National Aeronautics and Space Administration

SMA for highly constrained projects

Jesse Leitner, Chief SMA Engineer
NASA GSFC
Jesse “dot” “Leitner” at “nasa.gov”

Adapting Mission Assurance Workshop

Nov. 14, 2024

CLEARED FOR PUBLIC RELEASE

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

Outline

- What is a constrained project?
- Top priorities
- What is quality and why do we care?
- The two sides of quality
- Quality vs Reliability
- Streamlined reliability
- Risk
- Modernizing Risk Classification
- SMD Class D MAR
- EEE/EEEE parts

Top Priorities for constrained projects

- Safety first*
  - Do not injure people or the public
  - Do not damage your host
  - Do not cause collateral damage
  - Do not damage the environment
- Protect your ability to learn from failure and success
  - In many cases this should be higher priority than meeting other mission objectives
  - Think about how you can maximize the assurance that you'll obtain enough data to figure out what happened
  - Develop a notional "black box"

*damaging yourself is in the realm of "hardware safety" but it is in the category of programmatics, design, and reliability, not safety, since it is not more important than designing and testing a reliable system (e.g., if you bolt yourself into your car it might protect you in a collision, but if your car catches fire or you fall into the lake …)

What is a constrained project?

- A constrained project is one that doesn't have the time and/or money to perform all traditional practices
- Many constrained projects do not start out as constrained
- Most D and below projects are constrained at the start.
- Even Class A missions often move into this category late in development

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

Two sides of quality

- Features of the product
  - This is the essential element of quality because it represents the system in front of you
  - Determined by observation and testing to the extent possible
- Paperwork to show it
  - Certifications
  - Certificates of conformance
  - Test data with signatures
  - WOAs and travelers
  - This provides confidence in internal and ”molecular” aspects that could be the source of various types of latent defects
  - This is for the trust part. You can either trust or require paperwork, or a mix of both
  - Paperwork itself is never sufficient to guarantee a high level of quality

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.

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

Streamlined reliability highlights

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

Costly processes with minimal mission risk 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: enforcement of stringent requirements with minimal effect on performance or lifetime.
- Part-level radiation testing of every part and specific lot used

Cost-effective variants for low-risk mission

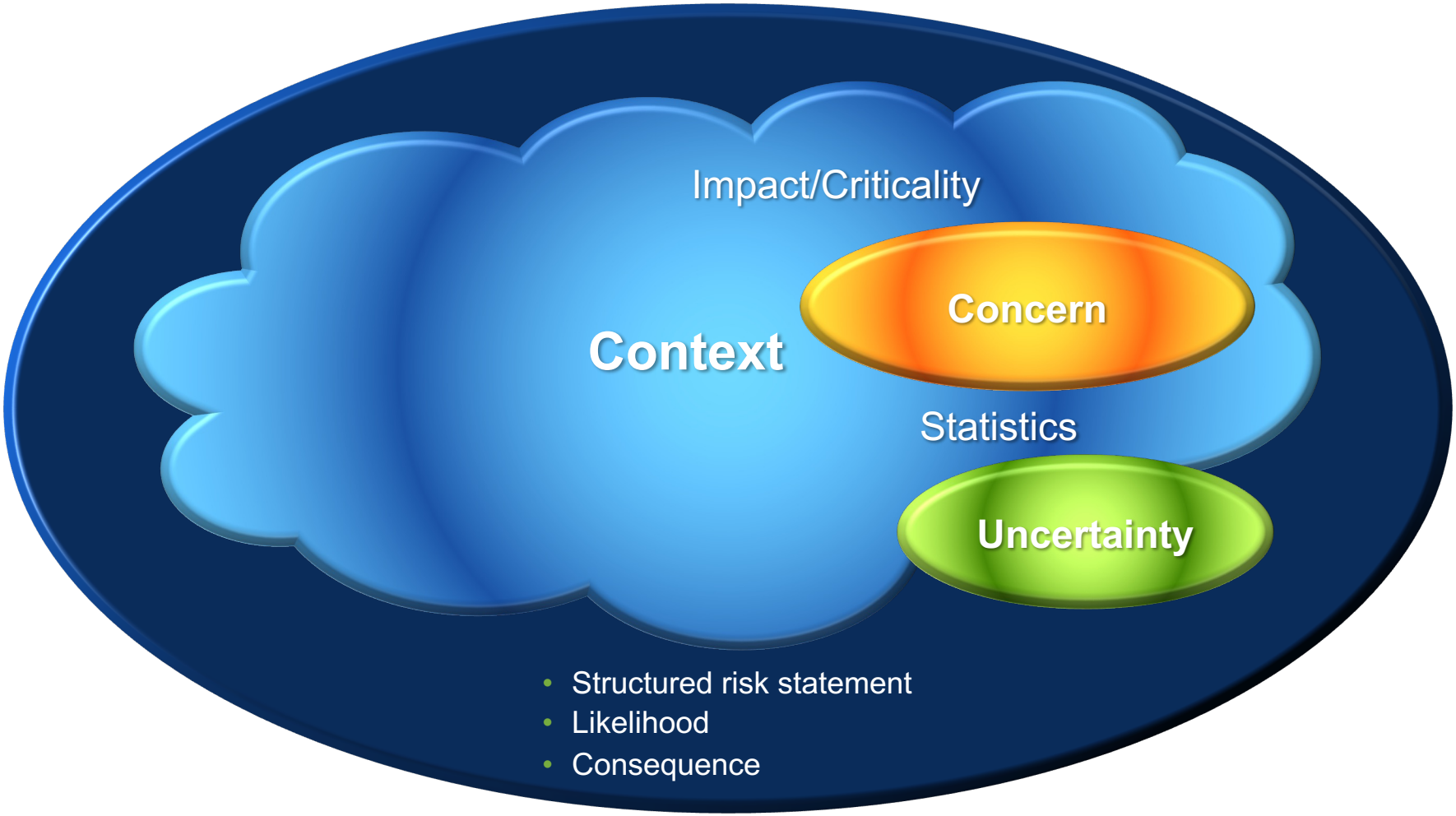
- Fault-tolerant and resilient architecture
  - Design to accommodate failures but don't design to expect failures
- Perform robust risk management with strict interpretations of risk
  - Risk should always have context
  - Concern/worry list may be maintained without context
- Extensive but intelligent 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

What is Risk?

- Definition: the combination of
  - a) the probability (qualitative or quantitative) that an undesired event will occur, and
  - b) the consequence or impact of the undesired event
  - c) a factual context or scenario that exists to cause the risk to be present
  - In short, risk is an expectation of loss in statistical terms based an existing condition.

- Categories of risk (consequences)
  - Technical (failure or performance degradation on-orbit)
  - Cost ($ it will take to fix the problem) } programmatic
  - Schedule (time to fix the problem)
  - Safety (injury, death, or collateral damage)

Anatomy of a Risk



What is risk classification?

- Establishment of the level of risk tolerance from the stakeholder, with some independence from the cost
  - Cost is covered through NPR 7120.5 Categories
- If we were to try to quantify the risk classification, it would be based on a ratio of programmatic risk tolerance to technical risk tolerance
  - For Class A, we take on enormous levels of programmatic risk in order to make technical risk as close to 0 as possible. The assumption is that there are many options for trades and the fact is that there must be tolerance for overruns.
  - For Class D, there will be minimal tolerance for overruns and a greater need to be competitive, so there is a much smaller programmatic risk "commodity" to bring to the table
- The reality is that the differences between different classifications are more psychological (individual thoughts) and cultural (longstanding team beliefs and practices) than quantitative
- In the newly released NPR 8705.4A, the practices associated with classifications are denoted "expectations", not formal requirements, not requiring waiver, but rationale for deviations to stakeholders in an "Assurance Implementation Matrix"

Risk Classification
(NPR 7120.5 Projects)

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

Risk Classification (GSFC)
(Non-NPR 7120.5 Projects)

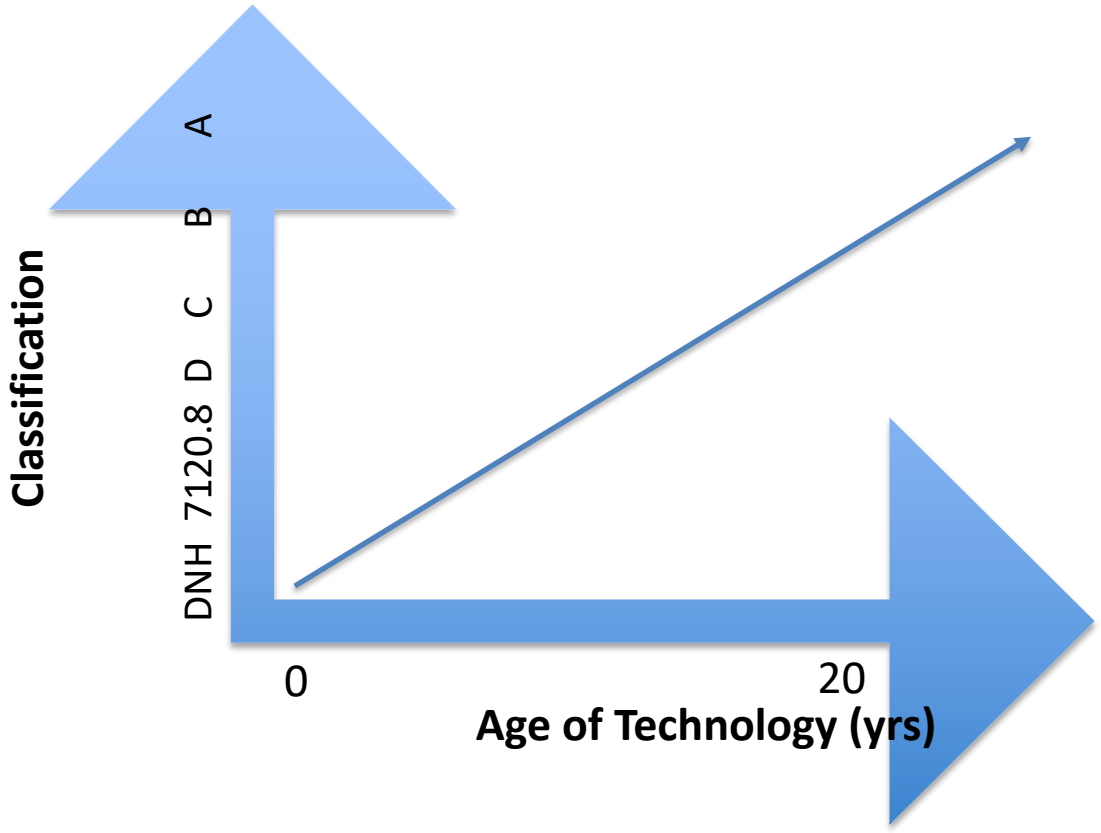
- **NPR 7120.8 "class" – Allowable technical risk is high**
  - Some level of failure at the project level is expected; but at a higher level (e.g., program level), there would normally be an acceptable failure rate of individual projects, such as 15%.
  - Life expectancy is generally very short, although instances of opportunities in space with longer desired lifetimes are appearing.
  - Failure of an individual project prior to mission lifetime is considered as an accepted risk and would not constitute a mishap. (Example: ISS-CREAM)
- ***"Do No Harm" Projects –*** If not governed by NPR 7120.5 or 7120.8, we classify these as "Do No Harm", unless another requirements document is specified
  - Allowable technical risk is very high.
  - There are no requirements to last any amount of time, only a requirement not to harm the host platform (ISS, host spacecraft, etc.).
  - No mishap would be declared if the payload doesn't function. (Note: Some payloads that may be self-described as Class D actually belong in this category.) (Example: CATS, RRM)

7120.8 and "Do No Harm" Projects are not Class D

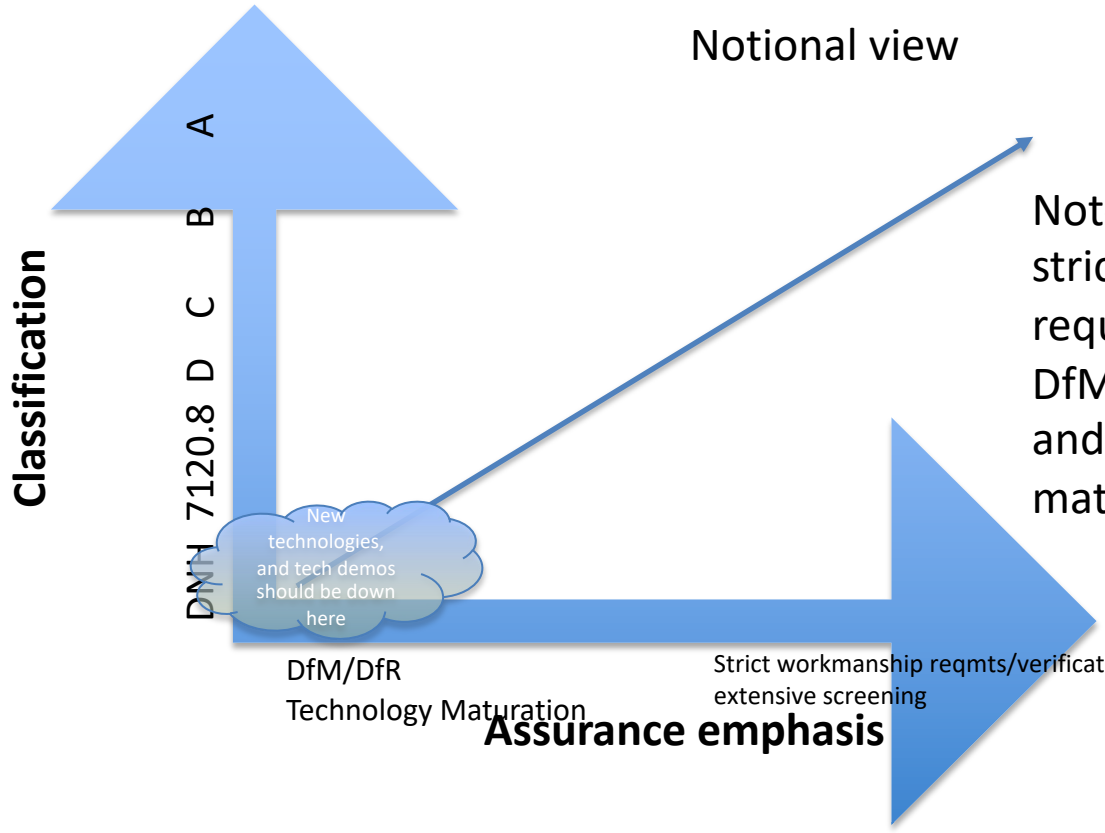
The left-hand-side vs right-hand-side

- The *left-hand side* of risk classification represents the mission attributes that are used to classify a mission, such as
  - National/science priority
  - Limited flight opportunities (e.g., planetary windows)
  - Cost
  - Lifetime
  - Partnerships
- The *right-hand side* of risk classification represents the recommended practices, based on the assigned classification
  - Workmanship
  - Parts approach
  - Printed circuit board approach
  - Etc
- In risk classification, the flow is only from left to right
  - The use of Class C practices does not indicate any type of lifetime
  - The use of Class A practices does not indicate any type of priority
  - Etc.

Risk Classification vs Technology state of the art



Risk Classification vs Assurance Methodology Focus



Note: application of strict workmanship requirements supplants DfM and DfR efforts, and hinders technology maturation.

Summary of expected assurance practices

Practice	A	B	C	D	7120.8/DNH
GMIPs	Extensive	Extensive	Limited	Minimal	Almost none
ARB/FRB/MRB voting	Voting on all	Voting on major	Participating	Participating	Open
EEE parts	Level 1	Level 2	Level 3	COTS	COTS
PCB reqmts	DS, ES, 3/A	DS, ES, 3/A	D, E, 3	D, E, 3	Class 2 or 3
PCB coupons	Independent	Independent	Supplier only	Supplier only	commercial
SPFs	Fully redundant	Mostly redundant	Selective redundancy	Mostly single string	Mostly single string
workmanship	S	S	No S	No S	commercial
Radiation	Lot-specific TID testing for SPF parts or board-level testing in high TID +rad-tol-design	Strategic testing, board level testing + rad-tol design	Rad-tol design, limited piece part approvals when board level analysis or testing not available	Rad-tol design, no piece part approvals	Based on lifetime and environment
Lifting	Standard suite of 6 practices	Standard suite of 6 practices	Standard suite of 6 practices	Vendor practices	Vendor practices

Top level comparison of select practices

	Class D/7120.8/DNH	Class B
Env test	TAYF, small margins. Ex: EMI-self-compat	TAYF + bullet proof + high margins. Ex: EMI-CS testing
Parts	Commercial, no extra screening	Screened to level 1 and 2 (extremely costly)
Workmanship	Use of experienced techs	Following strict requirements
Quality inspection	Minimal, selective	Extensive and intrusive
Printed circuit boards	Best effort Class 2 and 3	Class 3/A, DS, strict interpretation
Developer practices and oversight vs insight	Use of developers' own practices and commercial practices, selective insight	Discouragement of commercial practices, highly prescriptive, extensive oversight
MRB/ARB/FRB	Developer runs, NASA participates	NASA has voting/override authority

Oversight vs insight

- Oversight is the approach where the NASA organization with management authority has approval rights for most major decisions with a project
  - Requirements are most prescriptive
  - Inspections are most extensive
  - NASA personnel are voting members of the various boards
  - Workflow is often stopped for approval
  - Oversight is in conflict with most forms of commercial practices and, in fact, generally prevents the use of commercial practices
  - Well-aligned with cost-plus contracts
- Insight is the approach where the NASA organization with management authority has access to information about the work being performed and is invited to participate in discussions involving various unplanned activities but does not approve decisions
  - Requirements are more objectives-based
  - Inspections are very limited
  - NASA personnel participate on boards but don't approve decisions
  - Well-aligned with fixed price contracts.
- Generally A&B missions are aligned with oversight, while C&D missions are aligned with insight, whether it is purposeful or not.

Note on choosing elevated practices

- Choosing Assurance levels above the recommended levels for the given classification should be undertaken only with a careful risk-trade analysis as such an approach is not as simple as “paying a bit more for more reliability”.
  - Practices that exceed the available resources are likely to drive up programmatic and technical risk by reducing the resources available to complete the most important elements needed for success – finishing the test campaign and thorough resolution of problems encountered in integration and test.
  - Furthermore, such practices often involve overtesting or unrealistic testing that may prompt irrelevant failures or actual overstressing of flight hardware.
- The practices that involve greater levels of workmanship controls, restrictions on parts and materials, and inspection generally conflict with the technology maturation process (which requires flexibility and responsiveness to testing results and problem resolution).
  - Therefore, the importance of a technology demonstration or a mission that involves immature technologies is not an appropriate justification for selecting more stringent assurance activities in most areas.
  - In these cases, the assurance emphasis should be placed on design for manufacturability and design for reliability, as opposed to screening, workmanship controls, and inspection.

Current Risk Classification limitations and shortfalls

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

We are incentivizing continued use of old piece-part-centric practices rather than finding efficient, innovative, modern approaches of developing reliable missions

Risk Class vs Design Lifetime vs Lifetime

Mission	Year	Risk Class	Planned Lifetime	Actual lifetime	Why ended
EO-1	2000	C	1	17	fuel expended
GOES-L	2000	A	10	10	outdated
TDRS-H	2000	B	11	22+	active
NOAA-L	2000	C	2	13	"critical anomaly"
GOES-M	2001	A	5	12	thruster issues
Aqua	2002	A	6	20+	active
NOAA-M	2002	C	2	11	two instruments failed
TDRS-I	2002	B	11	20+	Valve issue, took 6 months to get to GEO
RHESSI	2002	D	2	16	communication problems
TDRS-J	2002	B	11	19+	active
ICESat	2003	C	3	7	laser failure
Aura	2004	B	6	18+	active
Neil Gehrels Swift	2004	C	2	17+	active (thermoelectric cooler failed shortly into mission, but successful operational workaround was put in place)
NOAA-N	2005	C	2	17+	active
GOES-N	2006	B	10	16+	active (USSF now)
ST-5 (3 S/C)	2006	C	90 days	100 days	demo complete
Fermi (GLAST)	2008	C	5	14+	active
GOES-O	2009	B	10	10	replaced (now on-orbit spare)
NOAA-N'	2009	C	2	13+	active
LRO	2009	C	3	13+	active
GOES-P	2010	B	10	12+	active
SDO	2010	B	5	12+	active

Glory	2011	C	3	0	launch failure
NPP-Suomi	2011	B	5	10+	active
TDRS-K	2013	B	15	9+	active
MAVEN	2013	B	2	7+	active
LandSat-8	2013	B	5	9+	active
LADEE	2013	D	100 days	223 days	objectives completed
TDRS-L	2014	B	15	8+	active
GPM	2014	B	3	8+	active
DSCOVR	2015	D	2	7+	active
MMS (4 S/C)	2015	C	5	7+	active
SMAP	2015	C	3	7+	Primary radar payload failed 7 months into mission – SEGR in the SAA, but team was able to get most science from the radiometer
GOES-R	2016	B	15	6+	active
OSIRIS-REx	2016	B	7	5+	active
ASTRO-H	2016	C	3	0	attitude control failure
NICER	2017	D	1.5	5+	active
JPSS-1	2017	B	7	4+	active
TSIS	2017	C	5	4+	active
TDRS-M	2017	B	15	5+	active
GOES-S	2018	B	15	4+	active
GEDI	2018	C	2	3+	active
ICESat-2	2018	C	3	3+	active
Solar Orbiter	2020	C	7	2+	active
JWST	2021	A	7	0+	active
Lucy	2021	B	12	0+	active
LCRD	2022	D	2	0+	active
GOES-T	2022	B	15	0+	active

New elements in GPR 8705.4A

- Standard component classifications based on the most recent number of times a component/assembly/system operated successfully for a certain number of years out of the total number of attempts
- Collective mission classification of multiple classified identical items

Standard component classification in GPR 8705.4A

- Components (assemblies through full spacecraft buses) classified holistically based on most recent performance at commensurate lifetimes
  - No piece-part-based Ps
  - Changes do not affect classification (changes, different environments, minor anomalies, etc. factor into acceptance, not classification)
- Class A components
  - Minimum 10 recent flights at 7-year lifetime or longer, number of successes out of last 20 flights divided by 20 >= 0.95 (or 100% for between 10 and 19 flights)
- Class B components
  - Minimum 10 recent flights at 5-year lifetime or longer, number of successes out of last 10 flights divided by 10 >= 0.90
- Class C components
  - Minimum 5 recent flights at 3-year lifetime or longer, number of successes out of last 5 flights divided by 5 > 0.80
- Class D components
  - Fully qualified per the GEVS requirements in the GOLD rules

While this is not a formal reliability calculation (which would require mission specific data), it provides strong evidence of a reliable design

Collective classification of multiple identical standard products

- There is a growing number of mission concepts that involve the use of multiple products such that one or more can fail, while still meeting mission performance requirements
- The extreme version of this involves missions that for various reasons would prefer (or even require) multiple spacecraft in lieu of one large spacecraft, but cannot afford the resources required for more than one spacecraft at the mission risk classification
- The only way to "raise" the classification through collective use of the same product is if the base product design has a formal classification that is based on some measure of reliability.
- To compute the classification of a collection of the identical objects, start with the following point reliability estimates
  - B: 0.9
  - C: 0.8
  - D: 0.66
- Next, use standard combinatorial reliability techniques to calculate a combined recent reliability estimate
- Finally, determine the collective classification based on the standard component reliability definition, considering past mission lifetimes and overall score

Findings

- The only connection between risk classification and lifetime is the fact that a small subset of Class C and D missions are fundamentally limited in utility or funding to operate
- While design lifetimes are generally driven by radiation, no mission lifetimes were limited by radiation, even though most missions have lasted 3 or more times their design lifetimes
- GSFC failed to recognize the enormity of the Swift mission results
  - First GSFC mission to fly a large percentage of COTS parts (~40%)
  - Sense at the time was that the mission would be lucky to last 2 years, based on parts and radiation
  - Mission parts level set at “3” and even after 17 years of operation with no parts failures* or notable radiation events, GSFC still considers level 3 *high risk* and only reserved for missions where failure is an option
  - No others have tried the Swift approach since and the results are often downplayed or simply ignored
  - There have been no on-orbit failures at all of level 3, level 2, or COTS parts used as is, even with extensive usage, but there have been several failures of level 1 parts (MIL-SPEC and upscreened COTS that were overtested) on-orbit.

*A thermoelectric cooler was DOA for undetermined causes

GMIPs are a risk trade

- As with most other SMA practices, GMIPs increase risk while buying it down
- The key is to have risk buy-down outweigh risk increase
- The more constrained the project the more likely GMIPs will result in a net increase in risk
  - Most importantly the following should be considered while imposing GMIPs on such a project
    - Criticality of the item (is the item itself a single point failure?)
    - Past experience with the product
    - Past findings on previous versions of the product
    - Past experience with the vendor/manufacturer
    - The potential to interrupt a development flow
- By definition, GMIPs cannot be performed on COTS products. If a GMIP is performed internal to a product, then the product is not COTS.

GMIPS: increasing vs decreasing risk

Decreasing Risk	Increasing Risk
Catch serious* nonconformances at the earliest possible stage	Interrupt development flow
Motivate the assembler to pay close attention to detail	Prompt rework for many nonconformances that do not entail risk
Document stages of development for future problem resolution	Prompt pre-emptive and sometimes undocumented rework
	Remove time available for completing testing and problem resolution
	Increase possibilities for pandemic exposure

**serious* meaning nonconformances that provide credible elevated risk of failure in testing or operation

Class D Principles: Dos & Don'ts

- ***Do:***
  - Streamline processes (less formal documentation, e.g., spreadsheet vs. formal software system for waivers, etc.)
  - Focus on tall poles and critical items from a focused reliability analysis
  - Tolerate more risk than A, B, or C (particularly schedule risk)
  - Capture and communicate risks diligently
  - Rely more on knowledge than *indirect* requirements
  - Put more decisions into the hands of the engineers on the floor.
  - Have significant margin on mass, volume, power (not always possible, but strongly desirable)*
  - Have significant flexibility on performance (level 1/level 2) requirements (not always possible, but strongly* *desirable)
- ***Don't:***
  - **Ignore risks!**
  - Reduce reliability efforts (but do be more focused and less formal)
  - Assume nonconforming means unacceptable or risky
  - Blindly eliminate processes

While the impression may be that a Class D is higher risk from the outside, if implemented correctly (and consistent with the intention), in reality the extra engineering thought about risk may actually reduce the practical risk of implementation.

*outside scope of MAR

National Aeronautics and Space Administration

SMD Class D MAR

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

Significant departures from common practices (1/3)

- Inherited items process
  - Allows a holistic, risk-based process based on
    - Prior history
    - Changes from previous (in H/W, S/W, operation, environment)
    - Past anomalies
  - Allows prior processes to be used without waivers
  - Decisions to use or impose additional tests, etc., based on risk
- GMIPs (consistent with NPR 8735.2B)
  - No predefined set of GMIPs
  - Based on upfront negotiation considering
    - assessment of developer's own inspection points
    - developer identified risks
    - project identified risks; and furthermore in response to events, such as failures, anomalies, and process shortfalls that prompt a need for further inspection.
  - Will be coordinated with the project to maximize efficiency and minimize schedule impact

Inherited items process principles

(apply to products used within their bounds and qualification ranges)

- Changing processes for a proven product is unlikely to improve, but more likely to degrade the product
- Changing processes for a proven product is most often not possible to do and doing so or attempting to do so will not only increase risk, but will substantially increase cost and development time
- GMIPs inserted into a standard build only cause a distraction from the standard build process and should only be attempted if there is a history of quality escapes that have entailed mission risk that GMIPs have caught for the product. Review of records for common standard components has not revealed any such escapes.
- Changing parts or part screening practices for a proven design or system will add both risk and cost to the system and likely will not be feasible
- Reliability analyses are needed only if a design is unproven
- The MAR requirements can be categorized as safety, quality, or reliability, but the purpose of quality requirements is to achieve reliability
  - Established standard products are already proven reliable and thus should not be assessed from a piece-part, one-of-a-kind design perspective

Significant departures from common practices (2/3)

- Workmanship
  - Workmanship standards (industry and NASA) provided as guidance, developer standard practices allowed
- EEE parts
  - Follows NASA-STD-8739.10 for Class D: Level 4 = COTS parts with no additional screening
  - Guidance provided to consider:
    - Prior usage of the part and qualification for the specific application
    - Manufacturing variability within lots and from lot to lot for parts
    - Traceability and pedigree of parts
    - Reliability basis for parts.
    - Parts stress/application conditions

Significant departures from common practices (3/3)

- Radiation
  - Emphasis on radiation-tolerant design
  - Part-by-part analysis and testing otherwise
- Printed Wiring Boards
  - Use own preferred standard
  - Project retains coupons or spare boards until mission disposal

Minor departures from common practices

- ARB/MRB/FRB
  - Government notified and invited to participate in type I (form, fit, function)
  - Type II – Government given access to, but timely notification not required
- Reliability
  - Project completes reliability analysis (e.g., FTA, FMEA) for faults that may lead to injury to personnel or the public, or produce orbital debris, or that may affect host platforms
  - Parts stress and derating analysis per EEE-INST-002 or comparable
- Software assurance
  - NASA-STD-8739.8 required
- Software safety
  - Safety critical elements determined from the hazard analysis and range requirements
- GIDEP: project shall take action to mitigate the effects of alerts on the project

Other elements

- Lifting
  - Vendor practices if command media exist
  - NASA-STD-8719.9 for all others
- ESD: ANSI/ESD S20.20-2007
- Lead-free and whisker controls required
- Assurance Plan for new digital electronic designs (FPGAs, ASICs, etc)
- Planetary Protection for outside of earth orbit
- Cybersecurity and Command Link Protection
  - FIPS 140-2 compliance (being superseded by NIST 800-53)
  - NASA-STD-1006A

What kinds of risks are acceptable?

- Those tied to compressed schedules and tight development constraints as long as there is a solid plan and acknowledgement of the challenging elements
- The use of new, modern, innovative approaches at development
- The use of yet-to-be-established standard or COTS components that are the only solution
  - Use of standard and COTS components outside of their qualified environment, or that are as of yet unproven when they constitute the only viable solution
    - Risk should be acknowledged with a plan for addressing or accepting
  - Note: Use of standard and COTS components that have been proven in the same environment for same time frame is lower risk than any piece-part assured approach
- The use of new select new technologies when necessary to advance science, with a viable plan for maturation and incorporation

National Aeronautics and Space Administration

EEE/EEEE parts considerations

www.nasa.gov

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

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 (in final independent comment disposition) 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. 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

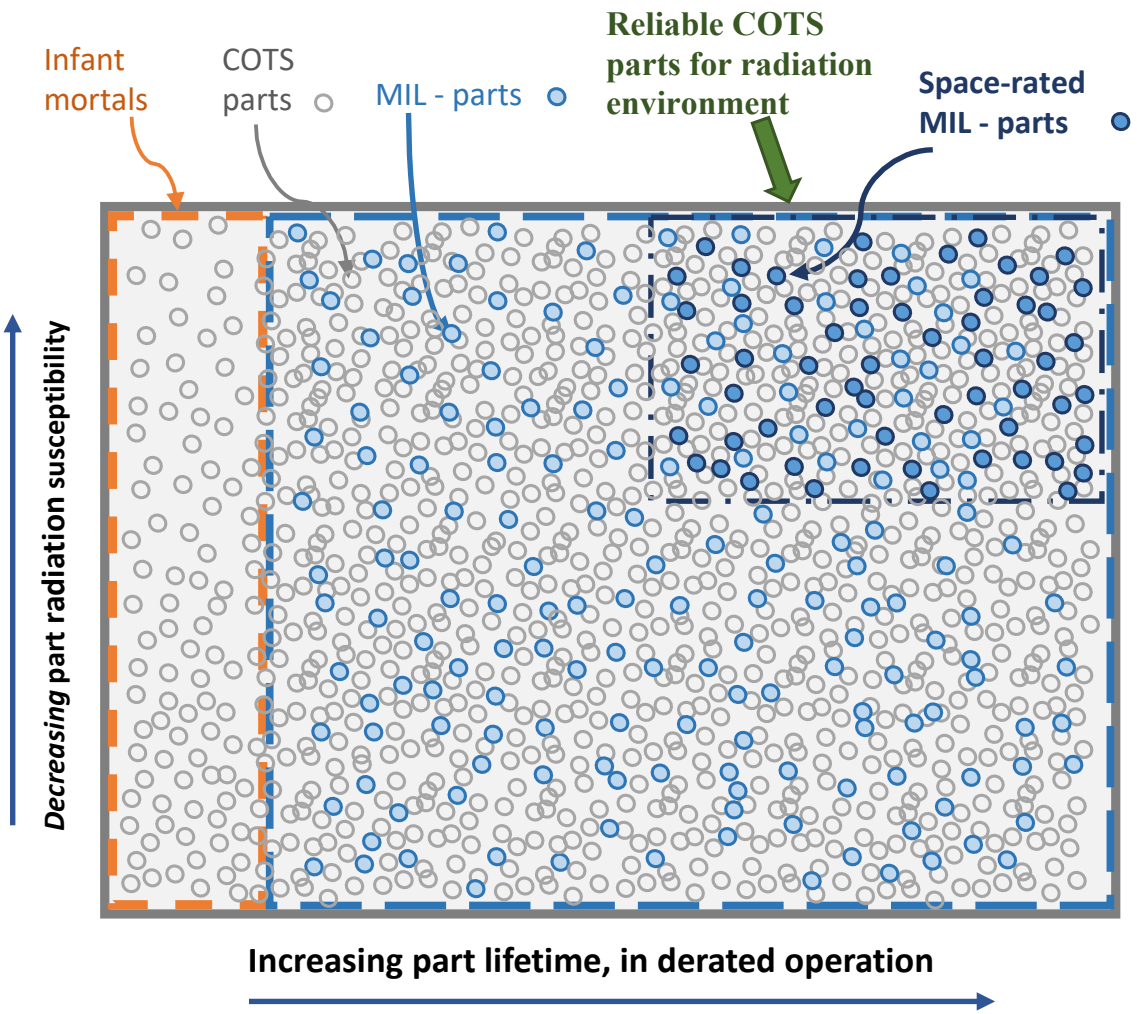
- Originated in DoD out of the need for tight uniformity and interchangeability of parts across the world
- Quality specifications were defined to cover the most extreme range of conditions
- The government controls the drawings, requirements, and specifications of such parts.
- Reliability is often 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.
- **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.

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.

Intelligent use of COTS parts

- Always use parts within the limits of their datasheets
  - Respect the datasheet!
- AEC-qualified parts (not just “for automotive use”) from leading manufacturers, produced under IATF 16949 will maximize reliability
- Use familiar parts when possible
- Avoid an approach that prompts you to use more parts as often happens with capacitors
- Conservative derating is good practice, but excessive and forced derating may result in need for many extra parts, a mass or space problem, or a weaker design with less margins.
- Use parts that the manufacturer declares to be for reliable use
- Use parts that have been established for over a year and in high volume production
- Buy parts from authorized distributors
  - There is no purpose in MIL-SPEC distributor restrictions when buying COTS parts
- There are many great options for “enhanced space” COTS parts for microcircuits and discretes
- Avoid requiring the tightest performance and tolerances from passive parts
- Strive for flexible resistance values (ranges) in current sensing applications
- Be sure that parts only offered with pure tin have matte tin finish, when available.
  - Give preference to manufacturers that use JEDEC tin whisker acceptance testing or similar approach
- Often increased performance and modern design and manufacturing drive increased reliability
- In some cases, you can only use what’s available against the guidance – accordingly assess and acknowledge the risk and explore reasonable mitigations

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 design practices
  - 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.**

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, 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

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.

Conclusions

- GPR 8705.4A includes some modernizing elements that begin to transform the philosophy of risk classification being largely about control of piece parts to one that considers holistic performance and reliability of system designs to classify them
- This approach enables GSFC, and ultimately NASA, to incentivize novel and innovative approaches to build reliable systems efficiently rather than to reward them for exercising traditional processes for piece-part control that may have little to no effect on the risk or reliability of the mission.
- Furthermore, it puts in place a technical foundation and structure to support the current wave of concepts that involve the use of multiple “lower-class” spacecraft to enable a higher-class mission.
- GPR 8705.4a is now baselined
  - Working with OSMA to institutionalize concepts at the Agency level

National Aeronautics and Space Administration

Example COTS space experiences

The SpaceCube

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE NASA Goddard

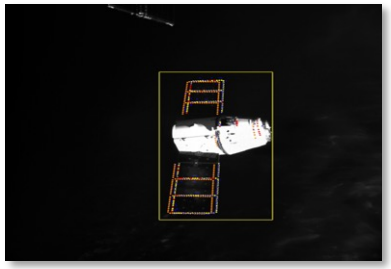
www.nasa.gov

Example: Raven Payload

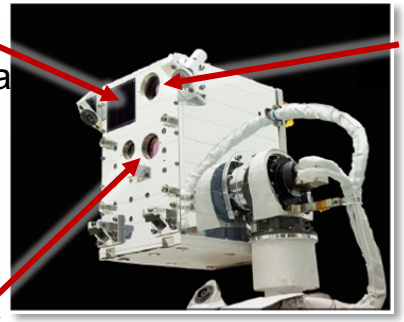
Objective:

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

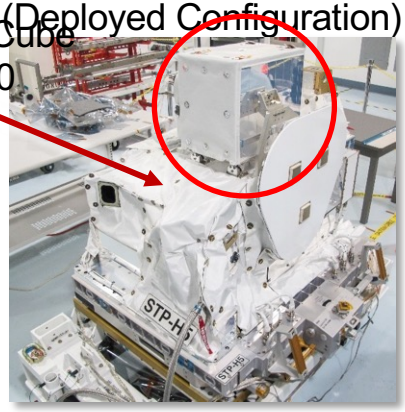


- Demonstrating that both cooperative and non-cooperative rendezvous can be accomplished with a single similar sensor suite



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.



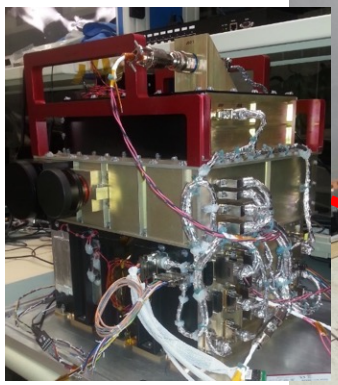
Raven installed on STP-H5
(Stowed Configuration)

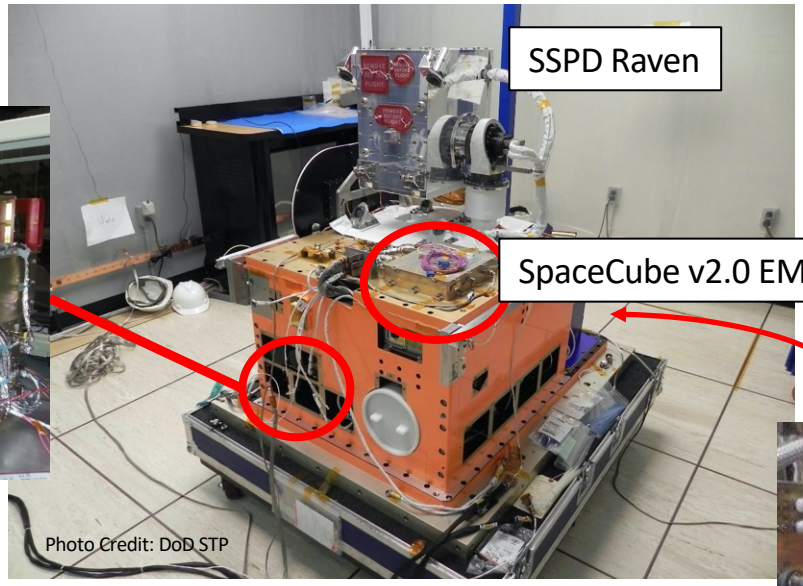
Cygnus Tracking

Example: STP-H5 ISS Payload

26% COTS Parts

ISEM, SpaceCube Mini





99% COTS Parts

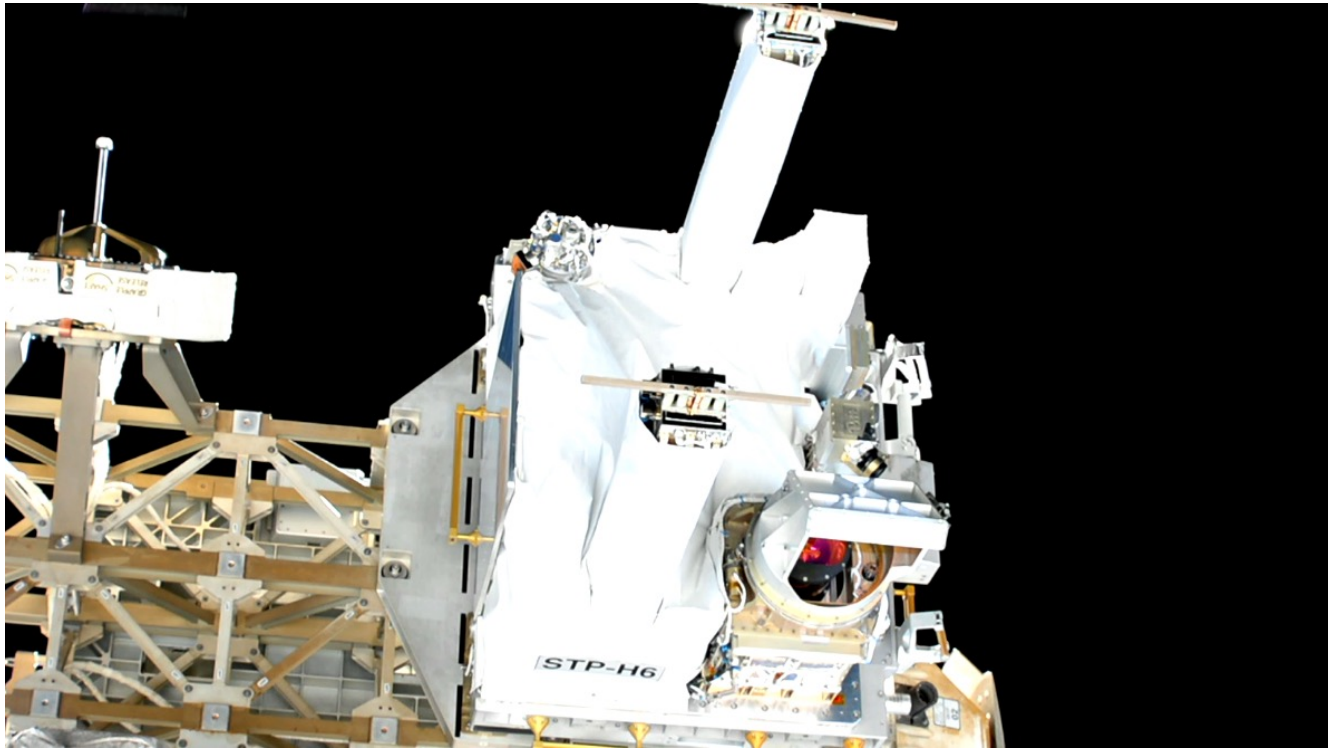
SpaceCube v1.0 CIB

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.

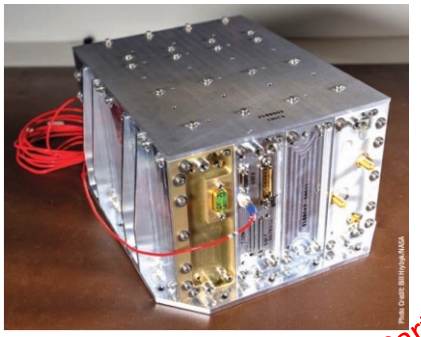
2/2017 - Current

Example: STP-H6 Payload



99% COTS Parts

SpaceCube v2.0 NavCube



1% COTS Parts

SpaceCube v1.0 CIB

SpaceCube Time-on-orbit (Oct 2021)

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
	Specific brand FPGAs	26
	Specific-brand 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

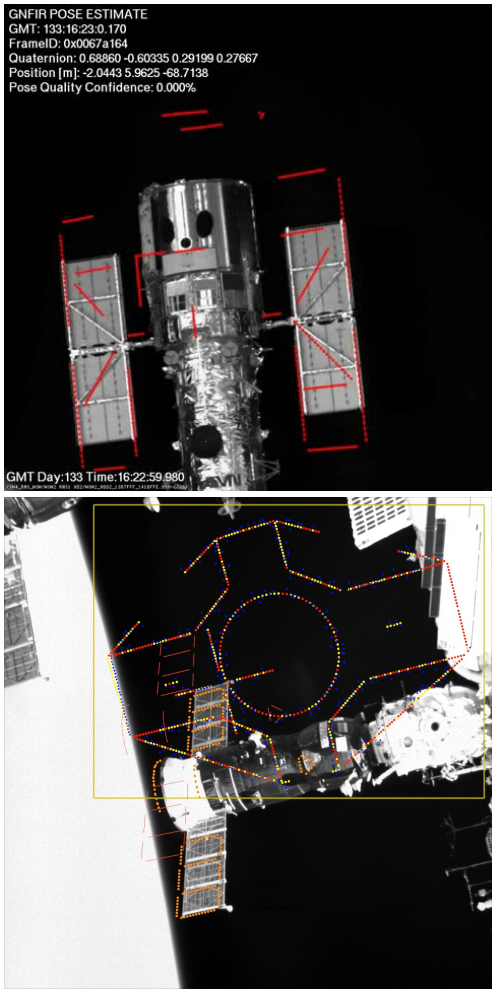
Application:
- Relative Navigation System
- Hubble Space Telescope Real-Time Tracking using 3x visual cameras

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



General principles for DNH projects

- **Avoid costly requirements that buy down little to no risk at high expense, such as**
  - EEE parts upscreening/MIL-SPEC parts
  - High-end printed circuit board reqmts
  - GMIPs without consideration of risk
  - Avoidance of commercial practices
  - Avoidance of new technologies
  - Strict workmanship requirements
  - Numerous protective barriers
  - Highly conservative practices (high cost and programmatic risk)
- **Freely depart from longstanding practices when they don't apply**
- **Do not place too much attention to piece parts, especially at the expense of system-level testing**
  - Use a "right-to-left" approach

Left-to-right vs Right-to-Left Development

- Left-to-right
  - Piece-parts-centric, broad requirements
  - System testing as resources remain
  - Least test-as-you-fly driven

Primary focus on resources put into Piece parts and screening

System test is subject to remaining resources

- Right-to-left
  - System test dominates
  - Use proven components as much as possible
  - Piece-parts focused on criticality and knowledge of parts
  - Most test-as-you-fly driven

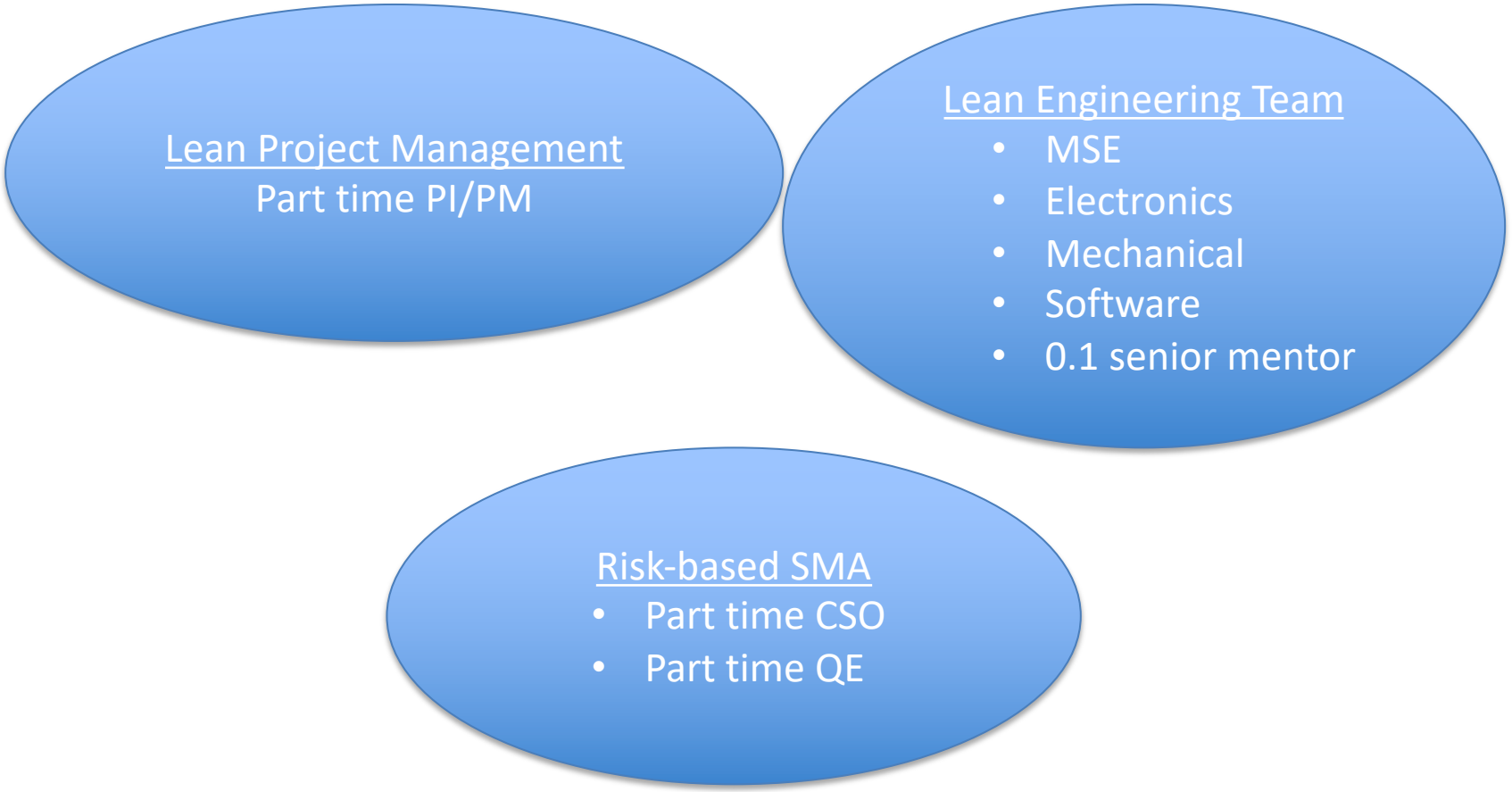
Piece parts and components based on history, secondary to system test

System test is primary focus

Challenge: Elements of a DNH program

- **Program-level reliability**
  - More science for less money if some individual projects are allowed to fall short of goals
- **Requirements commercially-driven and/or based on knowledge-driven assessment of risk**
  - Nothing required solely because we've always done
- **Focus is on system-level testing**
  - Piece part activities based on objective determination of risk
- **Testing centered on test like you fly**
  - avoid tests that prompt failures that are unlikely to be encountered on-orbit
- **Maximize system-level testing hours**
  - Intermediate testing and barriers of protection based on risk

Approach to Implementation



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 [acceptable*] risk
  - Ability to reset
  - Design for graceful degradation

*A stakeholder may decide that local mission-success-related risks that are unpalatable are acceptable to achieve the long-term greater good

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

Prime DNH concept attributes

High-risk, high-payoff science proof of concept

Low-cost implementation option (cubesat, ISS payload, CAPsat)

Short-term achievement potential

Feed-in or high-risk rejections from larger missions

Prior experience on A/C, sounding rockets, etc

Motivated PI who pushes boundaries, challenges conventions

Inherited items for cubesats

- Many standard CubeSat components now exist
- Substantial reliability benefits for using previously qualified items
- However, these give rise to constraints that may increase the system design challenge
- **In general, it may be desirable to treat the cubesat itself as an "inherited" or COTS item**
  - **Ensure mission success and reliability through holistic assessment, rather than piece parts approvals (alternate approach)**

Where do risks come in at launch?

- Unresolved risks carried in the project
- System-level testing not completed
- System doesn't function as expected at launch
- Few hours of failure-free operation at launch
- All problems not resolved by the time of launch
- Known risks at time of launch may be realized

Current status

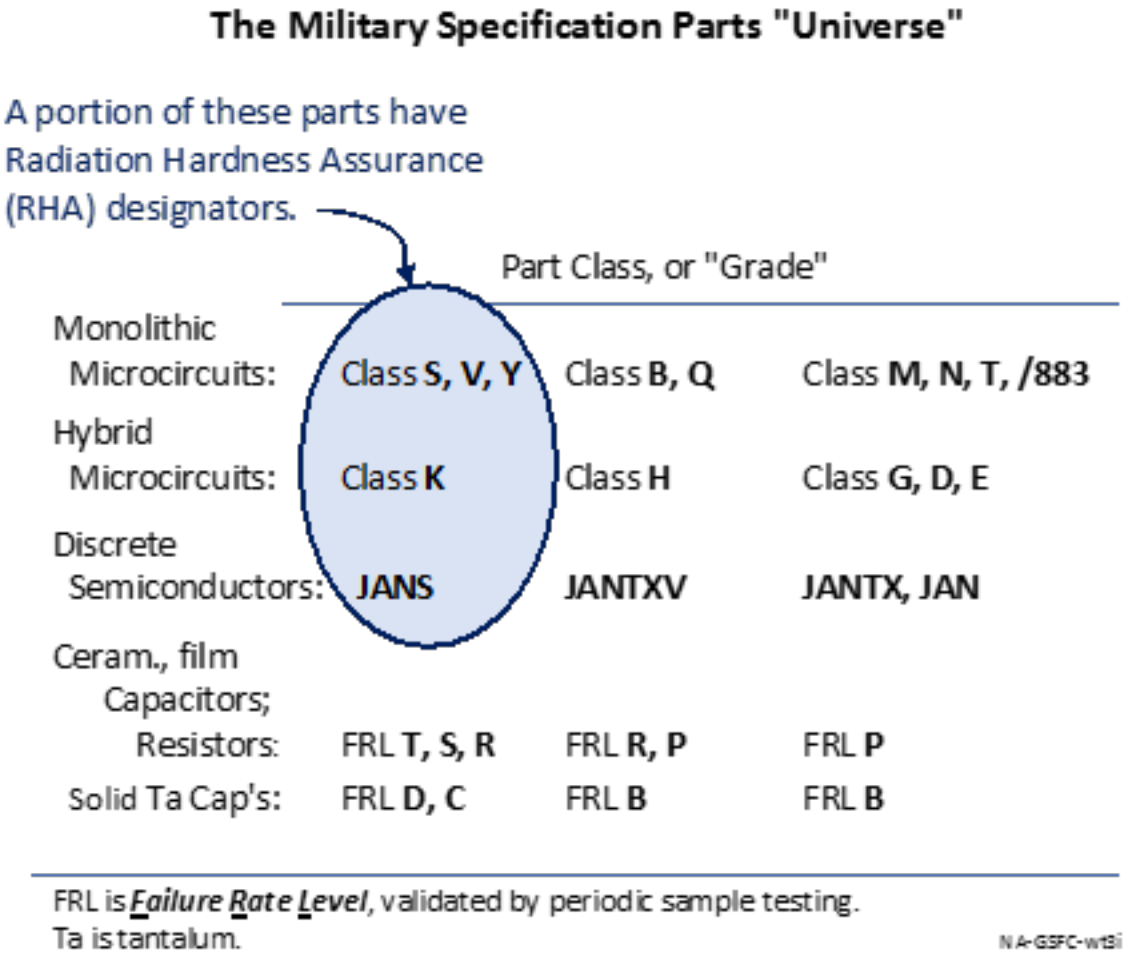
- Cubesat version of GEVS complete and incorporated in handbook
- Handbook is complete and baselined
- Supplemental file maintained as GSFC-HDBK-8007 Addendum (unofficial)
  - Contains updates based on cubesat development and operations learning

Summary

- Cubesats demand a unique approach due to a unique set of constraints
- Two approaches are suggested here
  - Prioritizing mission success activities by ratios of programmatic risk to technical risk and programmatic resources to technical risk
  - Holistic assessment of the cubesats, where piece parts are secondary contributing elements
- The Cubesat mission success handbook is baselined and, through an unofficial addendum is maintained as a living and growing reference.

Backup slides

RHA in the MIL-SPEC "universe"



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