National Aeronautics and Space Administration

Risk-based SMA for cubesats

Jesse Leitner, Chief SMA Engineer
NASA GSFC

December, 2016

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Outline

- Cubesat philosophy and constraints
- Risk Classification for cubesats
- Mission Success activities to reduce defects
- Risk-based SMA
- Scaling of efforts for cubesats
- Building a cubesat mission success strategy from ground up
- Cubesat lifetime
- Cubesat as an inherited item

Cubesat philosophy

- Understand the constraints
  - Size (space limitations)
  - Proximity of elements
  - Cost and schedule resources
- Recognize the limited reliability history
  - Cubesat level – few developments using “high reliability” approach
  - Cubesat components – very little reliability basis
- Develop new approach for establishing reliability
  - Will require time to accumulate on-orbit data for system reliability
  - Apply proven component-level accelerated testing approaches
    - Ensure accelerated testing is validated against actual product reliability experiences (based on product failures in a relevant environment) - be wary of “non-TAYF” lifetesting
    - Overly conservative approach will be a showstopper
  - Explore means for accelerated testing at system-level
  - **This is a ripe environment for model-based systems engineering and model-based mission assurance**
- Determine efforts that provide the best bang for the buck
  - Will not be able to afford typical minimum mission success activities for larger spacecraft
- At time of launch – be sure cubesat was thoroughly tested in environment and functions properly
  - Open questions (unresolved anomalies) and limited system testing time are reliability threats
- When possible, target constellation-level reliability
  - Never at the expense of the debris environment or threats to people or property on the ground

How do we best apply the available programmatic risk commodity and cost and schedule resources to make technical risk as low as possible?

What is risk classification?

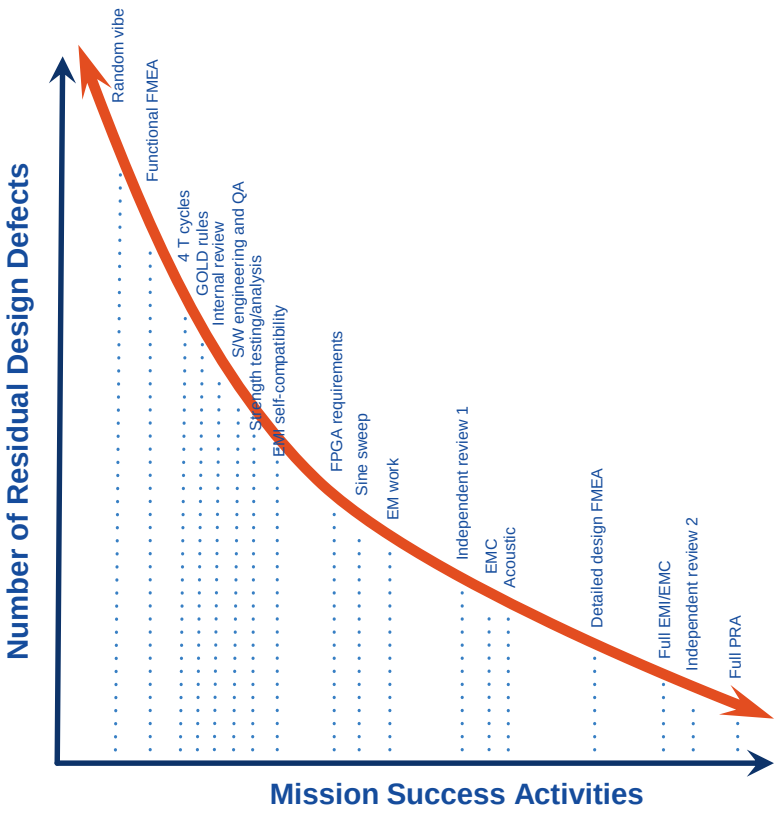
- Establishment of the level of risk tolerance from the stakeholder, with some independence from the cost
  - Cost is covered through NPR 7120.5 Categories
- If we were to try to quantify the risk classification, it would be based on a ratio of programmatic risk tolerance to technical risk tolerance
  - 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
- There is one technical requirement from HQ associated with risk classification: single point failures on Class A missions require waiver

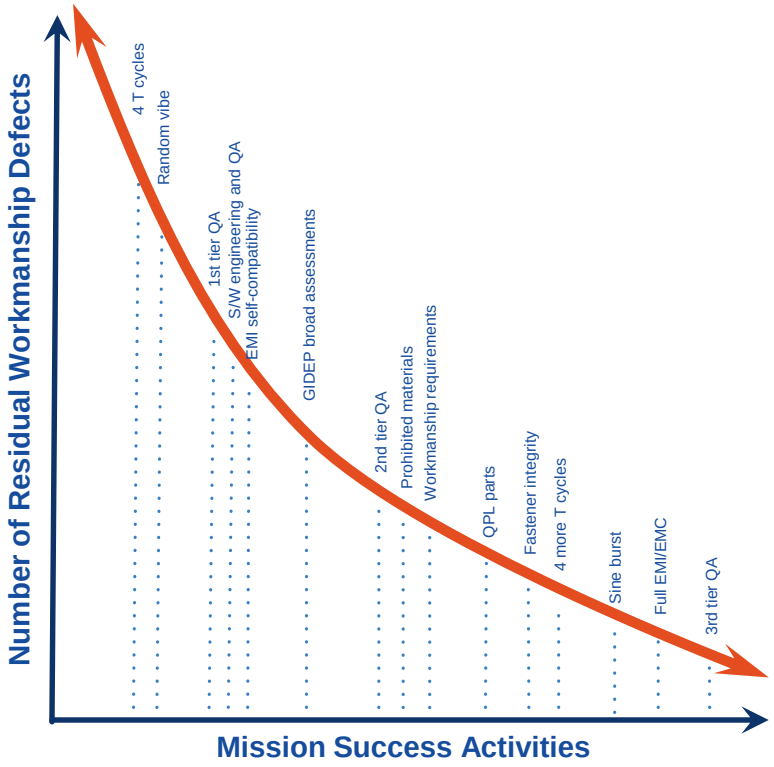
Risk Classification

- **NPR 7120.5 Class C: Moderate risk posture**
  - 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
- **NPR 7120.5 Class D: Cost/schedule are equal or greater considerations compared to mission success risks**
  - Allowable technical risk is medium by design (may be dominated by yellow risks).
  - 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
- **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)

Defects vs Mission Success

Risk can be characterized by number of defects that affect performance or reliability and the impact of each. Defects are generally of design or workmanship.

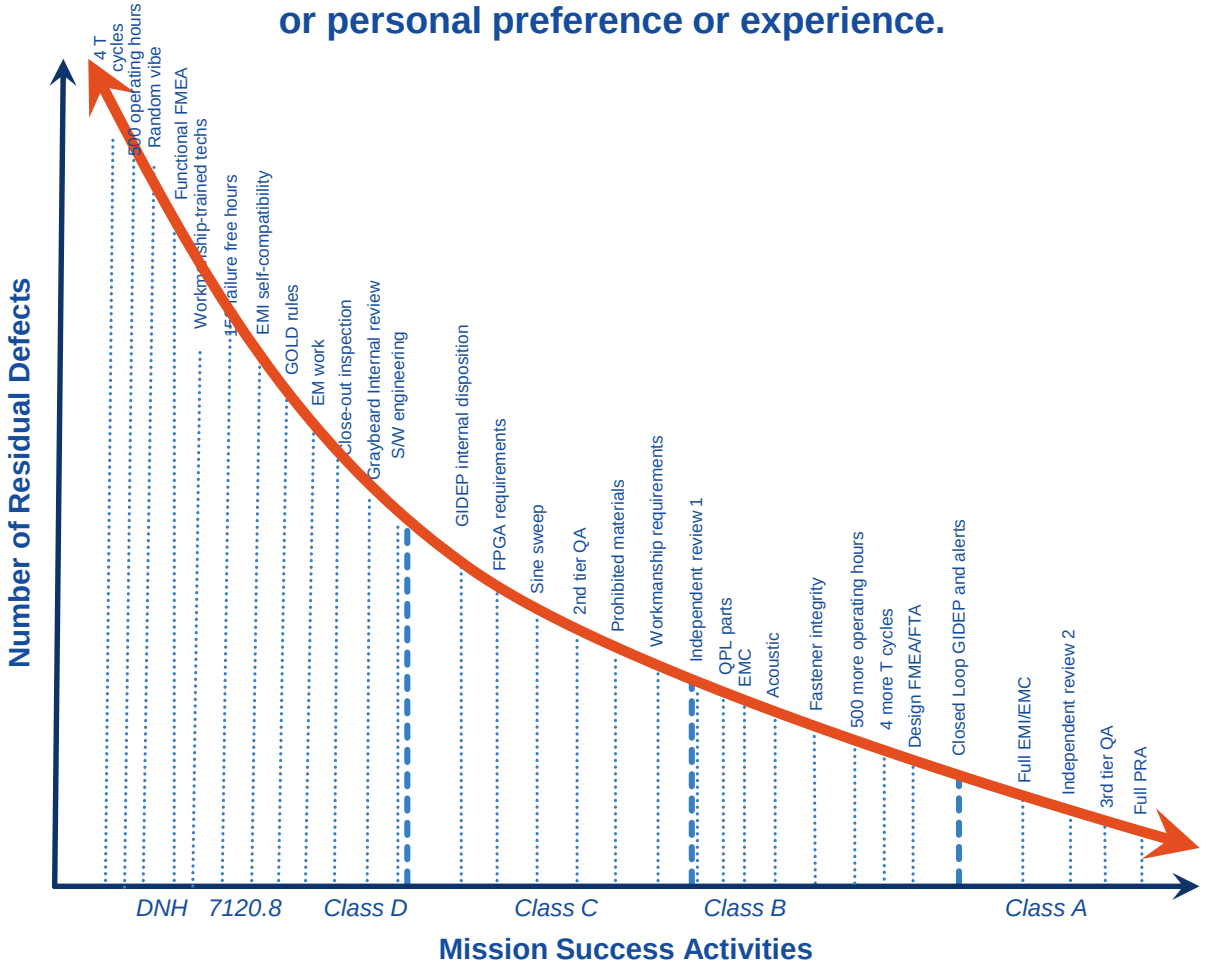




Note: A thorough environmental test program will ensure most risks are programmatic (cost/schedule) until very late, when time and money run out.

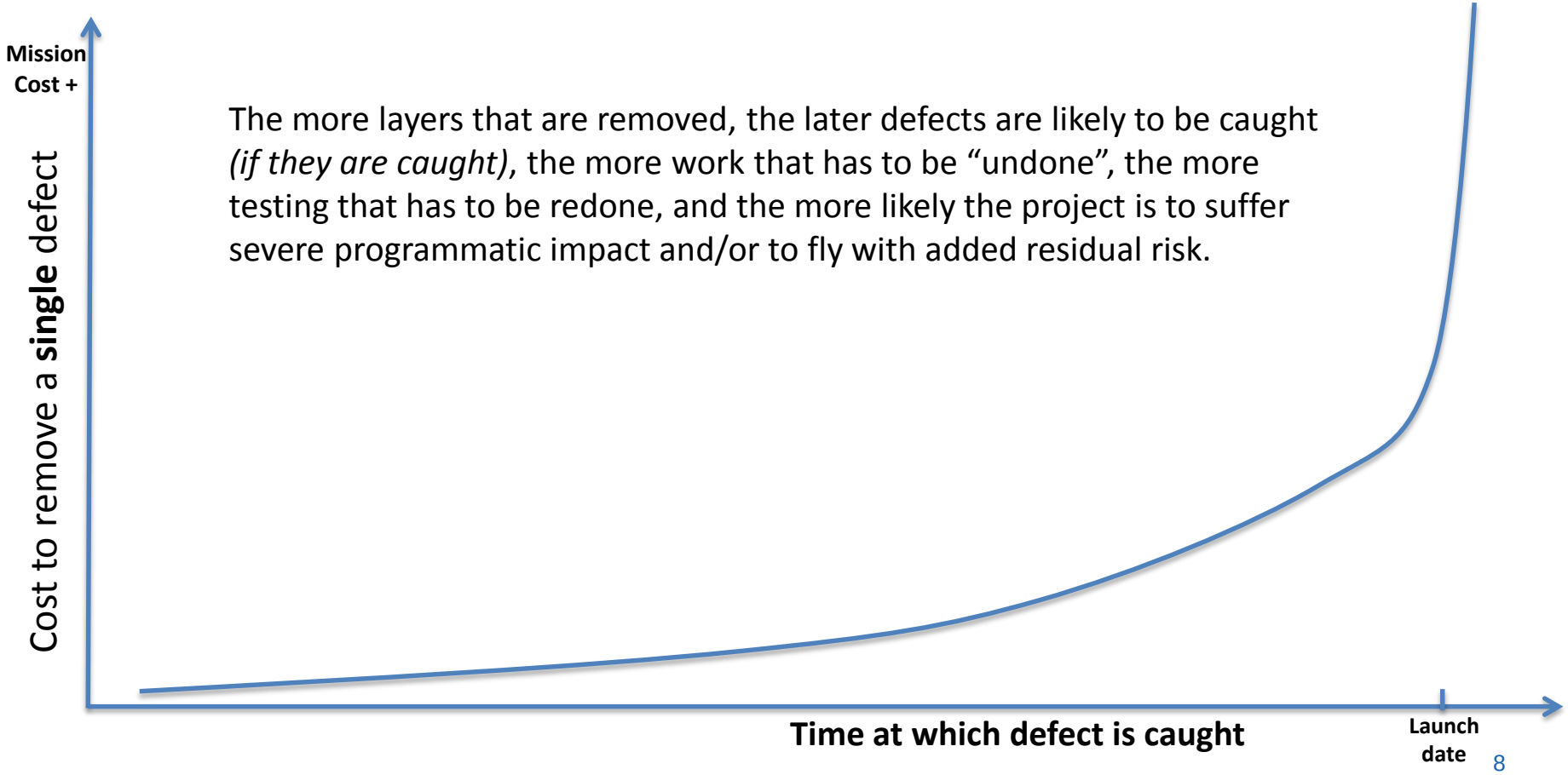
Defects vs Mission Success as a function of risk classification

Generally-representative example, prioritization may vary by mission attributes or personal preference or experience.



Programmatic risk of reduced efforts

Removing layers results in some defects not being caught, and some being caught later



What is Risk-Based SMA?

The process of applying limited resources to maximize the chance for safety & mission success by focusing on mitigating specific risks that are applicable to the project vs. simply enforcing a set of requirements because they have always worked

Risk-based SMA

- Risk-informed framework
- Risk-informed requirements generation
- Risk-informed decisions
- Risk-informed review and audit

Attributes of Risk-Based SMA

- *Upfront assessment* of reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied
- *Early discussions* with developer on their approach for ensuring mission success (e.g., use of high-quality parts for critical items and lower grade parts where design is fault-tolerant) and responsiveness to feedback
- *Judicious application* of requirements based on learning from previous projects and the results from the reliability/risk assessment, and the operating environment (Lessons Learned – multiple sources, Cross-cutting risk assessments etc)
- *Careful consideration* of the approach recommended by the developer
- *Characterization of risk* for nonconforming items to determine suitability for use – project makes determination whether to accept, not accept, or mitigate risks based on consideration of all risks
- *Continuous review* of requirements for suitability based on current processes, technologies, and recent experiences
- *Consideration* of the risk of implementing a requirement and the risk of not implementing the requirement.

Note: Always determine the cause before making repeated attempts to produce a product after failures or nonconformances

Scaling of efforts for cubesats

- In general, mission success activities for cubesats do not scale down linearly as compared to larger missions
  - Environmental test
    - Elements of “religion” (number of thermal cycles, sine vs random, etc) do not scale down
    - Time to reach thermal equilibrium does scale down
  - Inspection
    - Overhead of performing inspection at various points remains
    - Volume of inspection does scale down
  - Operating time
    - Operating time to ensure system-level design and workmanship issues are exposed does not scale down
  - Qualification of new elements does not scale down

Building an SMA approach from the ground up

1. Mission Success Tiers: For a given application, arrange mission success activities from *low ratio of programmatic risk to technical risk* and *low ratio of cost-and-schedule resources to technical risk* **to** *high ratio of programmatic risk to technical risk* and *high ratio of cost-and-schedule resources to technical risk*
2. Build mission success activity profile based on risk tolerance (risk classification): Recommend graded approach of applying activities starting from low ratios, working towards high, to build the lowest achievable risk posture holistically, within resource constraints
3. Expected lifetime: Apply processes and analyses that address lifetime concerns:
   - Limited life items
   - Expendables
   - Qualification period duration or accelerated life (or other reliability basis)

Sample from Tables (Mission Success lower tiers)

2A: Medium Ratio of Programmatic Risk to Technical Risk	2B: Medium Ratio of Programmatic Resources to Technical Risk
- Protoflight vibe - RS testing	- 3-6 TVAC cycles (after 2 earlier) - Level 3 EEE parts - 1000 or more hours of operation - Select mandatory inspection points - Use of formal WOA system - Select engineering units for high risk/new items - Focused engineering peer review - Fault-tolerant design using FMECA, FTA, and/or critical items analysis as a basis - Design for manufacturability - FPGA peer review - Observatory level qualification - Self-performed software assurance - GIDEP self-review - GOLD rules as guidance - Radiation qualification by similarity
3A: Low Ratio of Programmatic Risk to Technical Risk	**3B: Low Ratio of Programmatic Resources to Technical Risk**
- First two TVAC cycles, minimum 50 hours - Last 150 hours of failure free operation - Vibe at 1.05 flight levels - EMI self-compatibility - Radiation-tolerant design	- First four thermal cycles - EEE part derating - Parts stress analysis - Random vibe - First 500 hours of operation - Close-out inspection - Early holistic risk assessment - “iphone” photography - informal independent SME review (graybeard mentoring) - spare printed circuit board or coupon for future DPA

Sample from Tables (Risk Tolerance)

	7120.5 Class C	7120.5 Class D	7120.8	Do No Harm
Stakeholder perspective	An instrument or spacecraft whose loss would result in a loss or delay of some key national science objectives. New technologies may be employed that may not be fully compatible with some traditional requirements, requiring alternative approaches for ensuring mission success.	Cost and schedule are of equal or greater consideration compared to mission success risks. Allowable technical risk is medium by design (may be dominated by yellow risks). Many credible mission failure mechanisms may exist. New technologies may be employed that may not be fully compatible with some traditional requirements.	Acceptable technical risk is high. Some level of failure at the project level is expected but at a higher level (program level), there would normally be an acceptable failure rate of individual missions (such as 85% mission success rate over some time period). Premature failure of an individual mission is considered as an accepted risk, and not a mishap.	Acceptable technical risk is very high. There are no requirements to last any amount of time, only not to harm the host platform (ISS, host spacecraft, etc.). No mishap would be declared if the mission doesn't perform as planned. Such missions may be considered to be an "on-orbit environmental test".
Key emphasis	Robust testing and consideration of fault tolerance in the mission architecture and hardware designs	Thorough testing and some consideration of fault tolerance	"Program level" fault tolerance (some failures expected)	Protecting the host, learning from anomalies and failures
Tier selection	2A, 2B, 3A, 3B, select levels from 1A, 1B	3A, 3B, and select 2A and 2B elements	3A and 3B	Select 3A and 3B elements

Expected lifetime

	< 3 months	3-months-1 year	1-5 years	> 5 years
Main attributes	Min. 100 hrs system-level testing time. No additional EEE part or component screening or qualification (acceptance only) – does it function at launch	Min. 200 hrs system-level testing time. Selective part/component screening and qualification (beyond COTS) – thorough environmental test	Min. 500 hrs system-level testing time. Thorough part and component screening and qualification, thorough environmental test	Min. 1000 hrs system-level testing time. Complete part and component screening and qualification, testing consistent with large spacecraft
Limited life (LL) items, expendables	Sizing expendables is the primary consideration	Increased analysis or margins for expendables plus analysis or test for selected LL items	Increased analysis and margins for expendables plus analysis and test for most LL items	Increased analysis and margins for expendables plus analysis and test for all LL items

Other Processes

- Materials: NASA-STD-6016 with discretion
- Workmanship: NASA trained technicians
- ESD – aligned with sensitivity, not necessarily risk-tolerance
- Interface FMEA to protect the host platform and the environment
- Launch/range safety
  - Tailored NASA-STD-8719.24
  - LSP-Req-317.01 (for LSP hosted cubesats)
- Debris requirements from NPR 8715.6, NASA-STD-8719.14

Inherited Items Process

- Baselined in GPR 8730.5: SMA acceptance of inherited and build-to-print hardware
- Centrally handled for all projects to ensure that process is implemented uniformly and that prior analyses are used to the greatest extent
- Folds in the more traditional heritage reviews to this process

Example Standard Components

- Star Trackers
- Gyros/IMUs
- Reaction Wheel Assemblies
- Magnetometers
- Torquer bars
- Battery Relays
- High performance stepper motors and actuators
- Piezoelectric motors

“Traditional” GSFC SMA practices

- Strongly requirements-based
- Commercial practices only by exception
- Previously-developed and build-to-print items required to meet all requirements or work through standard MRB process
- Treatment of each item as if it is the first time we’ve seen it

Practices/features that have caused “unease” at GSFC

- Pure Sn/insufficient Pb/prohibited materials
- Board modifications (white wires, etc)
- Level 3 or COTS parts
- Use of bare board specs outside of our common requirements
- Use of unfamiliar workmanship standards
- Use of Table 2 or Table 3 materials

Previous approach of handling COTS/inherited/build-to-print items

- Generally bottoms up approach for each project
- Standard parts control board approvals
- Acceptance based on elements and processes vs component-level assessment
- Emphasis on requirements, risk generally considered when push comes to shove
- Rejection of modified boards based on quantity of modifications and appearance

These processes drive up cost and risk for larger spacecraft, would lead to demise of cubesat projects

Transition to Risk-based approach

- Early discussion about inherited items being brought to the table
- Directives for proactively handling inherited items
  - Based on changes from previous developments
    - Design
    - Environment
    - Failures and anomalies
  - Based on assessment of elevated risk
- Component level qualification and history
- Use of Commodity Risk Assessment Engineer
- Focus is on “what is new” and risk areas determined from past history

Standard Components CRAE

- Center lead over all Standard Components responsible for
  - Standard Components Commodity Usage Guidelines
  - Capturing lessons learned for each project usage, from procurement, through development, to on-orbit experiences
  - Interface to orgs outside of GSFC
  - Determining risk for unusual usage, or for nonconforming or out-of-family standard components
  - Establish testing and qualification programs as needed
- Focus on applying consistent processes across all projects, emphasizing the “deltas”, and not repeating the same requests
- Approval in the past may not guarantee approval on current project if the risk posture, lifetime, redundancy, or environment has changed

Standard Components Commodity Usage Guidelines

- GSFC-determined derating or usage limits for components
- History of workmanship standards applied, expectations, and ground experiences
- Known EEE parts outside of GSFC's experience base
- Known materials outside of GSFC's experience base
- Ground and on-orbit nonconformance, anomaly, and failure history
- Prior risk assessments

Acceptance of Inherited Items

- Information provided upfront
- Review and analysis
- Risk Assessment performed
- Risk LxC and statement provided to the CSO
- CSO and Project make the call on acceptance based on risk-level
- Results are documented at the Center level

Inheritance Process Overview

1.1 Develop Inheritance Plan:
- Identify potential components (spares, COTS, Std components, Build-to-Print) that are suitable for the mission**
- Determine data available from SC CRAE/ vendor/previous project.

1.2 Conduct mission suitability Analysis

Note 1: An initial SC CRAE contact meeting may be held to establish project intentions and risk posture as well as inheritance options

** Heritage type reviews may be a source for items

2.1 Gather and Prepare Inheritance Data Package (See Note 2) for each item or group of items
2.2 Distribute an Inheritance Data Package within 30 days of MCR/ATP
2.3 Convene Inheritance Review Panel (SC CRAE) even if no data supplied

Note 2: Include all data specified in GPR 8730.5 but at a minimum:

a) List of inherited items and statement of approach;
c) Summary results of qualification, acceptance, and/or testing completed, and comparison of current requirements;
d) Storage and/or Flight history of the items and specific attributes for each flight, including environments;
e) Ground and on-orbit performance violations anomaly and failure history including the determination of root causes;
k) The reliability analyses performed for the most recent version of the product.
l) Identification of significant changes in design, facility, process, subtier supplier, testing changes, company change of ownership, or any change from qualified unit to current unit

See GPR 8730.5 Section 4.7 for Software

3.1A Conduct Inheritance Review Panel Data Evaluations and/or Risk TIMs/WGs to formulate Risk Assessments including workmanship assessment.
3.1B Conduct formal inheritance review to acquire acceptance of project risk assessments in lieu of component level PDR/CDRs.
3.2 Identify/resolve open inheritance concerns, action items, and Discrepancies;

4.1 Prepare and Distribute Final Inheritance Data Package
4.2 Obtain Final Risk Assessments from SC CRAE and Inheritance Review Panel/SMEs. (See Note 3)
4.3 Update CUG with Inherited Item data gathered. (SC CRAE)

Note 3: The SC CRAE risk assessment will include resulting risk statement(s) with a likelihood and consequence in the standard GSFC 5x5 format with mitigation options or a statement that there is no elevated risk associated with use of the item I and in either cases a requirement tailoring recommendation. This will be in the form of a cover letter /memo for the final Inheritance Data Package.

5.1 Accept final SMA endorsement and Risk Assessment from SC CRAE/SMA
5.2 Include Inherited Item Risk Assessment results in upper-level milestone reviews.
5.2 Manage Risks Identified

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)**

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