as international entities needing space transportation. Implied in "operations" is the planning and acquisition of prime hardware and spares, maintenance, certification of procedures, training, creation of requirements for future development including performance improvement and the responsibility to determine readiness for all missions and the fulfillment of these missions safely.
1981	<p>The Panel suggests a technical audit of the application of redundancy concepts to Shuttle systems. From design reviews the ASAP believes that many systems can be simplified with both safety and cost benefits while other systems should be backed up further for operational safety. ASAP candidates for such a review are:</p> <ul style="list-style-type: none"> <li>Total hydraulic power system -- both for solid rocket and orbiter control -- including the use, numbers, configuration and location of auxiliary power plants.</li> <li>Basic control system architecture for aerodynamic controls, main engines, SRBs, and Orbiter control motors.</li> <li>Control of main engine thrust.</li> <li>Computer logic in normal and backup modes with a special effort to standardize programming for operations to prevent flight-to-flight and particularly last minute reprogramming.</li> <li>Electric power systems</li> <li>Avionics and communication</li> </ul>

Year	Conclusions/Recommendations
1981	<p>The current development state of the space transportation hardware suggests that a number of concept changes may improve operational safety, reliability and costs. In priority, the ASAP suggest:</p> <ol style="list-style-type: none"> <li>1. Investigating a main landing gear with more than two wheels per side and devices to avoid gravel "spray" which damages thermal protection tiles.</li> <li>2. Reviewing the need for control of SRB nozzles to maneuver the total vehicle. As performance of the control system evolves, it may be possible to revert to a programmed "trim" system on SRBs. In addition, when investigating lighter cases (composites) the separation and recovery systems should be reanalyzed to simplify.</li> <li>3. The automation and simplification of cockpit and routine crew duties, along with improved reliability of sensors.</li> <li>4. Review of the hysteresis of SIP Repeated missions will require SIP that is less susceptible to dimension changes with steady and vibratory loads.</li> <li>5. Reassessment of flight controls concepts. It is suggested that multiple control surfaces or drives be considered.</li> <li>6. Investigate non-hypergolic fuel and oxidizer for orbital boost, on orbit control motors, and APUs.</li> </ol>
1981	<p>For the remaining R&amp;D flights, it is suggested that a "redline" audit be made of limits that should not be exceeded for "ready to launch." It is poor practice to set conservative limits and then bypass them at last minute launch readiness conferences.</p>

# Appendix L. OCE Knowledge Sharing Forum Presentation

National Aeronautics and Space Administration



## Recurring Themes from Human Spaceflight Mishaps During Flight Tests and Early Operations

**Human Spaceflight Knowledge Sharing Forum**  
November 1, 2016  
Huntsville, Alabama


**Team Members:**  
Tim Barth  
*KSC/NASA Engineering and Safety Center*  
Donna Blankmann-Alexander  
*KSC/Abacus Technology Corporation*  
Barbara Kanki  
*Ames/Human Factors*  
Steve Lilley  
*Glenn/NASA Safety Center*  
Blake Parker  
*KSC/ASRC Aerospace*






## Background

- **Study goal:** Using selected flight test/early operations mishap investigations, identify recurring factor 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)
- **NESC and NSC 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)



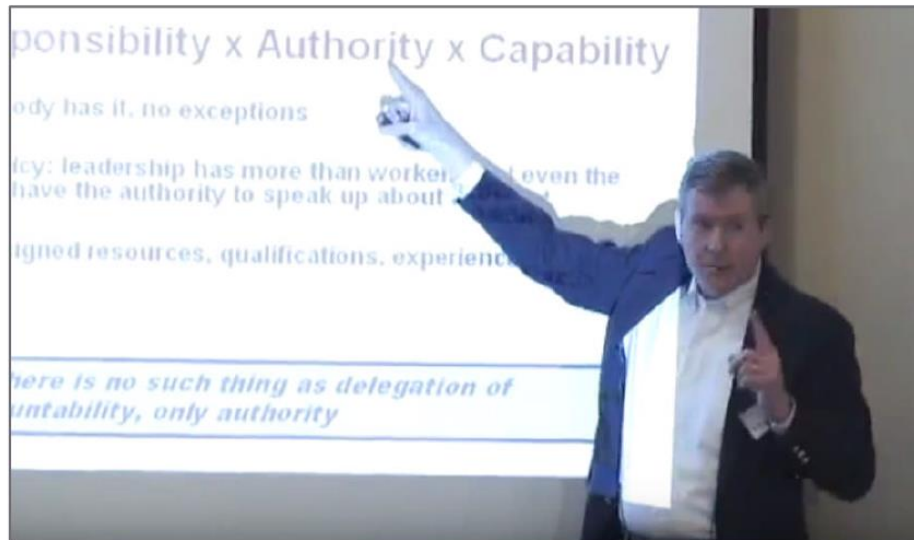
2

National Aeronautics and Space Administration





## Safety Accountability vs. Responsibility



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

National Aeronautics and  
Space Administration



## Study Evolution

- Shuttle Human Factors Team and Model (1990's - early 2000's)
- Columbia – systemic/recurring factor analysis methodology development (2003-2006)
- Shuttle Ground Processing Mishap Study – post Columbia; focus on safe fly-out for flight and ground crews (2006-2011)
- Shuttle Workforce Message from Bob Crippen (2010)
- “Tough Transitions” STS-1 System Failure Case Study (2011)
- Mars Science Laboratory (MSL) Ground Test and Checkout – recurring factor review of significant close calls (2012)



[www.youtube.com/watch?v=5vfyZtVPvfs](http://www.youtube.com/watch?v=5vfyZtVPvfs)

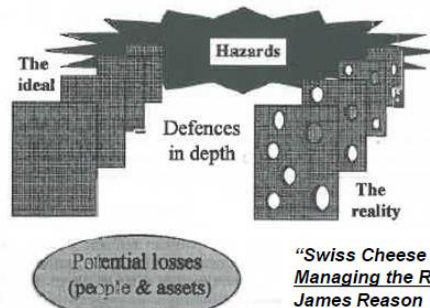
### MSL Ground Processing Close Calls

- Inadvertent crane “up” command after lifting and connecting the MSL Descent Stage Simulator (DSS) to the flight backshell interface
- Shipping GSE not removed before drill percussion test
- Cable installed in reversed position on flight fluid pump
- Flight Drill Bit Assembly (DBA) second alignment not performed



## Major Lessons from Shuttle and MSL Mishap Risk Reduction Efforts

- Need a conceptual organizational systems model as the basis for the analysis



- Organizational system-level issues recur because they are hard to fix
  - No silver bullets; requires sustained, data-driven effort
- Need to evaluate all contributing factors and causes
  - Because a contributing factor can be a cause in a different situation or on another day, and vice-versa

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."***

***"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***



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

National Aeronautics and  
Space Administration





## Human Spaceflight (HSF)-1 Mishaps

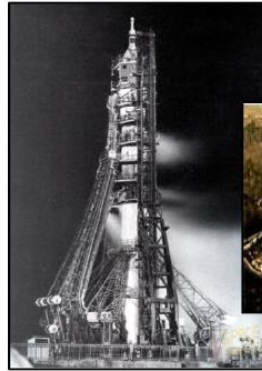
### Apollo-1 Crew Module Fire at Launch Complex 34

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



## HSF-1 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)


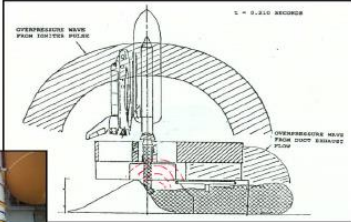


National Aeronautics and  
Space Administration






## HSF-1 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 


## HSF-1 Mishaps (continued)

**Ares-1X Steel Rod Mishap During Static Strip Test at KSC Parachute Refurbishment Facility**  
 September 5, 2007  
 Ground Crew Injury (1)



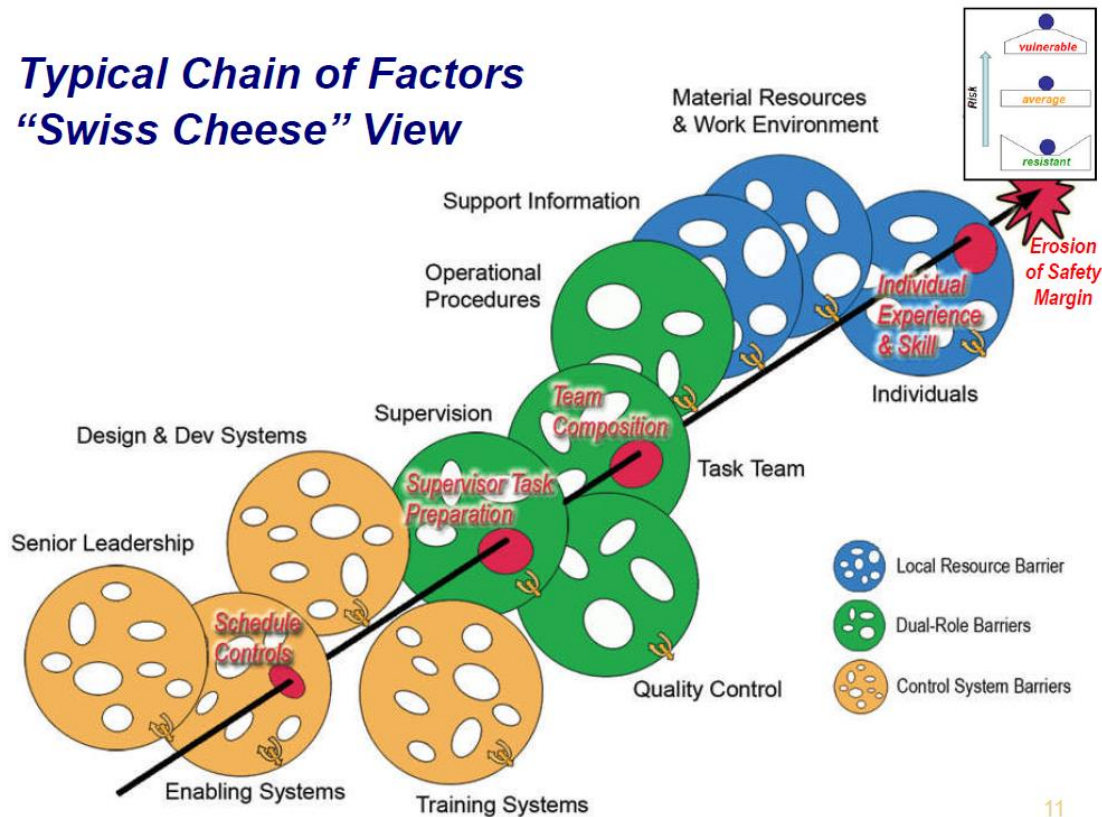
**SpaceShipTwo Test Flight Mishap**  
 October 31, 2014  
 Loss of Flight Crew (1), Flight Crew Injury (1), and Loss of Spacecraft



National Aeronautics and Space Administration 



## Typical Chain of Factors “Swiss Cheese” View



## Typical Chain of Factors: Taxonomy View

### Control System 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 Msmt LTA
  - SL6; Supplier-Subcont-Reg Relat Msmt LTA
  - SL7; Internal Relationship Msmt LTA
  - SL8; Strategic-Succession Planning LTA
- ES; Enabling Systems (8)
  - ES1; Administrative Controls LTA
  - ES2; Budget Controls LTA
  - ES3; Schedule Controls LTA
  - ES4; Tech Ctrls-Proc Chng Ctrls-Risk Msmt LTA
  - ES5; Human Resource Systems LTA
  - ES6; Procurement-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; Wkspce-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; Suprv Task Preparation LTA
  - SV2; Supervision During Task LTA
  - SV3; Poor Suprv Exmple-Excess Risk Taking
  - SV4; Suprv-Employee Relationship Msmt 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-Attk-Disc LTA, Willful Viol, Disruptive Behavior





## Study Inputs and References

- Detailed (micro) analysis of 8 human spaceflight (HSF)-1 mishaps
  - 180 factors/causes in 8 HSF-1 mishaps where investigation reports were available
  - 4 mishaps during ground ops; 4 mishaps during mission ops
- High-level (macro) analysis of Aerospace Safety Advisory Panel (ASAP) recommendations for human spaceflight programs
  - 513 recommendations from 1972-2012
- Historical independent assessment reports
  - Early Apollo Operations: Manned Space Programs Accident/Incident Summaries (1970), Cranston Research, Inc.
  - Early Shuttle Operations: Space Shuttle Productivity and Error Prevention (1981), Anacapa Sciences
  - Apollo Spacecraft White Paper, George M. Low
- Other special studies
  - Readiness for First Crewed Flight (2011), NESC
  - Technical Risk Identification at Program Inception (2014), Aerospace Corporation
- Human Spaceflight Subject Matter Expert (SME) inputs

Top 10

Top 6

National Aeronautics and Space Administration 




## Human Spaceflight SME's

<p><b>JSC:</b></p> <ul style="list-style-type: none"> <li>• Bo Bejmuk</li> <li>• Wayne Hale</li> <li>• Gary Johnson</li> <li>• Steve Lilley*</li> </ul> <p><b>MSFC:</b></p> <ul style="list-style-type: none"> <li>• Jim Blair</li> <li>• Bob Ryan</li> <li>• Don Hull*</li> </ul> <p><b>WebEx:</b></p> <ul style="list-style-type: none"> <li>• Mike Blythe</li> <li>• Nancy Currie-Gregg</li> <li>• TK Mattingly</li> </ul>	<p><b>KSC:</b></p> <ul style="list-style-type: none"> <li>• Jay Honeycutt</li> <li>• Bob Lang</li> <li>• Charlie Mars</li> <li>• Gerry Schumann</li> <li>• Bob Sieck</li> <li>• Tip Talone</li> <li>• John Tribe</li> <li>• Donna Blankmann-Alexander*</li> <li>• Barbara Kanki*</li> <li>• Tim Barth*</li> </ul> <p style="text-align: center;">*Facilitators</p>
---	--

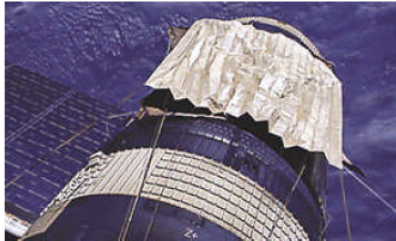
*Reminders from the experts:*

- Mishaps depend on a specific situation and set of circumstances where the various events, factors, and causes line up and lead to a bad day. In different situations, it is possible that Challenger or Columbia-type tragedies could have occurred on STS-1.
- In human spaceflight, every mission should be treated as an inaugural mission.

National Aeronautics and Space Administration 

## Study Results – Recurring Themes (1 of 6)

- **Insufficient technical controls or risk management practices**
  - 75% of occurrences were related to inadequate safety hazard/risk analysis and reviews
  - 17% of occurrences were related to inadequate FMEA/fault tree analysis
- **HSF-1 examples:**
  - *SpaceShip2: Scaled Composites' 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. (NTSB Finding #6)*
  - *Soyuz-1: The failure mode of the primary parachute's malfunction (jammed in its container), which caused backup chute failure as well, was not accounted for in the design.*
  - *Ares-1X: Even though the parachute riser lines were approximately 4 times longer than the riser lines on the Shuttle's drag chute, there was no requirement for engineering to perform a first-time GSE DE loads analysis of the test set-up or a readiness review for the initial Area-1X parachute static strip test.*
  - *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."*



National Aeronautics and  
Space Administration



## Study Results – Recurring Themes (2 of 6)

- **System design/development issues**
  - 60% of occurrences were related to inadequate testing and verification of system interfaces
    - Failure to "test like you fly"
  - 40% of occurrences were related to inadequate system trade-offs or analyses of material selections
- **HSF-1 examples:**
  - *Apollo-1: Teflon wire coating was chosen for superior insulation, chemical inertness and fire resistance. However, the soft, unprotected, thick-wall Teflon was susceptible to creep, cold-flow deformation and abrasion. Teflon coating wore away during installation and training. Exposed electrical wiring cracked and contributed to unending command module technical problems during tests. Five days before the fire, a frustrated Grissom hung a lemon from his yard on the simulator.*
  - *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: N2O tank design included several materials incompatible with N2O. The tank lacked a burst disc to protect against rapid over-pressurization.*
  - *STS-1 IOP: System Integration, responsible for liftoff environment definition, accepted the Tomahawk Ignition test as a sufficient simulation of SRB Ignition over-pressurization. Engineers did not fully appreciate the effect of the differences between the SRB and the Tomahawk Ignition characteristics.*



*"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

National Aeronautics and  
Space Administration





## Study Results – Recurring Themes (3 of 6)

- **Inadequate secondary verification methods**
  - 71% of occurrences were inadequate inspection requirements for known materials, safety, and contamination issues
    - Secondary verifications, not necessarily more inspections (i.e., system feedback, engineering evaluations)
  - 29% of occurrences were inadequate inspection requirements for real-time resolution of task design issues or challenges (deviations, changes to procedures)
- **HSF-1 examples:**
  - *Apollo-1: Given the fragile nature of the Teflon coated wiring, inadequate attention was given to the inspection of the wire bundles to detect abrasion or deformation.*
  - *Soyuz-1: There was no requirement to inspect the parachute container for contamination.*
  - *Skylab-1: There was no system feedback (such as a visual cue) to the technicians, quality inspectors, and engineers that a “tight fit” had not been achieved during rigging. Inadequate quality inspections.*
  - *STS-1: Applicable safety documents did not have sufficient requirements for atmosphere checks or verification of an air purge before aft re-entry. No oxygen deficiency monitoring system in the aft.*



The crews of Soyuz 1 and Soyuz 2 present themselves before the State Commission in front of the launch pad in April 1967. In the foreground from left to right are the primary crew of Vladimir Komarov, Valery Bykovsky, Yegor Gerasimov, and Aleksey Yeliseyev (in civilian clothes) and the backup crew of Yuri Gagarin, Andrian Nikolajev, Viktor Gorbatko, and Valery Kubasov (also in civilian clothes). Chief Designer Vladimir Glushko is visible in the background between Yeliseyev and Gagarin. (copyright Christian Lindner)

National Aeronautics and  
Space Administration



## Study Results - Recurring Themes (4 of 6)

- **Ground processing task analysis and procedure design issues**
  - 67% of occurrences were related to inadequate design of emergency/contingency/troubleshooting/nonstandard tasks
    - Incomplete or unclear procedures
    - Require AT LEAST same level of rigor in procedures, training, and system design for contingency/off-nominal ops as planned/nominal
  - 33% of occurrences were due to mismatches of task design with actual flight hardware
- **HSF-1 examples:**
  - *Apollo-1: The astronauts requested the emergency egress simulation be added to the end of the plug-out test because they were 3 weeks from launch and had not yet practiced an emergency escape yet. The plug out test did not require all the hatches be closed and locked.*
  - *Skylab-1: Stowing and rigging the large, lightweight micrometeoroid shield to the Orbital Work Shop (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 snug fit between the shield and the OWS wall could not be made.*
  - *Ares-1X: The initial Ares I-X strip test set-up combined components (forklift, a capstan winch, nylon break ties, and a nylon towline) in an untested combination. The nylon towline used to extract the parachute released a dangerous amount of stored energy upon failure.*



National Aeronautics and  
Space Administration

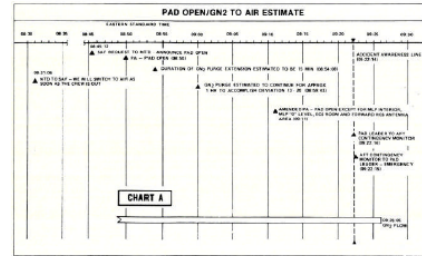


## Study Results – Recurring Themes (5 of 6)

- **Insufficient schedule controls**
  - 60% of occurrences were related to overly optimistic/aggressive schedules
  - 40% of occurrences were related to inadequate schedule integration between local work groups

- **HSF-1 examples:**

- **STS-1:** 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 side work to be approved and carried out in parallel with hazardous operations which increased risk and susceptibility to an accident. 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.
- **SpaceShip2:** The pressure to approve experimental permit applications within a 120-day review period...interfered with the FAA's ability to thoroughly evaluate the SS2 experimental permit application.
- **Apollo-1:** The Command Module was shipped to KSC with much open work. "There is an inference that the design, qualification and fabrication process may not have been completed adequately prior to shipment to KSC."



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

*"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

National Aeronautics and  
Space Administration



## Study Results – Recurring Themes (6 of 6)

- **Inadequate organizational learning**
  - 80% of occurrences were related to failures to learn from previous incidents or issues within the organization (similar mishaps, close-calls, or other precursor events)
  - 20% of occurrences were related to failures to learn from previous, well-documented mishaps outside the organization

- **HSF-1 examples:**

- **SpaceShip2:** 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 aviation (DOD and commercial), 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, well before the Apollo-1 fire. The test was conducted under a lower atmospheric pressure (only 5 psi to simulate cabin pressure in space) but a 100% O2 environment. The test incident report was classified.
- **STS-1:** Apollo-1 Congressional hearings uncovered a problem at KSC with timely submittals of operational checkout procedures to Safety for review in 1967. STS-1 procedures had the same problem.
- **Scaled Composites:** Multiple OSHA citations were issued before the mishap regarding lack of engineering controls to abate well-documented N2O storage and handling hazards.



SpaceShip2 Feather Lock System

*"There's no shortage of lessons, but learning is the issue"*

T.K. Mattingly

National Aeronautics and  
Space Administration





## Sample Questions for HSF Programs

- Are any of the recurring themes identified in the study applicable?
  - If so, have they been recognized? What current efforts are addressing them? Should new proactive risk reduction efforts be initiated?
- What hazards and risks have not yet been identified?
  - Are there any emerging or unique safety and technical risks associated with testing and early operations that should be considered?
- Are known hazards and risks being openly and candidly communicated throughout the organization?
- Are dissenting or alternate technical opinions supported and valued?
- Are known hazards and risks thoroughly, accurately, and consistently evaluated?
- Have system-level impacts of specific technical risks been evaluated?
- Have hazard and risk analyses been updated to reflect design and operational changes?

5X5 RISK MATRIX					
LIKELIHOOD	5	4	3	2	1
	5	4	3	2	1
	4	3	2	1	
	3	2	1		
	2	1			
CONSEQUENCES					
	1	2	3	4	5

- *What else can we do to reverse the HSF-1 mishap trend?*

*"Risks identified are rarely realized, risks realized were rarely identified."*

Aerospace Corporation Study, "Technical Risk Identification at Program Inception,"  
U.S. Space Program Mission Assurance Workshop, May 8, 2014

National Aeronautics and  
Space Administration



21

## 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 aft compartment mishap
  - April 12, 1981: STS-1 launch
- September 5, 2007: Ares-1X static strip test mishap
  - October 28, 2009: Ares-1X test flight

*"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: a Surgeon's Notes on an Imperfect Science*

National Aeronautics and  
Space Administration



22



## Available Resources

- **OSMA/NASA Safety Center**  
<http://www.nasa.gov/offices/nsc/home/>
  - System Failure Case Studies
  - NSC Cases of Interest
  - NASA Mishap Investigation Board Reports
  - Risk Management Handbook
  - SMA Technical Excellence Program (STEP)
  - Quality Audit, Assessment, & Review (QAAR)
  - OSMA News and Safety Messages
  - Independent Verification & Validation (IV&V) Services

*"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, Day of Remembrance Memo, January 29, 2009*

- **OCE/NASA Engineering and Safety Center**  
<http://www.nasa.gov/offices/nesc/home/>
  - Independent Assessment Reports
  - Technical Bulletins
  - NASA Technical Standards and Handbooks
  - Design, Development, Test, and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems
  - Readiness for Crewed Flight Report
  - On-line NESC Academy Courses
  - APPEL Courses and Case Studies
  - NASA Knowledge Map
  - Lessons Learned Information System (LLIS)

- **And Many More...**
  - Significant Incidents and Close Calls in Human Spaceflight (JSC SMA)
  - 100 Questions for Technical Reviews (Aerospace Corporation)
  - Industry & Other Agency Standards & Handbooks
  - Shuttle Knowledge Console

<https://skc.jsc.nasa.gov/Home.aspx#category=1235>

National Aeronautics and  
Space Administration



## Appendix M. Shuttle Processing Mishap Recurring Cause Study during Late Operations Phase

### ***Beyond Band-Aid Solutions: Proactively Reducing Mishap Risks***

*NASA Project Management Challenge 2010  
Daytona Beach, Florida  
February 9-10, 2010*

*Tim Barth  
Systems Engineering Office  
NASA Engineering and Safety Center*

*Mark Nappi  
Deputy Project Manager  
United Space Alliance*

1

### ***Acknowledgements***

- Donna Blankmann-Alexander
- Blake Parker
- Barbara Kanki
- Mark Nappi
- Pat Floyd
- Rich Harvey
- Mike Wetmore
- And many others...

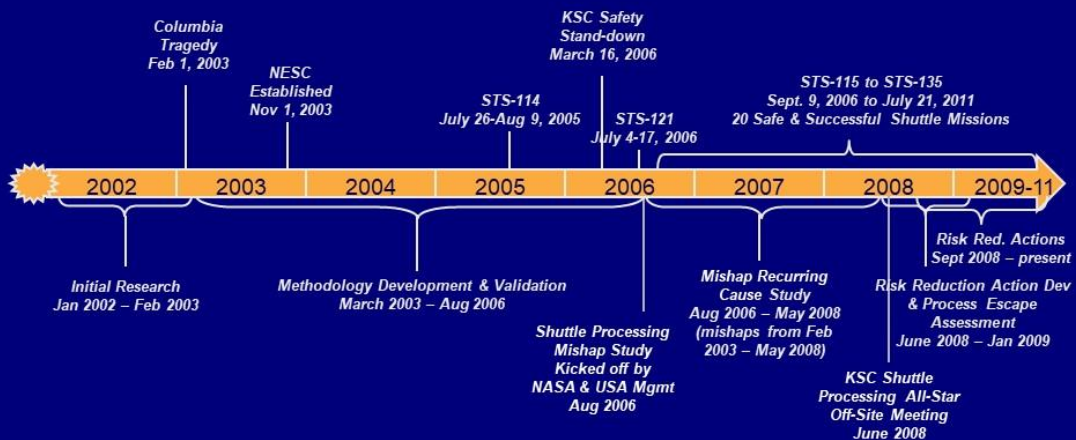
2

## Outline

- ✦ Background
- ✦ Methodology
- ✦ Event-Specific Risk Reduction Actions
- ✦ System-Level Risk Reduction Actions
- ✦ Summary and Lessons Learned

3

## Methodology Development and Implementation Timeline



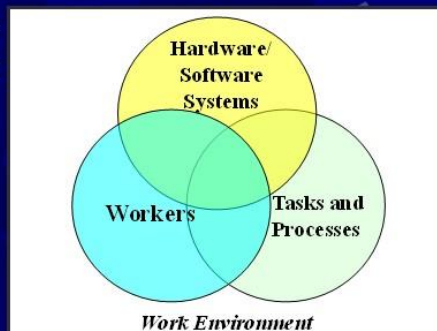
4



## Background

(August 2006)

- Safety performance in Shuttle ground operations over the history of the Shuttle Program is commendable
  - Many safety improvements over the years
  - We can (and must) still raise the bar
- KSC needs to proactively reduce mishap risks through Shuttle fly-out
  - Systems are stretched: significant numbers of hardware and software changes/challenges, process changes/challenges, and workforce changes/challenges happening at the same time
  - Making KSC organizational systems and processes more robust to handle these changes and challenges reduces the risks of mishaps, process escapes, and other adverse events



5

## Staying on the Cutting Edge of Investigative Methods and Tools

- Mishaps, close-calls, and process escapes are learning opportunities
- Steady evolution of investigative techniques and capabilities over the past 20 years in Shuttle ground ops
  - Joint NASA/Contractor Human Factors Team
    - Perry Committee
    - Human factors model
    - Human factors reps on investigation teams
  - Industrial and Human Engineering Groups
  - Standing Accident Investigation Boards
  - Additional investigation teams
    - White papers
    - Corrective Action Engineering
  - Software and experts for root cause analysis

*"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*

6

## Influence Chain Mapping Methodology

- Specifically designed to step back from individual mishaps to evaluate trends and patterns in contributing factors/causes in order to identify the most significant system-level safety issues
- Shuttle mishap “recurring cause” study
- Complements (does not replace) root cause analysis methods
- Explicitly models the influences between organizational systems and individual behaviors of front-line workers
- Emphasizes *absent* barriers/controls in addition to *failed* barriers/controls

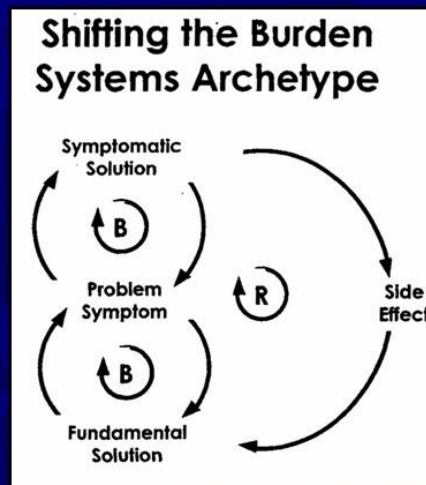
“The NESC gains insight into the technical activities of programs/projects through...systems engineering reviews and independent trend or pattern analyses of program/project technical problems, technical issues, mishaps, and close calls within and across programs/projects”

NESC Management Plan

7

## Fundamental (System-level) and Symptomatic Solutions

- Two “balancing processes” compete for control of a problem symptom
  - Proactive & reactive
  - Preventive & corrective
- Both solutions treat the symptom, but only the fundamental solution treats the system-level issue
  - Medical analogy: lung cancer
- Symptomatic solution frequently has the side effect of deferring the fundamental solution, making it harder to achieve

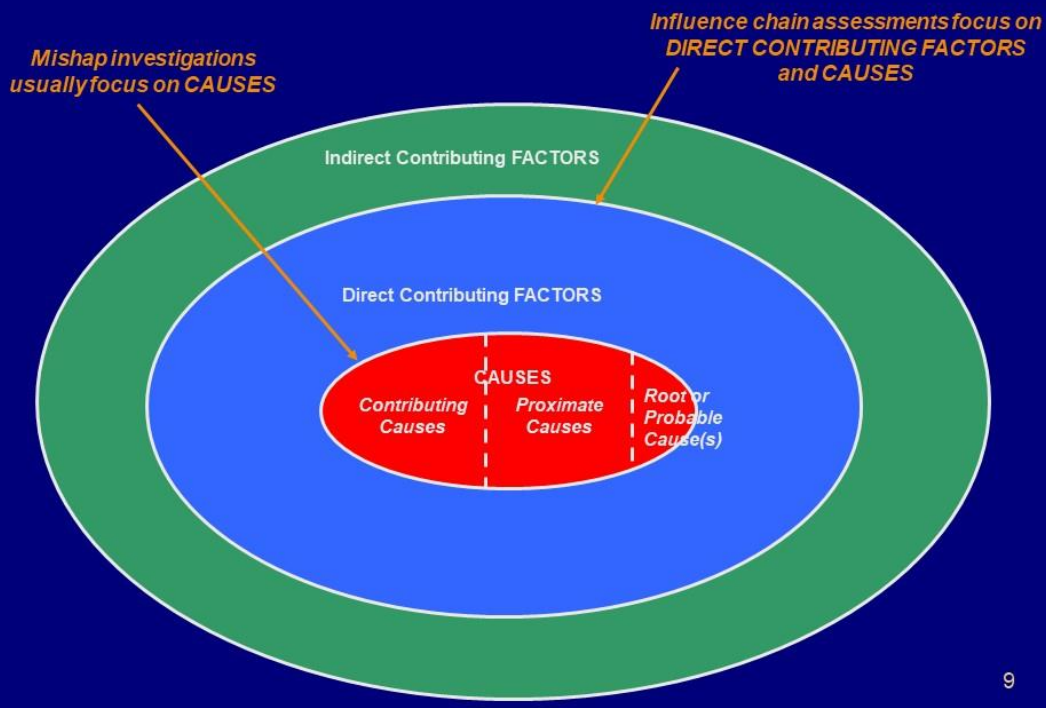


from Peter Senge, “Systemic Leadership and Change”

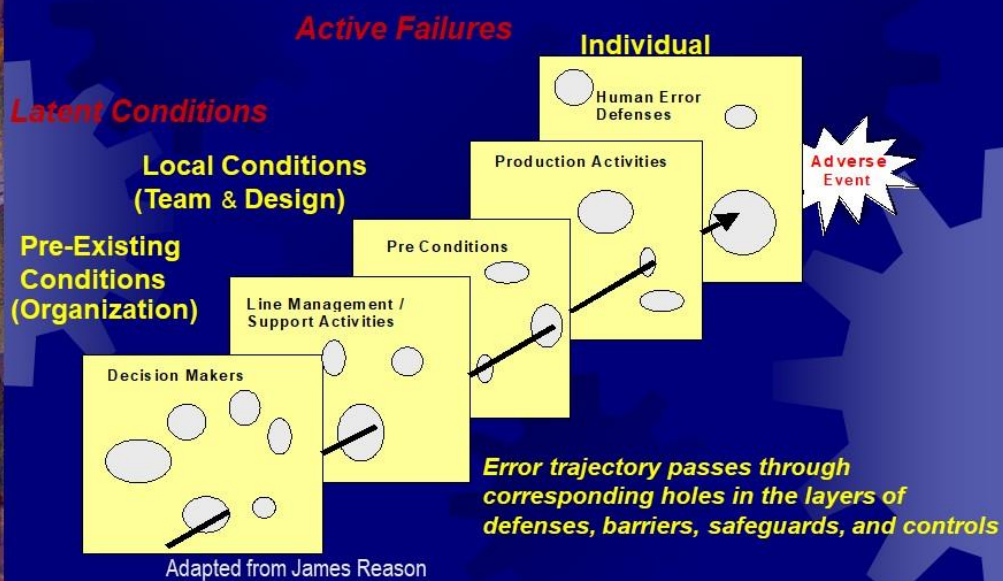
8



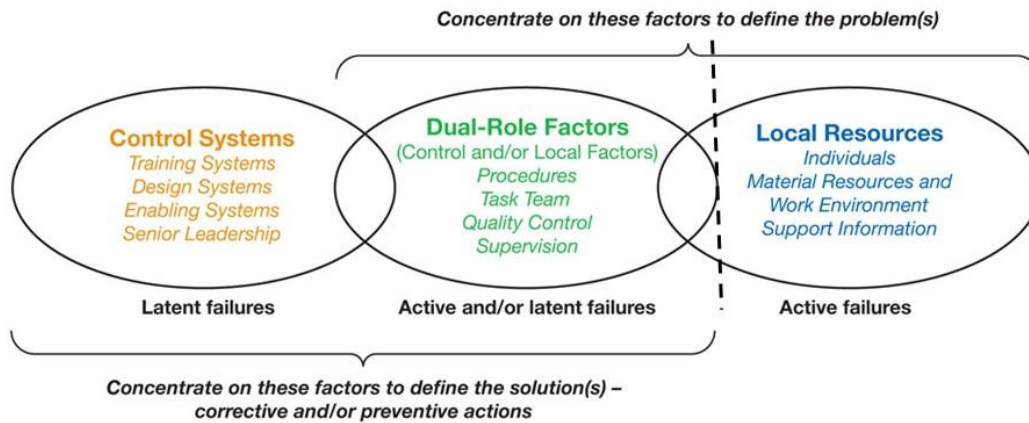
## Contributing Factors and Causes



## Swiss Cheese Model of Defenses



# Dual Role Model for Addressing System-Level Safety Issues



11

## Dual Role Taxonomy of Contributing Factors and Causes

### Control System 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; Administrative 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; Procurement-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; Wkspc-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

12

# Notional Influence Chain

## Control System 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 Mgmt 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; Administrative Controls LTA
  - ES2; Budget Controls LTA
  - ES3; Schedule Controls LTA
  - ES4; Tech Cntrl-Proc Chng Cntrl-Risk Mgmt LTA
  - ES5; Human Resource Systems LTA
  - ES6; Procurement-Logistics-Matrl Cntrl Systems LTA
  - ES7; Int Cont Imp & Org Learning Systems LTA
  - ES8; Cust-Stakeholder Feedback Systems LTA

- D5; Design & Development Systems (7)
  - D51; Support Equip-Tool Des & Dev LTA
  - D52; System-Part Des & Dev LTA
  - D53; Task Des & Dev LTA
  - D54; Wkspc-Work Env Des & Dev LTA
  - D55; Procedure Des & Dev LTA
  - D56; Training Course Des & Dev LTA
  - D57; 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 Awareness 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 →

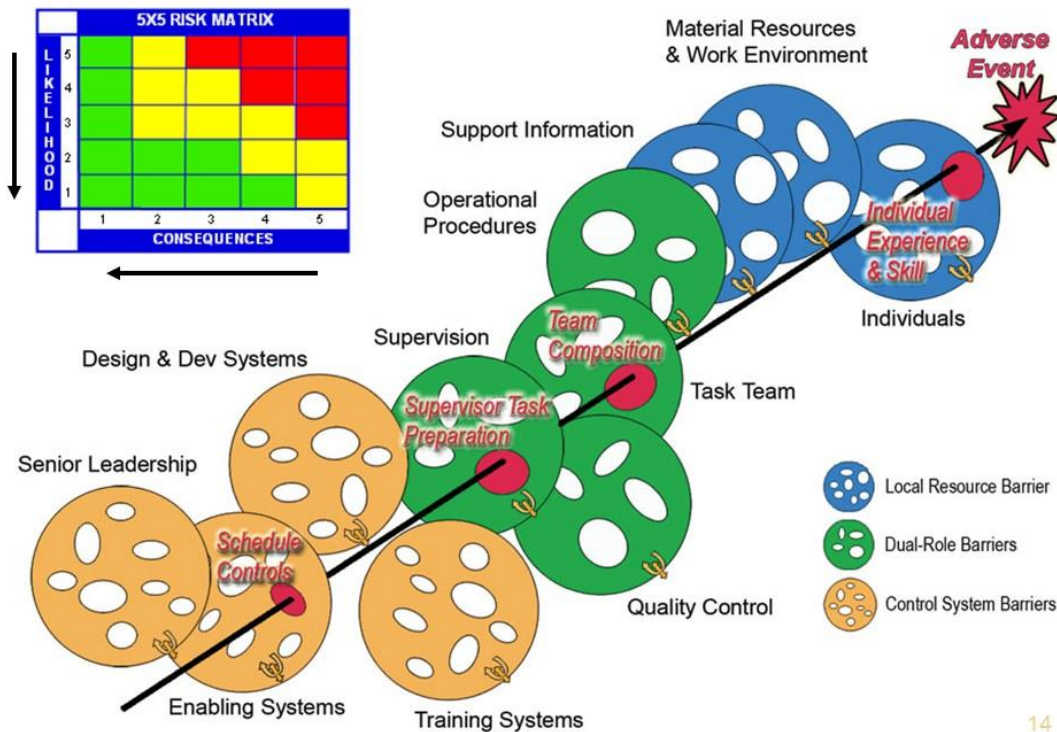
- SI; Support Information (5)
  - SI1; Written Support Info LTA
  - SI2; Verbal Support Info LTA
  - SI3; Support Equip-Tool Feedback LTA
  - SI4; System-Part Feedback LTA
  - SI5; Worker-Work Env Sensory Signals LTA

- 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

13

# Proactive Risk Reduction

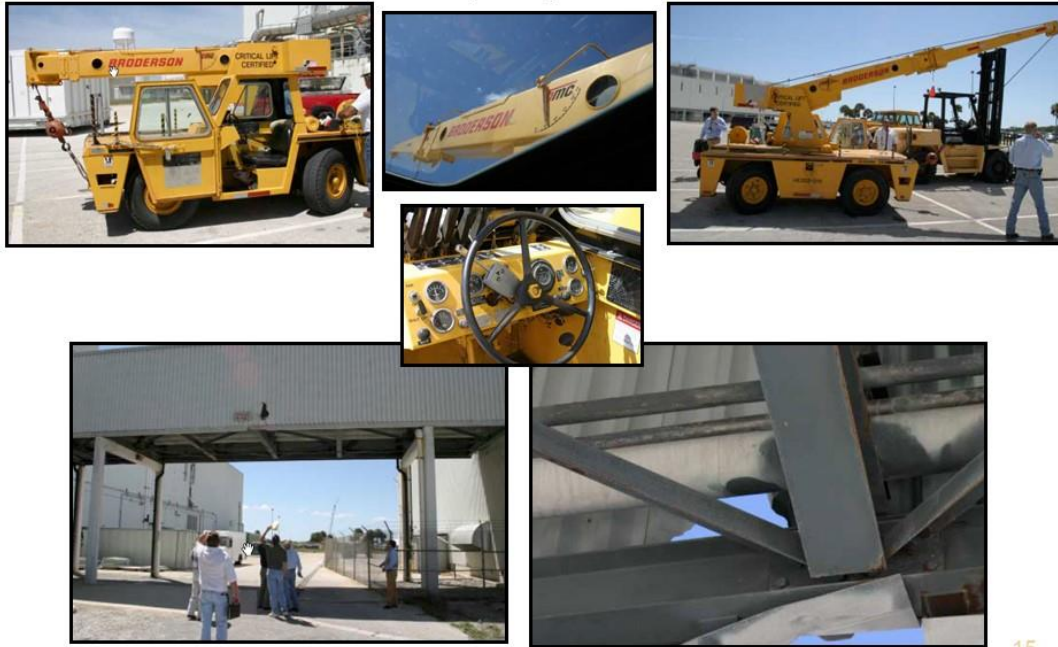


14



# Example Influence Chain Assessment: Mobile Crane Boom Impact With VAB

April 19, 2004



15

## Mobile Crane Mishap

### Influence Chain #1: Procedures

#### Control System 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 Mgmt 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; Administrative 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; Procurement-Logistics-Matd Ctrl Systems LTA
  - ES7; Int Cont Imp & Org Learning Systems LTA
  - ES8; Cust-Stakeholder Feedback Systems LTA
- D5; Design & Development Systems (7)
  - DS1; Support Equip-Tool Des & Dev LTA
  - DS2; System-Part Des & Dev LTA
  - DS3; Task Des & Dev LTA
  - DS4; Facility-Workspace Des & Dev LTA
  - 1a** **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 Awareness 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
  - 1b** **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
  - 1c** **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

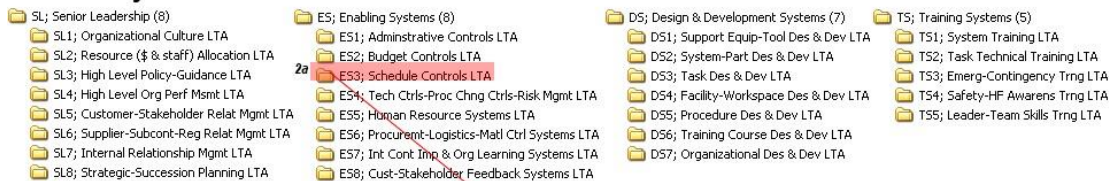
Key: IM Contributing Factor  
→ IM Influence Link

16

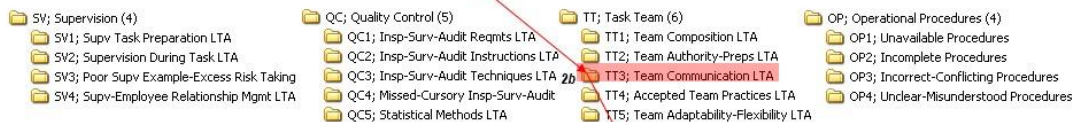
# Mobile Crane Mishap

## Influence Chain #2: Scheduling

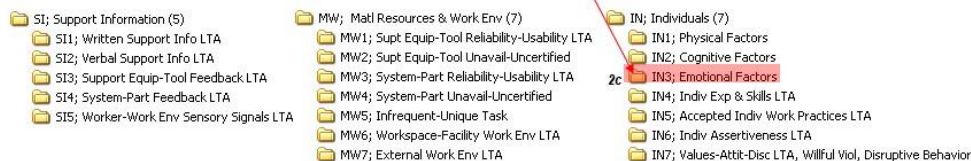
### Control System Factors



### Dual Role Factors



### Local Resource Factors

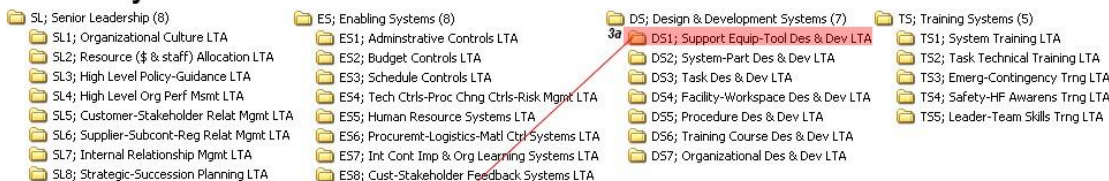


17

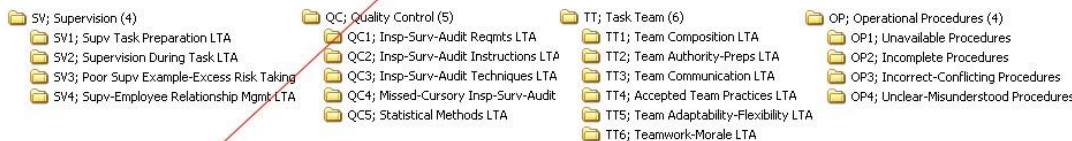
# Mobile Crane Mishap

## Influence Chain #3: Equipment Feedback

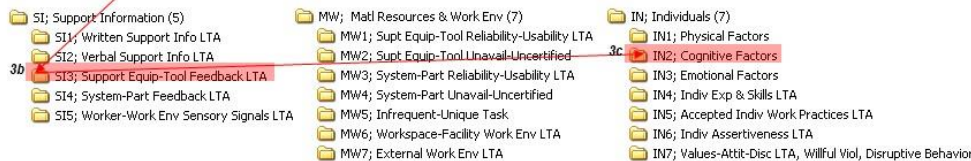
### Control System Factors



### Dual Role Factors



### Local Resource Factors



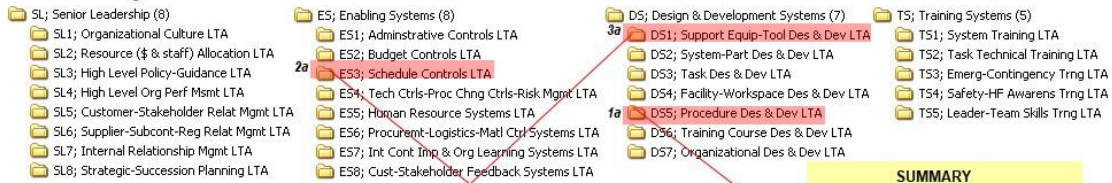
18



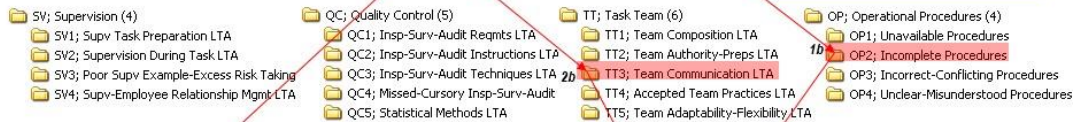
# Mobile Crane Mishap

## Summary of Contributing Factors and Causes

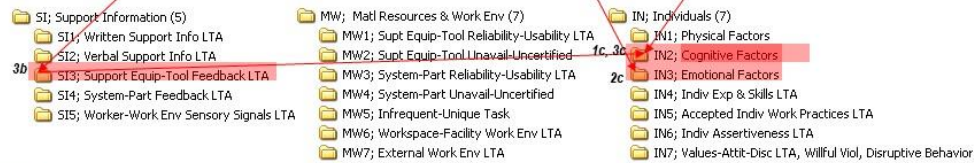
### Control System Factors →



### Dual Role Factors →



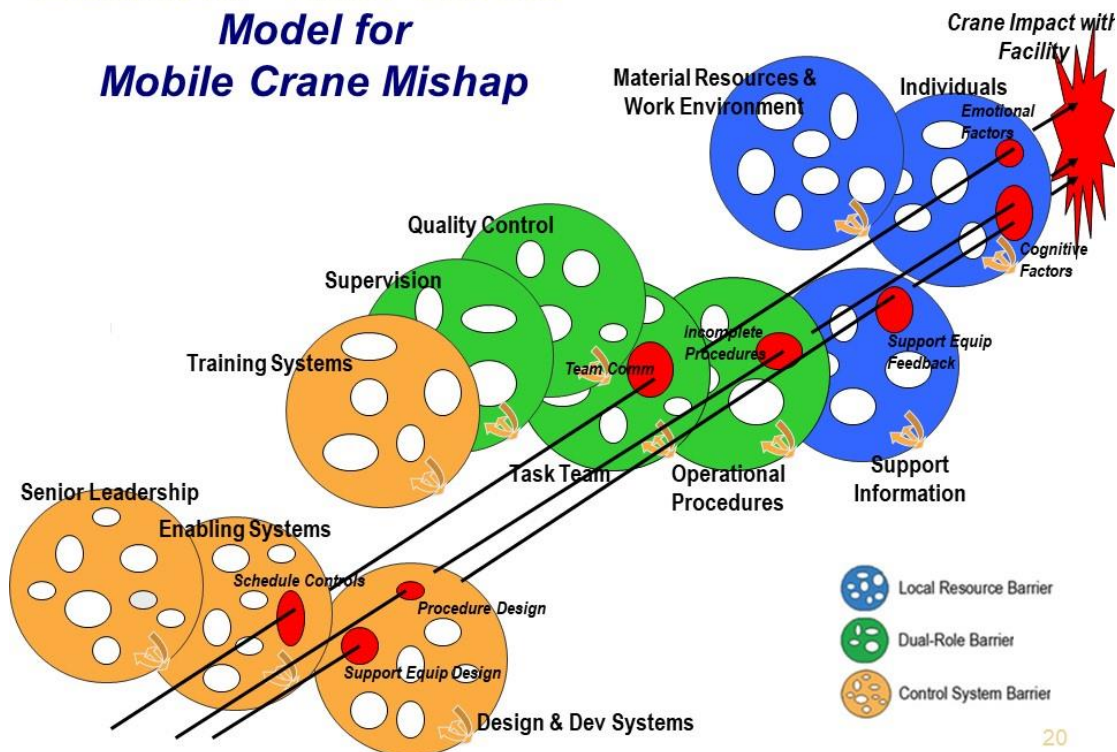
### Local Resource Factors →



**SUMMARY**  
 - 3 influence chains (major issues)  
 - 9 contributing factors

19

## Enhanced “Swiss Cheese” Model for Mobile Crane Mishap

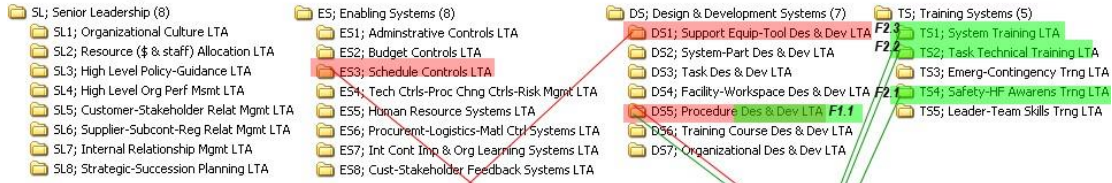


20

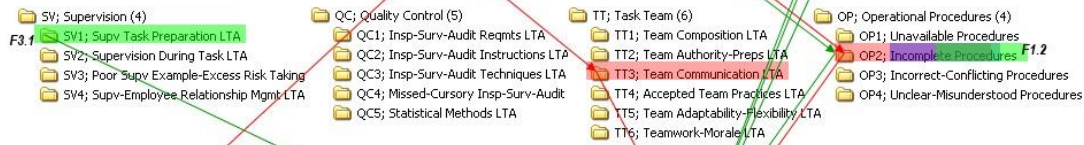
## Completed Influence Chain Map for Mobile Crane Mishap

**Influence Chain Cont. Factors + SAIB Findings + SAIB Recommendations**

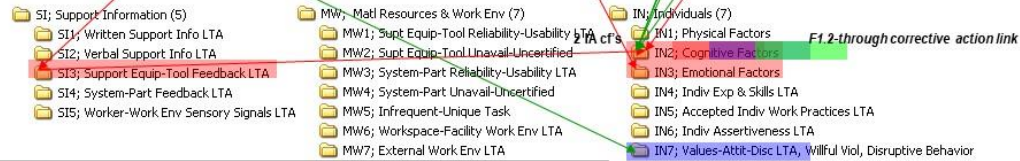
### Control System Factors →



### Dual Role Factors →



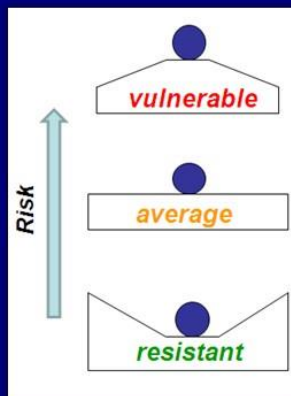
### Local Resource Factors →



21

## Event-Specific Risk Reduction Recommendations

- From a human-system integration perspective, a vulnerable system enables workers to make unintentional errors and/or cause collateral damage
- A well designed (robust or resistant) system enables workers to avoid errors and collateral damage
- Approx. 20 event-specific risk reduction recommendations implemented



**Accept Risks**

**Add Inspections and Warnings, Revise Training, Add Procedure Details**

**Equipment and/or Task Redesign, Add Physical Guards, Provide System Feedback**

**"To err is human, but errors can be prevented."**  
National Institute of Medicine

22



## Event-Specific Recommendations

### System Feedback Example

#### Crane Boom Impact with VAB Structure (04/20/04)

Install a sensor system with beepers and/or flashing lights on the mobile cranes that are activated when the cranes are moved in the destowed position, similar to backup beepers on trucks.



#### Similar Example from Industry



#### 1.3.3 Warning signals

The garbage truck was manufactured without an audible or visual alarm to warn the driver that the garbage box was in an elevated position.

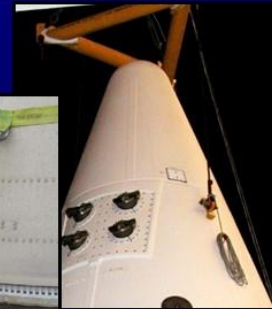
23

## Event-Specific Recommendations

### Support Equipment Re-Design Example

#### Freedom Star Retrieval Ship Frustum Incident (12/10/06)

Replace the polyester straps used to secure the frustum to the deck. Consider using steel cables and the frustum's cable attach points used for VAB stacking operations. (Similar recommendation submitted for Orion recovery operations)



#### NESC Composite Crew Module (CCM)

##### Ultra low- stretch straps



24



## Event-Specific Recommendations

### Future Programs Example

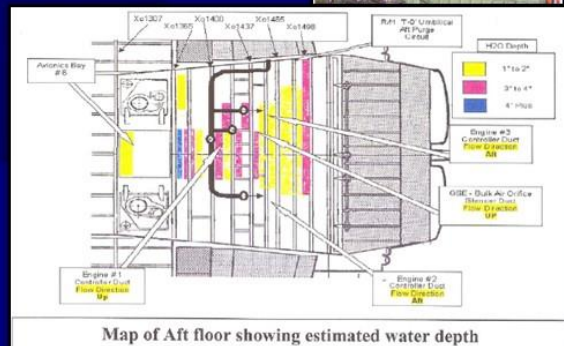
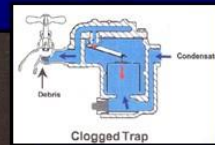
#### OV-105 Water Intrusion from MPPU (01/17/04)

In the MPPU refurbishment design plan, include sensors to monitor moisture/humidity extraction levels and to automatically warn the operator(s) if an anomaly occurs. Note: a redundant drain path does not address the risk of a common cause failure.

**Human Factors Engineering**  
**Pathfinder for GSE Design Teams:**  
 8 KSC teams, Nov. 2007 through  
 Feb. 2008 plus follow-on efforts



Shuttle Mini Portable Purge Unit (MPPU)



Map of Aft floor showing estimated water depth

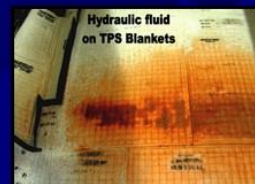
25

## Event-Specific Recommendations

### NASA Standards and Handbooks Example

#### OPF HB1 Platform System Leak onto OV-104 RH OMS Pod TPS (10/26/04)

Re-implement torque stripe requirements for facility KC/AA fittings.  
 (Input to KSC STD 512 for Ground System and Facility Designs)



Other NASA Standard inputs based on study results:

NASA-STD-5005 for GSE Design

NASA-STD-3001 Vol 2 Human Factors and Habitability (CxP HSIR)

CCT-STD-1150 Commercial Crew Transportation Ops (in work)

26



## Event-Specific Recommendations

### KSC-Level Team Example

#### HMJ Oxidizer Exposure (06/05/04)



##### Cause/Contributing Factor #1:

The task was designed to be performed with gloves, a splash apron, chemical goggles, and a face shield. The level of PPE was inadequate to protect the workers. The reliability of the PPE specified was ineffective for the task. Liquid oxidizer ran down the technician's glove and onto his exposed forearm.

##### Recommendation #1:

Modify Class C PPE requirements to having no exposed skin; hazmat type apparel.

##### Status:

KSC SCAPE Summit & Improvement Team

##### Cause/Contributing Factor #2:

The task for flight cap removal was classified as a "Class C/Modified Class C" operation. The basis for this assessment was "no potential for liquid flow (hypergolic fluids) and low potential for vapor release. Flight caps with liquid hypergolic oxidizer had been observed during this operation on several previous occasions and multiple technical waivers were made.

##### Recommendation #2:

Re-evaluate operations that currently have Class C PPE requirements but should be modified Class C or SCAPE operations.

##### Status:

KSC SCAPE Summit & Improvement Team

27

## Event-Specific Recommendations

### Technology Example

#### RMS End Effector Overheated (10/20/04)



##### Causes/Contributing Factors:

- RMS false alarms. None of the six standard fault indicators on the A8U Display & Control Panel illuminated in conjunction with the master alarm. When the manual mode switch was toggled to "automatic," it triggered the RMS master alarm. The alarm sounded because pin #38 was bent and contacted pin #30, which was associated with the end effector capture/release command path. The net effect of the pin contact was a stalled condition in the end effector capture system.

- Inspection Techniques LTA. When the QC performs an inspection after the soft mate, there is no guarantee that the actual mate is correct. The workers cannot verify that the actual connection is good (no bent pins). The QC inspector must assume that if the soft mate is ok, the actual mate will also be ok.

##### Recommendation:

Develop a new inspection tool/technology to address the system feedback issue (lack of system feedback if the pins are bent during connector mating). Develop a portable, hand-held instrument that can detect bent pins instead of relying on the soft mate technique.

##### Status:

- Input to KSC and Agency-level technology roadmaps.

28



## NASA Selects USA Quality Inspector for Space Act Award

**U**SA Senior Quality Assurance Inspector Christopher Smith from the Shuttle Avionics Integration Laboratory (SAIL) OV-095 Shuttle Test Facility was recently awarded the Space Act Award for inventing the TWINAX (twin axial) Cable Alignment Inspection Tool.

The Space Act Award is selected by the NASA Invention and Contribution Board (ICB) for inventions and other scientific and technical contributions that have helped to achieve NASA's aeronautical, technology transfer and space goals.

The TWINAX Cable Inspection Tool was invented for use during the Shuttle Cockpit Avionics Upgrade (CAU) to ensure correct alignment of the pin and socket contact assemblies for fiber channel cables and connectors. These cables and connectors would carry high-

speed flight control data signals from the Shuttle avionics loop, providing real-time flight information to the cockpit crew.

Before this invention, a precision device to inspect the contacts with the connectors did not exist. Pre-mate inspections were visual and not reliable in detecting tolerances for precise mating of the contacts with corresponding elements. Misalignment could cause damage to connections and possible data transfer failures, leading to the inability of flight control data reaching the Shuttle cockpit.

Smith's invention allowed quality assurance inspectors to detect bent contacts before connector mating occurred. The tool met NASA's cable harness inspection criteria, and its use would significantly reduce misalignment,

damage to flight hardware and risk to flight safety.

Although the CAU upgrade was canceled, the ICB selected Smith in April 2007 to receive the Space Act Award for his significant contribution to NASA's aeronautics and space activities.

Over the past 48 years, the ICB has issued more than 95,000 awards to NASA and its contractor employees as well as to other government, university and industry personnel. ■

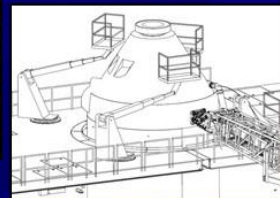


▲ USA's Christopher Smith demonstrates the TWINAX (twin axial) Cable Alignment Inspection Tool for which he was awarded the NASA Space Act Award.

29

## Event-Specific Recommendations Technology Example

### Bridge Bucket Contact with RMS (03/04/06) and similar Crane Mishaps



#### Causes/Contributing Factors:

- "SFOC Bridge Bucket & Spike Operator" training outline (OV-5AB-LSK), dated July 2004, states: "The potential for damage and injury from improper operation is high. There is no room for error in the processing of spacecraft." Class instruction emphasizes the need for OJT and mentoring during actual bridge bucket operations. (Note: There were no open high bays in which to practice the operation of the bridge bucket without a vehicle present). OPF 3 bridge bucket is different than OPF 1&2 bridge buckets.

*Note: similar causes/contributing factors with crane overturned at Pad B (01/31/05)*

- There are sensors on the bumper for the bottom of the bridge bucket, however, there are no sensors on the sides of the bridge bucket. There were side sensors in the past, but they were prone to causing false alarms. So the side sensors were removed, but they were not replaced with more reliable light contact or non-contact sensors.

#### Recommendations:

- Develop and implement training simulators for crane, heavy equipment, and bridge bucket-type operators.
- Advance the state-of-the-art in proximity sensors to improve reliability and accuracy.
- Require proficiency demonstration through OJT in addition to the classroom training; require crane/heavy equipment operators to have experience on specific models.

#### Status:

- Input to KSC and Agency-level technology roadmaps.
- Constellation Vertical Integration Element Handling and Access (VIEHA) – inputs for telescoping manlift non-contact proximity sensor study and ergonomic testing with bucket and hardware mockups.

30



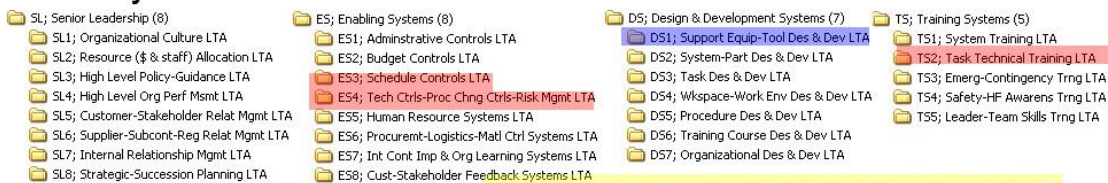
## Mishap Recurring Cause Summary

- ☀ Influence chain assessments were completed for over 60% of Standing Accident Investigation Board (SAIB) reports from February 2003 through May 2008
- ☀ Observed similar trends and patterns in contributing factors/causes to process escapes and process catches from August 2008 through January 2009
- ☀ Results of aggregate data analysis were used to formulate system-level risk reduction actions

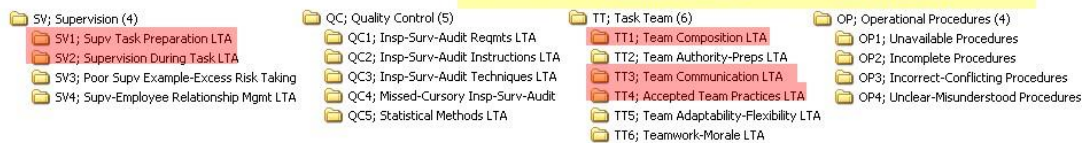
31

## Aggregate Data Analysis Results "Top 8" Proactive Risk Reduction Opportunities for Shuttle

### Control System Factors →



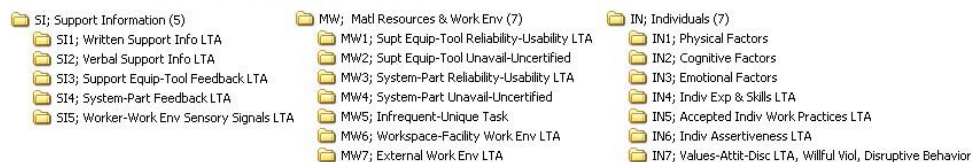
### Dual Role Factors →



Major Factors in Analysis:

- Control System or Dual Role Factor
- Non-design issue
- Frequency of occurrence
- Frequency unaddressed by SAIB
- Part of influence chains
- Emerging risk area

### Local Resource Factors →



Key:

Proactive risk reduction opportunity for Shuttle ground operations

32

## Major Factors in “Top 8” Selection

- Control system or dual role factor
- Frequency of occurrence
- Frequency unaddressed by Standing Accident Investigation Board (SAIB) recommendations
- Part of influence chains
- Emerging Risk Area

33

## Top 8 Proactive Risk Reduction Opportunities for Space Shuttle Ground Operations

- **Schedule controls**
  - 65% of occurrences were schedule issues related to troubleshooting/unplanned work and last-minute schedule changes
- **Supervisor task preparation**
  - 89% of occurrences were issues with worker assignments and supervisor preparation/experience
  - 67% resulted in significant schedule impacts (damage, extra troubleshooting) and 33% could have resulted in a Type A mishap
- **Team communication**
  - 88% of occurrences were related to peer communication within the immediate work team or between departments/work groups during task performance
  - 74% occurred during real-time troubleshooting tasks
- **Technical controls/process change controls/risk management**
  - 85% of occurrences were technical issues related to recognized problems that were uncorrected or inadequately corrected, or inadequate safety-hazard-risk reviews
- **Supervision during task**
  - **Note:** although this issue occurred several times, supervision during task is on the “top 8” list because it is an emerging risk area critical to successfully addressing other systemic issues
    - 100% of occurrences were issues with supervisor monitoring and oversight during the task
- **Accepted team practices**
  - 86% of occurrences were related to team shortcuts
  - 71% occurred in off-line areas
- **Team composition**
  - **Note:** although this issue occurred several times, team composition is on the “top 8” list because it is an emerging risk area critical to successfully addressing other systemic issues
    - 100% of occurrences were skill mix issues
- **Task technical training**
  - **Note:** although this issue occurred several times, task technical training is on the “top 8” list because it is an emerging risk area critical to successfully addressing other systemic issues
    - 50% of occurrences were related to insufficient OJT and mentoring
    - 67% were related to inexperience/skill issues

**Note: Top mishap risk reduction opportunity for future programs was better ground system/GSE design, including system feedback to ground crews**

34



## Development of System-Level Risk Reduction Actions

- ★ Selected Shuttle processing “all-stars” developed recommendations for actions focused on buying down the risk of mishaps and process escapes
  - Recognized leaders from Engineering, Shop, and Operations organizations in different facilities
  - Reviewed the data and applied their knowledge of operational practices
- ★ Some recommendations were not practical to implement at this point in the Shuttle Program
  - Good recommendations for future programs
- ★ Results presented to Ground Operations Steering Committee
  - Multiple iterations of risk reduction action plans

35

## Overview of System-Level Risk Reduction Actions

Proactive Risk Reduction Actions	Top 8 Proactive Risk Reduction Opportunities							
	Sched Controls	Supv Task Prep; Worker Assignmt	Team Comm	Tech Controls/ Risk Mgmt	Supv Monitor- ing	Accepted Team Practices	Team Comp/ Skill Mix	Task Tech Training
Implement performance self-assessments	X	X	X		X	X	X	
Implement “do not use or operate” tags				X				
Require systems training for personnel loaned to other facilities and programs							X	X
Enhance ground operations risk assessment procedures			X	X				X
Deploy floor engineers through the Problem Resolution Center	X		X	X				
NASA/USA Flow Management workshop; expand scope of Support Action Center	X	X					X	
Provide Crucial Conversations training for managers	X		X	X				
Provide Task Team Roles and Responsibilities (TTR&R) training for shop floor personnel		X	X			X	X	
Communicate internal best practices through safety advocates			X			X		
Perform predictive control analyses				X				
Modify process surveillance sampling activities to monitor best practices and proactive risk reduction actions				X	X	X		
Apply new investigation methodology to future adverse events: independent review before executive endorsement				X				
Develop and distribute a safety message from the STS-1 Pilot to the Shuttle workforce addressing recurring causes of mishaps	X		X		X	X		

Additional info in next slides

36

## Performance Self-Assessments

- ★ Designed to stimulate a two-way conversation between supervisors and employees to identify:
  - What went well (recognize successes)
  - Opportunities for improvement (identify and manage risk)
  - Positive behaviors (reinforce and encourage)
- ★ Similar to post task de-briefings
- ★ Minimum 1x/month
- ★ Listen and learn: “together we’re smarter and safer”

37

## “Do Not Use or Operate” Tags

- ★ Visual operational constraint system to alert and inform personnel of the following conditions:
  - Out of configuration hardware with potential to be forgotten
  - In-process work unattended for more than one shift
- ★ Replaces an ad hoc system (tape) for stationary GSE panel set-ups and portable GSE
  - OSHA lock-out tag-out (LOTO)
- ★ Operating procedure released



DO NOT USE OR OPERATE	
KSC FORM 4-002 (REV. 04/04)	
DATE APPLIED	_____
ITEM	_____
WAD NO.	SAMPLE
REASON	_____
TASK LEADER:	
NAME	_____
OFFICE	_____
PHONE	_____
NO.	_____
DO NOT USE OR OPERATE	

38



## Systems Training for Loaned Personnel

- \* A new process to reduce risks of mishaps associated with personnel loaned to other facilities or Programs
  - Flight systems, unique facility systems, and GSE
  - The need for support and applicable skills are matched to a group capabilities model
  - Identifies requisite skills and provides management the opportunity to assure any deltas to equivalent training are addressed before work begins
- \* Prior to returning to the home department, the employee receives notification to review current policies/practices



39

## Risk Assessment Enhancements

- \* Ground Operations Risk Assessment (GORA) performed for any first-time or infrequent task, unplanned task (especially unplanned work performed in previously closed out work areas), troubleshooting, hazardous jobs, or tasks with unusual test assemblies/setup
- \* Scope of each Process Failure Modes and Effects Analysis (PFMEA) and GORA includes pre-ops and close-out inspections
- \* Require an assessment of similar operations for associated mishaps or process escapes
- \* Technician and human factors engineering support
- \* Team members communicate identified risks
- \* NESC support to KSC Risk Review Board

STS 117



STS 124



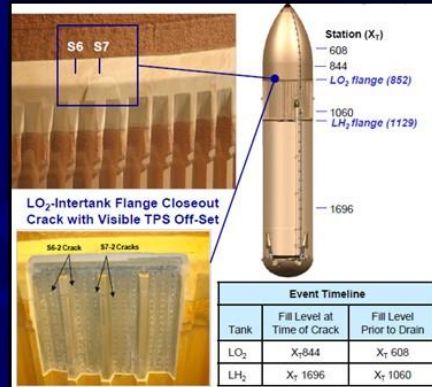
STS 128



40

## Problem Resolution Center and Flow Management Workshop

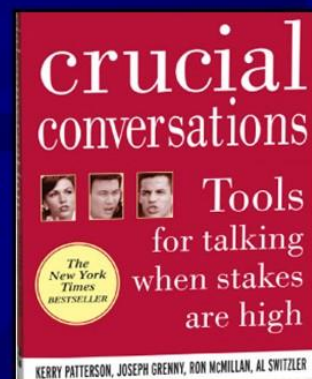
- ★ Problem Resolution Center deploys floor engineers to "hot spots" to help resolve technical and scheduling issues real-time
  - Roving troubleshooters
- ★ Joint NASA/USA Flow Management Workshop addressed the following issues (what to do, what NOT to do):
  - Workload vs. right resources
  - Constellation and Shuttle co-existence
  - Uncertainty
  - Critical skills and sharing resources
  - Maintaining focus and attention to detail



41

## Crucial Conversations Training

- ★ Communication skills training to increase trust and dialog during Shuttle fly-out and transition
- ★ Focus is on making it safe to talk about anything by creating mutual purpose and mutual respect
- ★ Approximately 500 USA Ground Operations and NASA Shuttle Processing managers, supervisors, leads, and informal leaders received training




42





## Shuttle Workforce Message from Bob Crippen



**Bob Crippen**  
*Former Astronaut and KSC Center Director*

(Video may take a few minutes to load. Run time is approx 8 minutes)

### Crip's Key Points

- We depend on you, the people that are hands-on, to be our first line and our last line of defense. If you see something that is not right, stop the work and bring it to management's attention.
- Management and leadership need to keep their fingers on the pulse of the program. Go out where the people are doing the work.
- Schedule pressure will always be there, but schedule pressure is not worth compromising the safety of the people working on the vehicle or the vehicle itself.
- Communication is extremely important. Communication is a two-way street.
- An accident is usually caused by a chain of events. All we need is one person to break that chain and prevent the accident.
- Continue to be diligent and follow the processes which are so critical, but also have a bigger view. Look at what is going on around you.

*"We depend on you for a strong, safe finish to the Program."*

43

## Major Insights

- **An appropriate systems model is needed to identify and evaluate system-level issues**
- **Need to evaluate all contributing factors and causes to get to system-level issues**
  - Because a contributing factor can be a cause in a different situation or on another day, and vice-versa
  - Recurrence data (vs. individual root causes)
  - Interactions or influences between causes/contributing factors
- **System-level issues recur because they are hard to fix**
  - Bad habit analogy
  - Requires understanding of the data to develop fixes
- **Independent review of mishap investigation reports provides value**
  - Ensures all causes/contributing factors are identified and addressed (systems perspective)
  - Enables a database to analyze trends & patterns
  - Provides a larger "menu" of potential corrective/preventive actions
    - Examples: standards, new technology inputs, Center-level issues, design issues
- **No silver bullets; requires sustained, orchestrated effort grounded in data**
- **Influence chain mapping methodology and recurring cause analysis complements root cause analysis efforts for individual mishaps**

***"Complex systems sometimes fail in complex ways. Sometimes you have to work pretty hard to pin down those complex failure mechanisms. But if you can do that, you will have done the system a great service."***

*Admiral Gehman, Chair of the Columbia Accident Investigation Board*

44

## Summary

- Proactive risk reduction actions will continue through Shuttle fly-out
- Study results have also been applied to Constellation system designs
  - Human factors engineering pathfinder for ground support equipment (GSE) design teams
  - GSE design reviews
  - Ground operations planning and operability enhancements
  - Orion processing and assembly

*"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, Day of Remembrance Memo, Jan 29, 2009*

*"Space Shuttle safety is not a random event. It is derived from carefully understanding and then controlling or mitigating known risks."*

*Richard Covey, Florida Today, January 15, 2009*

45

## Backup

46



## Carrots and Crabgrass

(Different Types of Roots)



*"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."*

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

47

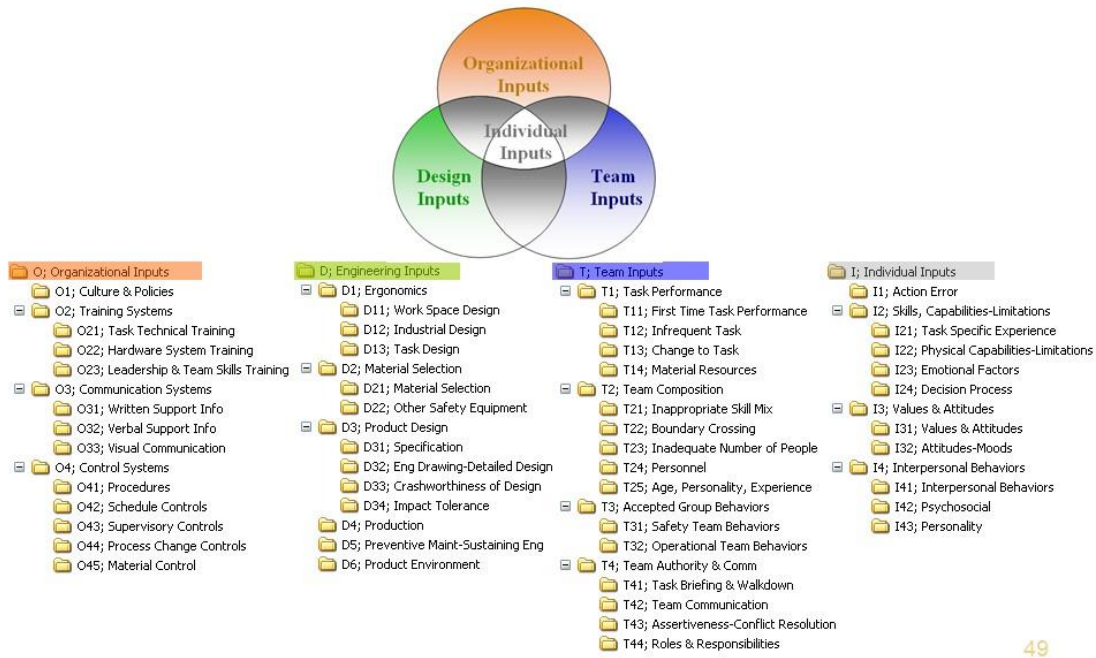
## Additional Quote

***"We know that single causes are rare, but we don't know how small events can become chained together so that they result in a disastrous outcome. In the absence of this understanding, people must wait until some crisis occurs before they can diagnose a problem, rather than be in a position to detect a potential problem before it emerges."***

***To anticipate and forestall disasters is to understand regularities in the ways small events can combine to have disproportionately large effects." (Karl Wieck)***

48

# Shuttle Operations Contributing Factor Taxonomy Human Factors Event Evaluation Model - 6/11/03 revision

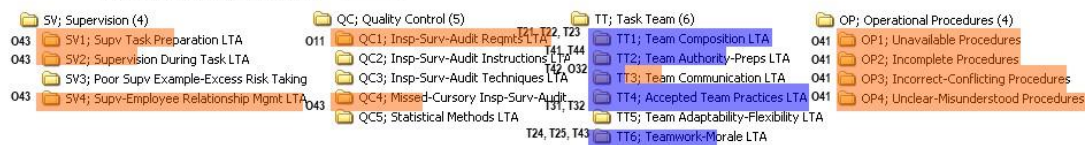


## Comparison of Dual Role Taxonomy and Shuttle Taxonomy

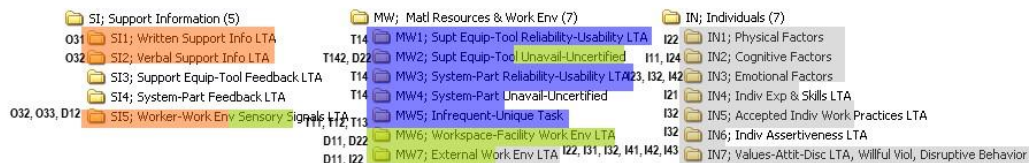
### Control System Factors



### Dual Role Factors



### Local Resource Factors



#### Key:

Shuttle Processing Taxonomy  
Top-Level Categories

Shuttle Processing Taxonomy  
Subcategory Codes (examples)

Organizational Inputs (O)    Engineering Inputs (D)    Team Inputs (T)    Individual Inputs (I)

I24, I11, T14, O44

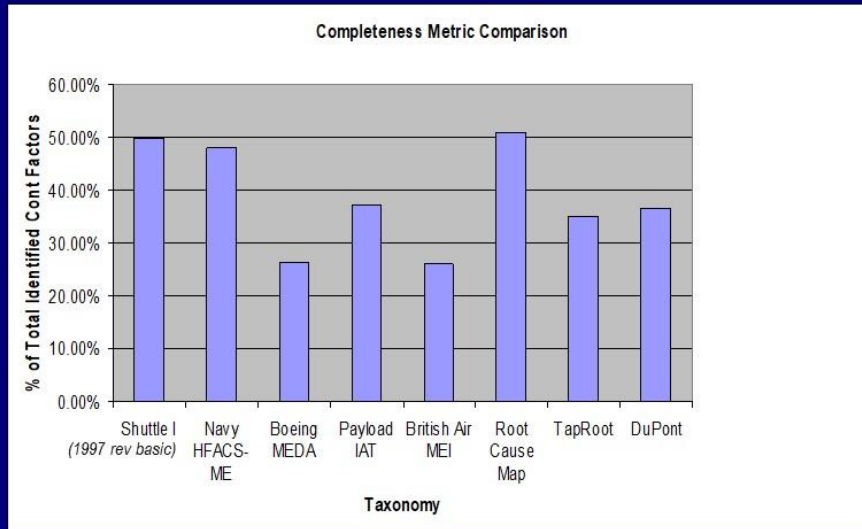
**Note:** Uncovered or partially covered categories represent additional categories or subcategories in the dual role taxonomy.

50



## Taxonomy Comparative Analysis

- Spreadsheet tool developed
- 20+ taxonomies analyzed, 8 taxonomies fully “coded”
- 364 distinct contributing factor categories
- Significant improvement opportunities identified for each taxonomy



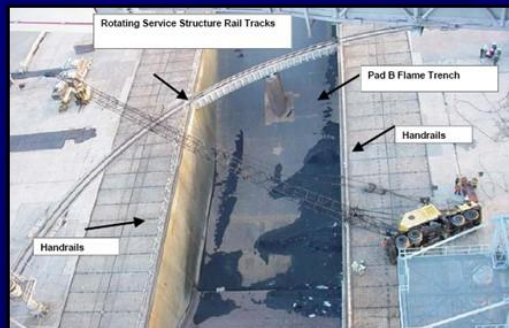
51

## Event-Specific Recommendations

### Additional Examples

#### Crane Overturned on Pad B Surface (01/31/05)

Install tire pressure indicators in crane tires to provide visual indications of low tire pressure and potential instability issues.



52

## Event-Specific Recommendations Technology Example

### LC39B N2O4 Oxidizer Exposure Injury (07/09/04)



#### Causes/Contributing Factors:

- A risk management issue was associated with the standard procedure of sniffing for leaks with equipment after a technician had already detected an odor. The leak detection equipment readings were used to specify the hazard, not the detection of the odor by the technician. The equipment/technology issue is associated with the limited capability of the leak detectors. The practice of sending people into an area with equipment to try to find a leak when a hazardous odor was already detected by a human was questionable. A leak detector reading of 0 ppm did not mean the leak wasn't present – just that the leak couldn't be detected with the equipment in that particular operational environment. The practice would have been acceptable only if the capability of the leak detection device was beyond the capability of the human nose.

- A technology issue was associated with the capability of the leak detectors. The leak detectors were not sensitive enough to support this operation. Several readings of 0 ppm were registered, but, when the fitting was bagged after the mishap, discoloration resulted, confirming the leak. The leak detector was not reliable in the operational environment.

#### Recommendation:

Develop more sensitive, more reliable leak detection equipment for the KSC outdoor operational environment (hot, humid, breezy).

#### Status:

- Input to KSC and Agency-level technology roadmaps.

53

## Additional “Gold Nuggets” - Examples

### SCAPE Suit Oxidizer leak (06/26/03)

Impose strict limits on the number of suit repairs and/or implement a used suit validation/certification procedure. For example, pull suit off-line every ten patches to recertify the suit.

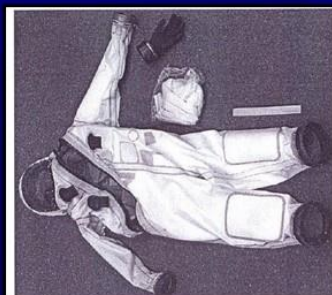


Figure 1  
As-received PHE, left hand glove, and undershirt in bag.

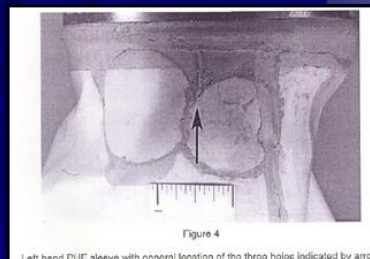


Figure 4  
Left hand PHE sleeve with general location of the three holes indicated by arrow

54



## Influence Chain Mapping Summary

➤ Influence chain map assessments were completed for 20 Standing Accident Investigation Board reports from February 2003 through May 2008

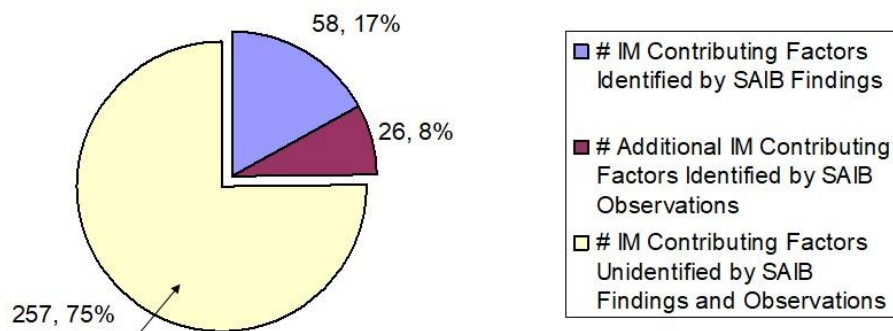
	Total	Min	Ave	Max
# of Contributing Factors	341	8	17.1	29
# of Influence Chains	93	2	4.7	7
Ave. Influence Chain Length: # of Contributing Factors			3.7	

➤ Observed similar trends and patterns in contributing factors/causes to process escapes and process catches from August 2008 through January 2009

55

### How the SAIB Reports Identified IM Contributing Factors

(20 mishaps, 341 contributing factors)



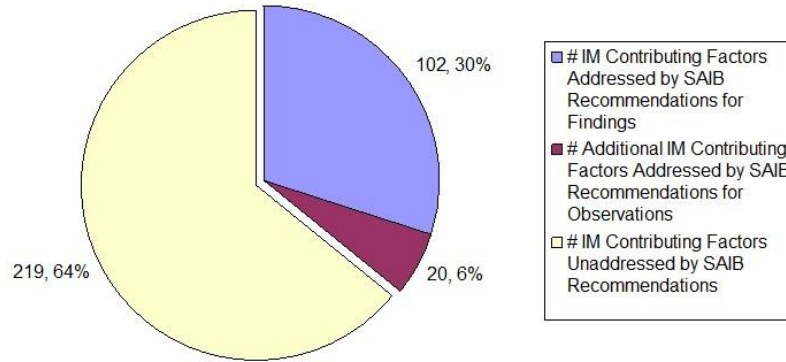
#### Additional data:

- 36% (93 of 257) of the IM contributing factors unidentified by SAIB findings and recommendations are in categories not covered by the USA Human Factors taxonomy
- 12 additional SAIB findings did not address any IM contributing factors
- 49% (41 of 84) of the IM contributing factor categories and SAIB finding categories were in agreement
- 16% (41 of 341) of the IM contributing factors were identified AND SAIB categories were in agreement with IM categories

56

## How the SAIB Reports Addressed IM Contributing Factors

(20 mishaps, 341 contributing factors)



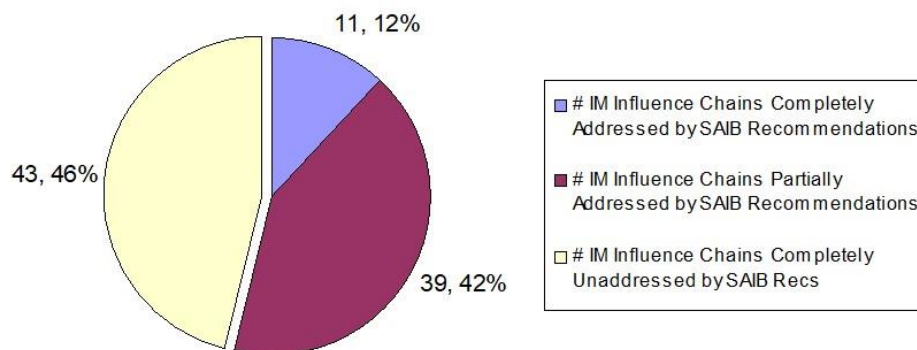
### Additional data:

- 18% (62 of 341) of the IM contributing factors were identified AND addressed by the SAIB reports

57

## How the SAIB Reports Addressed IM Influence Chains

(20 mishaps, 93 influence chains)

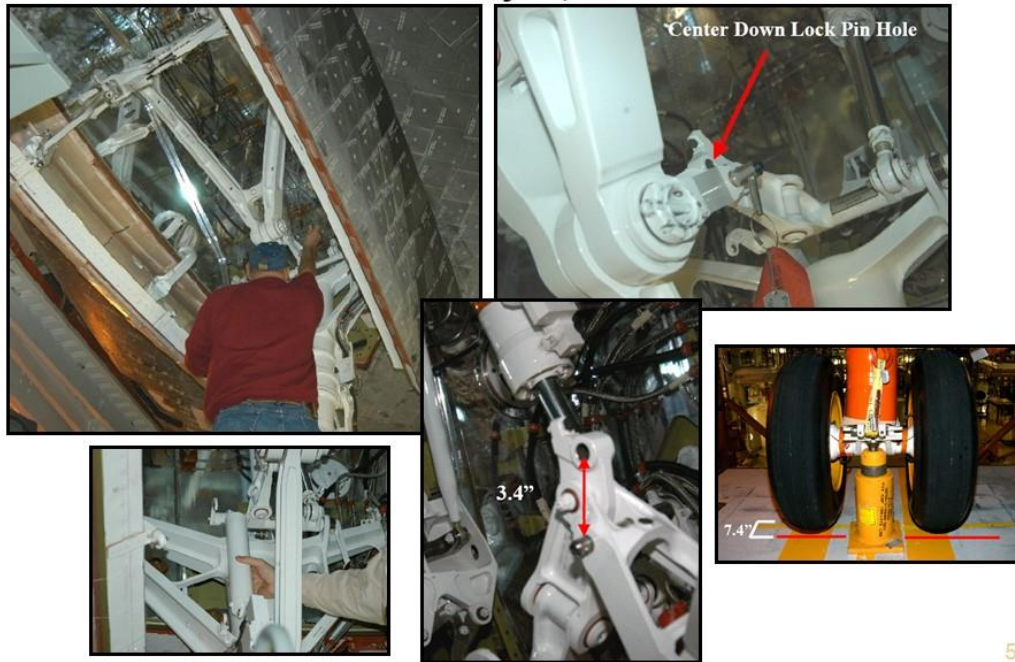


### Additional data:

- 29% (72 of 248) of the IM "influence links" (the relationships between contributing factors) were addressed by SAIB recommendations

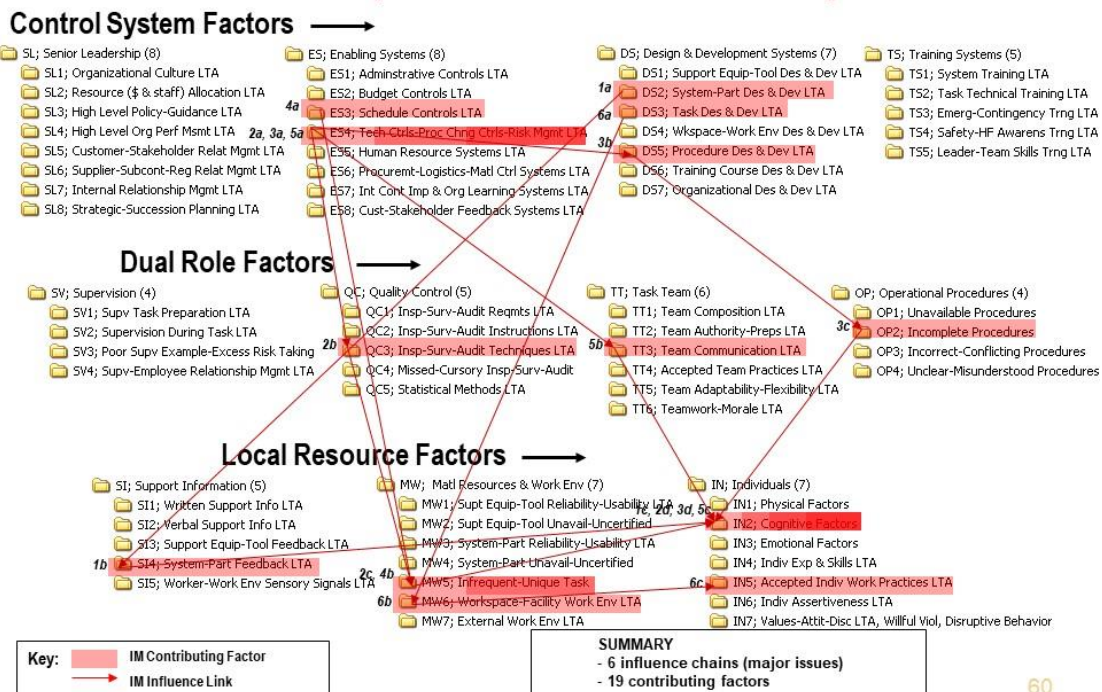
58

## Example Influence Map Assessment #2: OV-105 NLG Movement During Jack Transfer January 20, 2006



59

## OV-105 NLG Movement Close Call Completed Influence Chain Map



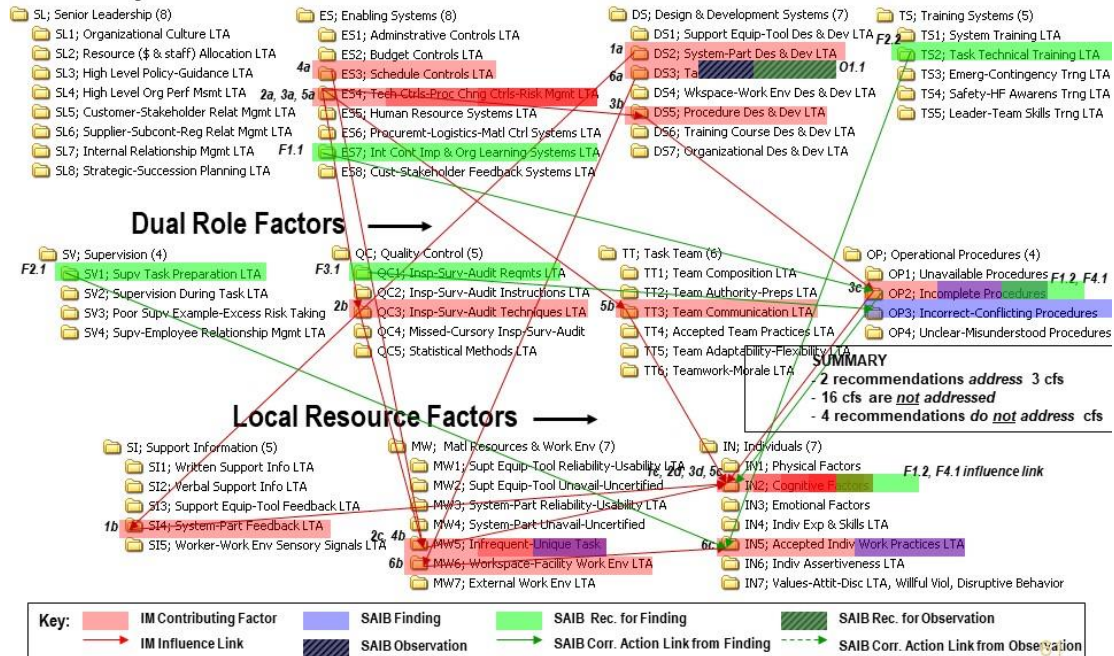
60



# OV-105 NLG Movement Close Call

## Cont. Factors + SAIB Findings & Obs + SAIB Recommendations

### Control System Factors



## Summary of NLG Close-Call

- Influence Map**
  - 6 influence chains (major issues)
  - 19 contributing factors
- SAIB Report**
  - Findings and Observations**
    - 4 findings *identify* 3 contributing factors in 3 influence chains
    - 1 observation *identifies* 1 additional contributing factor
    - 15 contributing factors are not identified
  - Recommendations for Findings and Observations**
    - 2 recommendations *address* 3 contributing factors in 2 influence chains
    - 4 recommendations do not address contributing factors
    - 16 contributing factors are not addressed (3 complete influence chains and 3 partial influence chains)
- "Gold nugget" recommendation for addressing the dominant influence chain**
  - Only perform NLG ops with hydraulics (a constraint to perform this operation is orbiter power up), except in an emergency situation
- Additional gold nugget recommendations**
  - Ensure inter-system constraints (i.e., bungee installation) are discussed in an engineering forum
  - Re-implement using red tags as a visual indicators for non-standard configurations or out-of-configuration
  - Perform task analyses for mechanical tasks where visual inspections may be impaired by visual angle, obstructions, etc.
  - Ensure only work stands or ladders that allow visual verification of hardware are used to support jack transfer operations

### X-31 Lessons Learned Video from Dryden: Breaking the Chain



(Video may take a few minutes to load. Run time is approx 40 minutes)

#### X-31 Mishap Background

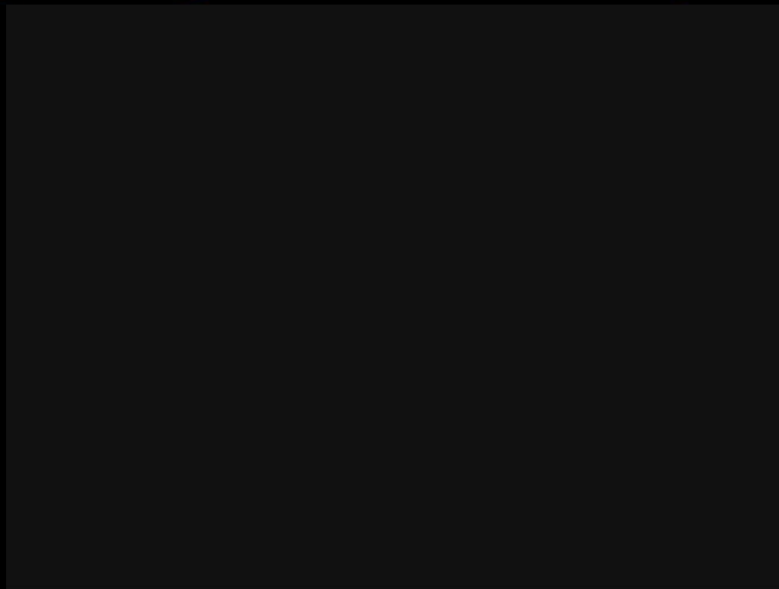
- The X-31 program regularly flew several flights a day, accumulating over 550 flights with a superlative safety record. The accident occurred on the third and last flight of the day on January 19, 1995. It was the final flight of Plane #1, which was scheduled for retirement after wheel stop.
- The proximate cause of the mishap was a blocked Pitot tube (due to icing) which sent erroneous readings to the flight control computers. Underlying issues included incomplete/improper interpretation of hazard analyses, a breakdown in configuration management and change documentation, and failure to impose proper operational controls and take preventive actions.

#### X-31 Key Points for the Shuttle Team

- Be wary of configuration changes. Plane #1 was flying with a new Pitot tube and the heater was not connected.
- Pay attention to warning signs. The first signs of trouble began to appear when the pilot reported airspeed far above what was even possible at his angle of attack. No one in the control room caught the significance of that discrepancy, or, if they did, no one spoke up.
- Communicate and fix known problems. The chase plane pilot could not hear any

63

## ***Lessons Learned from X-31 Mishap at Dryden Flight Research Center (DFRC)***



64

## **Appendix N. Examples of NESC Assessments that Address Mishap Recurring Causes**

### **Integrated Hazard Development Process Assessment (primary mishap recurring cause addressed: inadequate technical controls/technical risk management practices)**

This assessment was to gain an understanding of the integrated hazard process, identify any gaps (e.g., missed causes, cause tree incompleteness, or missed hazards), and suggest improvements to the process.

### **Pyroshock Technical Support Activity (primary mishap recurring cause addressed: system design and development issues)**

A loads and induced environments team requested an independent evaluation of pyroshock data. Analyses were required to convert supplied data from the frequency domain to the time domain, assess the data quality and shock levels, and provide a summary of results and potential issues with the data quality and shock levels. Data was provided for different locations on the launch vehicle and for some of the datasets it was found, that there is a large disparity between maximum and minimum shock response spectra at low frequencies, possible saturated signals, and that there are unrealistic Fourier magnitude profiles. This led to the conclusion that the datasets that exhibit this behavior have inherent data quality issues. Of the examples provided for the data quality investigation, there were two faulty data sets, three good data sets, and one acceptable data set.

### **Evaluation of Occupant Protection Requirement Verification Approach (primary mishap recurring cause addressed: system design and development issues)**

This assessment was to perform a review of the test methods used to ensure that the crew safety requirements were properly developed. The requirements included a combination of acceleration load requirements and anthropomorphic test device (ATD) injury assessment reference values. The NASA contractors are required to provide Programs with their verification approach to demonstrate compliance with occupancy requirements using a combination of modeling, analysis, and tests. Since ATDs and ATD models have been developed for use in the automotive industry, their use in the multi-axis dynamic accelerations of launch and reentry and the potential interactions with launch and entry suits and crew seats must be validated. The accuracy of the results acquired from their models and simulations must also be verified.

### **Systems Engineering and Integration Processes (primary mishap recurring cause addressed: system design and development issues)**

The objective of this assessment was to evaluate the adequacy of SE&I processes and functions. During a design review, engineering managers made an observation that, although the design was reviewed as planned, the Systems Engineering and Integration (SE&I) processes necessary for controlling and producing the design were not fully evaluated. In addition, recent observed failures pointed to flaws in general SE&I processes assumed to be in place and effective in the certification strategy. These functions include configuration management, technical risk management, requirement verifications and validations, materials and processes, and acceptance testing.

### **Material Compatibility for Bellows (primary mishap recurring cause addressed: system design and development issues)**

An NESC assessment team developed a test program to better understand the material compatibility of zero-fault-tolerant thin-walled pressure boundaries (TWPB). This was to help the Program meet the intent of the Agency Best Practice and Guidelines for TWPB for Human Spaceflight Applications and thereby improve reliability of the TWPB. The TWPB capsule's propulsion system that are addressed in this assessment are the bellows in the service module propulsion system valves. These isolation valves are subject to numerous fluids during manufacturing, assembly, and test, and they operate with storable propellants, monomethyl hydrazine and mixed oxides of nitrogen.

### **Automotive and Non-Automotive Commercial-Off-The-Shelf (COTS) Electrical, Electronic, and Electromechanical (EEE) Parts Testing (primary mishap recurring cause addressed: system design and development issues)**

NASA is a relatively low volume consumer of high reliability EEE parts and has typically used United States military specifications and standards (MIL-PRF- 38535, MIL-STD- 883, MIL-STD-750, etc.) for EEE parts procurement criteria. The military standardization system ensures that parts made to these specifications are built, screened, and qualified to the same standards by different manufacturers, regardless of the application or the procurement volume. Select NASA Programs, Projects, and organizations are considering a non-traditional approach to EEE parts selection, qualification, and screening for avionics systems. These programs propose to use automotive and non-automotive COTS EEE parts with no parts level screening and qualification, but only board and/or box-level testing. This assessment determined that destructive physical analysis showed a defect rate of more than 20% distributed across manufacturers and part category. Part-level testing was recommended as was mission environment, application, and lifetime-based radiation testing.

### **Avionics Architecture Review (primary mishap recurring cause addressed: inadequate technical controls/technical risk management practices)**

NESC assessed the fault tolerance and redundancy of a proposed flight avionics systems non-deterministic architecture for crewed missions. This effort was required to validate the level of fault tolerance and redundancy of the flight avionics systems based on EEE requirements and to identify candidate EEE parts for in-depth review. Fault tolerance and redundancy of the avionics architecture, in addition to short mission duration, have been cited as rationale for the use of nontraditional approaches for EEE parts selection, qualification, and screening.

### **Assessment of Capsule Dynamics in the NASA Vertical Spin Wind Tunnel (primary mishap recurring cause addressed: system design and development issues)**

Rather than accepting the estimated capsule reentry aerodynamic data which had been developed using an original capsule configuration, NESC funded an experiment to determine the reentry aerodynamics of a new capsule configuration. The assessment showed that the regions of stability and instability of the two configurations were not at the same angles of attack.

### **Assessment of Viscous Effects on Launch Vehicle Ground Wind-Induced Oscillations (primary mishap recurring cause addressed: system design and development issues)**

Contractors are qualifying launch vehicles for wind-induced oscillations (WIO) using a markedly different approach from that historically used by NASA. They are using a contractor whose

primary expertise is in the civil engineering market. NASA has been designing vehicles for ground-wind loads based on a predicted WIO lock-in (a match between the vortex shedding frequency of the vehicle and the natural frequency of the vehicle) based on wind tunnel testing that attempts to minimize the difference between test and flight Reynolds number. Contractors are not designing to lock-in and are testing at Reynolds numbers that are much lower than flight or the Reynolds numbers attainable in NASA's larger scale wind tunnel facilities. The contractors also attempted to simulate atmospheric turbulence generated by surrounding structures and landscape features in their wind tunnel tests. No data exists to know which technique is best for determining critical wind conditions and the resulting WIO-induced loads. This assessment was to compare the two techniques.

**Evaluation of Flight Test Article Design for Parachute Transonic Inflation Risk (primary mishap recurring cause addressed: system design and development issues)**

High-altitude and high-Mach number parachute-deployment data does not exist for a contractor's capsule. The contractor and their parachute vendor are currently collaborating in an attempt to leverage heritage test data from Mercury, Gemini, and possibly other programs to qualify by similarity. NASA completed a similar exercise in-house and determined that the results were insufficient to address transonic wake effects. This assessment was to evaluate if a drop-test article could be designed to fill the gaps in reentry data.

**Ground Operations Human Factors Task Analysis (primary mishap recurring cause addressed: inadequate task analysis and design processes)**

An NESC request for technical support was submitted as a result of discussions regarding disposition of a Review Item Discrepancy (RID) submitted by NESC. The RID identified a gap in ground operations task design and analysis methodologies. The RID suggested that the program "consider developing and implementing a human factors-based task design and analysis methodology for selected operations based on factors such as (but not limited to) criticality/complexity of human-system interfaces, hazards, hands-on labor hour estimates, and critical path considerations." Potential benefits of a robust task design and analysis methodology include additional improvements in flight crew safety (through reduced risks of undetected ground crew errors and collateral damage), ground crew safety (through prevention of mishaps, close calls, and process escapes), operability, efficiency, and critical path performance.



REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>						
1. REPORT DATE (DD-MM-YYYY) 03/23/2020		2. REPORT TYPE Technical Memorandum			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Recurring Causes of Human Spaceflight Mishaps during Flight Tests and Early Operations				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Barth, Timothy S.; Lilley, Steve K.; Kanki, Barbara G.; Blankmann-Alexander, Donna M.; Parker, Blake				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER 869021.01.07.01.01		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) NASA Langley Research Center Hampton, VA 23681-2199				8. PERFORMING ORGANIZATION REPORT NUMBER L-21130 NESC-RP-12-00823		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001				10. SPONSOR/MONITOR'S ACRONYM(S) NASA		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) NASA/TM-2020-220573		
12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified - Unlimited Subject Category 16 Space Transportation and Safety Availability: NASA STI Program (757) 864-9658						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT An analysis of recurring causes underlying human spaceflight mishaps that occurred during flight tests and early operations was performed. Eight mishaps from the Apollo, Soyuz, Skylab, Space Shuttle, and Constellation Programs and commercial suborbital systems were included in the study. Detailed event analyses were performed for the historical mishaps and aggregate data analyses conducted to identify recurring issues, and the nine most frequent issues were identified.						
15. SUBJECT TERMS Mishaps; NASA Engineering and Safety Center; Flight Test						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)	
U	U	U	UU	241	19b. TELEPHONE NUMBER (Include area code) (443) 757-5802	