National Aeronautics and Space Administration

Phasing COTS parts into low-risk-tolerant missions

Jesse Leitner, Chief SMA Engineer, NASA GSFC

Jesse “dot” “Leitner” at “nasa.gov”

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

Outline

- Electrical, electronic, electromechanical, and electro-optical (EEEE) parts assurance history
- NASA Electronic Parts and Packaging (NEPP) Program trends
- Commercial Off The Shelf (COTS) vs MIL-SPEC dilemma
- Current approach of phasing in COTS
- Parts Evaluation & Acceptance Laboratory – building (reconstructing) an essential Agency capability
- Summary

Background

- Updates in Agency guidance and requirements, combined with the results of NESC COTS parts assessments (Phases I & II) as well as mission experience at GSFC and in the wider community, have fueled an expansion in the use of COTS parts within NASA Class D and sub-Class-D robotic missions.
- Drastic changes in the balance between government and commercial use of electronics, combined with advances in technology and manufacturing capability, will soon necessitate an inevitable transition to COTS being the dominant class of parts to be used in low risk-tolerance applications and missions.
- Analyses and measures used as a basis to justify COTS in applications with a medium to high tolerance for risk may not be sufficient to provide confidence for use in applications with a low tolerance for risk.
- Given that application of MIL-SPEC processes *exactly as defined* is not effective for qualifying and accepting COTS parts, a different approach is needed to enable the use of COTS parts in Class A and B robotic, as well as human space flight missions.

What is the fundamental message, and what isn't it?

- When developing a mission, we need to choose the best parts for the job – they may be MIL-SPEC, they may be COTS, they may be custom
  - When properly selected, MIL-SPEC and COTS parts can have a basis for reliability
  - Sometimes there are no parts available or even existing to do the job for the mission that have a basis for reliability
    - In that case, design practices and system fault tolerance must account for the shortcomings
- There are many limitations for MIL-SPEC parts and those limitations are growing as technology and manufacturing evolve
- **COTS (with no caveats) covers an infinite trade space and critical thinking, sound judgment, and understanding of the concepts of quality and reliability are essential to find the right subset of the trade space**
- This is not a message to blindly use COTS parts
- This is not a message that COTS parts are always the best solution
  - The best solution comes out of a part-by-part determination that considers performance, reliability, availability, usage constraints, and cost

Addressing radiation is no different or even more expansive when making broader use of COTS parts

The world has changed

- The MIL-SPEC system was devised when there was limited manufacturing capability for electronics – there was little assurance that parts would work reliably
- Parts were designed prescriptively and quality metrics were established relative to the designs
- Since there were no established reliability or statistical process controls, we had to use extensive strict quality requirements to make sure that current products had minimal variability relative to previous products
- MIL-SPEC levels that involved progressively more testing, higher sample sizes, and more stressing testing were introduced
- Since then commercial manufacturing capability with statistical process controls and high-volume production dwarfed and far surpassed the MIL-SPEC system.
  - With high-volume and statistical process controls, reliability now can be established directly
  - NASA and DoD did not recognize the advanced capability of the commercial sector and demanded additional screens to be applied to parts to try to make them mimic MIL-SPEC parts and hopefully screen in quality and reliability
    - Documentation stated (with limited justification in specific contexts) that higher levels equated to higher reliability, but actually quality was conflated with reliability in general
- As technology evolved, the MIL-SPEC parts could not keep up
  - Attempts to apply MIL-SPECs to noncompliant parts became more futile as part technologies have evolved

Transition from compliance to knowledge

- At NASA's inception, there was no commercial electronics infrastructure to develop or assure reliable parts
- Challenges in Skylab drove an approach to standardize parts with extensive controls
- This standardization largely froze the technology, which was necessary at the time, and effective for a long time.
- These building blocks formed a religion that could be carried through a compliance approach
- ”Grading” was brought in, which gave some flexibility, but largely became arbitrary and minimally exploited, out of fear and misunderstanding
- Attempts to standardize new parts coming out simply freeze the technology and stifle innovation, although such an approach has a limited place for cases where we simply want to build multiple copies of the same item (years ago, we combed ebay to buy 086 processors to support the Shuttle)
- Compliance to an old arbitrary system no longer makes sense
- Parts are often key elements of technology advancement and innovation
- Automotive electronics quickly took over the market, but instead of being concerned only with safety and reliability (as in government space), efficiency, cost-effectiveness and technology were also key drivers
- While the current compliance exercise should be dropped, the need for knowledgeable people and a knowledge base is essential

NESC COTS study

- Originally formed to support the Commercial Crew Program and its heavy use of COTS
- Turned to focus on the overall problem of selection, evaluation, screening, qualification, and usage in robotic and human-rated space systems
- Phase 1 introduced several new ways of looking at COTS and key terminologies to help the agency understand ways to use COTS successfully
- Phase 2 has extensively dispelled myths and established a framework for new approaches to use COTS parts reliably
  - Reliable usage centers around the concept introduced in the Phase 1 study, the Industry Leading Parts Manufacturer (ILPM), and the specific selection of Established parts

This presentation was largely motivated and informed by the NESC COTS study, but it goes well beyond the findings and message of the study

ILPM

ILPM: a COTS manufacturer that produces high quality and reliability parts that do not require additional screening and lot conformance testing, common in today's requirements for using "non-standard" parts in space

- Implements a "Zero Defects" program, as described in AEC-Q004 or a similar source.
- Designs parts for manufacturability, testability, operating life and fielded reliability.
- Manufactures parts on automated, high-volume production lines with minimal human touch labor.
- The manufacturer understands and documents all manufacturing and testing processes and the impacts and sensitivities of each process step on product characteristics and quality.
- The manufacturer's end-product testing includes 100% electrical verification of datasheet parameters.
- The manufacturer implements rules for removing outlier parts and removing abnormal lots; these rules may apply either in-process or with finished parts.
- The manufacturer implements a robust change system that assures all major changes are properly qualified and that customers are notified of major changes
- The manufacturer implements a robust Quality Management System acceptable for spaceflight.

Each organization should maintain its own list of ILPMs

Established Part

- Produced using processes that have been stable for at least one year so there are enough data to verify the part's reliability;
- Produced in high volume. High volume is defined as a series of parts sharing the same datasheet having a combined sales volume over one million parts during the part's lifetime;
- 100% electrically tested per datasheet specifications, minimally at typical operating conditions and is in production prior to shipping to customers. Additionally, the manufacturer must have completed multi-lot characterization over all operating conditions cited in the part's datasheet, prior to mass production release. Thus, production test limits are set for typical test conditions sufficient to guarantee that the parts will meet all parameters' performance specifications on the datasheet;
- Produced on fully automated production lines utilizing statistical process controls (SPC), and undergoes in-process testing, including wafer probing for microcircuits and semiconductors, and other means as appropriate for other products, e.g., passive parts. These controls and tests are intended to detect out of control processes and eliminate defective parts at various stages of production.

COTS parts

- Parts for which the part manufacturer solely establishes and controls the specifications for performance, configuration and reliability, including design, materials, processes, and testing without additional requirements imposed by users and external organizations. It is typically available for sale through commercial distributors to the public with little or no lead time.
- Manufacturers design for reliability and employ continuous improvement processes and advanced manufacturing techniques
- Manufacturers perform their own qualification tests based on how the parts are manufactured and how they are intended to be used
- Reliability is established by volume
  - Reliability is essential to stay in business, so it is self-controlled and *stable*
  - Low volume parts have questionable and uncertain reliability, and thus must be assured by additional means
- Vendor screening and testing processes assure uniformity and that each part performs as intended, while avoiding damaging or degrading parts through additional handling, use of unknown test equipment, and overtesting
  - Parts not going through vendor screening and testing processes have uncertain linkage back to the historical usage needed to form a basis for reliability
- **High-volume parts from reputable vendors that go through 100% vendor screening covering all datasheet parameters have the best opportunity for reliable usage, when used well within rated limits (including radiation*) because testing is most closely linked to actual manufacture and usage.**

*Radiation is a system-level phenomenon that is not sufficiently addressed at the piece-part level

MIL-SPEC parts

- Originated in DoD out of the need for tight uniformity and interchangeability of parts across the world
- Quality specifications were defined to cover the most extreme range of conditions
- The government controls the drawings, requirements, and specifications of such parts.
- Reliability is often declared based on accelerated testing combined with many stringent requirements and other forms of extreme tests
- Some specs/requirements included based on past lessons learned or past indicators of infant mortality
- Originally, MIL-SPECs were the only reasonable approach to procure parts that were necessary to function reliably.
- Thus MIL-SPECs were the best existing source to obtain parts to use in space systems
  - The government monitored parts manufacturing and testing
  - Failure rates from highly-accelerated tests were used to predict reliability and verify that issues were not appearing in manufacturing.
- **MIL-SPEC parts arbitrarily link to reliability because they are assured by quality specifications that may not represent actual usage or manufacture, and may overtest parts by using standard screening practices. Since reliability is a by-product, it is far from guaranteed***

*many MIL-SPEC parts go through extended reliability testing but the testing is not relevant to the actual usage and it does not address the types of failures typically encountered with MIL-SPEC parts

NASA-screened COTS parts

- COTS parts that are screened and/or qualified (level 1 or 2) using MIL-HDBKs via a document such as EEE-INST-002.
- Reliability is equivalent to that of COTS parts except that MIL-SPEC tests are applied to the parts, resulting in extra handling and frequent overtesting relative to the part application and often to its datasheet. Thus this option provides the greatest uncertainty for reliability, especially if the COTS parts are low volume or low quality to start with.

What are the key drivers for using COTS?
(Not necessarily all at once)

- The need to employ technologies from the past 15 years
- The need for parts that are available
- The need for parts that are affordable
- The need for parts that are the most reliable
- The need for parts that meet mission requirements

Why have COTS been perpetually deemed "unreliable" or "low-grade"

- The COTS definition is infinite
  - This is exacerbated by an infinite number of definitions
    - COTS is often a "label" used at a manufacturer with a local definition
  - "Reliability" defined by the worst elements in the broad category
- MIL-HDBK-217
  - Arbitrary "failure rates" (PEMs 60-600x MIL-SPEC without any current foundation)
  - Approach (along with similar handbooks) has become engrained across the traditional aerospace contractor community
  - Standard "probability of success" (Ps) requirements have demanded its use
- Issues with the plastic used in PEMs in the 70's and 80's.
  - Took time to work through challenges to get the materials and manufacturing right
  - e.g. moisture in the plastics were interacting with aluminum, resulting in corrosion
  - Problem was solved in the late 80's and PEMs ultimately surpassed hermetic ceramics in part-level reliability (failure rates)
- Myths about COTS vs radiation

Why have COTS been perpetually deemed "unreliable" or "low-grade" (cont'd)

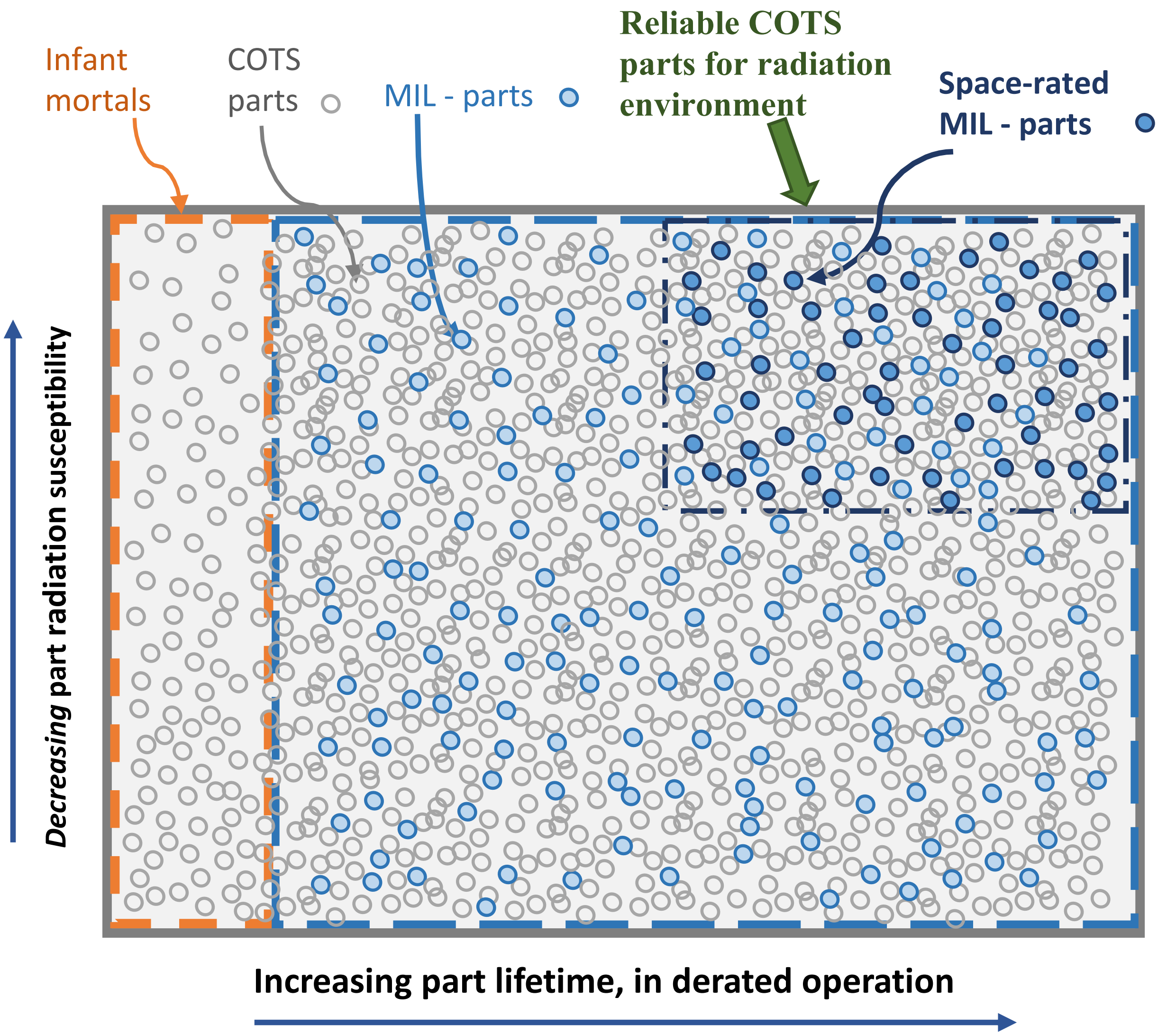
- There was a semi-conscious decision dating back to the 70's that all electronic parts flying in space must be rad-hard (by some definition),
  - radiation problem is best solved at the part level,
  - experiences in developing Skylab that concluded that given the immature manufacturing processes at the time it was much better to maximize part assurance practices at the time of manufacture then to add processes later or catch problems in testing.
- Class S part was born
  - Over time, "Class S" became conflated with other MIL-SPEC classifications and radiation hardness was subsequently conflated into the mix,
    - Trapped the community into the mantra that only "Class S" parts can be flown in space; anything else would be a disaster.
    - Had the unfortunate additional consequence that if a failure of a "Class S" part occurred, it was clear that all had been done, and there was no need to take things any farther to challenge whether part of the "Class S" mantra had contributed to the problem.
  - A "Class S vs COTS" notion would perpetuate. In parallel, commercial manufacturing processes were improving and far surpassing this MIL-STD-based control system, which was frozen in time at its inception and unaffected by commercial markets or improving technologies.

Reliable COTS

- Verify part meets Mission Environment, Application, and Lifetime requirements
  - Radiation verified at the part level (RHA in the datasheet is one approach)*, circuit level (circuit design, fault tolerance, circuit protections), or system level (shielding, fault tolerance)
- Use parts from an ILPM
- Use Established parts
- Recognize contexts for risk
- Respect the datasheet (processing, testing, and usage)
  - Do not screen parts outside of datasheet levels
- Do not repeat manufacturer tests
- Low field failure rate or DPPM
- Relationship with manufacturer for transparency and trust

*radiation hardness or tolerance of individual parts is not sufficient for performance in severe radiation environments, as evident from SMAP

The Infinite "Space" View of COTS



Context for Risk in Parts

COTS

- Parts with special features that are difficult to manufacture consistently (never available on MIL-SPEC)
  - e.g., extra-low ESR and ESL ceramic capacitors
- Parts used in brutal operating regimes
  - High-voltage (particularly > 3 kV)
  - Cryo
- Low volume and hand-produced parts
  - Lack a basis for reliability and often do not have optimized manufacturing processes
- Parts used in extremely sensitive (poor) designs (based on variability of parameters not in part spec)
- Parts used in applications in which the environment is unknown
- Parts from unknown or poor-performing vendors (no recent examples)
- No “hi-rel” or automotive parts available

MIL-SPEC

- **All risk-contexts for COTS, plus:**
- Low-volume parts
- Lead time and costs can reduce system-testing resources
- Designed for old manufacturing processes and broad environments
- When used broadly, they can bring false hope and extensive problems may ensue
- Processes will miss new manufacturing flaws
- Performance and reliability not driven by the need to stay in business
- Performance limitations may lead to weak designs

NASA-screened COTS

- **All risk-contexts for COTS, plus:**
- Parts are often overtested since MIL-SPEC testing regimes are not related to actual usage and parts are often not designed or optimized for such regimes
- False hope that screening is relevant to operation
- False hope that screening, testing, and qualification increase reliability or quality
- The prospect for burying a problem or reduced lifetime into a part by the “overtest by design”.

Note that the contexts for risk in COTS parts all arise from mission performance requirements that would be present no matter which parts approach is used, so they apply to all cases.

Benefits vs Detriments of increasing EEE-INST-002 levels

Benefits of increasing levels	Detriments of increasing levels
More testing of parts	Reliability of non-MIL-SPEC parts is reduced as levels increase
Better ability of some parts to withstand overtesting and misapplication/misuse	More handling of all parts increases risk that a self-induced problem will occur
Many people feel better and more comfortable	Increasingly more difficult to obtain – exacerbates the supply chain problem
	Prevents the use of recent technology
	Excessive cost
	Low volume for most with no basis in reliability

Brief history of parts assurance

- Prior to the initiation of full-cost accounting (FCA), NASA had in-house Center capabilities to evaluate, test, and characterize EEEE parts, which were used to develop Preferred Parts Lists (PPLs) and ultimately the NASA Parts Selection List (NPSL). Many such capabilities still exist in a limited fashion, but not to the breadth and depth required to cover the whole spectrum of COTS parts that are considered for space applications.
- These capabilities served not only to establish a basis for characterizing suitability of parts for the full range of applications, but also to ensure that there was a cadre of individuals with detailed understanding of specific parts to assure the proper usage in specific applications.
- On the advent of FCA, the resources were no longer available for such upfront capability, and acceptance of parts was largely deferred to the in-line activities of projects, forcing an approach of using predetermined broad measures, such as the use of MIL-SPEC parts or other parts that had already been placed on to the NPSL (which was frozen in time).
- As time progressed, new parts were proposed for use, and without the in-house capability, documents such as EEE-INST-002 were constructed to provide an algorithm or cookbook to apply in-line to accept parts.
- Since the MIL-SPECs had become the tried-and-true means of assuring parts, the EEE-INST-002 document became the means of applying the MIL-SPECs to unfamiliar parts to “upscreen” them to build confidence in them in a similar fashion to MIL-SPECs.

NEPP Program Budget History Snapshot

Indicative of institutional budget decline affecting crosscutting in-house technical capabilities

FY19 Budget: $6.875M

FY20 Budget: $6.797M

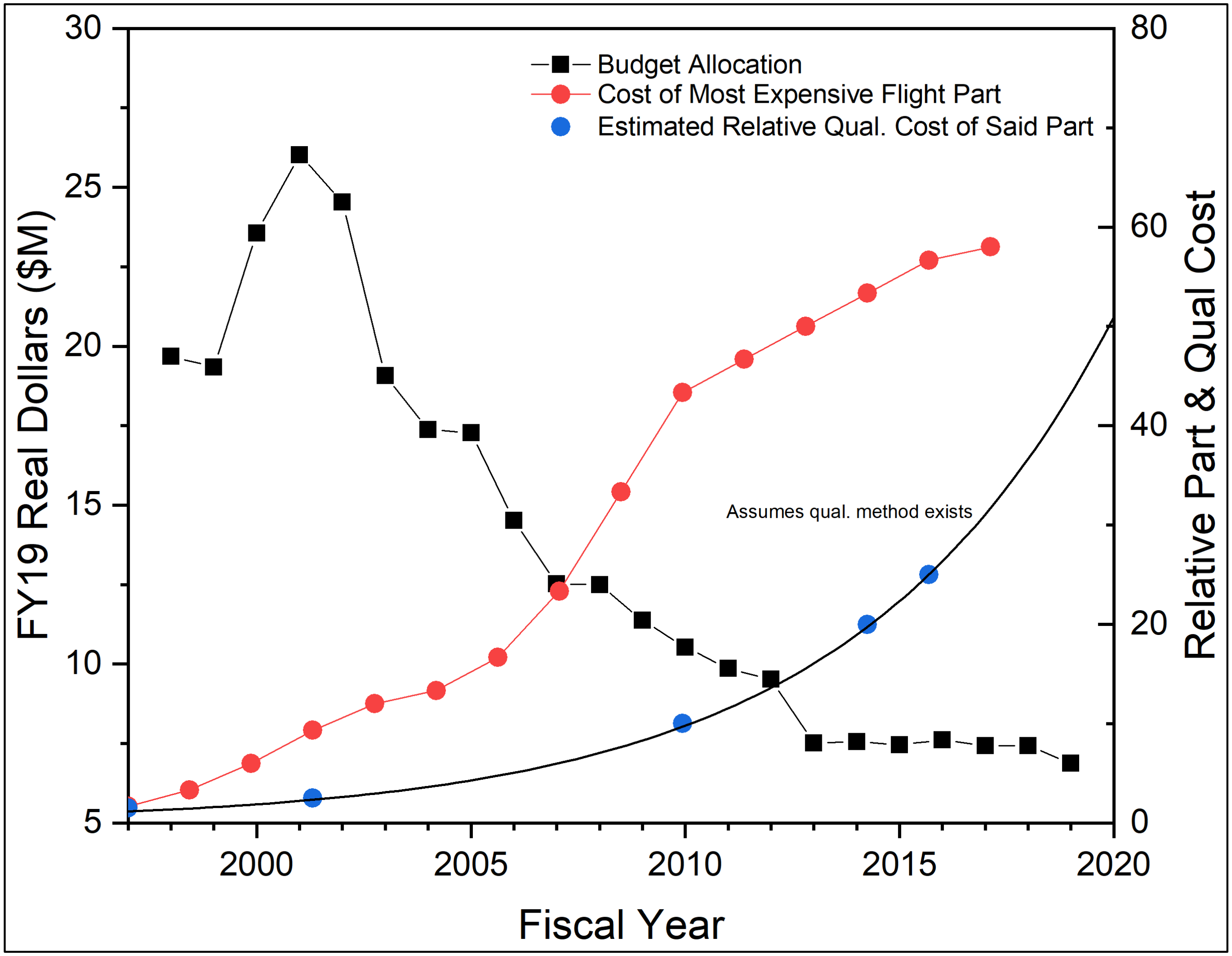
FY21 Budget: $6.673M

FY22 Budget: $6.460M

FY19 – FY22 Δ: -6% / -$415k

Responsibilities & much of the scope have remained constant or grown

Actual needs (proposal based) are >$15M/yr for just the NEPP Program, let alone required agency capabilities



Flight programs / projects have a fixed budget – spending more on parts and less on support

Current Conflicts

- MIL-SPECs, by definition, fundamentally limit technology
  - The broad environmental ranges required and the ability to tolerate many forms of overtest (inherently a derating), drive firm “catalog limits”, which have been in place since inception
  - There are not and will not be well-defined “parts categories” to cover many new classes of electronics technology
- The use of MIL-SPECs to accept and qualify COTS parts conflicts with many of the premises of COTS parts
  - MIL-SPECs involve many test levels that are not based on the actual manufacturing processes or application use of the parts
  - COTS parts are optimized to levels laid out in their data sheets, which would very often be different from MIL-SPEC testing levels (neither necessary or sufficient for properly characterizing the parts for acceptance)
    - MIL-SPEC testing levels can overtest COTS parts, resulting in misleading data and/or reduced reliability and damage to parts

Soon there will be no choice

- Instruments are appearing for high end missions that cannot be manufactured with MIL-SPEC parts or parts that can be effectively screened into compliance using EEE-INST-002
  - It is a virtual certainty this will be the case for the next major flagship space telescope
- Fully COTS spacecraft are soon to be ubiquitous and over time, some will stand out as long-term reliable
  - As long as we continue to equate EEE-INST-002 screening and qualification with reliability, we will continue to misrepresent reliable systems based on COTS as “unreliable”.
  - Such spacecraft will always be frowned upon for usage within NASA
- Availability of MIL-SPEC parts, especially level 1 and many types of space-grade, is becoming a growing challenge, in addition to the growing excessive costs.

Can we slow down the use of COTS?

- The use of COTS is already here, no matter what requirements we impose
  - The only question is whether we want to put a spacecraft on-orbit or not
- COTS parts are not brought forward into our projects because someone wants to save a few dollars or a few weeks or eke a little bit of extra unnecessary performance.
- COTS parts are needed in order to fly mature technologies from the last 25 years
- COTS parts are needed to make systems more reliable
- COTS parts are needed because they are available
- COTS parts are needed because they do not involve excessive costs for non-value-added activities

The use vs non-use of COTS in our systems is a simple prohibition question. There is no way to stop them – you simply need to place the right boundaries to properly use them without damaging them or inflating costs unnecessarily. The tighter boundary you place on them, the more likely you will encourage poor choices and bad practices

Some recent history of COTS EEEE parts in space

- 2004: Swift mission flies 40% COTS EEEE parts (with level 3 upscreening)
- 2013-2017: Multiple Spacecube variants with up to 99% COTS EEEE parts (no upscreening)
- Numerous Ames missions, 100% COTS EEEE parts (no upscreening)
- Ingenuity: 99% COTS EEEE parts with focused screening
- SpaceX: Mostly COTS EEEE parts
- SSTL: Mostly COTS EEEE parts(several decades)
- AFRL's Ascent: 100% COTS EEEE parts (GEO)
- Newspace: almost 100% COTS EEEE parts and components

SpaceCube Time-on-orbit

As of Oct 2021 (STP-H6 was turned off Dec 9, 2021 to make room for the next instrument)

Project	Version	Part Req	BOM Count	Operation Months	Xilinx Quantity	COTS %	COTS Months
RNS	v1.0	2+	3700	0.0833333	4	1%	3.08333
MISSE-7	v1.0	N/A	3100	90	4	2%	5580
SMART	v1.5	N/A	1000	0.0333333	1	95%	31.6667
STP-H4 CIB	v1.0	N/A	1500	30	2	1%	450
STP-H4 ISE2.0	v2.0-EM	N/A	1250	30	3	98%	36750
STP-H5 CIB	v1.0	N/A	1500	46.933333	2	1%	704
STP-H5 ISEM	v2.0 Mini	N/A	1000	46.933333	1	26%	12202.7
STP-H5 Raven	v2.0-EM	N/A	1500	46.933333	3	99%	69696
RRM3	v2.0	N/A	1429	36.666667	2	65%	34057.8
STP-H6 CIB	v1.0	N/A	1500	31.833333	2	1%	477.5
STP-H6 GPS	v2.0	N/A	1157	31.833333	2	65%	23940.3
Restore-L Lidar	v2.0	3	2000		2	0%	N/A
STPSat6	v2.0 Mini	N/A	1500		1	98%	N/A

Totals	Units Flown	11
	Commercial FPGAs	26
	Commercial FPGA Device-Years	83
	Part Years	57213
	COTS Parts Years	15324

Also to note: We flew many COTS components on some of these projects:

- ISE2.0, SMART, and ISEM all flew COTS cameras that were ruggedized. SMART flew COTS SATA drives.
- Raven flew a $5 USB interface card to an IR sensor
- STP-H5 and -H6 have CHREC Space Processors (CSPs) that were 95% COTS components. See references for more info on CSP results (no failures to date)
- RRM3 suffered a failure (outside of SpaceCube) that may have involved a specific COTS part, but the part was used in a stressing condition that any part would eventually fail.
- NavCube Commercial vendor populated PWBs

About MIL-SPEC "upscreening" of COTS parts – what did Swift tell us?

- Why would it ever make sense to apply a 30-50-year-old test to a recently designed and manufactured component?
- Can you make a poorly-selected part high quality or high reliability by applying tests to it?
- Why did we not learn this lesson from Swift (2004)? Can we learn it today, 18 years later?
  - "SWIFT BAT parts engineering successfully executed a parts control and test program that assured that all parts met or exceeded Grade 3 [sic] program requirements, including radiation tolerance. There were a few scattered failures during parts testing, but the subsequent failure analyses revealed that the failures were due to mishandling or improper testing at the board or box level."
  - But yet, "Design engineers elected to select plastic parts, which allowed the use of state-of-the-art devices that provided the advantages of lower power, volume, and weight. However, commercial-grade parts are designed for a very different set of operating conditions than those found in a space application. A full and thorough evaluation is needed for any part type proposed for space flight use like the ones used on the SWIFT BAT project." ---- is this really the lesson we should have learned?

Broad sweeping statements are used even when context is available

Phasing COTS Into Low Risk-Tolerant Missions

- Agency guidance and requirements have been formalizing COTS as the baseline approach, at least from a requirements and expectations standpoint, for Class D and below robotic missions.
- The current NESC studies on the use of COTS have dispelled many misconceptions and outdated assertions about COTS, in addition to providing recommendations for reliable use of COTS with proper understanding and risk context.
- GSFC has taken the results of the NESC study and formulated recommendations for reliable use of COTS parts, emphasizing them in Class D, but also referencing use concepts for missions with less tolerance for risk.
- It is inevitable that at some point the parts selected for Class A and B missions will become dominated by COTS parts that cannot effectively be screened or qualified by MIL-SPEC processes.

A new approach is needed that is centered upon developing means or conditions of acceptance of COTS parts that is driven by data and contexts for risk, rather than a cookbook

Post-NESC COTS report parts assurance

- Nearly two decades after the development of EEE-INST-002, with minimal updates since, a new approach for parts assurance is needed
- The primary outdated element of 002 is the handling of COTS EEEE parts
  - Manufacturing capabilities have changed (and improved) drastically since the practices of EEE-INST-002 were initiated
  - The differences in the screening processes vs the design and manufacture of the parts have become drastic in many cases
- The NESC COTS study has revealed many avenues for reliable use of COTS parts without relying on such screening methodologies
- Some strategic work is needed to fully institutionalize the broad use of COTS across all mission classes, but the tools are available to pilot a new approach, while a capability is developed in parallel
  - The need for a wider door for COTS entry is here today, but we'll need to step through it carefully and gradually

Transition to “three-option” parts assurance

Assurance Level	PEAL option	MIL-SPEC option	COTS option
1	VHCAI or VHCWP1	Class S, V, Y monolithic microcircuits Class K hybrid microcircuits JANS discrete semiconductors FRL T, S, R capacitors and resistors or M123 FRL C and D tantalum capacitors	ILPM & relationship with mfr & Established Part & High Volume & 100% mfr electrically tested & Statistical process control & zero-defects policy
2	HCAI or HCWP2	Class B or Q monolithic microcircuits Class H hybrid microcircuits JANTXV discrete semiconductors FRL P capacitors and resistors FRL B tantalum capacitors	ILPM or AEC qualified under IATF 16949 & 100k or more in production & Minimum 1 year in production & AQL of 0.4 or better
3	MCAI or MCWP3	Class M, N, T, or /883 monolithic microcircuits Class G, D, or E hybrid microcircuits JANTX discrete semiconductors FRL B capacitors and resistors	Automotive or hi-rel part from reputable (proven flight history) mfr or high-volume part, mfr relationship, low field failure rate
4	N/A	N/A	no restrictions

What should be done about radiation?

- Using new parts and new technologies will demand a new approach for radiation
- Any expectation that all or most parts will be rad-hard or tested for radiation from their current lots will simply cause many to collapse under their own weight (including many that have been in space successfully for decades)
- Any expectation that radhard parts are necessary and sufficient for successful on-orbit operation will lead to disappointment (as in SMAP)
- Use good system design practices – transition from rad-hard parts to rad-hard by design
  - Protect/derate your MOSFET; understand combined circuit/radiation effects!
  - Implement TMR on FPGAs
  - Be sure your processor circuit is resettable
  - Employ EDAC and protect your memory
- Use familiar parts
  - New sensitive part types (CMOS, processors, MOSFETs, memory, etc) in critical applications should invoke testing or sufficient protection
- Use components that have flown in similar environments
- NVRAM and front-line protection parts radhard
- Perform strategic testing as part of an overall parts characterization activity and remove most testing from the backs of projects (PEAL)
- **Learn from on-orbit experiences! Do not use ground-testing as your primary means for radiation assurance – it will provide a hard barrier against moving forward for many mission concepts.**

New technology does not mean less reliable or radiation sensitive

- Which has greater reliability?
  - a space-proven non-RHA part using TMR
  - An RHA part without TMR
- Which has greater reliability?
  - One RHA MOSFET with 40 nm gate oxide in an SMD-2 package
  - Three non-RHA MOSFETs with 5 nm gate oxide in DPAK

P/N	IRHNA57160	STD100N10F7
VDSS	100V	100V
ID	75A	80A
RDS(on)	12 mΩ	8 mΩ
Package	SMD-2 (~232 mm^2)	DPAK (~60 mm^2)
Weight	3.3 g	0.33 g

Where has the current radiation approach bitten us?

- Chandra: piece-part level radiation assessment of detectors did not account for the orientation effect in the system, which attenuated in one direction, amplified in the other.
- Hubble SM-1: a susceptible "space-grade" optocoupler lacked necessary circuit protection (filter); subsequently HST largely goes dormant in SAA
- SMAP: JANSR (radhard, "level 1", space-grade) MOSFET experienced combined circuit effects when switching, with SEEs in the SAA, causing regular exceedance of rated voltage, ultimately causing gate rupture, and thus taking out the radar.
- Many missions have been forced to change out components with lesser components or at the expense of extreme programmatic hits based on finely prescribed piece-part radiation requirements

Will use of COTS cause a radiation nightmare?

- It certainly can if you're in a radiation environment and you pretend it's not there, but that has **nothing** to do with COTS.
- Typically, about 90% of the overall part count even for large missions are not radiation-hardness-assured (because they don't need to be).
  - The majority of places where COTS are really needed are for non-susceptible parts, such as most passives
- The problem is no different from that of using a 5962-XXX microcircuit or a JANS2NXXXX BJT (neither of which is radiation hardness assured)
- For reference, an IRHM58160 is a COTS part (and it is radiation hardness assured).

- No matter whether you use COTS, MIL-SPEC or "special drawing" parts, radiation should be addressed in the same way
- As we transition to newer technologies and higher performance, we will have to think about radiation mitigation in different ways because parts with RHA will almost always be multiple generations behind
  - However, some of the new technology parts will be less susceptible to radiation by the nature of their designs (thinner gate oxides, etc)

Intelligent use of COTS is of insignificant difference from our current parts assurance practices from a radiation standpoint

Parts Evaluation & Assessment Lab (PEAL)

- Reinstitution of a major institutional capability that assured reliable parts usage in the early days of NASA
- Driven by the reality of dominance of COTS in the market, the necessity to exploit commercial capabilities, and gain the confidence needed to fly parts in low-risk tolerance missions.
- NASA employees and in-house contractors
  - Select and procure parts for characterization
    - Consider unfamiliar parts used and proposed on new and recent missions as top priority
    - Gather input from scientists, component designers, instrument developers
    - **Primary focus should be on part technologies, though specific "part number" assessments should also be performed to properly evolve from current approaches and to monitor trends in specific part design changes over time**
  - Determine screening and lot acceptance tests (LAT) to be employed for future project usage
    - or determination that manufacturer screening/LAT or statistical process controls as designed are sufficient
  - Establish tactical and strategic radiation assessments
  - Perform reliability testing and analyses
  - Determine required post-procurement actions (if any) for each part
  - Maintain parts selection list
    - Part-number-specific assessments over time can be used to characterize evolving trends for some individual part designs to understand risks of obsolescence and the motivations for changes in part design and manufacture
- This is a strategic, Agency-level activity that provides structure for parts selection and acceptance for future missions, not a part acceptance laboratory for missions in development

Approach

- Establish lab space at one or more Centers
- Procure or using existing test equipment
- Assign a core body of PEAL engineers
- Develop parts procurement plans
- Design testing plans
  - Accelerated
  - Nominal
  - DPA
- Procure parts
- Test parts
- Perform reliability analyses
- Develop part technology usage guidelines
- Link in supply chain assurance functions
- Form and maintain “preferred” or “NASA” parts list
- Radiation effects and susceptibility are incorporated into testing and reliability analyses

Initial resource estimate

- 12 FTE/WYE
- Laboratory space
- Test equipment (much already exists or being procured through other means)
- Procurement of EEEE parts (100,000+)
- Procurement of test printed circuit boards

- Approximately $40M initial first year investment
- Approximately $8M (FY23 year dollars) sustained annual investment
- Possible reimbursable elements

- Will displace well over $100M spent by projects
- Impact is multi-$B.

Benefits of PEAL

- Keep a cadre of NASA personnel aware of the risk factors, concerns, capabilities, and aspects of usage of all EEEE parts.
- Maintain a list of known actions to take given the part technologies involved and in some cases specific part numbers
- Maintain an understanding of linkages between such factors as derating (including related to radiation) and reliability (or lifetime in environment, etc)
- Provide a convenient part selection list for projects
- Track parts supply chain concerns, risks, and issues across all parts categories.
- Establish and maintain a NASA-internal list of Industry Leading Parts Manufacturers
- Move the radiation characterization effort up front to support multiple projects, to replace overconstraining piece-part compliance approach

Provide the necessary confidence needed for using COTS and other types of specialized and custom parts in critical applications. Emphasize the capability developed.

Summary

- The foundation and mechanisms to phase-in COTS parts for Class D and below missions have been established.
- The NESC COTS studies have helped to characterize the context for reliable COTS parts usage in missions with allowable low to moderate risk tolerance.
- The NESC COTS studies have not on their own established a basis for acceptance of COTS parts for Class A and B robotic missions, to some extent Class C missions, or human space flight missions without substantial pre- and post-procurement actions.
- Given the decline of in-house assessment activities to support the NASA part selection list, the Centers have lost their knowledge and capability in dealing with and understanding reliability or necessary screening processes for COTS parts.
  - The result is extremely costly practices to deal with the inevitable growth in the use of COTS parts in NASA missions
  - Further, there is no robust capability to facilitate full scale usage of COTS in low-risk tolerance missions
- A concept has been proposed to revitalize and strengthen in-house capabilities that support development and maintenance of an evolved and complete NASA part selection list
  - This will enable cost avoidance and savings of $B and optimize EEEE parts usage on future Class A and B missions, while creating significant new size, weight, power, and performance trade spaces.

BACKUP

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Major part failures and issues since 2005

Mission	Occurrence	Location	Part	Result	Root Cause	Lesson
SMAP	power supply failure	On-orbit	JANSR MOSFET	Radar failure	Use of piece part RHA to mitigate radiation	Radiation must be solved at the circuit and system level
SAC-D	Power supply failures	On-orbit	NASA-screened (level 1) COTS DC/DC converters	(Extended) mission failure	Parts were overtested in screening	Respect the datasheet in handling, testing, and usage
MMS	Part screening and lot acceptance challenges	Ground	NASA-screened COTS HV801 optocoupler	Significant reduction in back-end testing	Use of low-volume hand produced parts well outside of proven bounds	Be sure all specialized low-volume parts have been proven for the current envmt or plan on full qual program. NASA screening cannot overcome parts that are not proven for application
MMS	Part failures	On-orbit	NASA-screened COTS HV801 optocoupler	No appreciable effect	Use of low-volume hand produced parts well outside of proven bounds	Fault-tolerant design can be very effective when parts are not perfect
MMS	Part failure due to corrosion	Ground	JANS BJT	Late failure, rework	Reliance on hermeticity to avoid corrosion, absolute reliance on JANS for perfect parts	JANS requirements do not assure perfect parts

Major part failures and issues since 2005

Mission	Occurrence	Location	Part	Result	Root Cause	Lesson
GOES-R	Part corrosion failure in I&T	Ground	JANS BJTs	$multi-M cost increase, launch slip	Reliance on hermeticity to avoid corrosion, absolute reliance on JANS for perfect parts	JANS requirements do not assure perfect parts, requirements for hermeticity can elevate risk of corrosion
GOES-R GLM	Part anomalous performance and failure after testing over datasheet limits	Ground	NASA-screened COTS LICCs (low ESL MLCCs)	Programmatic hit	Variability in specialized parts, COTS parts tested over datasheet levels (by manufacturer per demands from prime)	Do not test COTS parts over rated datasheet values unless it is part of a proven manufacturer package
LCRD	Part anomalous performance and failure after testing over internal element limits	Ground	NASA-screened Custom VCSO	Programmatic hit	Custom part not fully understood by manufacturer, part overtested in screening	Before applying screening tests to custom parts, be aware of limites
SDO	Circuit misbehavior	On-orbit	M55681 Level 1 MLCC	EVE instrument failure	(1) MIL-SPEC Level 1 Assurance is neither necessary nor sufficient to assure parts to be good for use. (2) Per standard Agency and GSFC practices, parts were tested in non-flight conditions	Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and broad problems Manufacturers are best tuned to identify processes needed to assure reliability of components based on their own manufacturing processes, experiential observations, and usage

Major part failures and issues since 2005

Mission	Occurrence	Location	Part	Result	Root Cause	Lesson
LandSat-8	Persistent TIRS instrument safeholds	On-orbit	M55681 Level 1 MLCC	Switch to open loop pointing	(1) MIL-SPEC Level 1 Assurance is neither necessary nor sufficient to assure parts to be good for use. (2) Per standard Agency and GSFC practices, parts were tested in non-flight conditions	Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and broad problems Manufacturers are best tuned to identify processes needed to assure reliability of components based on their own manufacturing processes, experiential observations, and usage
Insight	Part corrosion failure in I&T	Ground	JANS BJTs	$multi-M cost increase to GOES-R, launch slip for GOES-R	Reliance on hermeticity to avoid corrosion, absolute reliance on JANS for perfect parts	JANS requirements do not assure perfect parts, requirements for hermeticity can elevate risk of corrosion

Major part failures and issues since 2005

Mission	Occurrence	Location	Part	Result	Root Cause	Lesson
SMAP	power supply failure	On-orbit	JANSR MOSFET	Radar failure	Use of piece part RHA to mitigate radiation	Radiation must be solved at the circuit and system level
SAC-D	Power supply failures	On-orbit	NASA-screened (level 1) COTS DC/DC converters	(Extended) mission failure	Parts were overtested in screening	Respect the datasheet in handling, testing, and usage
MMS	Part screening and lot acceptance challenges	Ground	NASA-screened COTS HV801 optocoupler	Significant reduction in back-end testing	Use of low-volume hand produced parts well outside of proven bounds	Be sure all specialized low-volume parts have been proven for the current envmt or plan on full qual program. NASA screening cannot overcome parts that are not proven for application
MMS	Part failures	On-orbit	NASA-screened COTS HV801 optocoupler	No appreciable effect	Use of low-volume hand produced parts well outside of proven bounds	Fault-tolerant design can be very effective when parts are not perfect
MMS	Part failure due to corrosion	Ground	JANS BJT	Late failure, rework	Reliance on hermeticity to avoid corrosion, absolute reliance on JANS for perfect parts	JANS requirements do not assure perfect parts
GOES-R	Part corrosion failure in I&T	Ground	JANS BJTs	$multi-M cost increase, launch slip	Reliance on hermeticity to avoid corrosion, absolute reliance on JANS for perfect parts	JANS requirements do not assure perfect parts, requirements for hermeticity can elevate risk of corrosion
GOES-R GLM	Part anomalous performance and failure after testing over datasheet limits	Ground	NASA-screened COTS LICCs (low ESL MLCCs)	Programmatic hit	Variability in specialized parts, COTS parts tested over datasheet levels (by manufacturer per demands from prime)	Do not test COTS parts over rated datasheet values unless it is part of a proven manufacturer package
LCRD	Part anomalous performance and failure after testing over internal element limits	Ground	NASA-screened Custom VCSO	Programmatic hit	Custom part not fully understood by manufacturer, part overtested in screening	Before applying screening tests to custom parts, be aware of limites

How are automotive and hi-rel COTS defined?

- Declared by the manufacturer to be intended for reliable usage
- Characterized by extensive in-production and/or post-production screening or electrical testing as evidenced by one or more of the following
  - Description in the datasheet
  - Manufacturer-provided documentation, such as
    - Production Part Approval Process (PPAP) document
    - Quality Manual
    - Website detailed technical information provided
  - Parts are qualified to the pertinent AEC Q-category specification (Q100, Q101, Q200)
  - Production is managed under IATF 16949 quality management system (QMS)

Current options for use of COTS EEEE parts in the agency

- Class D and sub-Class D: no restrictions at the agency level, COTS EEEE parts are recommended. Smart selection and use of COTS is always encouraged
  - Known parts from reputable manufacturers, sold for reliable use
  - Respect the datasheet
- Class C (level 3): Automotive and manufacturer hi-rel COTS EEEE parts are compliant as-is IAW NASA-STD-8739.10. Language being incorporated into GSFC SMA MAR templates for Class C.
- All Classes: Standard components that include internal COTS EEEE parts accepted based on history of the item relative to the current environment (part selection and assurance delegated to standard component manufacturer)
- All Classes: Pilot implementation of “three-option” part assurance

National Aeronautics and Space Administration

MIL-SPEC vs COTS parts reliability

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

www.nasa.gov

Quality and Reliability

- Quality is the totality of features and characteristics of a product or service that bear on its ability to satisfy given needs.
  - In many cases quality is defined by specifications that do not actually link to performance
  - In some cases, such specifications are egregiously more stringent than the application warrants
    - We can coin this term *misguided quality* when the second half of the quality definition is missing
- The reliability of a system is its ability to perform (or the probability to successfully perform) the necessary functions within expected life cycle exposure conditions for a required period
  - Reliability of a system is established through
    - A design that has minimal sensitivity to normal disturbances on the system
    - Established past history of the same product
      - Similar products may be used as a basis but the translation to the current product may be complex
  - We often do not have access to design details for many products, which leads to reliance on
    - Knowledge of the developer's capability to develop reliable products
    - Use of a proven design and tight control of variability

    to establish the reliability basis or claim
- Sometimes the original definition for quality of a given commodity or product is no longer meaningful
  - Technology and manufacturing have changed
  - Evolution of the product design has surpassed the quality definitions
- In many cases, manufacturers use the term *reliability* to represent *quality*
  - This is a practice that is based on past MIL-SPEC definitions.
  - Often the quality definition for a product loses its meaning over time (due to, e.g., manufacturing changes)

Misguided quality

- Imposing stringent and excessive numbers of requirements relative to what is needed to achieve required performance and reliability
- Blindly enforcing extensive requirements on manufactured hardware without considering effects of existing assembly vs that of rework
- Using flight and/or qualification unit testing requirements that greatly exceed mission requirements, thus providing misleading results or overstressing or reducing the life of flight hardware
- Misapplying stringent, but proven, requirements or tests to application areas outside of their original intent and design

Radiation

- Radiation hardness (RH) is a multi-dimensional property of any part that describes intrinsic abilities to tolerate various radiation environments
  - Effects to be concerned with include total ionizing dose, total non-ionizing dose, and single-event effects – all of which depend on the mission, environment, application, and lifetime
- Radiation concerns are the same whether a part is COTS, MIL-SPEC, or NASA-screened COTS
- Overattention to radiation at the piece-part level has often supplanted the far more important concept of radiation-tolerant design (leading to a mission failure)
  - Note that some radiation effects can only be accurately characterized at the part-level, though that does not necessarily verify whole-of-system performance. In some cases, the fact that the radiation effects are only apparent at the part level is actually due to attenuation of the effect in the circuit. The understanding of this attenuation is one facet of radiation-tolerant design.
- All parts have a particular level of radiation susceptibility, but only some parts have details in their data sheets, and those details, when present, may be inadequate for a given mission, environment, application, and lifetime. Furthermore, piece part performance is often not indicative of circuit performance.
- Why is there less concern about radiation in MIL-SPEC parts?
  - Often in the space community, the MIL-SPEC term is used only to represent the small "space-grade" subset.
- Does RH of parts in one lot imply the same level of hardness in another lot?
  - Only if RH is in the datasheet (COTS or MIL-SPEC)
    - Any part without RH in the datasheet is not optimized or even controlled for RH, and thus requires further consideration for suitability
    - Furthermore, RH relative to some conditions (e.g., SEE) may provide no indication of RH to others (e.g., TID)
  - However, if it can be confirmed that the part has not changed, one can consider the attributes of the part and the environment to determine whether there are new risk factors in the different lot (COTS or MIL-SPEC). <u>There is no valid reason to discard knowledge obtained from prior lots of the part of the same construct.</u>
- Is past use of the exact same part in space in the same environment (MIL-SPEC or COTS) sufficient to guarantee its future use?
  - No, because the concern is overall radiation tolerance of the design, not radiation hardness of the parts. The previous design may have been radiation tolerant, while the current design may not be.

Radiation is a system-level problem that we have been traditionally (and unfortunately) largely addressing at the part level

Reliable COTS

- Verify part meets Mission Environment, Application, and Lifetime requirements
  - Radiation verified at the part level (RHA in the datasheet is one approach), circuit level (circuit design, fault tolerance, circuit protections), or system level (shielding or fault tolerance)
- Use parts from an ILPM
- Use Established parts
- Recognize contexts for risk
- Respect the datasheet (processing, testing, and usage)
  - Do not screen parts outside of datasheet levels
- Do not repeat manufacturer tests
- Low field failure rate or DPPM
- Relationship with manufacturer for transparency and trust

Early failure likelihood comparison

	Established COTS Parts (microcircuits, discrete semiconductors, capacitors, resistors)	MIL-SPEC Parts (microcircuits, discrete semiconductors, capacitors, resistors)	NASA-screened COTS Parts (microcircuits, capacitors, resistors)
Attributes	1. Produced by an ILPM 2. Automated production line 3. High-volume parts 4. 100% electrical testing 5. Reliability monitoring 6. Process and parts qualification 7. Typically, non-standardized drawings and datasheets 8. Not typically space radiation qualified 9. May or may not be designed for launch and deep space environments.	1. Automated production line 2. Typically not high-volume 3. 100% screened 4. Lot acceptance performed 5. Process and parts qualified by DLA 6. Standardized drawings, data-sheets and MIL specifications 7. Not typically space radiation qualified 8. May or may not be designed for launch and deep space environments.	1. May or may not use automated production line 2. May or may not be high-volume 3. Post procurement 100% screened 4. Lot acceptance tested 5. May or may not have standardized drawings or datasheets 6. Not typically space radiation qualified 9. May or may not be designed for launch and deep space environments.
To achieve *very low* part-level early failure likelihood	- Review datasheet and use the parts within their limits. - Obtain design lifetime from the ILPM. - Verify with ILPM attributes 2-6. - Verify with ILPM that part's field failure rate is < 10 ppm. - Check part prior history including Alerts, similar designs, etc. - Ensure part performance meets application and mission requirements. - Derate Passive parts per EEE-INST-002 guidelines. - Derate microcircuits and discrete semiconductors using engineering judgement per datasheets.	- Review datasheet and use the parts within their limits. - Check prior history of the part including Alerts, similar designs, etc. - Ensure part performance meets application and mission requirements. - Derate parts per EEE-INST-002 guidelines.	- Select establish COTS parts. - Use parts within datasheet limits. - Lot acceptance testing and screerning per EEE-INST-002. - Derate parts per EEE-INST-002 guidelines.
To achieve *low* part-level early failure likelihood	- Review datasheet and verify by additional analysis and/or testing, if needed, that part meets MEAL requirements. - Obtain design lifetime from the ILPM. - Verify with ILPM attributes 2-6. - Verify with ILPM that parts field failure rate is < 25 ppm. - Check part prior history including Alerts, similar designs, etc. - Ensure part performance meets application and mission requirements. - Derate Passive parts per EEE-INST-002 guidelines. - Derate microcircuits and discrete semiconductors using engineering judgement per datasheets.	- Review datasheet and verify by additional analysis and/or testing, if needed, that part meets MEAL requirements. - Check part prior history including Alerts, similar designs, etc. - Ensure part performance meets application and mission requirements. - Derate per EEE-INST-002 guidelines.	- Select established COTS parts. - Lot acceptance test and acreen per EEE-INST-002 guidlines. - Derate per EEE-INST-002 guidelines.

Risk Mitigation vs Risk Avoidance

- Risk mitigation
  - Understand actual risks associated with the parts used, COTS or MIL-SPEC
  - Understand and control, when necessary, the risk factors associated with COTS
  - Assure usage of COTS is consistent with their manufacture and datasheet restrictions
- Risk avoidance
  - Ban the use of anything that may involve risk in some scenario, rather than when there is a context for risk in the current scenario
  - Do not perform the function if it requires COTS because COTS are unfamiliar and require a different approach.
  - Using MIL-SPEC parts when established COTS are better fits does not avoid risk; it just converts a fear to a design-based risk.

Current Conflicts

- MIL-SPECs, by definition, fundamentally limit technology
  - The broad environmental ranges required and the ability to tolerate many forms of overtest (inherently a derating), drive firm “catalog limits”, which have been in place since inception
  - There are not and will not be well-defined “parts categories” to cover many new classes of electronics technology
- The use of MIL-SPECs to accept and qualify COTS parts conflicts with many of the premises of COTS parts
  - MIL-SPECs involve many test levels that are not based on the actual manufacturing processes or application use of the parts
  - COTS parts are optimized to levels laid out in their data sheets, which would very often be different from MIL-SPEC testing levels (neither necessary or sufficient for properly characterizing the parts for acceptance)
    - MIL-SPEC testing levels can overtest COTS parts, resulting in misleading data and/or reduced reliability and damage to parts

National Aeronautics and Space Administration

Example COTS space experiences

The SpaceCube

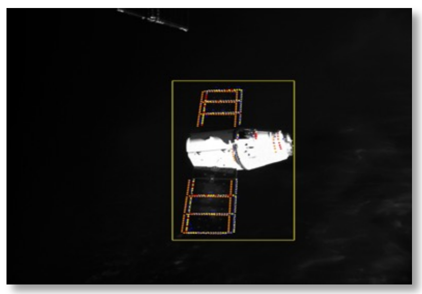
SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Example: Raven Payload

Objective:

To advance the state-of-the-art in rendezvous and proximity operations (RPO) hardware and software by:

- Providing an orbital testbed for servicing-related relative navigation algorithms and software
- Demonstrating relative navigation to several visiting vehicles:
  - Progress
  - Soyuz
  - Cygnus
  - HTV
  - Dragon

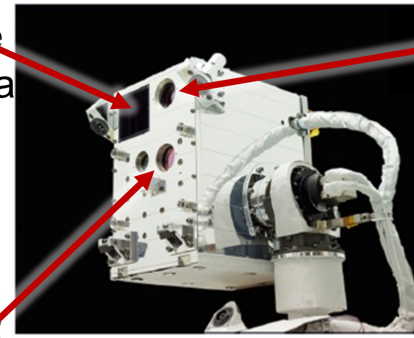


- Demonstrating that both cooperative and non-cooperative rendezvous can be accomplished with a single similar sensor suite

Visible Camera

Infrared Camera

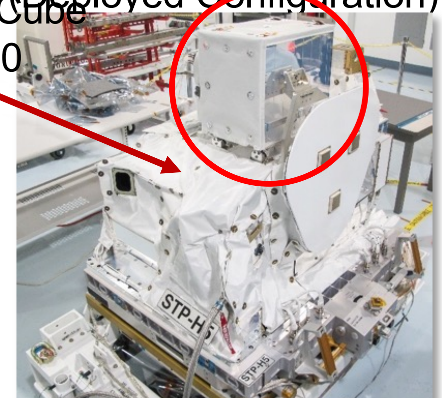
LIDAR



Raven
(Deployed Configuration)

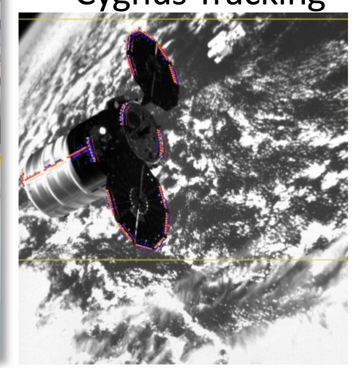
$20M+ payload reliant on confidence in the SpaceCube computer, which in this case was pre-populated with 99% COTS Parts, and then thoroughly tested.

SpaceCube v2.0



Raven installed on STP-H5
(Stowed Configuration)

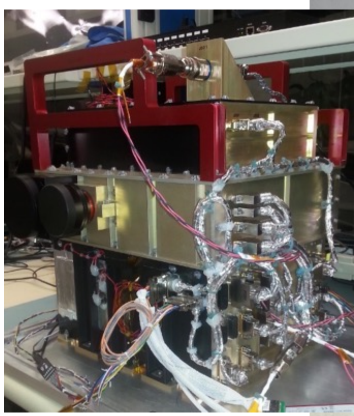
Cygnus Tracking

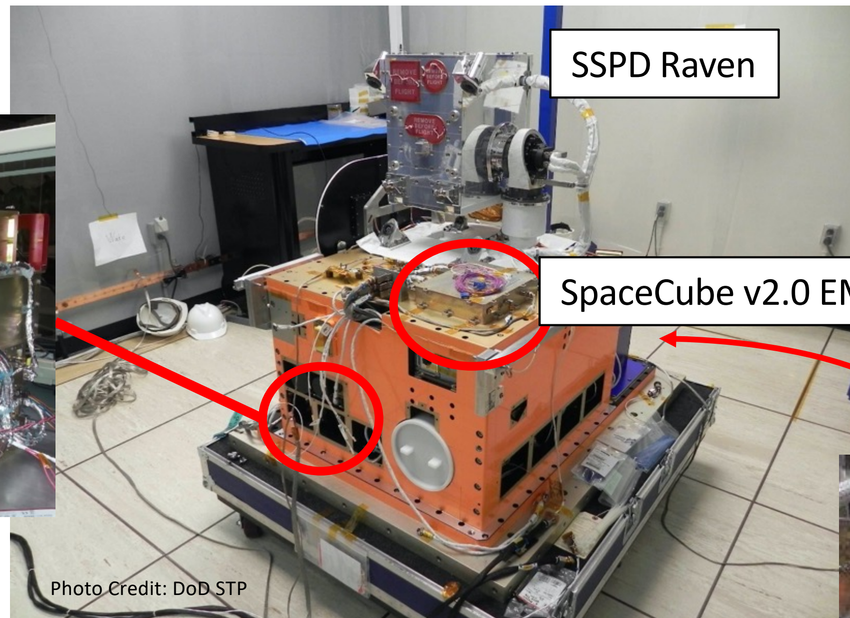


Example: STP-H5 ISS Payload

26% COTS Parts

ISEM, SpaceCube Mini





99% COTS Parts

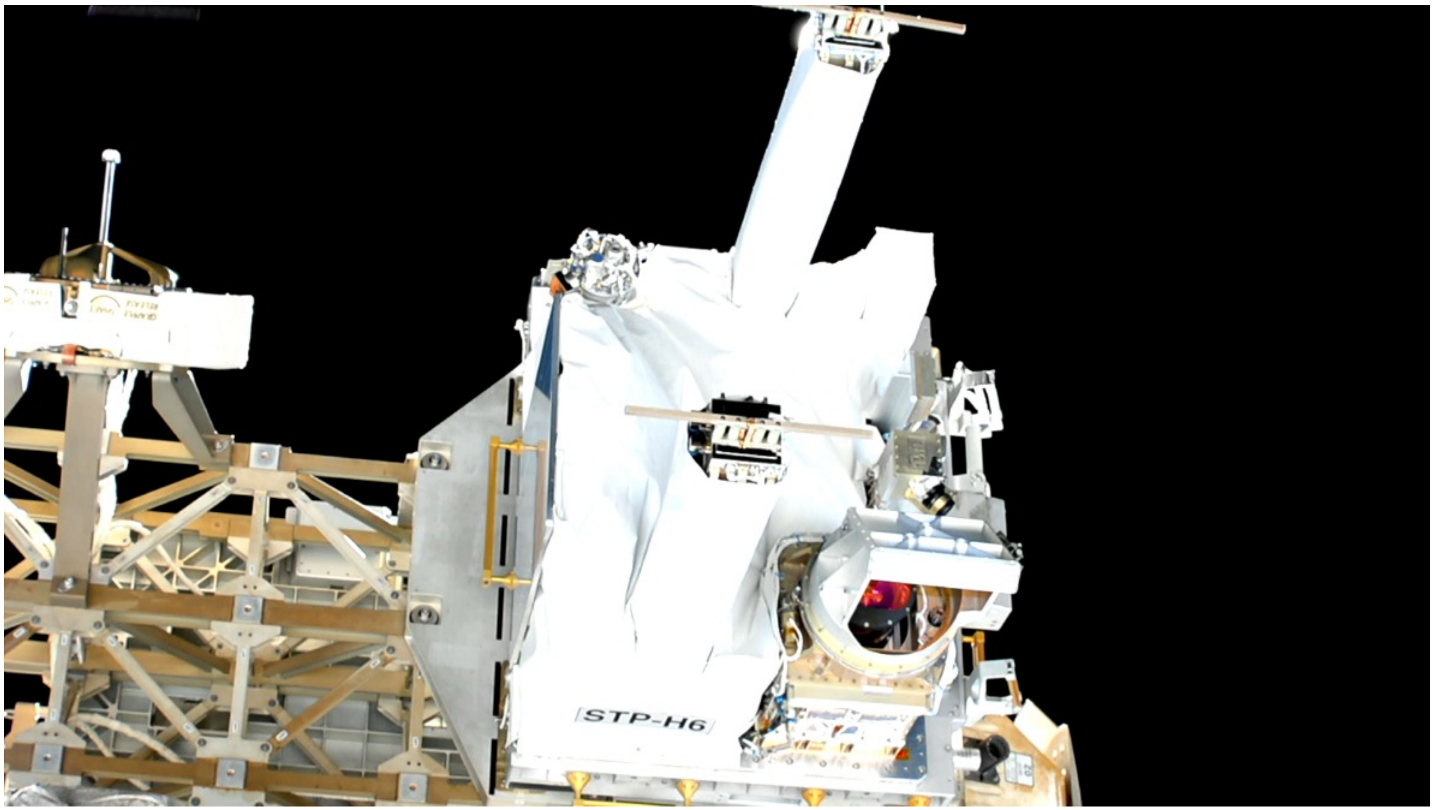
SpaceCube v1.0 CIB

1% COTS Parts

The Space Test Program-H5 (STP-H5) external payload, a complement of 13 unique experiments from seven government agencies, is integrated and flown under the management and direction of the Department of Defense's Space Test Program.

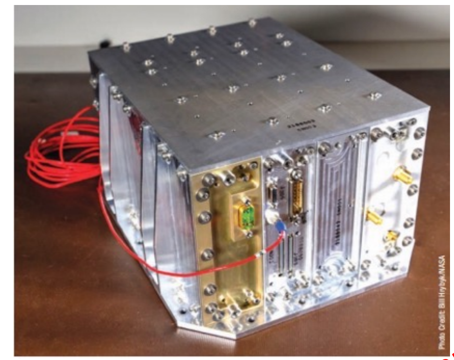
2/2017 - Current

Example: STP-H6 Payload



99% COTS Parts

SpaceCube v2.0 NavCube



1% COTS Parts

SpaceCube v1.0 CIB

SpaceCube Time-on-orbit

Project	Version	Part Req	BOM Count	Operation Months	Xilinx Quantity	COTS %	COTS Months
RNS	v1.0	2+	3700	0.0833333	4	1%	3.08333
MISSE-7	v1.0	N/A	3100	90	4	2%	5580
SMART	v1.5	N/A	1000	0.0333333	1	95%	31.6667
STP-H4 CIB	v1.0	N/A	1500	30	2	1%	450
STP-H4 ISE2.0	v2.0-EM	N/A	1250	30	3	98%	36750
STP-H5 CIB	v1.0	N/A	1500	46.933333	2	1%	704
STP-H5 ISEM	v2.0 Mini	N/A	1000	46.933333	1	26%	12202.7
STP-H5 Raven	v2.0-EM	N/A	1500	46.933333	3	99%	69696
RRM3	v2.0	N/A	1429	36.666667	2	65%	34057.8
STP-H6 CIB	v1.0	N/A	1500	31.833333	2	1%	477.5
STP-H6 GPS	v2.0	N/A	1157	31.833333	2	65%	23940.3
Restore-L Lidar	v2.0	3	2000		2	0%	N/A
STPSat6	v2.0 Mini	N/A	1500		1	98%	N/A

Totals	Units Flown	11
	COTS FPGAs	26
	COTS FPGA Device-Years	83
	Part Years	57213
	COTS Parts Years	15324

Also to note: We flew many COTS components on some of these projects:
- ISE2.0, SMART, and ISEM all flew COTS cameras that were ruggedized. SMART flew COTS SATA drives.
- Raven flew a $5 USB interface card to an IR sensor
- STP-H5 and -H6 have CHREC Space Processors (CSPs) that were 95% COTS components. See references for more info on CSP results (no failures to date)
- RRM3 suffered a failure (outside of SpaceCube) that may have involved a specific COTS part, but the part was used in a stressing condition that any part would eventually fail.
- NavCube Commercial vendor populated PWBs

Side-by-Side Comparison – Proper use of COTS

Platform:
- SpaceCube v1.0

Parts:
- Level 1 and Level 2 Parts

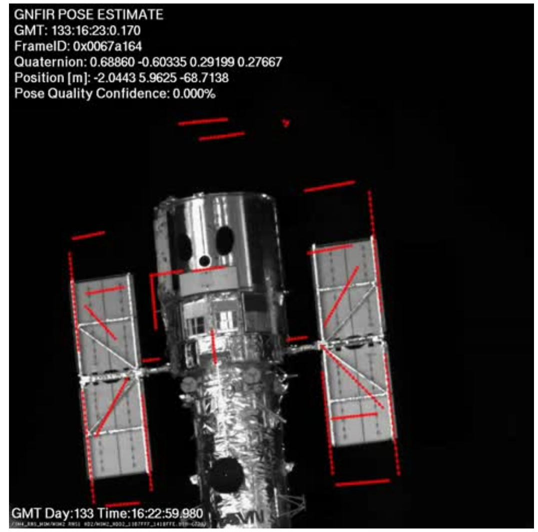
Application:
- Relative Navigation System
- Hubble Space Telescope Real-Time Tracking using 3x visual cameras

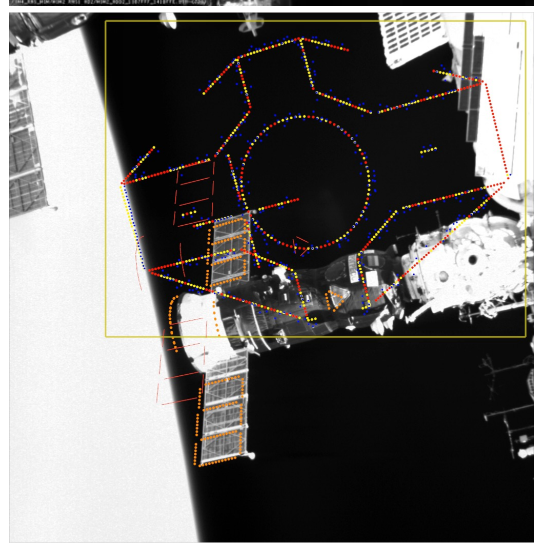
Identical Rigorous Design and Test Philosophy

Platform:
- SpaceCube v2.0

Parts:
- Commercially screened Parts (i.e. COTS)
- Ability to use any level of parts

Application:
- Raven Relative Proximity Ops
- ISS visiting vehicle real-time tracking using visual, Lidar, and IR instruments





Brief history of parts assurance

- Prior to the initiation of full-cost accounting (FCA), NASA had in-house Center capabilities to evaluate, test, and characterize EEEE parts, which were used to develop Preferred Parts Lists (PPLs) and ultimately the NASA Parts Selection List (NPSL). Many such capabilities still exist in a limited fashion, but not to the breadth and depth required to cover the whole spectrum of COTS parts that are considered for space applications.
- These capabilities served not only to establish a basis for characterizing suitability of parts for the full range of applications, but also to ensure that there was a cadre of individuals with detailed understanding of specific parts to assure the proper usage in specific applications.
- On the advent of FCA, the resources were no longer available for such upfront capability, and acceptance of parts was largely deferred to the in-line activities of projects, forcing an approach of using predetermined broad measures, such as the use of MIL-SPEC parts or other parts that had already been placed on to the NPSL (which was frozen in time).
- As time progressed, new parts were proposed for use, and without the in-house capability, documents such as EEE-INST-002 were constructed to provide an algorithm or cookbook to apply in-line to accept parts.
- Since the MIL-SPECs had become the tried-and-true means of assuring parts, the EEE-INST-002 document became the means of applying the MIL-SPECs to unfamiliar parts to “upscreen” them to build confidence in them in a similar fashion to MIL-SPECs.

Root causes and lessons learned from past failures

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

TIRS on-orbit SSM anomaly

Approximately 10 months after LandSat-8 was launched an anomalous trend was noted in the –EV MCE (mechanism control electronics) current on the TIRS A side electronics. Over time the –EV MCE current began to grow at an exponential rate, initiating an anomaly investigation. A lengthy investigation did not confirm root cause. However, a conductive anodic filament (CAF) growth was suspected, at the time, of creating a short path within the A-side electronics. To prepare for a possible loss MCE loss, tests were conducted to understand SSM (scene select module) drift without positive feedback control.

Following the recommendations from the A side ARB investigation, TIRS was swapped to the B side electronics to collect optimal science for the 2015 agricultural growing season. Approximately 5 months after resuming nominal TIRS B-side operations, anomalous current indications were observed in the +EV MCE current.

TIRS on-orbit anomaly cont'd

- During preparation for TIRS-2, Code 300 was reviewing anomaly history of TIRS, noting the behavior and open items on the fishbone (Ishikawa) diagram
- Code 300 was concurrently performing reverse bias capacitor testing to support projects using the Express Logistics Carrier (ELC) on ISS.
- On-orbit leakage current behavior on TIRS bore a striking resemblance to reverse bias capacitor performance in our ELC ground testing
- Capacitor polarities in all related components on TIRS were thoroughly examined
  - Polarity was correct at all levels
- Code 300 requested that spare boards be brought out of storage to be powered up
- Shortly after power-up, the board started to exhibit the leakage current reflecting the on-orbit behavior
  - Many attempts were made to power cycle the boards, induce recovery, or otherwise affect the current profile, with mixed results
- We placed a thermal camera over the board to watch for hot spots

TIRS on-orbit anomaly cont'd

- After weeks of operation, noticeable locations of excessive temperature rise were seen on the board
- These were located in the vicinity of some RC filters feeding into amplifiers on the board
- Probe measurements were taken at points on the bank of filters that indicated reduced voltage (and hence current leakage) at at least two of the caps.
- GSFC parts branch (Code 562) brought in a thermal camera with high spatial resolution that identified that the hot spots were unequivocally located on two of the capacitors themselves.
- The focused heating combined with the fact that the capacitors were hand-soldered ceramic caps (not recommended for handsoldering) strongly indicated that they were cracked.
- Board and x-ray inspections performed did not show signs of cracking
- The process then began to remove the suspect parts from the board for failure analysis and replacement.

TIRS on-orbit anomaly cont'd

- This was the first instance we had seen of cracked capacitors making it through I&T undetected and becoming anomalous on-orbit
  - In this case, the cracks were internal to the parts and they may not have even formed until the hardware had been on-orbit for a while, or the crack may have initiated upon installation and propagated over time.
- C-mode Scanning Acoustic Microscopy (C-SAM) was performed on the anomalous parts on the boards, which subsequently showed signs of delamination internal within the parts that lined up with the hot spots.
- Fortunately, we had hundreds of spare capacitors from the LDC (1011-BY) enabling some lot-based views.
- A large-scale C-SAM effort was undertaken, showing that about 50% of the parts had delaminations internal to the pristine parts, in many cases similar to those present in the anomalous parts.
- While the hot spots lined up with the delamination features, testing revealed that the delamination features were not failure or degradation mechanisms, but they were signs that there may have been a lot problem

Fault Tree

Leakage Current trips safehold in TIRS

Loss of resistance in at least one MLCC

Conductive path across opposing electrodes

Internal crack in part

Silver Migration

Longstanding manufacturing flaw

Past Observations entirely blamed on handsoldering

Weakness in BX ceramic

MIL-SPEC not perceptive to manufacturing flaw

MIL-SPEC tests overtest without ability to perceive subtle signs of overstress

Root Cause 1: MIL-SPEC Level 1 Assurance is neither necessary nor sufficient to assure parts are good for use. Additionally, in some cases, weaker parts may be degraded without knowing overtest has caused overstress

Root Cause 2: Per standard Agency and GSFC practices, parts were tested under non-flight conditions. Testing at the piece part level did not expose the manufacturing flaw, which only appeared after installation. Piece-part testing per the MIL-SPEC was ineffective, giving a false sense of confidence.

Lessons Learned

- Manufacturer knew of problem for years but was unaware that the problem could materialize without manual soldering or touch-up.
- Manufacturer placed greater emphasis on meeting the MIL-SPECs over product quality because customer expectations and contractual documentation are focused on meeting MIL-SPECs
  - Government and industry believed MIL-SPECs assured product quality and part reliability

Lessons:

1. Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and wide-spread problems
2. Manufacturers are best tuned to identify processes needed to assure reliability of parts based on their own manufacturing processes, experiential observations, and usage, but MIL-SPECs take precedence over manufacturer-established assurance processes for MIL-SPEC parts

Standard product capacitor concern

- After 5 years of successful testing and on-orbit operation of a widely-used standard space component with no failures or degradation, a DPA was performed on a hybrid (*model* 2) part as a matter of course before a new batch of components was about to begin development. The DPA indicated cracks in capacitors internal to the hybrid, thus prompting an investigation into the depth and breadth of the concern. As is common in the space community, the vendor relied on MIL-SPECs for screening and qualifying parts that were outside of the MIL-SPEC catalog as a standard practice. In this case, MIL-PRF-123 (M123) was applied to the capacitors and MIL-PRF-38534 (38534), Class K (level 1) to the hybrids. Both of these processes constitute extreme levels of testing with little to no relevance to the manufacture or usage of the parts, and even the screening portion of the test applied to all of the parts would constitute an egregious overtest. Nonetheless, the screening processes indicated that a small percentage of the capacitors formed cracks and/or lost significant insulation resistance as a result of going through these two rounds of testing, most likely as a result of 38534 since most cracks were on the outside, but not seen when installed into the hybrids. The screening results indicated that there was a manufacturing weakness in a small percentage of the parts that prevented them from handling the extreme combined conditions of M123 and 38534. Not only were no failures or anomalies experienced in nominal use over several years, but attempts to provide aggressive burn-in testing to hybrids that were known to have problematic capacitors in them all resulted in low-to-normal impedance, but well above levels that would be low enough to affect performance. This was consistent with the fact that no parts had indicated off-nominal performance in nominal testing and application. It is conceivable that even the weaker parts would have been reliable for all applications with little uncertainty, but the fact that all went through M123 and 38534 tests brought up much uncertainty.

Fault Tree

Caps in model 2 hybrids found to be cracked or low in resistance during DPA and part level testing

Stress due to installation in model 2 hybrid

Stress in model 2 hybrid design

overstress due to 38534 testing unique to model 2 hybrid design

Manufacturing weakness in small percentage of caps in 1520

38534 testing is not test as you fly

38534 testing is significantly more stressful than application

There is no nondestructive way to determine whether testing overstressed parts

No determination was made of degradation to the parts

Design of parts is outside of M123 catalog, highly sensitive

Manufacturer not experienced with building the specific part

Root Causes:

1. The use of MIL SPEC screening and qualification processes for part designs (both the capacitor and hybrid) that were not within the intended performance range of the MIL SPECs used
2. False confidence created that one reputable vendor's successful use of a mismatched screening and qualification process with a specialized part design implies that another reputable vendor would have the same results
3. MIL-SPEC Level 1 Assurance used as sole determinant of parts being good to use, but is neither necessary nor sufficient to assure parts to be good for use. Additionally, in some cases, weaker parts may be overtested without knowing overtest has caused overstress

Lessons Learned

- Standard component manufacturer has certainly demonstrated a working process that has withstood the test of time. However, there may have been at least a semblance of luck that the capacitor manufacturer for years has been able to produce this specialized part robustly enough to withstand the M123 and 38534 (after being installed into the hybrid) screening processes uniformly across the lot
- Hindsight is 20/20 – the burn-in failure of the two model 2 hybrids should have set off more flares. While it may well not have meant that the parts are unusable, it should have indicated that some aspect of the design, testing, or manufacture required further study

Lessons:

1. Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and broad problems
2. Be sure that multiple discrepancies in part testing give rise to not only a characterization of usability of parts, but also their ability to withstand the tests and overall effectiveness of the tests

Conclusions

- The use of MIL-SPECs to assure parts has been largely successful since the earliest days in space
- Over recent decades however, technologies and manufacturing processes have advanced, while the MIL-SPECs have not kept up and cannot keep up
  - The extreme specifications fundamentally limit the technology
  - The extreme testing and hermeticity expectations often cause bigger problems than those they are trying to solve
- Several major part failures have occurred that have resulted in serious programmatic problems, major mission anomalies, and mission failure
- While this does not mean that MIL-SPECs should be completely discarded, it should be understood that they will often not be the best means for reliability
- Since COTS are designed, developed, and tested pertinent to the actual manufacture and usage environment, they are much more inclined to be reliable than MIL-SPEC or NASA-screened parts.
- However, the open-ended nature of COTS brings challenges in understanding how to procure and use them reliably
- Unfortunately myths, misunderstandings, and misleading statements have unjustifiably pigeonholed COTS into a high-risk category over the years.