National Aeronautics and Space Administration

Phasing in COTS EEE parts in NASA

Jesse Leitner, Chief SMA Engineer, NASA GSFC

Jesse “dot” “Leitner” at “nasa.gov”

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

www.nasa.gov

Outline

- NESC COTS study
- Term definitions
- Commercial Off The Shelf (COTS) vs MIL-SPEC dilemma
- Quality vs Reliability
- Radiation
- Why is COTS necessary?
- Risk mitigation vs risk avoidance
- Summary

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 (nearing completion) 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

ILPM

ILPM (current definition): 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[8] 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 (current definition)

- 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. They are typically available for sale through commercial distributors to the public.
- 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 electrical testing/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.**

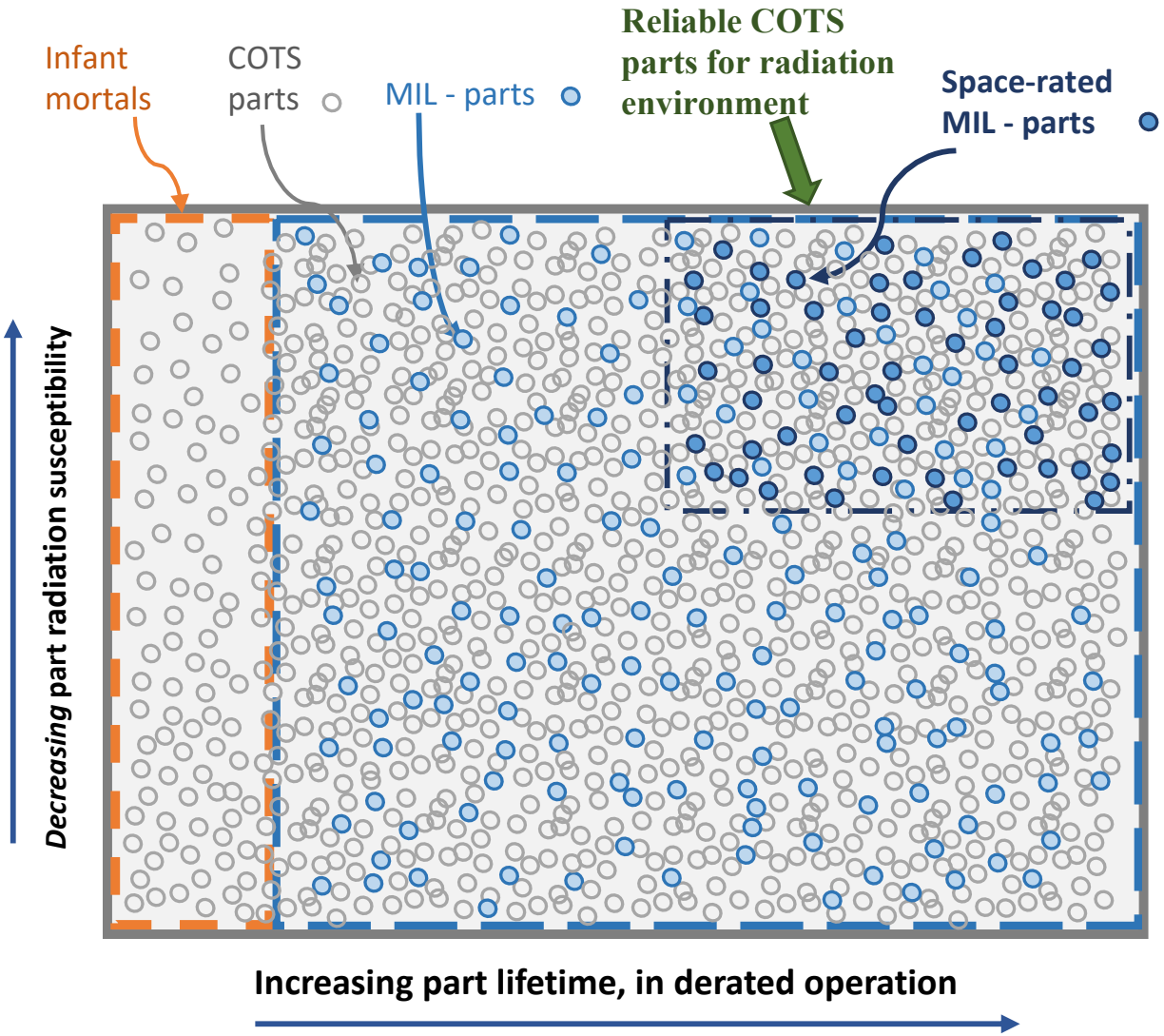
MIL-SPEC parts

- 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**

NASA-screened COTS parts

- COTS parts that are outside of the MIL-SPEC “catalog” parameters 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, often resulting in overtesting relative to the part application and to its datasheet. Thus this option provides the greatest uncertainty for reliability, especially if the COTS parts are low volume.

The Infinite "Space" View of COTS



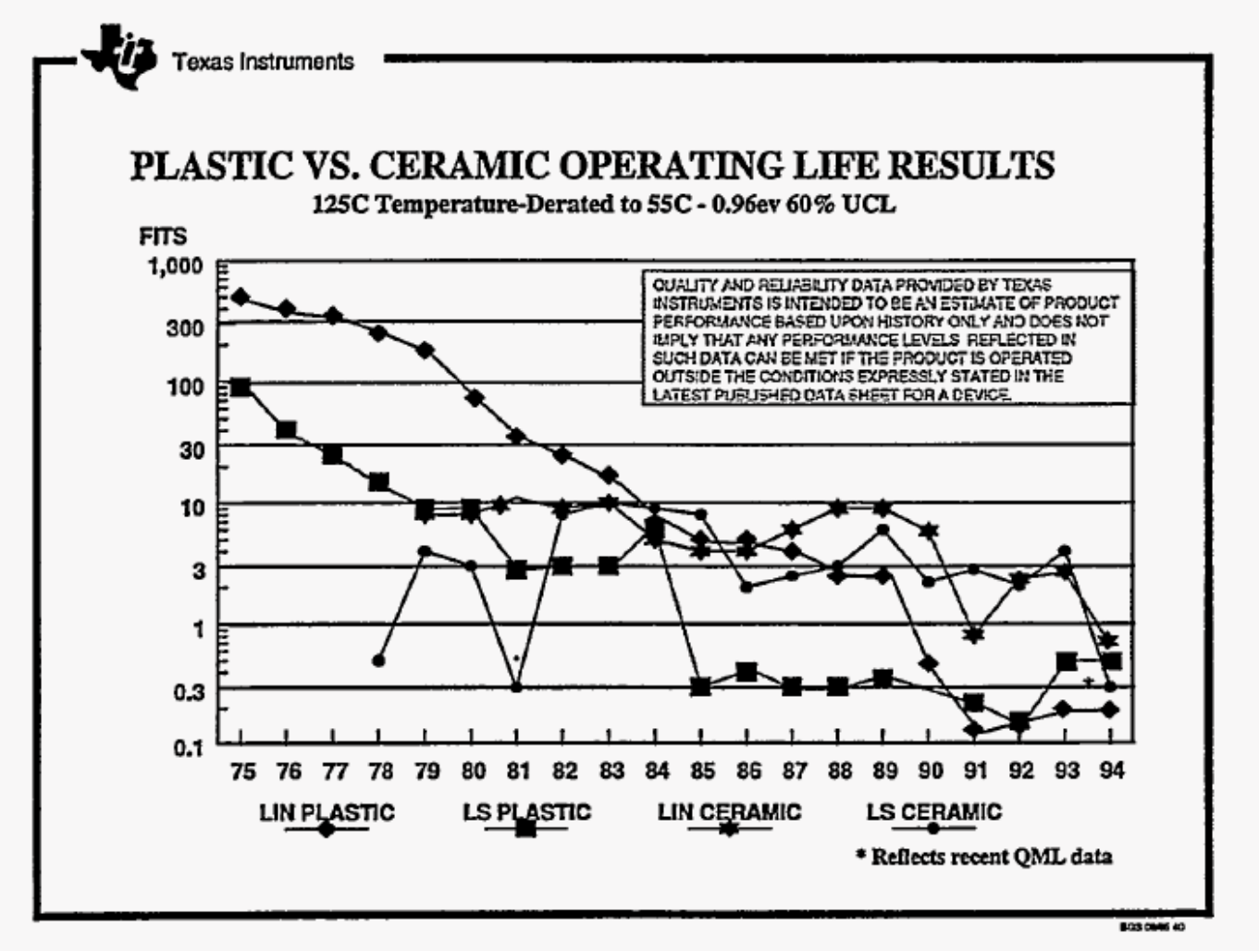
Why have COTS been perpetually deemed "unreliable" or "low-grade"

- 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.

What did we know in 1994?



Note that in 1984, LS (TTL logic) plastic crossed over LS ceramic and has been consistently better since that time. In 1986, LIN (linear) plastic crossed over LIN ceramic and has been consistently better since that time. In 1994, the failure rates for the ceramic parts made a considerable improvement and essentially merged with the rates for their plastic counterparts. This coincides with the change from QPL, where the product was made on separate military production lines controlled by DESC, to QML where the product was made on commercial lines.

https://digital.library.unt.edu/ark:/67531/metadc677817/m2/1/high_res_d/444032.pdf

TI Plastic vs Ceramic lifetimes 1975-1994

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
    - 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.

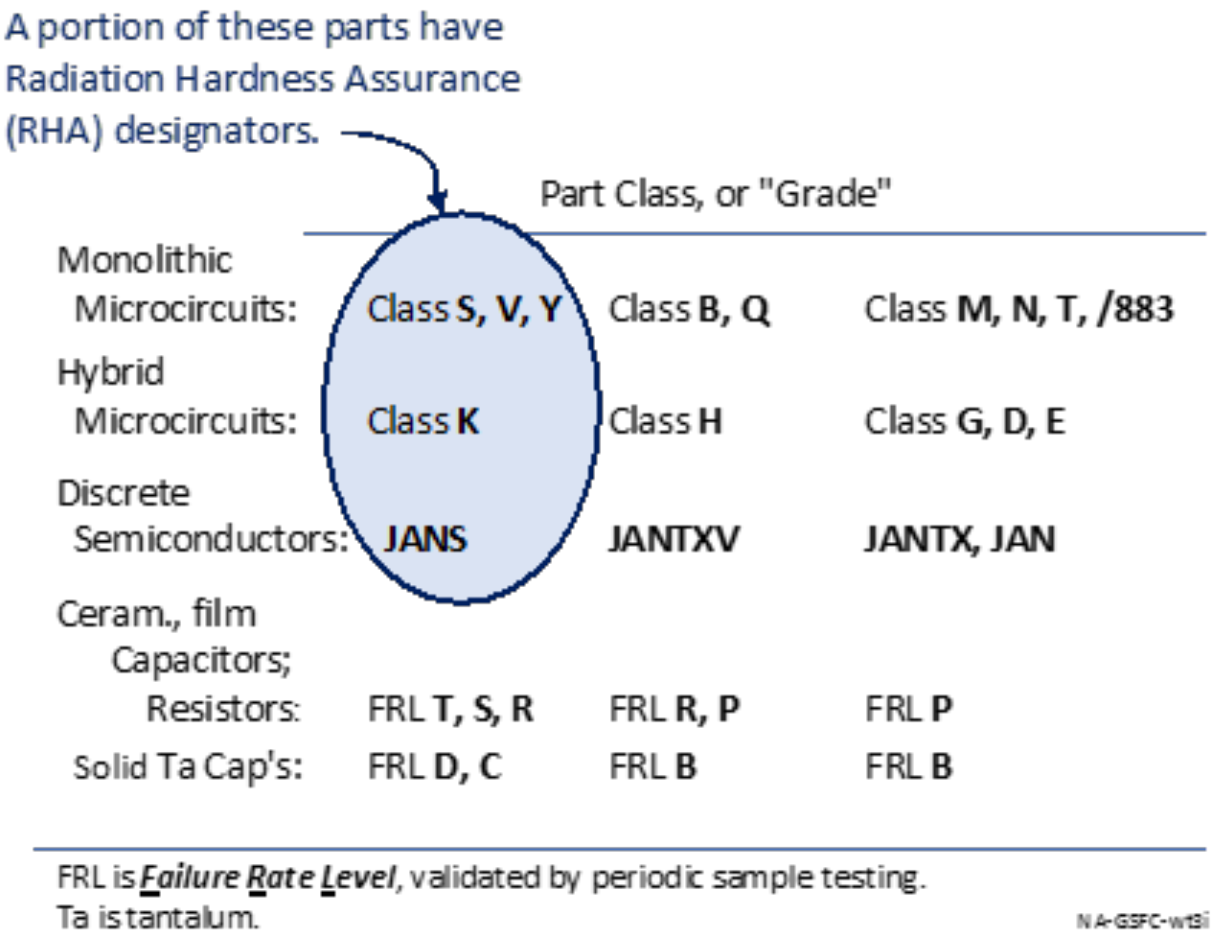
Radiation

- 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). There is no valid reason to discard knowledge obtained from prior lots of the part of the same construct.
- 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

RHA in the MIL-SPEC “universe”

The Military Specification Parts "Universe"



Note that V, Y, K, and JANS parts are not required to have radiation hardness assurance guarantees.

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.

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
- Recognized 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.

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

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

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.

National Aeronautics and Space Administration

Example COTS space experiences

The SpaceCube

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

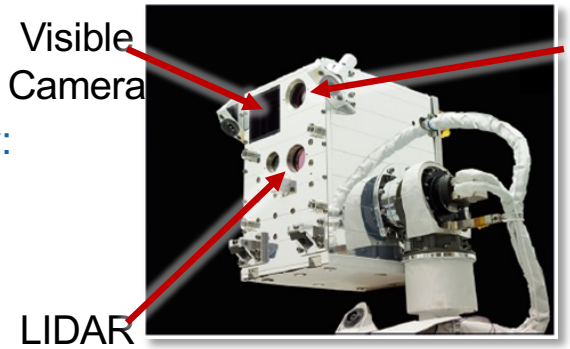
Example: Raven Payload

Objective:

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

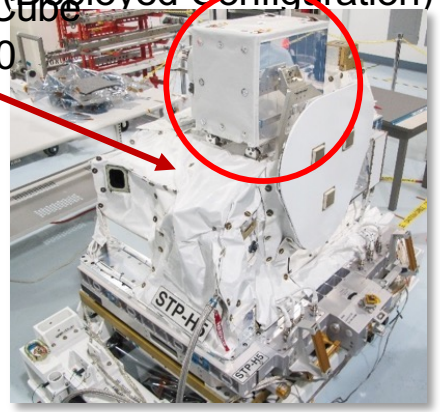
- Providing an orbital testbed for servicing-related relative navigation algorithms and software
- Demonstrating relative navigation to several visiting vehicles:
  - Progress
  - Soyuz
  - Cygnus
  - HTV
  - Dragon

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



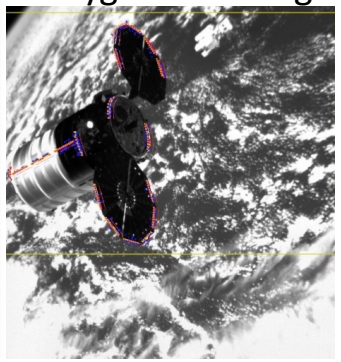
Raven
(Deployed Configuration)

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



Raven installed on STP-H5
(Stowed Configuration)

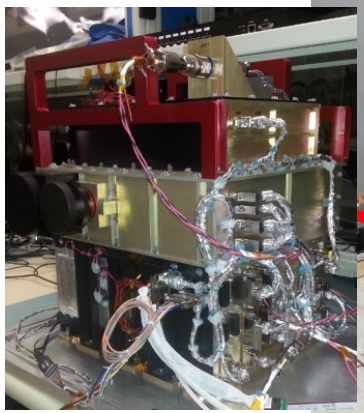
Cygnus Tracking

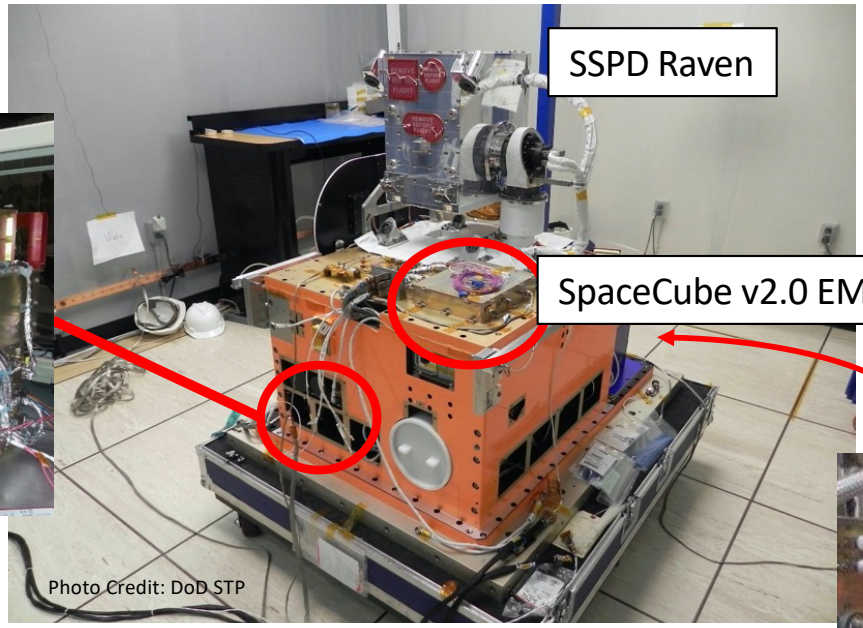


Example: STP-H5 ISS Payload

26% COTS Parts

ISEM, SpaceCube Mini





99% COTS Parts

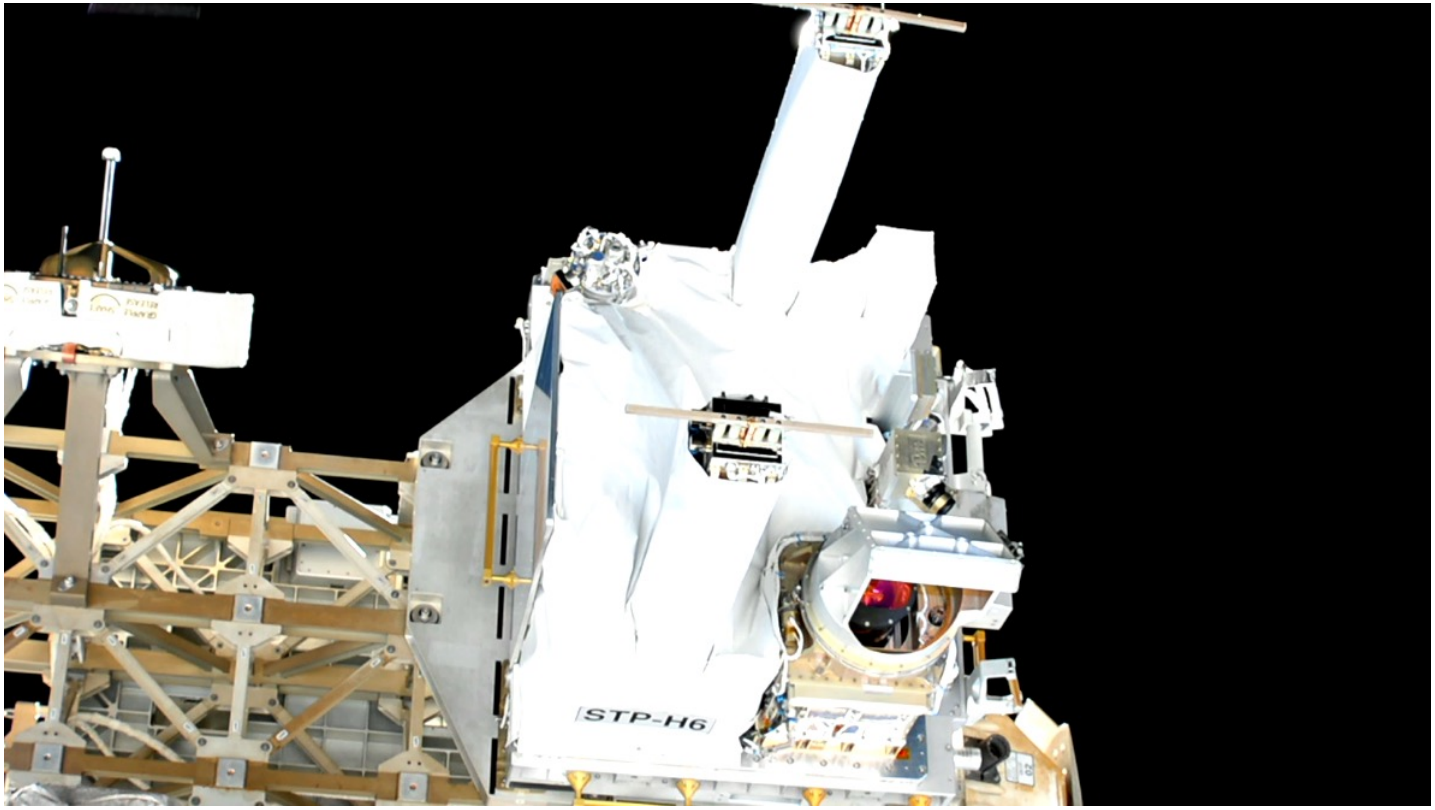
1% COTS Parts

SpaceCube v1.0 CIB

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.

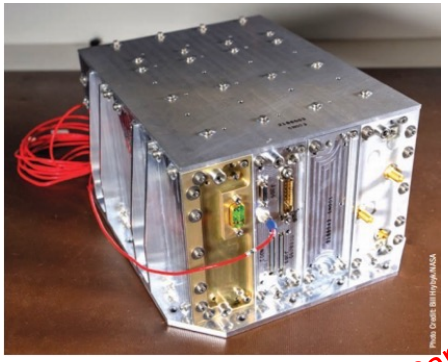
2/2017 - Current

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
	Xilinx FPGAs	26
	Xilinx 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

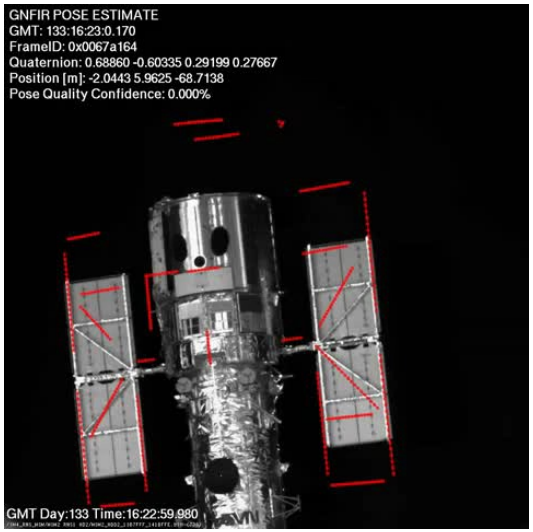
Application:
- Relative Navigation System
- Hubble Space Telescope Real-Time Tracking using 3x visual cameras

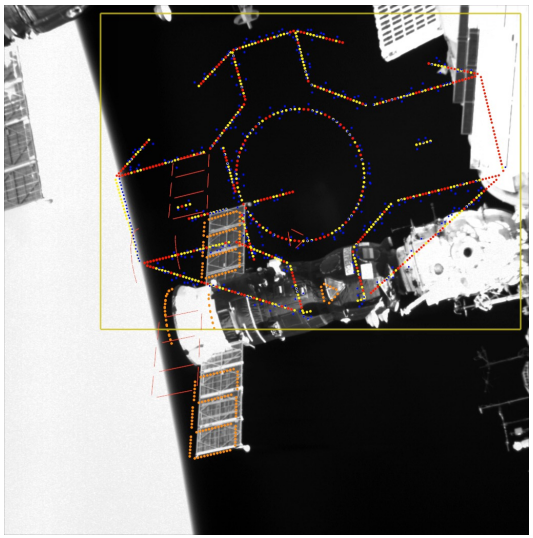
Identical Rigorous Design and Test Philosophy

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.

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

Summary

- There is a misperception that the need to use COTS parts is an exception in cases where there are extreme cost constraints or the need for an extremely aggressive level of performance
- In fact, a broad use of COTS is required for virtually any advanced component based on technologies from the last 15 years
- The frozen-in-time MIL-SPEC system has become dwarfed by the commercial electronics industry and no longer provides the same reliability advantages that it once had over the commercial market.
- It is essential to learn how to harness the capabilities of the COTS marketplace to avoid having the agency surpassed by a large swath of the space community.

BACKUP

Phasing in COTS

- 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.

National Aeronautics and Space Administration

MIL-SPEC vs COTS parts reliability

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

www.nasa.gov

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

National Aeronautics and Space Administration

Root causes and lessons learned from past failures

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

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

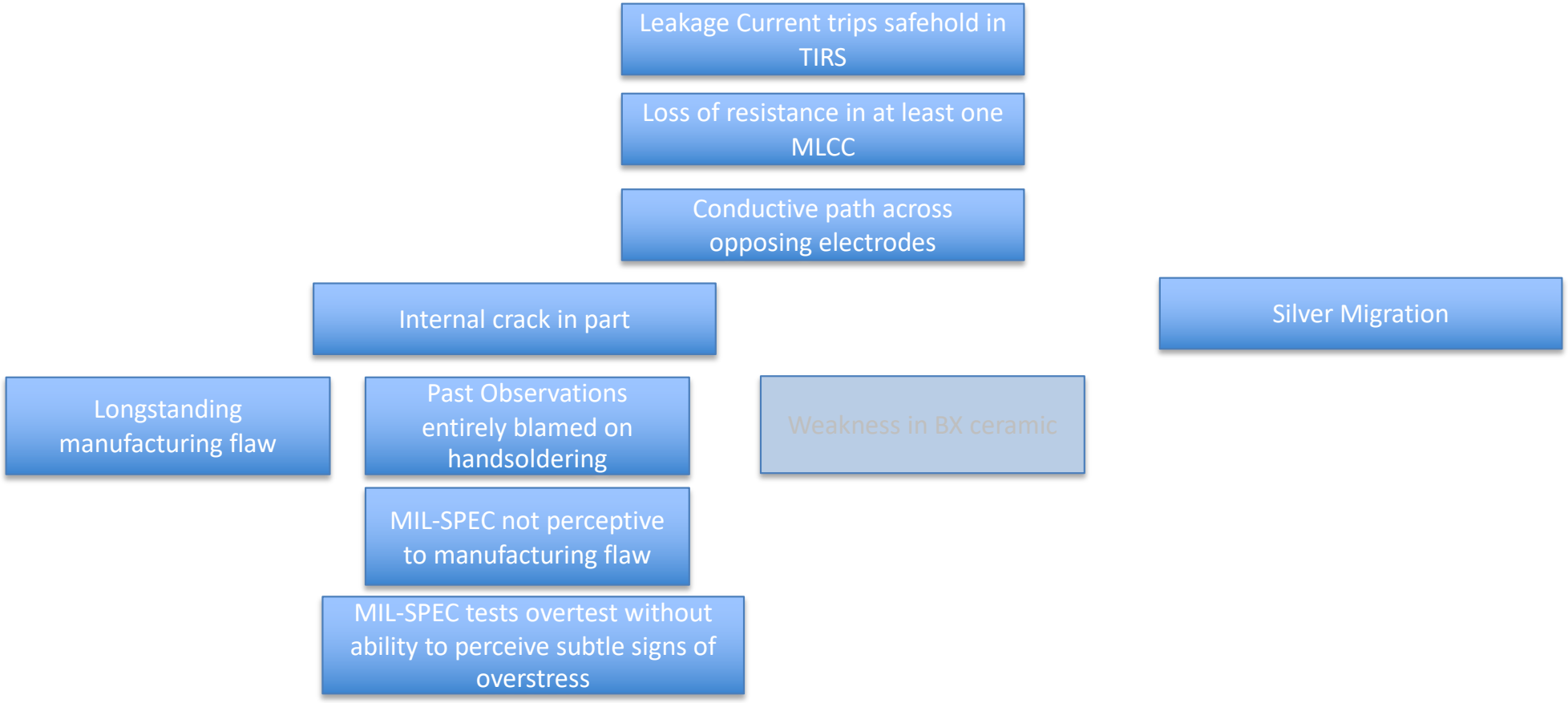
- This was the first instance we had seen of cracked capacitors making it through I&T undetected and becoming anomalous on-orbit
  - In this case, the cracks were internal to the parts and they may not have even formed until the hardware had been on-orbit for a while, or the crack may have initiated 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

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

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

Fault Tree



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

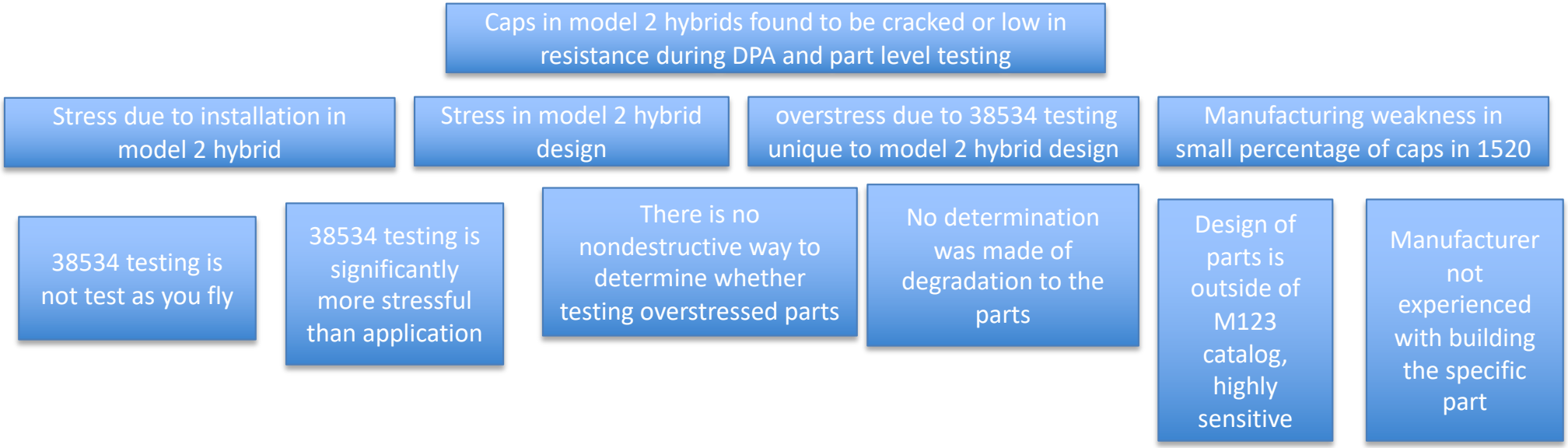
Standard product capacitor concern

- 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.

Testing Results

Infant Mortality after Overtest	TAYF after Overtest	TAYDF after overtest	OTAYF after Overtest
1 “hybrid model 1”	5 years of standard operations with no anomalies for component model 1 and model 2	Additional capacitor stress testing	Hybrid model 2 confidence testing
~15 (?) “hybrid model 2”		statistics	All problematic caps leveled off
statistics			

Fault Tree



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