How can we efficiently build a Spacecraft that has Longevity? Experiences from the GSFC perspective to inform Lunar Exploration and Science Orbiter's architecture

National Exploration Science Forum 2023

Charles Baker, LExSO MSE

July 2023

Spacecraft Longevity Introduction

- Spacecraft longevity in practice has been related to: 1) mission class; 2) did we test it long enough and resolve all the anomalies to be beyond the bath tub curve; 3) consumables budgets, and 4) how components are designed and tested.
- Mission class has been perceived as one of the primary ways to drive longevity.
- But higher mission class is a significant cost and mission driver.
  - Parts selection from mil standard parts and parts qualification adds to development time and cost.
  - Largely redundant (often erroneously interpreted as fully redundant) adds to launch mass and increases testing complexity (which may reduce the amount of testing in the nominal configuration).
  - Lower Risk Posture drives significant additional processes and quality assurance analyses.
  - Significantly greater sparing and life testing required
- This discussion focuses on whether this is indeed the best way to achieve longevity efficiently or whether there are more efficient ways to achieve longevity.
- Empirical evidence shows that lower mission classes that implement effective risk reduction and selective redundancy generally results in long life at a lower Spacecraft bus cost.
  - Lower Spacecraft cost generally enables a more capable payload.

Mission Class Definitions from Jesse Leitner

- Class A: Lowest risk posture by design
  - Failure would have extreme consequences to public safety or high priority national science objectives.
  - In some cases, the extreme complexity and magnitude of development will result in a system launching with many low to medium risks based on problems and anomalies that could not be completely resolved under cost and schedule constraints.
  - Examples: HST and JWST
- Class B: Low risk posture by design
  - Represents a high priority National asset whose loss would constitute a high impact to public safety or national science objectives.
  - Examples: GOES-R, TDRS-K/L/M, MAVEN, JPSS, and OSIRIS-REX
- Class C: Moderate risk posture by design
  - Represents an instrument or spacecraft whose loss would result in a loss or delay of some key national science objectives.
  - Examples: LRO, MMS, TESS, and ICON
- Class D: Cost/schedule are equal or greater considerations compared to mission success risks
  - Technical risk is medium by design
  - Many credible mission failure mechanisms may exist. A failure to meet Level 1 requirements prior to minimum lifetime would be treated as a mishap.
  - Examples: LADEE, IRIS, NICER, and DSCOVR

Jesse Leitner's thoughts on Mission Class versus overall Risk Posture

- While the classification communicates a level of risk tolerance for a mission and subsequently expectations for the high-level practices to be employed to maintain that posture, the resulting mission may have lost its connection to the original risk posture intended:
  - Class A mission may fly with dozens of yellow technical risks
  - Class D mission or below may fly with no yellow or red risks
- It is not unlikely that a well-managed and engineered Class D mission or below would fly with lower overall risk than a complex, one-of-a-kind Class A mission.
  - The extra efforts in engineering thought and the emphasis on risk in driving development activities, combined with reduced complexity, can work together to establish a very low risk posture
- Class A [and B] missions tend to rely more on broad, sweeping processes, that can be very costly, that have their own associated risks that tend to be ignored

Jesse Leitner's thoughts on Mission Assurance

- Approach is almost entirely based on piece-parts
- Largely, classification is dialed up or down based on classical "levels of assurance"
  - Number of specifications
  - Stringency of specifications
  - Level of oversight (insight)
  - Amount of screening performed
  - Amount of testing above operational levels performed
- There is no correlation between levels of assurance and actual performance or reliability
- Most importantly, there is no means for products that have little to no government piece-part level controls, but that perform reliably and consistently to achieve higher classification
  - This applies to most ubiquitously-used standard components such as star trackers, reaction wheel assemblies, IMUs, etc.
- This will apply to a growing number of full spacecraft
  - Time will come soon that spacecraft that have consistent repeat performance will be classified lower than spacecraft that are either one-of-a-kind or limited history but with extensive piece-part controls

Jesse Leitner's thoughts on Reliability

- ***The reliability of a system is its ability to perform the necessary functions within expected life cycle conditions for a required period***
- Typical NASA systems are "designed" to last 3-5 years but end up lasting well over 10 years.
  - *Other than by carefully resourcing limited-life items and expendables, improperly derating electronic components, or carefully planning out accumulated radiation effects, there is no practical way to design a system to last only 3-5 years.*
  - *Systems typically fail due to*
    - A design problem not encountered or resolved in testing (e.g, a corner case or problem with undetermined/uncorrected root cause)
    - A radiation hit or other environmental effect (e.g., micrometeoroid)
    - Wear out or depletion (fuel, battery, etc)
    - A latent defect in workmanship that is exacerbated by an otherwise mild environmental condition
    - Less common: latent part/component defect. Recent serious latent defect examples involved low volume parts and old specs that were overly trusted

Jesse Leitner's thoughts on Robust* Design

- Assessment of tall poles, critical items, and credible faults
- Design for manufacturability
  - *Not consistently employed*
- Fault and radiation tolerant design
  - *(selective) redundancy*
  - *Fault-tolerant design*
  - *Design for minimum risk*
  - *Ability to reset*
  - *Design for graceful degradation*

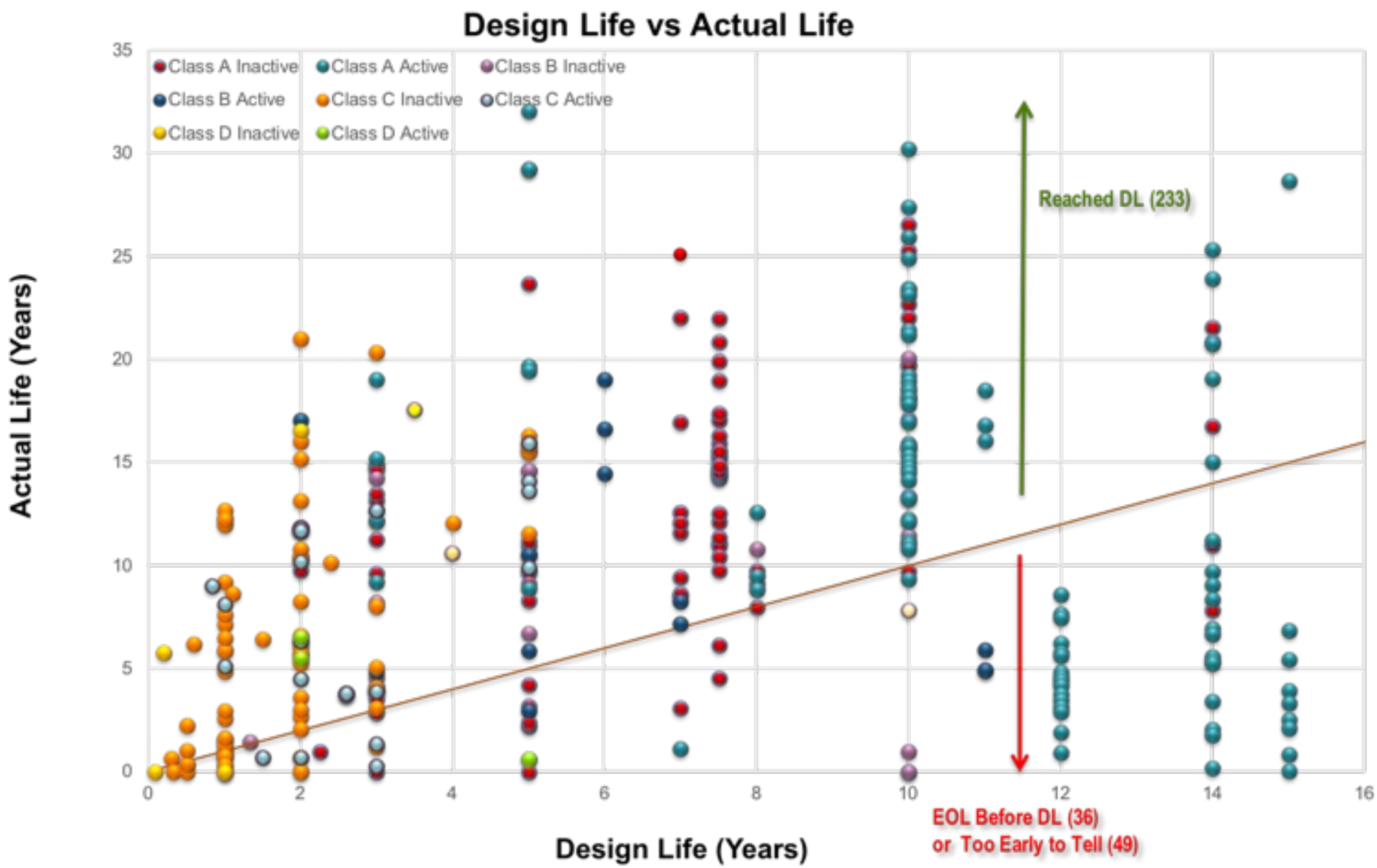
*performance achieved in the presence of disturbances and uncertainties

So what does this mean?

- Challenging missions with high complexity and low TRL have a higher failure rate regardless of Mission Class or Mission Assurance Activities.
- Keeping mission targeted, low on complexity, minimizing low TRL systems, that focus on risk management that offers the best risk reduction can be very reliable independent of mission class.
- This doesn't mean that the mission life doesn't benefit from:
  - Selective redundancy and oversized power systems.
  - Life testing of mechanisms and other custom components.
  - Comprehensive Orbiter level testing.
- But this can always be done independent of mission class.

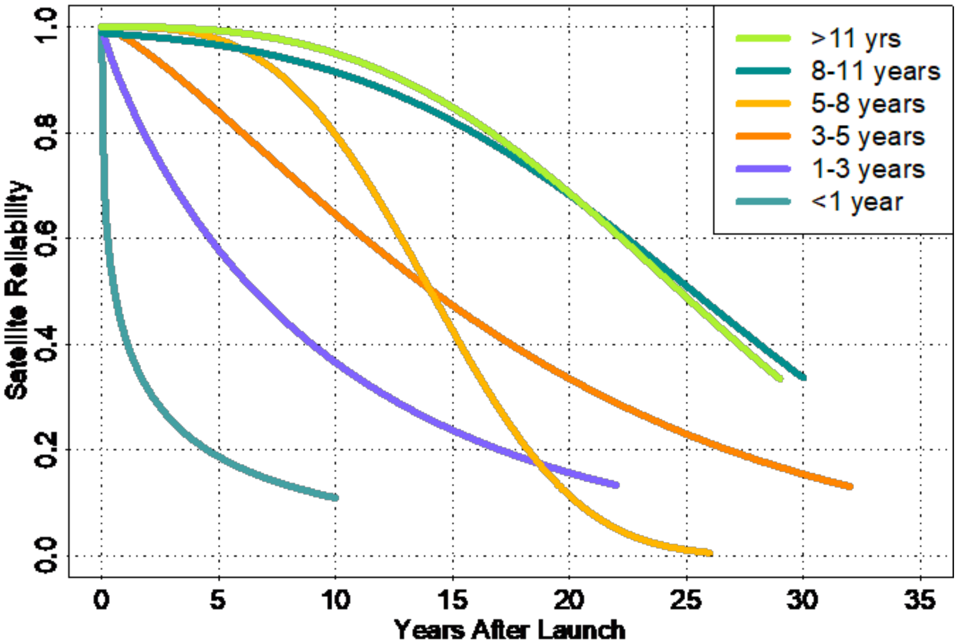
Results Based on Mission Class From: AEROSPACE REPORT NO. TOR-2019-02620

2019 Satellite Lifetime Study



Reliability Curve and Conclusions From: AEROSPACE REPORT NO. TOR-2019-02620

2019 Satellite Lifetime Study



- Satellite design life for both U.S. military and civil and commercial satellites increased from 1980 to 2018.
- There is clear differentiation in design life based on mission class (U.S. military and civil) or cost tier (commercial).
- 87% of U.S. military and civil and 75% of commercial satellites have met or exceeded design life to-date.
- Many satellites have launched too recently to tell if they will meet intended design life.
- Mean actual life and predicted success rate are higher across the board for U.S. military and civil satellites than for commercial satellites.
- Reliability curves show a more gradual drop-off for longer design life satellites.
- Commercial reliability curves show a consistently steeper drop-off than U.S. military and civil reliability curves.

Single String compare to Block Redundancy in GSFC managed SC (looking at failures from 2000-2015) shows reliability is higher than Aerospace study average

Prob of success for GSFC single string Using provided failure and hour estimate	Years	Probability of success for a GSFC block redundant design	Active	Standby
0.99	1	1.00	0.99992664	0.99996321
0.98	2	1.00	0.99970905	0.99985369
0.97	3	1.00	0.99935096	0.99967269
0.97	4	1.00	0.99885598	0.99942143
0.96	5	1.00	0.99822768	0.99910114
0.95	6	1.00	0.99746955	0.99871301
0.94	7	1.00	0.996585	0.99825823
0.93	8	1.00	0.99557739	0.99773798
0.93	9	0.99	0.99445	0.9971534
0.92	10	0.99	0.99320604	0.99650564
0.91	11	0.99	0.99184866	0.99579582
0.90	12	0.99	0.99038096	0.99502505
0.89	13	0.99	0.98880595	0.99419443
0.89	14	0.99	0.98712661	0.99330504
0.88	**15**	**0.99**	**0.98534584**	**0.99235795**

What components drive mission lifetime?

Subsystem	Components	Why it is limited life	Mission Impacted (requiring operational management)
ACS	Mini Inertial Measurement Units	Angular Rate sensors have a limited life	STEREO, TIMED, LRO, DSCOVR, MAVEN etc.
ACS	RWA	Moving Mechanisms have limited life, these missions benefited from redundancy	GPM, SWIFT, FUSE, Kepler
Mechanism	SADAs	SADAs tend to run hot and have higher lubricant boil off	TRMM, FERMI, LRO
EPS	Battery Capacity	Battery capacity fades due to cycles and deep discharges	LRO, Terra, AIM, SWIFT, IRIS, MAVEN
EPS	Solar Array Strings	Strings on the Solar Array fail due to MMOD & workmanship	Mission tend to oversize
Telecom	TWTA and Modular	Anode Voltage needs to be increased with time and can suddenly fail. New modulators are tricky	JPSS 2, TeSat
Telecom	Transponder failure	New transponders can have anomalies that prevent commanding	JPSS, AIM

Selective redundancy can alleviate the Risk

Subsystem	Components	Can you easily fly a spare?
ACS	Inertial Measurement Units	Yes or use an SSIRU that is internally redundant, consider whether gyro-less mode can meet pointing requirements
ACS	Star Trackers	Yes, alleviates reset problems if you have two, Galileo have been the easiest to implement. Having two is recommended (viewing different areas of the sky), but don't necessarily need a spare.
ACS	CSS	Yes, fade occurs
ACS	RWA	Yes
EPS	Battery Capacity	Oversized batteries can lose cells and sections
EPS	Solar Array Strings	Oversized Solar Arrays can lose strings
Telecom	Ka Modulator/EPC/TWTA	Yes
Telecom	X-Band Transponder	Yes, need to understand likelihood of failure
Propulsion	Thrusters	Yes
Timing	Oscillator	Yes

Conclusions

- Mission Class can be a significant cost driver for Class A and B missions and on cost constrained missions can reduce the payload allocation.
- Demonstrated Lifetime of class C missions tends to well exceed mission lifetime requirements.
- GSFC missions tend to have reliability higher than all government led missions for single string missions.
- Smart selective redundancy mitigates some of the lower mission class risk.