TRENDS IN HUMAN SPACEFLIGHT: FAILURE TOLERANCE, HIGH RELIABILITY AND CORRELATED FAILURE HISTORY

Carrie Green[(1)], Maria Havenhill[(2)], Deboshri Sadhukhan[(3)], John Bobanga[(4)], Joyoshri Sadhukhan[(5)], Matthew Fiedler[(6)]

[(1)]NASA, 21000 Brookpark Rd., Cleveland, OH 44135, USA, Email:Carrie.L.Green@nasa.gov
[(2)] NASA, 21000 Brookpark Rd., Cleveland, OH 44135, USA, Email:Maria.A.Havenhill@nasa.gov
[(3)] NASA, 21000 Brookpark Rd., Cleveland, OH 44135, USA, Email:Deboshri.Sadhukhan@nasa.gov
[(4)]NASA, 21000 Brookpark Rd., Cleveland, OH 44135, USA, Email: John.O.Bobanga@nasa.gov
[(5)] The Ohio State University, Columbus, OH 43210, USA, Email:Sadhukhan.2@buckeyemail.osu.edu
[(6)] The Ohio State University, Columbus, OH 43210, USA, Email:Fiedler.32@buckeyemail.osu.edu

ABSTRACT

In a half century of human spaceflight, NASA has continuously refined agency safety and reliability requirements in response to mission demands, critical failures, and technology development. Early spacecraft, including Mercury, Gemini and Apollo vehicles, were highly reliant on dissimilar redundancy and demonstrated test margins. Later programs, such as the reusable Space Transportation System (STS) and International Space Station (ISS), introduced probabilistic studies and isolated two-failure tolerance to improve robustness at the expense of added complexity. More recently, the Orion Multi-Program Crew Vehicle (MPCV) program adopted universal single-failure tolerance with two categorical exceptions; Zero-Failure Tolerant (0FT) and Design for Minimum Risk (DFMR) hardware. Failure tolerance variances are defined and managed in accordance with agency human-rating requirements, and require concurrence from program Technical Authorities (TA) as well as the MPCV Safety and Mission Assurance Safety and Engineering Review Panel (MSERP).

To understand and reaffirm standards applied to Apollo, Space Shuttle and Orion vehicles, Orion and Deep Space Gateway Safety and Mission Assurance (S&MA) representatives conducted accelerated research to compare unique safety and reliability criteria against ground and flight anomalies, based on information contained in post-mission reports and the Problem Reporting and Corrective Action (PRACA) database. In some cases, high-profile failures and narrow escapes have reinforced decisions to maintain or adapt safety requirements. In others, empirical trends have highlighted the need for vigilance and innovative safety guidelines. Given the inability to achieve absolute compliance with evolving safety and reliability requirements, the team conducted a targeted review of DFMR and 0FT propulsion elements within the framework of changing system design, inspection, materials and process developments to formulate conclusions on technological maturity, failure density, and net changes in safety risk. Based on the aggregate performance of high-reliability and failure-tolerant systems, the authors have attempted to establish best practices and guidelines to inform future program decisions.

On a somewhat cautionary note, this study is not intended to direct a universal set of requirements for future missions based on prior lessons learned. Spacecraft safety is a multi-variable problem, and attempts to mitigate past failures will not guarantee future success. However, this assessment offers a retrospective review of policy changes, implementation and effectiveness. In the future, NASA, European Space Agency (ESA) and industry partners may benefit from a more robust correlation between requirements and performance, as space-faring nations work toward more challenging, complex and long-duration commercial and deep-space ventures.

1. ARCHIVAL RECORDS

"Those who cannot remember the past are condemned to repeat it." – George Santayana

In the fifty years that have elapsed since the Apollo 11 moon landing, the National Aeronautics and Space Administration (NASA) has dedicated resources to collect, archive and maintain our invaluable space-faring records. From the Apollo experience reports to the Space Shuttle Problem Reporting and Corrective Action (PRACA) database, an expansive reference library is available for those trained in the art of data collection and management.

Unfortunately, for the average practitioner, many of these program records are not yet available online. Instead, a large number of Gemini, Apollo and Space Shuttle Program documents are being stored at NASA facilities and National Archives locations across the United States. While carefully maintained, these file sets contain hundreds of boxes without a corresponding index, and folders are often empty aside from a few obsolete cross-references to microfiche copies of critical

historic files, including the Apollo Failure Modes and Effects Analyses (FMEA) and Probabilistic Risk Analyses (PRA). Failure reports are also largely scattered and illegible, making for long hours of research and unfulfilled leads.

Compounding the difficulty of maintaining historic documents in hard copy, online records present a unique set of challenges. Heritage Space Shuttle pre-flight reports from the 1980's and 1990's are currently stored in outdated and unsupported file formats, leaving the research team with partial records and large gaps in early and mid-program data.

In spite of these obstacles, the local S&MA research team spent two weeks at various National Archives facilities, and collected a plethora of detailed design and production reports that offer a unique perspective on many of the the same issues facing human-spacefaring enterprises today. Hundreds of Apollo, Shuttle and Orion records were pulled and digitized to assess single-point failures, failure criticalities, corrective actions and general lessons learned. This interim report offers preliminary insight into previously untapped cross-program data analysis, and provides a framework for future research in this field.

2. FMEA CRITICALITY COMPARISON

2.1 Human-Rated Bipropellant Propulsion Systems

Apollo, Space Shuttle and Orion propulsion subsystems were generically designed with a similar set of guidelines to enable active pressurization, pressure relief, propellant distribution, and attitude and translation control [1][2][3]. However, as bipropellant system technology has remained fairly static since the 1960's, qualitative and quantitative failure tolerance requirements have changed much more frequently. Apollo initially mandated a probability of safe crew return design standard (0.999) and employed redundancy wherever practical, with specific exceptions for the structure, heat shield, and certain portions of the main propulsion systems. The Space Shuttle directed a fail-safe design for all nominal and abort conditions, managing exceptions through Critical Items Lists (CIL) [4]. And early Orion requirements defaulted to two-failure tolerance, but later evolved to specify no less than single-failure tolerance with provisions for zero-failure tolerant exceptions pending MSERP and technical authority concurrence [5].

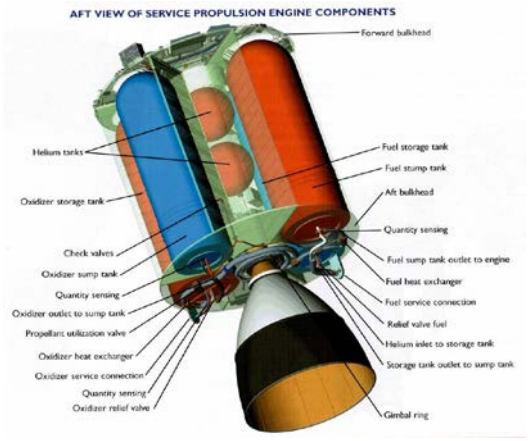

Figure 1. Apollo Service Propulsion System (SPS)

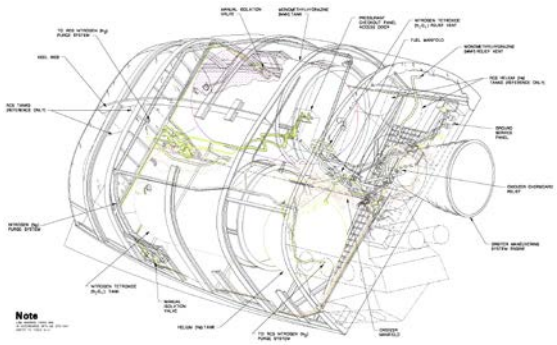

Figure 2. Shuttle Orbital Manoeuvring System (OMS)

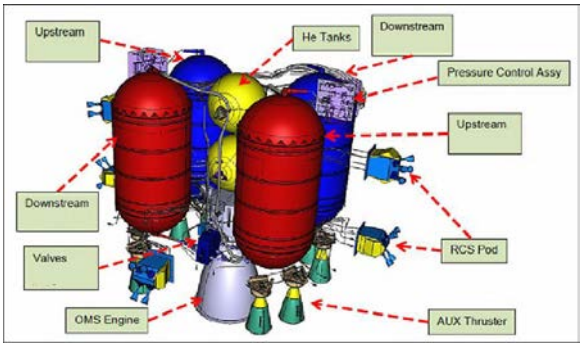

Figure 3. MPCV Orion European Service Module (ESM) Propulsion Subsystem

To compare unique propulsion design attributes across multiple systems, a diagnostic tool was developed to generically map component types, prevalent failure modes and criticality designations from vehicle to vehicle. As noted previously, Apollo Crew and Service Module (CSM) and Space Shuttle Orbital Manoeuvring System/Reaction Control System (OMS/RCS) hardware FMEAs were not available within advertised folders at the National Archives. In the absence of this data, S&MA representatives defined criticalities based on

design files, an Apollo Single Point Failure (SPF) analysis [6] and a comparative FMEA analysis on the Shuttle Knowledge Console [7]. Relative criticalities were then compared across programs as follows:

- (+1) Additional redundant instrumentation, increased failure tolerance
- (-1) Additional hardware or failure modes, decreased failure tolerance

Aggregate results for each type of hardware are summarized in Table (1), and causal factors are addressed in Table (2).

Component	Orion vs. Apollo	Shuttle vs. Apollo
Burst Disc/Relief Valves	-1	0
Check Valves	0	-3
Engines	-2	6
Fill/Drain Valves	0	0
Filters	-1	-1
Lines	1	0
Pressurization Valves	-2	-4
Propellant Valves	0	-3
Pyro Valves	-3	0
Regulators	1	1
Sensors	7	8
Tanks	0	0

Table 1. Multi-Vehicle Qualitative Failure Modes and Effects Analysis Comparison

Component	FMEA Distinctions
Burst Disc/Relief Valves	Pressurization system architecture
Check Valves	Common feed system, internal and/or external check valves
Engines	Feed system complexity, pneumatic redundancy
Fill/Drain Valves	Pressurization and propellant fill/drain valve failure tolerance
Filters	Single-point blockage failures
Lines	Elimination of flexible line bellows
Pressurization Valves	Vapor migration protection, improved instrumentation, cross-feed complexity
Propellant Valves	Tank isolation complexity, non-isolatable bellows
Pyro Valves	Additional valves
Regulators	Improved instrumentation
Sensors	Improved instrumentation
Tanks	All propellant leakage assumed to be a worst-case Criticality 1

Table 2. FMEA Criticality Differences

For this particular study, crew survival methods, including cross-feed and lunar module recovery, were not considered in the raw criticality scores; however, these systems could influence the survivability of select failures including external leakage and blockage.

3. FAILURE HISTORY CORRELATION

3.1 Analysis Methodology

As described above, the quantity and quality of readily available failure history data was somewhat limited. A few additional, important caveats are highlighted below.

Data acquisition for Apollo proved to be the most challenging piece of this investigation. Flight data was generally available in post-mission reports; however, ground data was limited to sparse carbon copy Discrepancy Reports (DR) that were collected and scanned at various National Archives locations. While the Apollo ground failure database may not have been complete, the raw number of retrieved DRs was within family with respect to recovered space shuttle and Orion files.

Shuttle flight reports and pre-flight reports, while extensive, were also not converted to an appropriate Microsoft Office format within sufficient time to support this study. Due to the large volume of Orbital Manoeuvring System (OMS) and Reaction Control System (RCS) data, this study has been constrained to OMS data for forty-five (45) missions between Space Transportation System STS-31 and STS-114. All OMS and RCS flight failures have been captured in Mission Evaluation Reports (MER) and are included in this report.

Finally, Orion propulsion anomalies were limited to data contained within the cross-program Problem Reporting and Corrective Action (PRACA) database. These reports were also somewhat incomplete considering open component and vehicle qualification testing, and unproven flight performance.

For the purpose of this study, criticality assignments on all discrepancy reports were universally adapted to reflect Orion FMEA ground rules and assumptions, as defined in the Orion MPCV Program Hardware Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) Requirements Document [8]. Interfacing ground system, electrical system and thermal system failures were excluded from each data set, and are considered forward work.

3.2 Anomalies over Time

The following trend charts reflect Apollo, Space Shuttle and Orion anomaly counts for a given failure criticality over time.

3.2.1 Ground Anomalies over Time

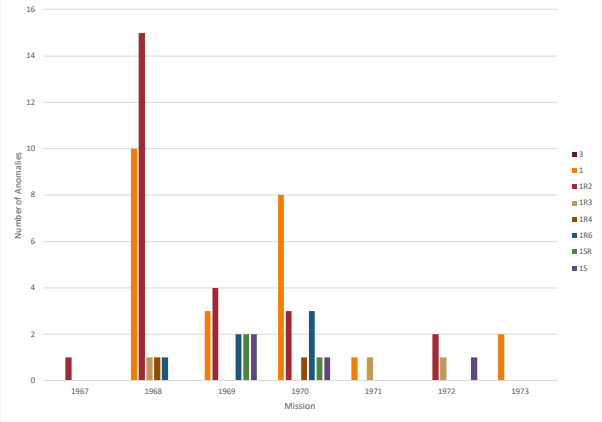

Figure 4. Apollo Propulsion Number of Ground Anomalies by Year

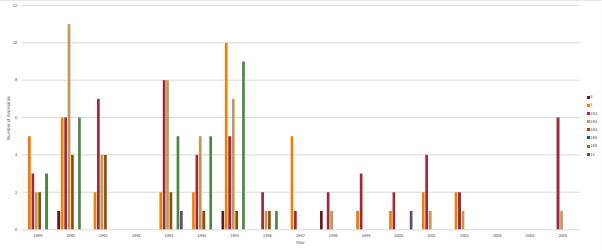

Figure 5. Space Shuttle Propulsion Number of Ground Anomalies by Year

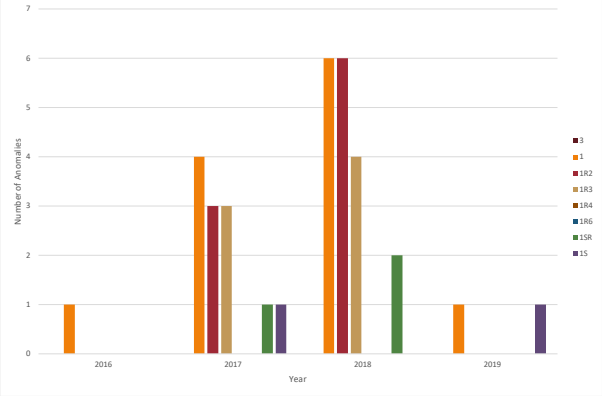

Figure 6. Orion Propulsion Number of Ground Anomalies by Year

3.2.2 Flight Anomalies over Time

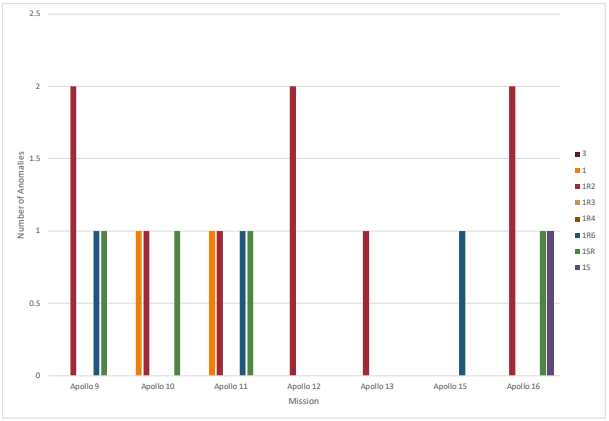

Figure 7. Apollo Propulsion Number of Flight Anomalies by Mission

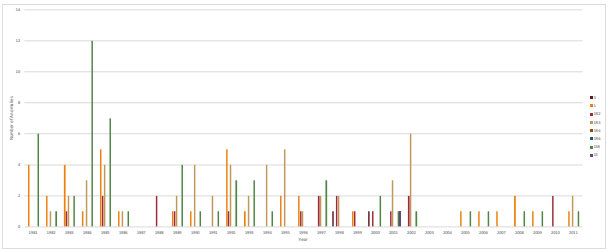

Figure 8. Space Shuttle Propulsion Number of Flight Anomalies by Year

3.2.3 Timeline Analysis Summary

Plotting the severity and quantity of major anomalies for a given vehicle campaign highlighted several interesting trends. First, as anticipated, failures occurred at a higher frequency earlier in each program, reinforcing program development risk and infant mortality.

Criticality 1 failures were also somewhat prevalent, although most were attributable to propellant leakage from tanks, lines and engine valves. The frequency of these events generally decreased over the time, but the high density of leakage failures highlighted the importance of adequate leak detection.

Finally, a broader distribution of lower-criticality failures was observable in Apollo and space shuttle plots as a direct result of the expansive feed system redundancy present in these systems. Regardless, all vehicles featured roughly the same magnitude of Criticality 1/1R2 failures (maximum: 6-15 occurrences per year on the ground, 2-5 occurrences per year in flight).

3.3 Anomalies by Component Type

3.3.1 Ground Anomalies by Component Type

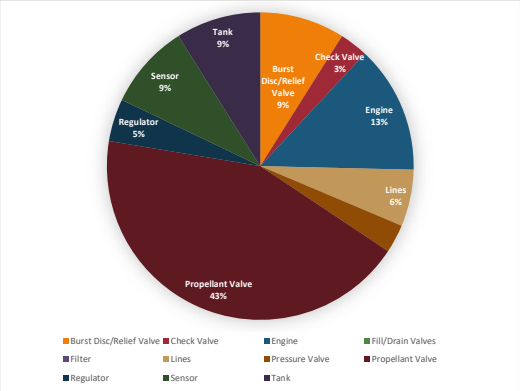

Figure 9. Apollo Propulsion Ground Anomalies by Component

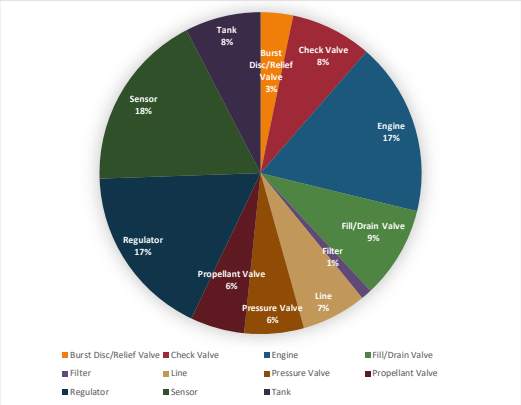

Figure 10. Space Shuttle OMS Propulsion Ground Anomalies by Component

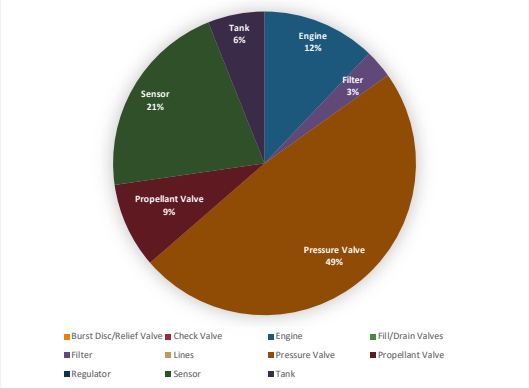

Figure 11. Orion Propulsion Ground Anomalies by Component

3.3.2 Flight Anomalies by Component Type

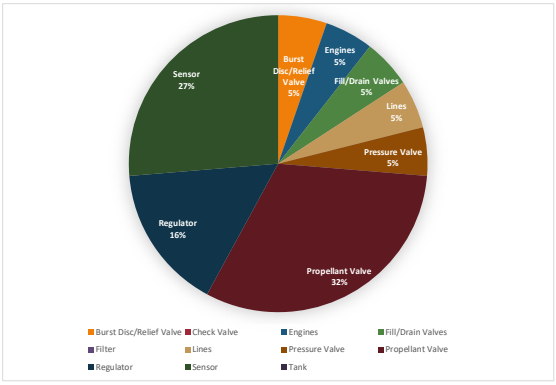

Figure 12. Apollo Propulsion Flight Anomalies by Component

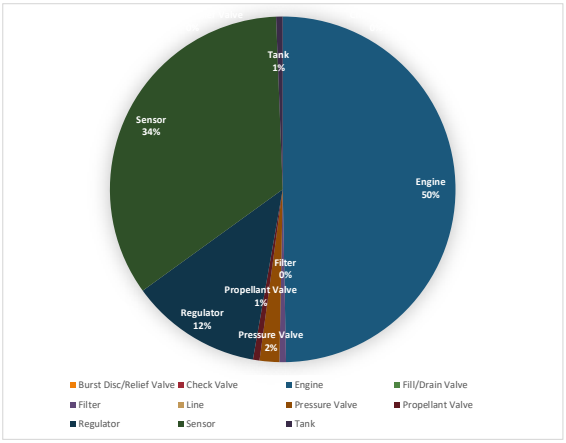

Figure 13. Space Shuttle Propulsion Flight Anomalies by Component

3.3.4 Composition Analysis Summary

Plotting failures by component type was also useful, and allowed the team to shed perspective on the prevalence of certain types of hardware failures. One particularly interesting trend centred around the close relationship between ground and flight distributions on each vehicle. The propagation between ground and flight reinforced the importance of good component design principles, and the potential for recurring issues throughout the project life cycle for a given part.

Taking the data as a whole, valve failures were very common, and sensor failures became more prominent on space shuttle and Orion spacecraft as designers incorporated additional instrumentation. Engine failures were a fairly uniform contributor on the ground, although flight failure density was highly dependent on

a predisposition toward leakage and failed-off conditions.

3.4 Anomalies by Criticality

3.4.1 Ground Anomalies by Criticality

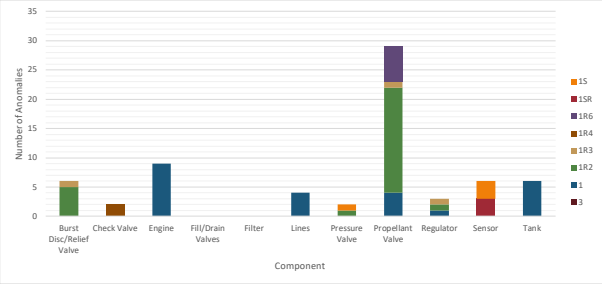

Figure 14. Apollo Number of Ground Anomalies by Component based on Criticality

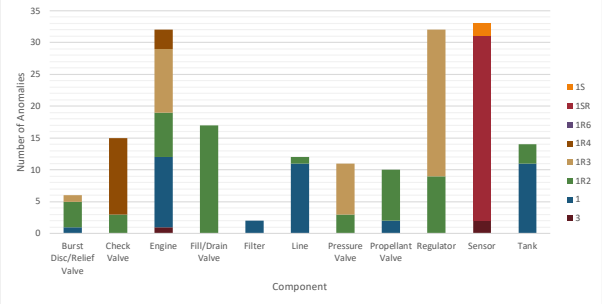

Figure 15. Shuttle OMS Number of Ground Anomalies by Component based on Criticality

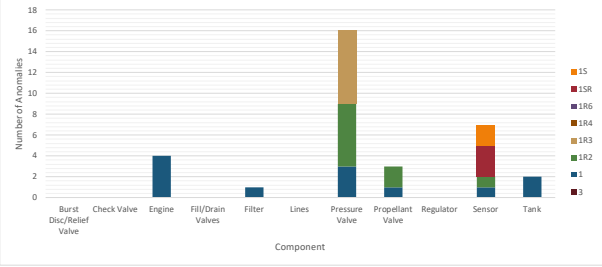

Figure 16. Orion Propulsion Number of Ground Anomalies by Component based on Criticality

3.4.2 Flight Anomalies by Criticality

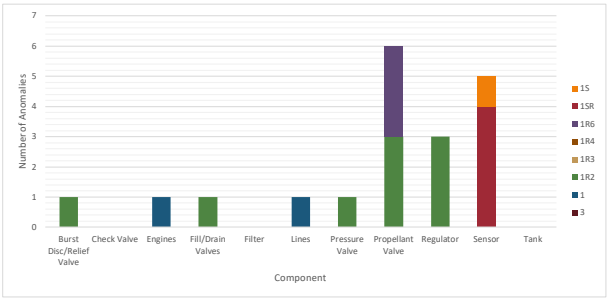

Figure 17. Apollo Number of Flight Anomalies by Component based on Criticality

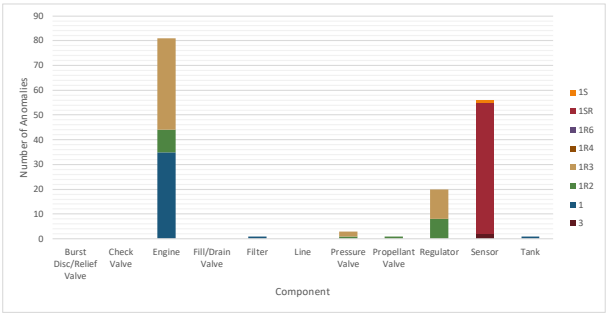

Figure 18. Space Shuttle Number of Flight Anomalies by Component based on Criticality

3.4.3 Criticality Analysis Summary

Comparing flight and ground criticalities per vehicle yielded results that were very similar to the last data set; specifically, ground failures appeared to be precursors for failures in-flight. While the magnitude of each vehicle's contributions remained the same, the criticality of flight failures was somewhat reduced, implying somewhat effective screening methods prior to each mission. Of the many component types, sensor, engine, valve and regulator failures were more likely to propagate to flight.

Most plots indicated the highest-density failures were observed on Criticality 1, 1R2, 1R3 and 1SR components. The prevalence of these issues and the large number of "close calls" reinforced the benefit of maintaining current agency failure tolerance requirements, at a minimum.

4. CONCLUSIONS

A preliminary comparative failure history analysis was developed to support risk-informed decisions for

human-rated missions. Additional research is required to define all corrective actions; however, interim recommendations include additional controls for high-density Criticality 1 anomalies, including additional process inspections, cleanliness verifications, and targeted lessons from prior programs.

As a secondary observation, a standalone review of human spaceflight failure history allowed the team to recognize common failures across multiple programs. Several examples are highlighted below. In the future, additional coordination is needed to establish an effective framework for capturing valuable mitigations from prior programs, to ensure failures are not regularly repeated.

Common Failures across Multiple Programs

- Failed-closed pressurization valves
- Latch valve degaussing
- Loose sensor wires
- Bellows leakage at both welds and convolutes
- Fuel and Oxidizer Reaction Products (FORP)
- Valve and tank gauging failures
- Internal leakage of helium regulators and valves
- External leakage of main engine pneumatic pack
- Burst disc rupture
- Excessive pull-in voltage
- Internal leakage of ball valve shaft seals
- Valve leakage due to pilot seat contamination

From a data integration standpoint, the team would like to reiterate the need to finish reviewing and tabulating space shuttle RCS ground anomalies (all), space shuttle OMS ground anomalies (missing years), qualification anomalies (all) and additional Apollo reports. These missing data sets will continue to be developed and included in future versions of this assessment.

Finally, the S&MA research team would like to offer a few general process observations to improve failure history research, going forward. NASA documentation at the National Archives was extremely difficult to retrieve in a short amount of time, and required personnel and financial resources. To minimize these demands, multiple agencies stands to benefit from retrieving, digitizing and managing these reports in a controlled searchable platform. A shared database would ensure files are subjected to a consistent set of screens for sensitive but unclassified (SBU) and Personal Identification Information (PII), while helping design engineers make critical decisions. As deep-space missions drive higher technical and programmatic risks, a cross-program knowledge-sharing system would pay countless dividends in employee productivity, minimized ground and flight delays, and improved system reliability.

8. ABBREVIATIONS AND ACRONYMS

0FT	Zero-Failure Tolerant
CIL	Critical Items List
DR	Discrepancy Report
DFMR	Design for Minimum Risk
ESA	European Space Agency
FMEA	Failure Modes and Effects Analysis
ISS	International Space Station (ISS)
MER	Mission Evaluation Reports
MPCV	Multi-Program Crew Vehicle
MSERP	MPCV Safety and Mission Assurance Safety and Engineering Review Panel (MSERP)
NASA	National Aeronautics and Space Administration
OMS	Orbital Manoeuvring System
PII	Personal Identification Information
PRA	Probabilistic Risk Analysis
PRACA	Problem Reporting and Corrective Action
RCS	Reaction Control System
SPF	Single Point Failure
SBU	Secure But Unclassified
STS	Space Transportation System

9. REFERENCES

1. Formatted by Wood, B., NASA (1969). Apollo Operations Handbook, Block II Spacecraft, Volume 1, Spacecraft Description, SM2A-03-Block II-(1), SID 66-1508, 15 October 1969, pp 175-162.

2. Curated by Dimukes, Kim, NASA (2002). Shuttle Reference Manual (1988). https://spaceflight.nasa.gov/shuttle/reference/shutref/orbiter/.

3. ESA (2018). Orion Propulsion. https://www.esa.int/Our_Activities/Human_and_Robotic_Exploration/Orion/Propulsion.

4. NASA Engineering and Safety Center (NESC) (2007). Design, Development, Test and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems, RP-06-108, pp 33.

5. Krevor, T., Epstein, G., Benfield, P. & Deckert, G. (2009). Leveraging Reliability in Support of Risk Balancing and Weight Reduction on Orion, AIAA 2009-6725, pp 3.

6. NASA (1968). CSM 101 Criticality I and II Single Point Failure Summaries, SD68-547.

7. NASA (1994). Shuttle OMS RCS FMEA Summary.

8. NASA (2014). Orion Multi-Purpose Crew Vehicle (MPCV) Program Hardware Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) Requirements Document, MPCV-70043, Revision A.