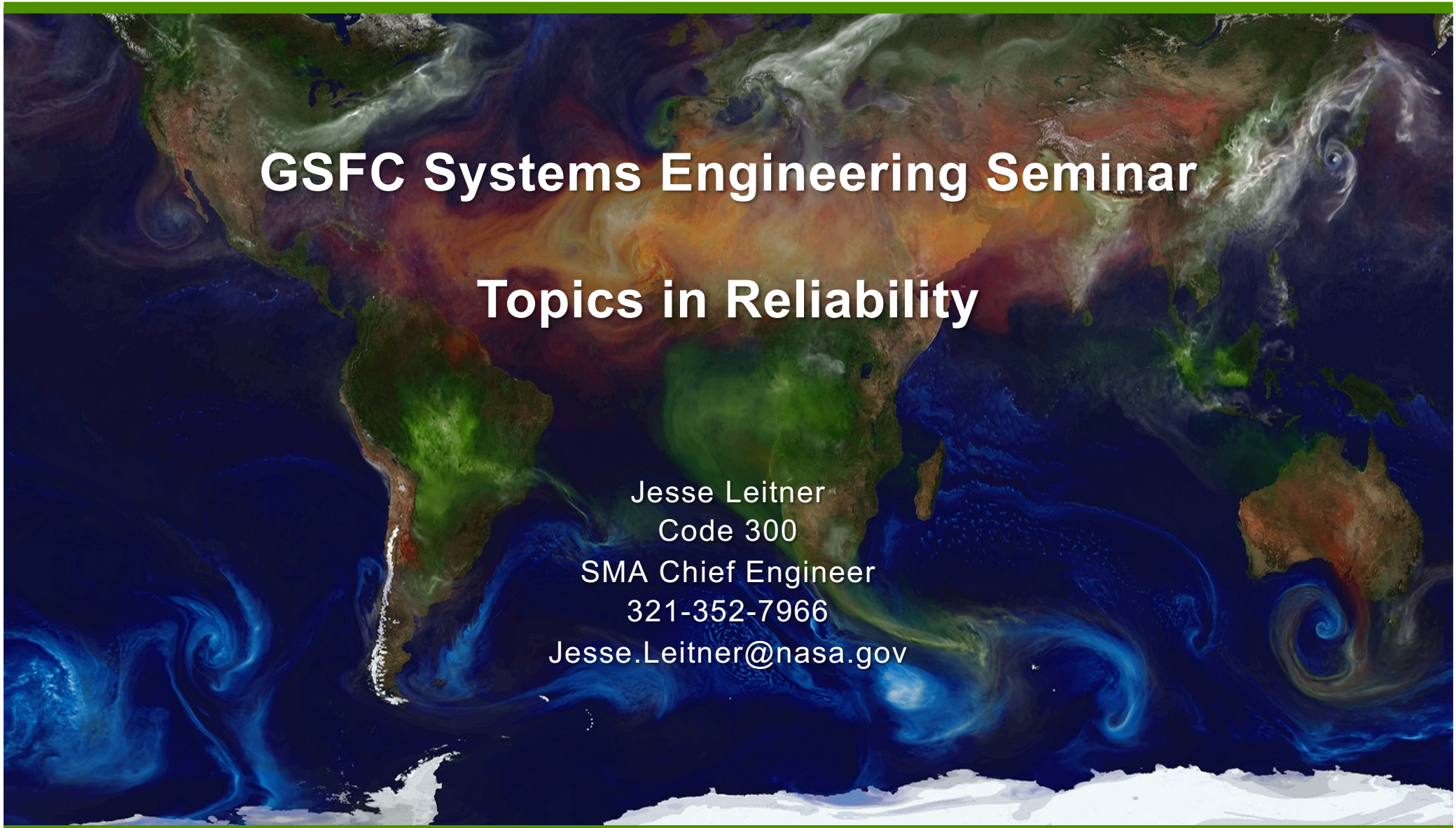


GSFC Systems Engineering Seminar

Topics in Reliability

Jesse Leitner
Code 300
SMA Chief Engineer
321-352-7966
Jesse.Leitner@nasa.gov

Why are we here?

- Reliability at GSFC and within the agency has become a term more aligned with slang or feelings than with the actual definition of the term
  - The result has been that actions are often justified to be “for reliability” that do not actually assure or impact reliability in a positive way
- Many reliability practices are tied to outdated or debunked types of analysis
- Capabilities across the space community have changed dramatically from those originally in place at the inception of the space program, but our practices have changed very little.
- Changes to traditional practices are often simply declared to be reliability threats (or “elevated risk”)

We need to transform our thinking about reliability

Reliability

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

In what forms does reliability come?

- Design
  - Fault-tolerance
    - Redundancy
    - Graceful degradation
  - Radiation mitigation
- Volume of production and successful operation
  - Statistical process controls
  - Established quality practices
  - Complete testing by the manufacturer

Graceful degradation

- A design approach that allows high performance achievement with moderate to low confidence and minimum performance achievement with high-confidence.
  - Minimal reliance on individual piece parts
  - Low risk for attempting bold accomplishments
  - Straightforward opportunity for dissimilar redundancy
- Example:
  - Detector array with 80 elements, 40 required for minimum success, 60 for full success, 80 for “overkill” performance

Flavors of reliability

- Mission Reliability: the probability that a mission will operate for the required amount of time at the required level of performance
- Design Reliability: The extent that the inherent features of the design of a system assure the system's ability to operate at a required amount of time under a nominal set of faults and disturbances
- Reliability Prediction: The use of analytical or experimental techniques to estimate the reliability of a system given contextual information
- Established Reliability: Past performance of a system design and manufacturing approach in a given operational environment with statistics to support its future reliability with a given level of confidence.

Reliability paradigms

1. Simple design; basic (old) technology; limited manufacturing capability; limited, prescribed quality control practices (i.e., how we must be if we want to operate in space); emphasis on piece-part controls; commercial systems deemed “unreliable” because vendors can’t be trusted under any circumstances.

2. Complex designs, cutting edge technology, advanced manufacturing capability, rigorous quality controls and methodology, design for reliability, statistical process control, and intelligent use of established (usually commercial) products for routine elements

We’ve been trying to live in 1, but we need to be in 2 in NASA

What is quality and why do we care?

- 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 does not apply
- Quite simply, we need quality as a means to get reliability (or safety) and to assure consistency
  - Quality on an individual product tells us that it is a good reproduction of previous working versions and that it is built as designed
  - A developer's quality practices tell us that we can expect future versions to be representative of the previous versions
- But remember, no level of quality can make up for a bad design, and thus quality is in no way sufficient to obtain reliability
- Furthermore, if we forget that reliability is the end game, we might lose sight on what's important and top priority

Quality and Reliability

- As mentioned earlier, quality is the totality of features and characteristics of a product or service that bear on its ability to satisfy given needs.
- 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

Quality and Reliability (cont'd)

- 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.
  - One key reason for it is that when there is not sufficient volume to establish reliability, quality is the only tool you are left with
  - Often the quality definition for a product loses its meaning over time (due to, e.g., manufacturing changes)
  - The conflation of quality and reliability is a major contributor to the retention of outdated practices

Is Quality just reliability on Day 1?

- This is a common statement
- It can be correct, but not always
- The quality requirements would have to be well-aligned with the design, the design itself would have to be proven reliable, and meeting the quality requirements would have to be sufficient on their own to assure that the system functions reliably.

Past myths

- A collection of quality requirements assures reliability
- Reliability can be screened-in to parts
- Individual part reliabilities can be rolled up to predict system reliability (Ps)
- The imposition of Ps requirements promotes good practices, even if the Ps estimate is invalid
- “Quality” parts are the key to reliability
- Our traditional parts requirements assure the highest quality and thus the highest reliability
- Part-level radiation hardness requirements are key drivers for space mission reliability

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

Misguided reliability

- Putting extensive resources focused on mission reliability (vs design reliability) for a mission with primary emphasis to mature technologies, demonstrate technologies, or perform first time use of mature technologies
- Enforcing quality requirements under the guise of reliability, when the quality requirements are not linked to the prevention of failure mechanisms or recovery from faults.
- Emphasizing reliability testing that is not relevant to the operation of the system at hand, e.g., that are based on a different mission profile
- Mixing the flavors of reliability and subsequently making impactful decisions

Costly processes with minimal reliability payoff for 10-year missions

- Use of level 1 or level 2 MIL-SPEC parts as a minimum or level 1/level 2 screening and qualification of non-MIL-SPEC parts or strict level 3 screening
- Rigid application of most stringent printed circuit board specs
  - Multiple layers of PCB coupon approvals
- Re-qualification of qualified devices
- Overly strict enforcement of workmanship requirements
- Misguided quality

Cost-effective variants for a low-cost, forward-leaning, reliable mission

- Fault-tolerant and resilient architecture
  - Design to accommodate failures but don't design to expect failures
- Perform robust risk management with strict interpretations of risk
  - Risk should always have context
  - Concern/worry list may be maintained without context
- Extensive but intelligent use of COTS EEE parts
  - Do not change out parts from proven designs
  - Do not assume MIL-SPEC or "NASA-screened" parts to be "highest reliability" choice

Robust* Design

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

*performance achieved in the presence of disturbances and uncertainties

Sound risk management

- Capture risks based on existing threats to performance and reliability
- Consider all possible sides of each risk and trade risks in a balanced way
  - Avoid over-attention and mitigation to some risks at the expense of others
- Apply requirements based on the best understanding of risk at the time
- Characterize risk for nonconforming items to determine suitability for use and avoid scrapping or rebuilding items without understanding risk of use
- Avoid the common “ugly = risky” determination

National Aeronautics and Space Administration

Parts and printed circuit boards

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

Parts and reliability testing

- Testing of parts can inform reliability prediction and establish certain quality measures
- Reliability of parts is established by volume of production, feedback from field usage, statistical process control, and in-process quality controls
- Practically speaking, reliability testing of parts does not in general establish long-term reliability
- Accelerated testing may be used for prediction but might provide a poor estimate for properly derated part operation
  - For many part types, especially passives, operation below a particular stress level will never activate a wearout or failure mechanism

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. 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.**

*radiation requirements must be addressed based on circuit design, shielding, and usage rather than individual part performance

MIL-SPEC parts

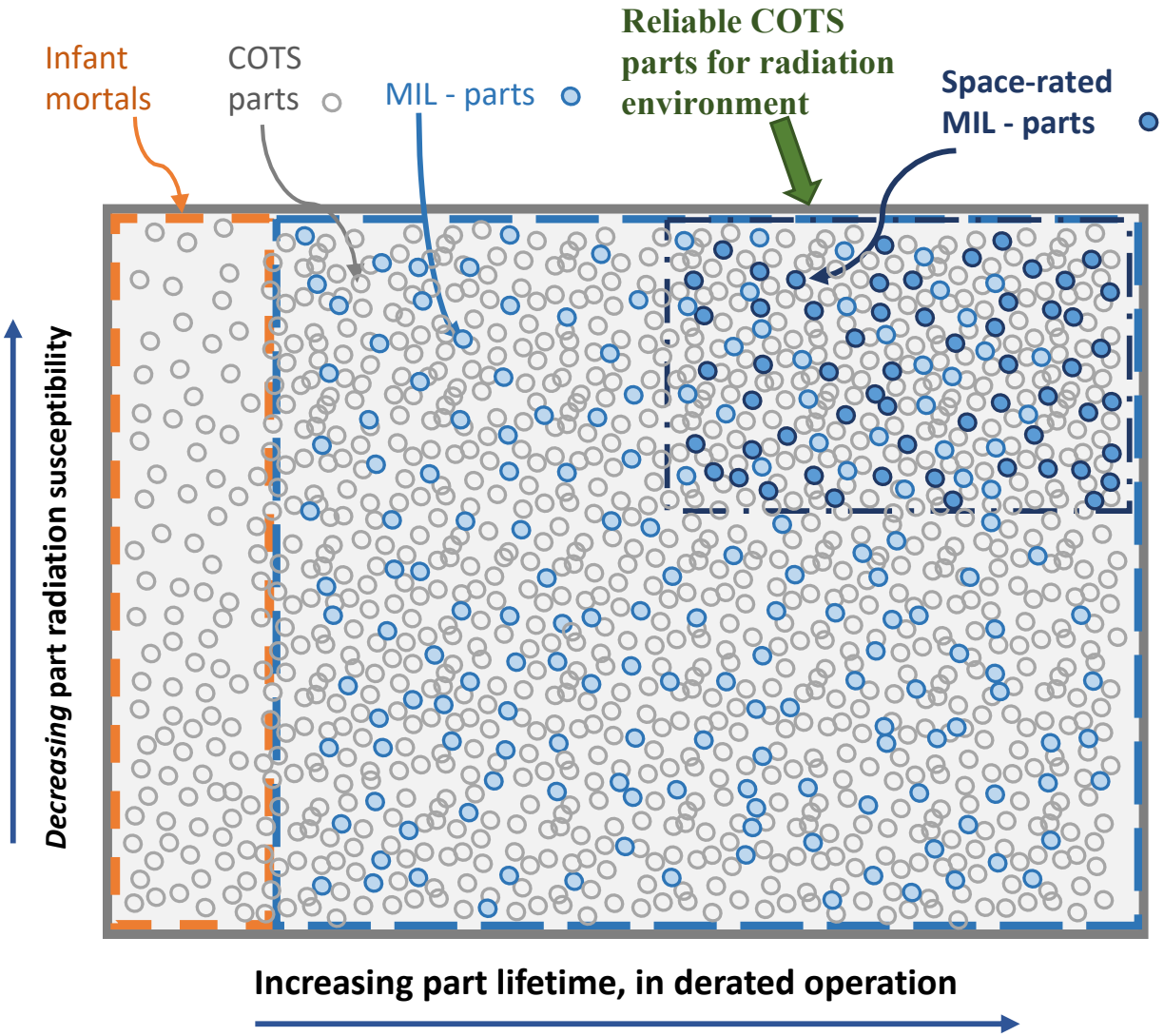
- Originated in DoD out of the need for tight uniformity and interchangeability of parts across the world
- Quality specifications were defined to cover the most extreme range of conditions
- The government controls the drawings, requirements, and specifications of such parts.
- Reliability is often 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.
- **In general, 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 regular reliability testing to assure reliability; however, the reliability is of minimal relevance to typical use and does not address periodic flaws that escape the MIL-SPECs that actually result in failures

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



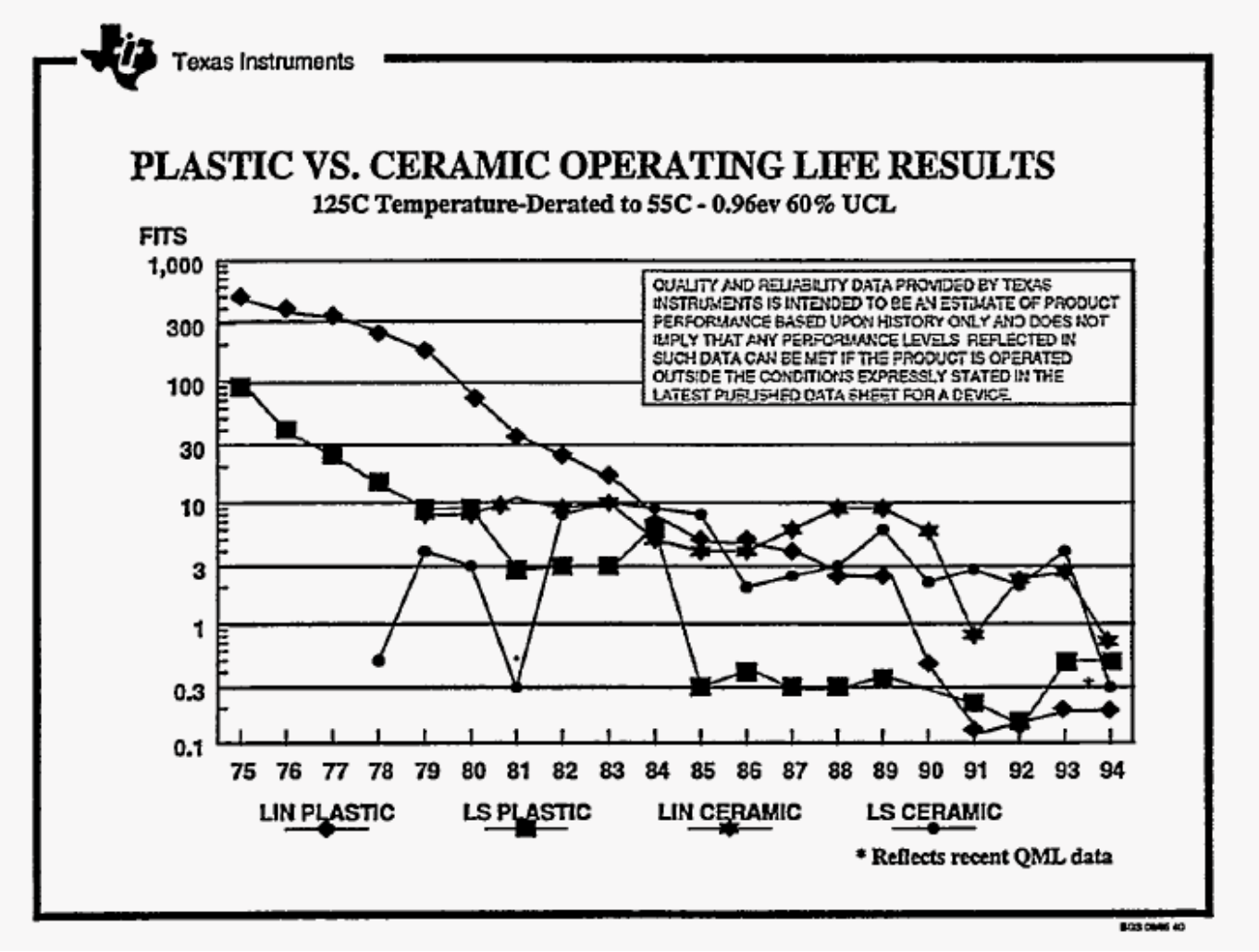
Why have COTS been perpetually deemed "unreliable" or "low-grade"

- 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

Origin of the space grade part

- 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.

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

Radiation: what do we care about?

1. How a part performs in a worst-case exposure in a radiation chamber (i.e., guaranteed minimum dose to single-event resilience)
   - Rad-hard (i.e., radiation-hardness-assured) parts are the answer
   - Wafer-lot-specific radiation testing of non-RHA parts

2. How parts perform in a circuit within a spacecraft or instrument in space
   - Radiation-tolerant circuit designs/circuit protections
   - Shielding
   - Operational constraints
   - Experience with susceptible part types in the environment
     - CMOS/MOSFETs
     - Processors
     - Memory
     - etc
   - Testing to fill gaps for unknown parts

Traditional space approach: "1 is needed for 2" will freeze us in the past as *oldspace*

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, including “rad-hard by design” techniques
  - Protect and derate your MOSFET!
  - 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
- **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.**

Conclusions on COTS vice MIL-SPEC

- 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
- Furthermore, the arbitrary use and definition of the term COTS across manufacturers exacerbates the confusion about reliability of COTS parts
- Unfortunately myths, misunderstandings, and misleading statements have unjustifiably pigeonholed COTS into a high-risk category over the years.
- The trade is statistical process control over high volume and current manufacturing and technology capabilities vs older processes, constrained technology, and lot-based control

Printed circuit boards

- Quality levels
  - Class 1 (general electronics)
  - Class 2 (dedicated service electronic products)
  - Class 3 (“high-reliability” electronic products
  - Class 3/A or “S” (space-grade electronics)
- Nonconformances
  - How do they link to risk?
    - Is there a credible failure mechanism?

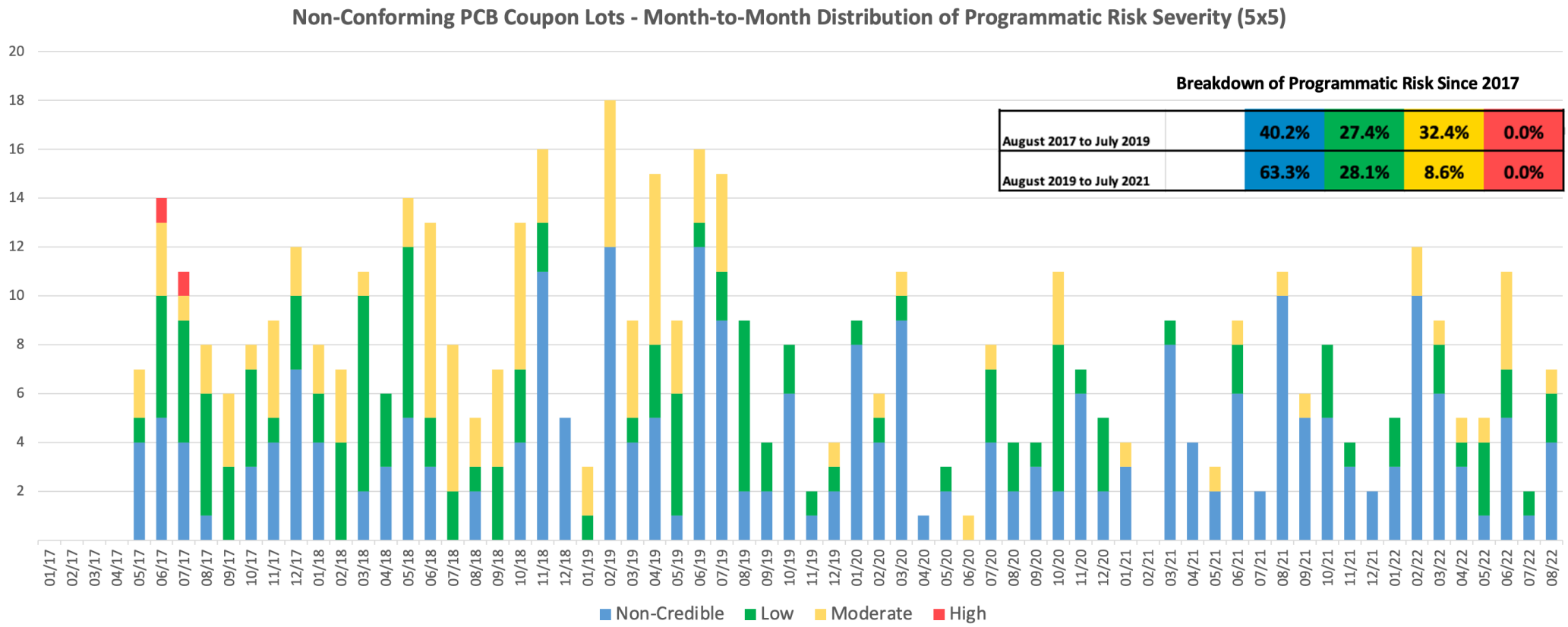
There is no broad correlation between quality levels themselves and reliability or lifetime; however, some vendors do not put in the same effort to produce a working product for Class 1 and Class 2 builds as they would for 3 or higher. Around 20% of nonconformances result in elevated risk of failure.

PCB specifications and reliability

- As with hermeticity, many workmanship requirements, and various other specifications, PCB specifications (verified by coupon analysis) are largely in place to assure reliability during ground-testing
  - Coupon nonconformances that do involve elevated risk largely indicate programmatic risk (a potential failure during testing).
  - Except in some very remote circumstances, technical risk due to common nonconformances would only come about if system testing (in particular TVAC) is limited or if telemetry is not sufficiently monitored during testing.
  - Within the first 100 hours of vacuum testing, the moisture is drawn out of the board, exposing undesired conductive paths
- Under the constraints and limited capacity for overrun of Class C missions and below, the programmatic risks associated with the coupon process itself outweigh the programmatic risks bought down by the process, which is why GSFC-STD-8001 recommends no independent coupons for Class C and below (vendor/developer coupons used as standard practice are expected). The "no independent coupons" for Class C and below is NOT to allow more risk.

The typical result of overindulgent piece-part practices for Class C and below is the reduction of back-end processes (thus increased mission risk) or cancellation

Month-to-Month NC Coupon Risk Severity (Programmatic)



Component vs Piece-part reliability

- Often we have put an emphasis on piece-part quality (per traditional definitions) over component reliability
- Reliability is established by volume and control of quality
- The most reliable system is the one that has flown the most times successfully as a system
  - Changing piece parts, materials, or processes internal to an established system will simply negate the established reliability
- If a full spacecraft has been proven reliable, then there is no valid basis to change what has been proven
  - Verification of quality controls and consistency at the manufacturer assure reliability of future systems.
- Never let piece part concerns outweigh proven system reliability, unless the piece part concerns involve a change in the part, in the usage of the system, or the environment.
- Piece part assessments are neither necessary or sufficient for the reliability of a system

Lessons learned from recent mission failures

- Neither part upscreening or use of MIL-SPEC parts provides protection against a poor or overly-sensitive design, i.e., “high-reliability parts” do not mitigate risks of a weak design. Furthermore, there is no longer a clear distinction in general between a “high-reliability” part and a “low reliability” part.
- There is no indication that any level of part screening affects mission reliability or lifetime
- Components that have demonstrated performance issues tend to continue to do so
  - In some cases proper context indicates problem areas (e.g, temperature profile)
  - Some tend to skew the overall reliability estimates for particular component types (e.g., RWA)
- Over-reliance on piece-part level screening or use of MIL-SPEC parts leaves an opening for manufacturing flaws not addressed by the MIL-SPECs
  - One unique parts manufacturing issue led to major anomalies or failures on at least four missions, for Level 1-compliant MIL-SPEC parts
- A weak linkage between mission operations activities/teams and engineering development and testing teams can leave a hole for a repeat of problems
  - When an on-orbit part failure is indicated with confidence on-orbit, the development and testing records for the parts in question should be reviewed as a top priority
- Beware of agendas that may be in force from subject matter experts on ARBs
  - Be sure that the caveats associated with failure theories are understood
  - Be sure that there is a clear rationale for de-prioritizing open items on the fishbone or cause tree
- Take note of and capture risks for items with unexplained out-of-family performance in I&T
- A smart use of fault-tolerance can go a long way when parts or components are used that have a spotty or uncertain history

Hearts, minds, and culture

- When mission success has prevailed and processes have remained the same for decades, it is hard for people to conceive that change is in order
  - Not everyone understands that in almost every significant field continuous improvement and the perpetual need to do more with less are essential
  - In some cases we don't recognize or appreciate the changing world around us or that we may be in process of being surpassed.
- Change has been a long haul, especially for Class B national asset missions because for practices that have long been perceived as critical for mission success, a "money is no object" approach has been taken with the perception that the risk and financial impacts of those processes are as simple as "essential to reliability" and "a small percentage of the budget"
  - In some cases, no amount of data, analysis, and overall evidence are sufficient to change the culture
  - Of course there is a comfort that if I do what we've always done and we fail, then I am covered, but if I am part of a change that is perceived as trying to save a few pennies, then I will be blamed
  - Some change will have to be forced through and stakeholders, customers, and developers must all contribute to the change.

Summary and thoughts

- Producing and putting into service reliable hardware involves a holistic approach involving good design, good assurance practices, good testing practices, good component and material usage, risk management, and sound review.
- But just as importantly it is aided by a strong infrastructure and culture in which designers are trained and mentored by experienced engineers, and who understand the tasks at hand.
- In order to be cost-effective, efficient, and to operate at the lowest overall level of risk, be sure that processes employed are based on substantive understanding of risk rather than traditional processes
- Overattention to piece parts without a basis and understanding of substantive risks in a highly constrained project will tend to draw resources away from back-end testing and problem-solving efforts, and may increase the chances of a premature failure.

National Aeronautics and Space Administration

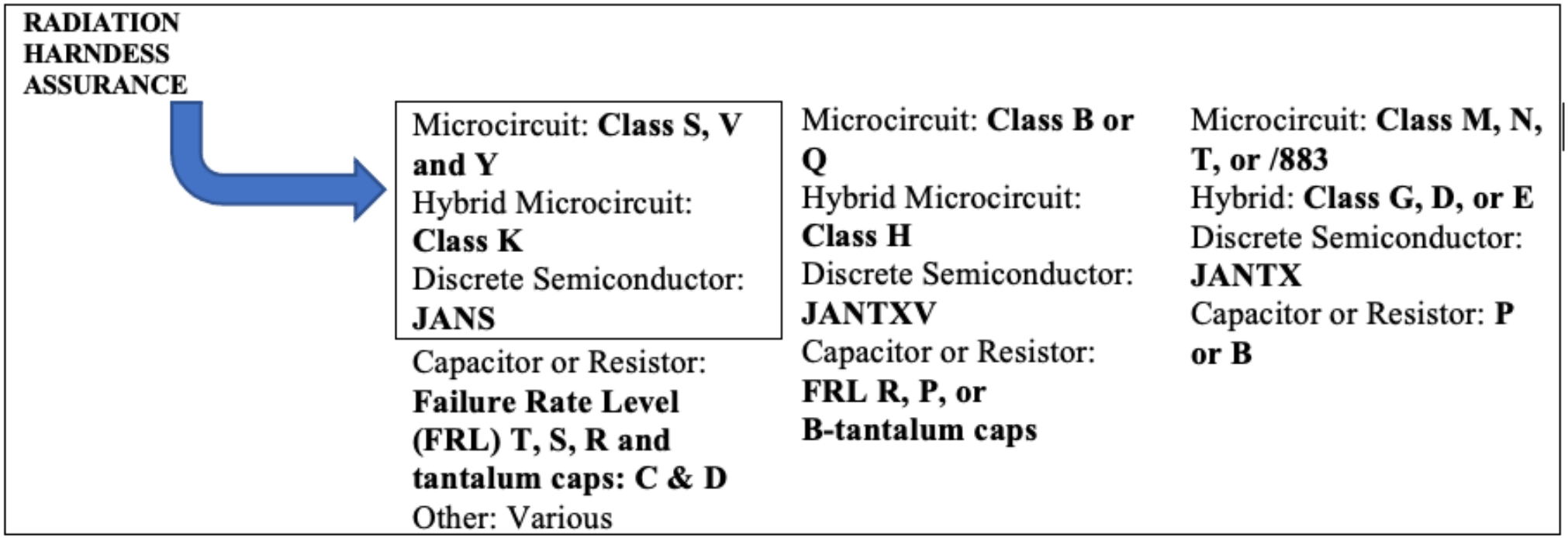
BACKUP

www.nasa.gov

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

MIL-SPEC RHA



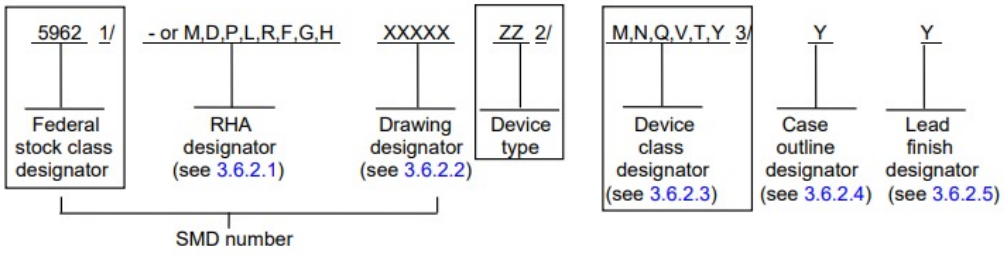
MIL-SPEC RHA subset. Note that V, Y, K, and JANS parts are not required to have radiation hardness assurance guarantees.

MIL-SPEC RHA cont'd

3.6.1 Index point. The index point, tab, or other marking indicating the starting point for numbering of leads or for mechanical orientation shall be as specified in the device specification and shall be designed so that it is visible from above when the microcircuit is installed in its normal mounting configuration. The outline, or solid equilateral triangle(s), which are used as an electrostatic identifier (see 3.6.7.2), may also be used as the pin 1 identifier.

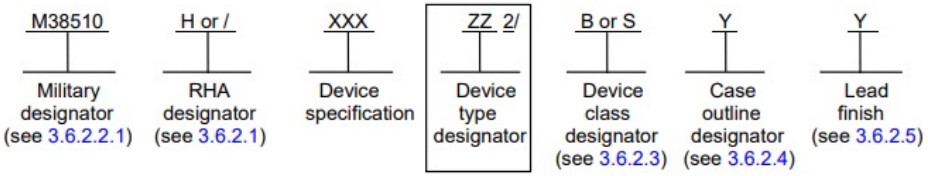
3.6.2 Part or identification number (PIN). Each QML microcircuit shall be marked with the complete PIN. The PIN may be marked on more than one line provided the PIN is continuous except where it "breaks" from one line to another. As of revision B of MIL-PRF-38535, several types of documents are acceptable for use when specifying QML microcircuits. They are MIL-M-38510 device specifications and SMD. The PIN marked on those parts under QML shall be the same as when supplied by the manufacturer prior to being listed on the QML-38535. The "Q" or "QML" designator combined with the listing of that PIN on a particular vendors QML listing shall indicate the fact that the manufacturer of the device is QML certified and qualified for the processes used to build that product. The PIN system shall be of one of the following forms, as applicable to the SMD or MIL-M-38510 device specification used for production:

a. SMD PINs shall be as follows:



For packages where marking of the entire SMD PIN and all other required topside markings are not possible due to space limitations, the manufacturer has the option of leaving the "5962-" off the marking. The allowance for optional marking will be indicated in the individual SMD. For RHA product using this option, the RHA designator shall still be marked.

b. Device specification documents, originally published prior to 27 July 1990, shall be as follows:



All new PINs specified by new documents, originally published after 27 July 1990, shall be in accordance with the one part-one part number system.

All PINs specified by existing device specifications with the number assigned prior to 27 July 1990, may use either the original assigned PIN or the one part one-part number system with the first two digits in the drawing designator being "38" and the last three being the device specification number (e.g., M38510/00101BAC shall become 5962-3800101BAC).