Risk-Based SMA

Dr. Jesse Leitner
Chief Safety & Mission Assurance Engineer
NASA GSFC

February 13-20, 2020

Agenda

- Risk Classification
- Layered risk reduction efforts to eliminate defects
- GPR 8705.4
- Risk-based SMA attributes
- Lessons Learned and New Positions
- Inherited items process
- EEE parts
- Materials
- Printed Circuit Boards
- Alert and advisory handling

Goals of this series

- Convey the concept of risk-based SMA and risk-based thinking
- Promote thoughts about how to address a variety of common situations encountered in space flight projects
- Encourage local organizations to establish their own processes for risk-based SMA
- Provide examples from everyday occurrences on flight projects
- Recommend a balance between authoritative oversight and thoughtful insight
- Encourage other SMA and engineering organizations to improve upon the concepts and approaches presented here
- Encourage implementers to consider all aspects of risk when making a decision, including the risk associated with simply following the requirements
- Not to tell you what you have to do to perform risk-based SMA

Important concepts to consider

- Virtually any activity performed to assure a system's success also drives up risk somewhere in the system or development process
- Processes for mission assurance and environmental test in general involve trading resources and programmatic risks to buy down technical and programmatic risks
  - Under resource constraints, being overindulgent on requirements and process control may result in driving up risk more than buying it down (e.g., applying broad Class B processes for a Class C mission), not simply spending too much money, e.g.:
    - reducing system-level testing time
    - moving items onto the critical path
    - overtesting or overstressing parts or other hardware
    - damaging hardware in conditions unlikely to be encountered on-orbit
    - reducing time available to resolve all problems encountered
  - **Understanding this concept is key to implementing risk-based SMA**
- The risk trades associated with standard mission assurance and environmental test activities differ significantly with application, e.g., space vs sounding rocket vs aircraft/balloon
  - Applying space practices to, e.g., an atmospheric payload is not necessarily "conservative" at the system level

Risk classification

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

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 in the current NPR 8705.4: single point failures on Class A missions require waiver

Requirements vs guidelines

- Document language (circa 2004):
  - Centers and Mission Directorate may develop and update policies, standards, and guidelines to adapt and expand upon the examples in Appendix C for the unique needs of their programs and projects. Each subset of guidelines described by the examples in Appendix C is intended to serve as a starting point for establishment of assurance criteria, mission design, and test programs tailored to the needs of a specific project. **The intent is to generate discussion of implementation methodologies in order for the programs, projects, Centers, the GPMC, and the Mission Directorate to make informed decisions**
  - This does not limit or constrain the flexibility of a project to deviate from the guidelines, provided that the concurrence and approvals of cognizant Center organizations, GPMCs, and the Mission Directorate are obtained for the specific project approach.
- Appears to be an implicit requirement as worded
  - However, “In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall."
  - In general, a requirement cannot be imposed without a shall.
  - To some extent this also applies to the SPF entry for Class A
- No matter what the interpretation, communication is important
  - Good practice to present how a project aligns with NPR 8705.4 and why it deviates
- In the 2019-2020 update to NPR 8705.4, projects will produce an SMA Implementation matrix that describes the activities they are taking on, relative to the guidance table, and obtain concurrence from the mission directorate.

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

Risk Classification Notes

- A project's risk classification has two distinct elements
  - The stakeholder's expectations for risk-reduction activities driven by risk-tolerance and resources available (this is the risk classification itself), based on a standard Agency (for 7120.5 missions) or Center (for non-7120.5 projects) model
  - The developer's implementation, meeting the intent of the stakeholder risk classification, which may not perfectly align with the Agency or Center model (because the Agency and Center models are provided for guidance, not rigid requirements).
- This can cause confusion when this is not understood, as the two elements can be mixed up.
  - For example, some organizations in the Agency commonly use virtually all Class B processes (at excessive cost and development time) to develop Class C missions.
  - Sometimes terms such as "Class C-", "Class D+", "Class C tailored" are used, which emphasize the confusion, since there are no such classifications and such terms are really describing developer's implementation

Risk Classification Notes (cont'd)

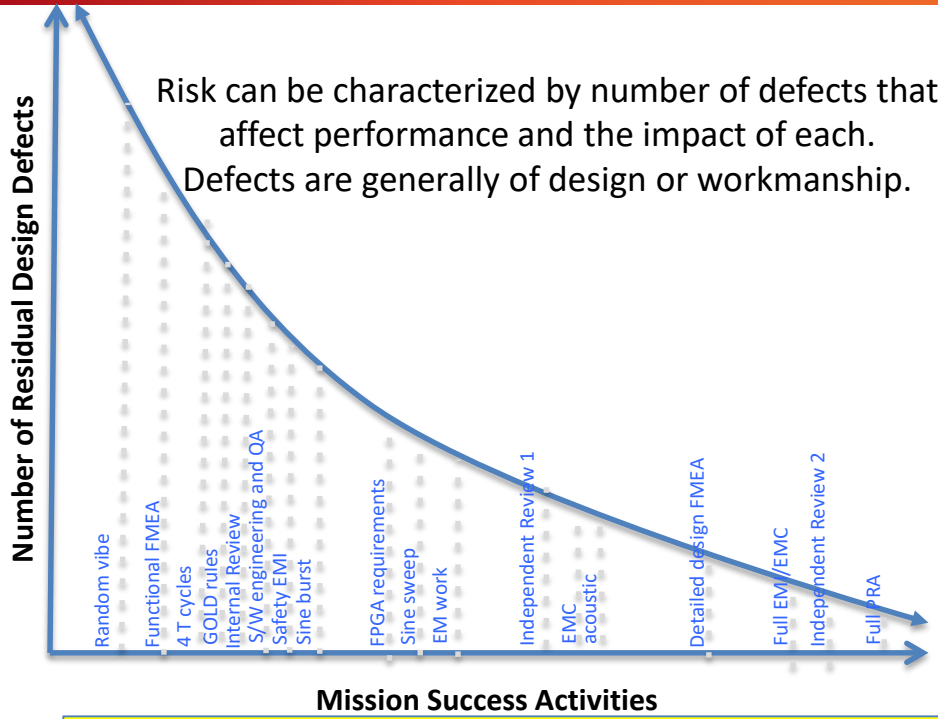
- While the classification communicates a level of risk tolerance for a mission and subsequently expectations for the high-level practices to be employed to maintain that posture, the resulting mission may have lost its connection to the original risk posture intended
  - A Class A mission may fly with dozens of yellow technical risks
  - A Class D mission or below may fly with no yellow or red risks
- It is not unlikely that a well-managed and engineered Class D mission or below would fly with lower overall risk than a complex, one-of-a-kind Class A mission.
  - The extra efforts in engineering thought and the emphasis on risk in driving development activities, combined with reduced complexity, can work together to establish a very low risk posture
  - Class A missions tend to rely more on broad, sweeping processes, that can be very costly, that have their own associated risks that tend to be ignored

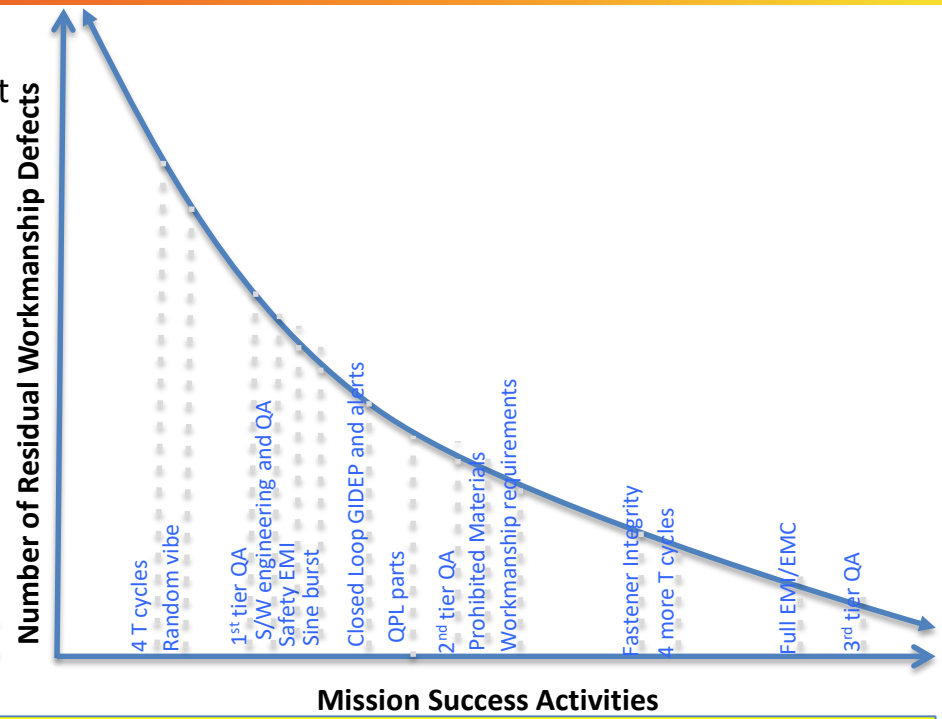
Risk Classification Trends

- **Stepping from A, B, … "Do No Harm" results in:**
  - More control of development activities at lower levels; people actually doing the work
  - Less control by people who are removed from the development process
  - Less burden by requirements that may not affect the actual risks for the project
  - More engineering judgment required
  - Less formal documentation (does not relax need to capture risks nor does it indicate that processes should be blindly discarded)
  - Greater understanding required for reliability and risk areas to ensure that requirements are properly focused, risk is balanced to enable effective use of limited resources, and that good engineering decisions are made in response to events that occur in development
  - Emphasis on Testing/Test results to get desired operational confidence
  - Greater sensitivity to decisions made on the floor

Characterizing Risk

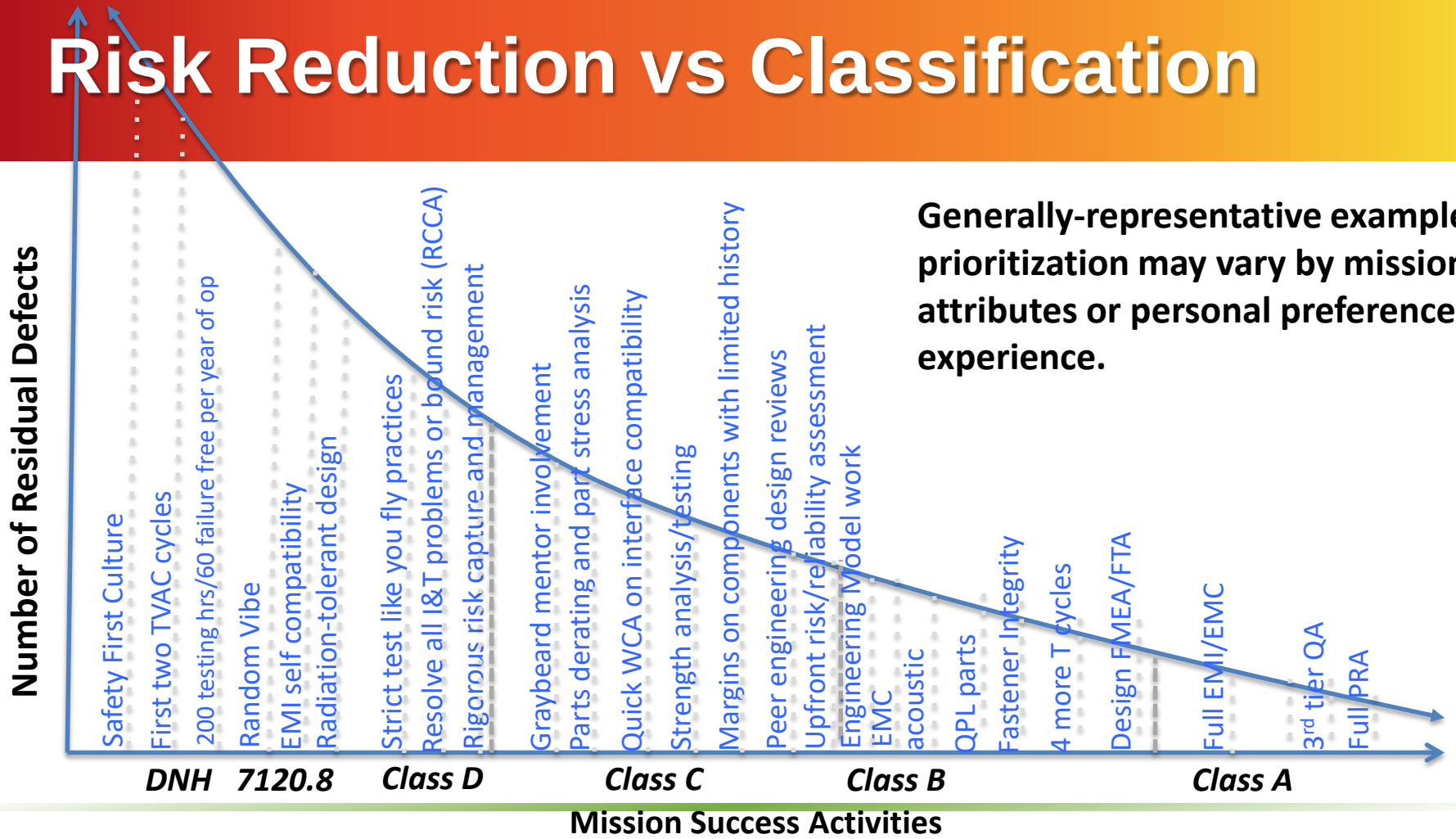
Risk can be characterized by number of defects that affect performance and the impact of each. Defects are generally of design or workmanship.





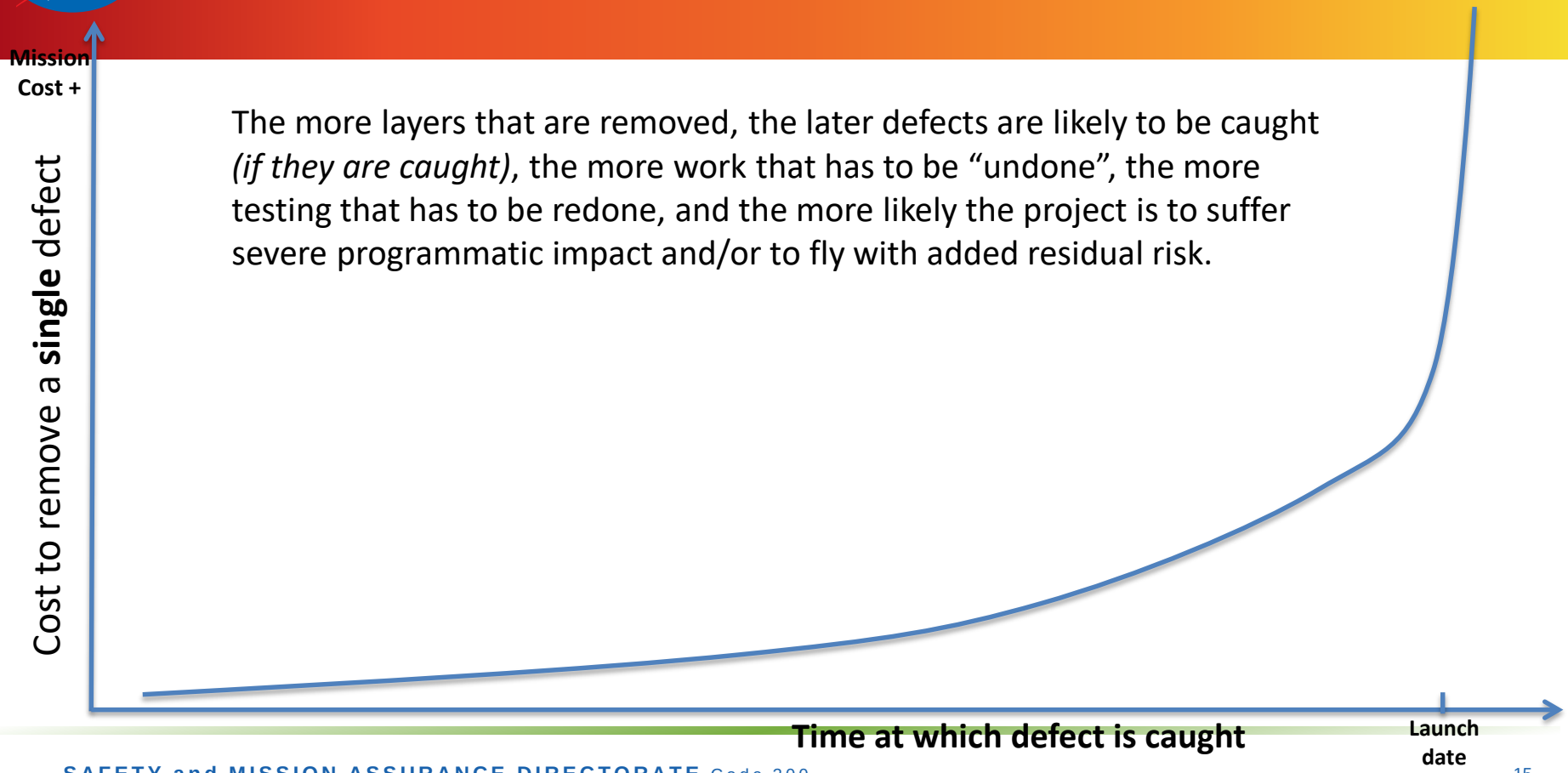
Note: A thorough environmental test program will ensure most risks are programmatic (cost/schedule) until very late, when time and money run out

Risk Reduction vs Classification



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

Effect of Removing Risk-reduction layers



The more layers that are removed, the later defects are likely to be caught *(if they are caught)*, the more work that has to be "undone", the more testing that has to be redone, and the more likely the project is to suffer severe programmatic impact and/or to fly with added residual risk.

GPR 8705.4: Risk Classification and Risk-Based SMA

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

GPR 8705.4

- GSFC implementation of NPR 8705.4
- Formalizes Risk-based SMA as GSFC policy
- Risk Classification Definitions
- Risk-based nonconformance handling
  - Do not reject without understanding the risk
  - Determine cause of NC before reproducing the item (even from different vendor)
- Guidelines for activities vs mission class
- Ultimately will be one element used to develop project Mission Assurance Requirements vs mission class
- How does a project demonstrate that they are developing a Class “X” product?
- How do we convey to a vendor what we expect for Class “X”?

Mission Success Activities vs. Risk Posture (example elements)

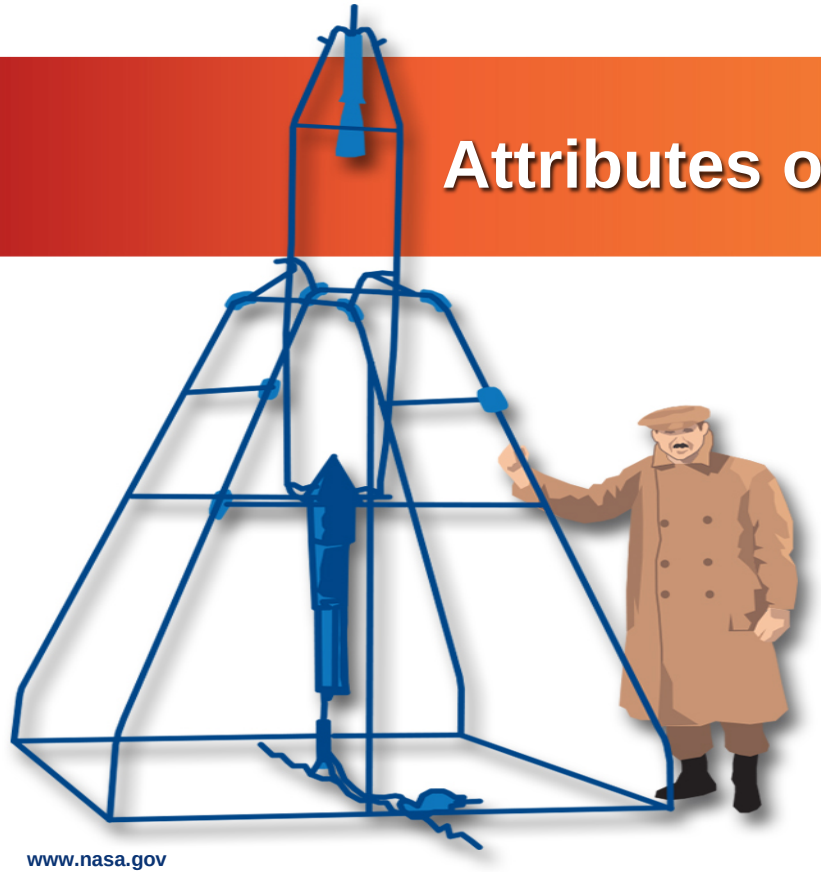
Technical Categories	Class A	Class B	Class C	Class D	Ground System (GS)	7120.8 Class	Do No Harm (DNH)	Hosted Payload Class (host requirements)
Single point failures (SPF)	Any SPF against Level 1 requirements necessitates a specific waiver, SPF analysis expected per GPR 7123.1	Particular attention to avoidance, tracking, and mitigation, SPF analysis expected per GPR 7123.1. Highly fault-tolerant, through redundancy and other means.	Selective redundancy for tall pole items, tracking, and communication, tall pole, critical item, or SPF analysis	SPF, critical item, or tall pole analysis up front, communication of results. Selective redundancy where cost effective.	N/A	Project best effort. Tracked in project documen-tation.	Project best effort	NASA review of design history
EEE Parts	Level 1 parts per EEE-INST-002; DPA performed per S-311-M-70; Counterfeit Avoidance requirements per 500-PG-4520. 2.1;	Level 2 parts per EEE-INST-002 except Level 1 parts for single point failures and hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance	Level 2 parts per EEE-INST-002 for missions greater than 2 years except Level 1 parts for hybrids containing active components and Level 3 parts may be used for fault tolerant, non-critical	Level 3 parts per EEE-INST-002 except Level 2 parts for hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance requirements	For custom designed module, quality level of parts selected needs to be consistent with the criticality of the module.	Best commer-cial practices, advise on part selection & derating. ISO certified facilities preferred.	Best commer-cial practices, ISO certified facilities preferred.	Host practices. Advise on part selection & derating.

**Excerpt from GPR 8705.4*

Class D (and below) 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 requirements
  - Put more authority in the hands of PMs and PIs.
  - ~~Have significant margin on mass, volume, power (not always possible, but strongly desirable)~~
  - Have significant flexibility on performance 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.



Attributes of Risk-Based SMA

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

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

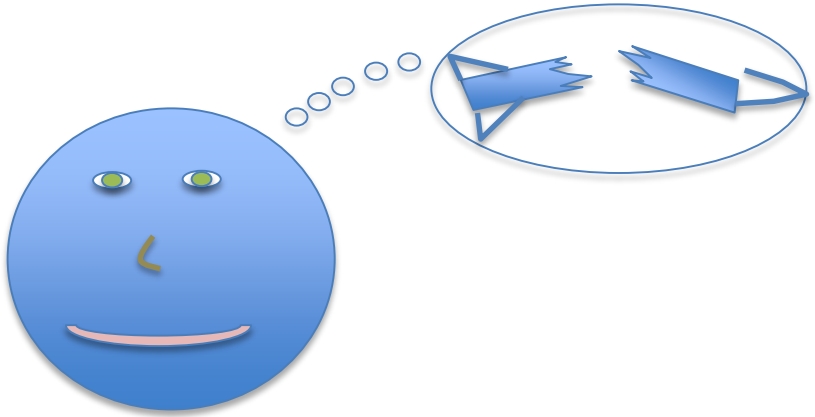
- Risk-informed framework
- Risk-informed requirements generation
- Risk-informed decisions
- Risk-informed review and audit

Attributes of Risk-Based SMA

- *Early discussions with developer on their criteria and approaches for ensuring mission success (e.g., use of familiar parts and components for critical items and unfamiliar parts where design is fault-tolerant) and responsiveness to feedback*
- *Upfront assessment of design, operations, reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied*
- *Judicious application of requirements based on learning from previous projects, the results from the reliability/risk assessment, and the operating environment (Lessons Learned—multiple sources, Cross-cutting risk assessments etc.)*
- *Continuous assessment of risks (safety, technical, and programmatic together to assure all factors are considered) to design performance, availability, manufacturability, operations/testing, and robustness in response to testing, revision, risk mitigations, and remediation.*
- *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

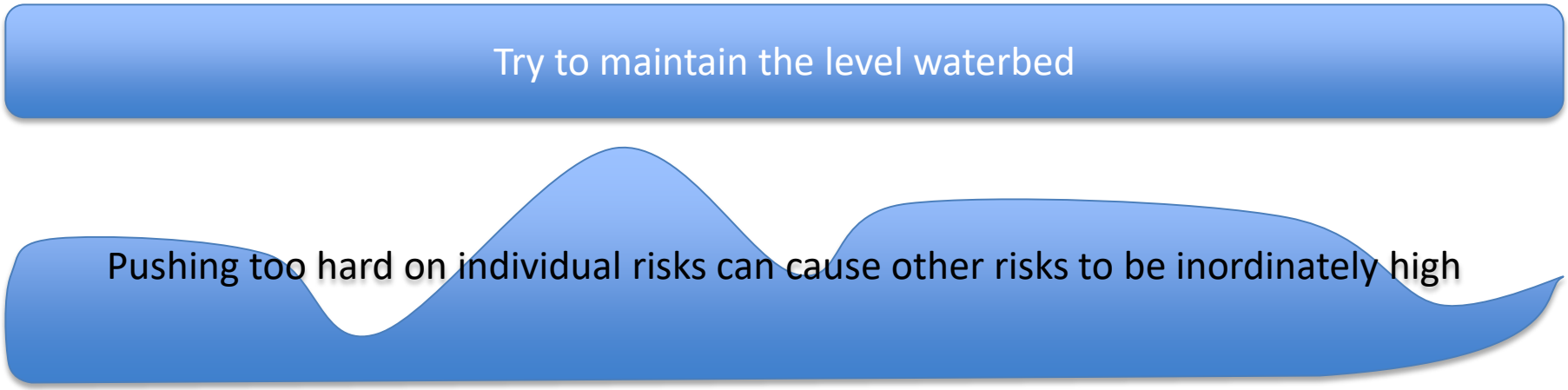
Risk vs Possibility



- Failure modes and mechanisms can appear through
  - Analysis and simulation
  - Observation
  - Prior experiences
  - Brainstorming “what if” scenarios
  - Speculation
- These all constitute *possibilities*
- There is a tendency to take action to eliminate the possibilities of severe consequences
- When a possibility is combined with an environment, an operating regime, and supporting data, a risk can be established – this is core to the engineering process
- Too much attention to eliminate possibilities can lead to excessive cost and unbalanced risk

Balanced Risk (maintaining a level waterbed)

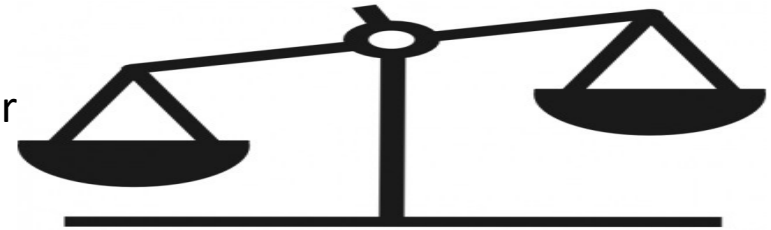
- A systems approach of looking across all options to ensure that mitigating or eliminating a particular risk does not cause much greater risk somewhere in the system



Unbalanced Risk Example

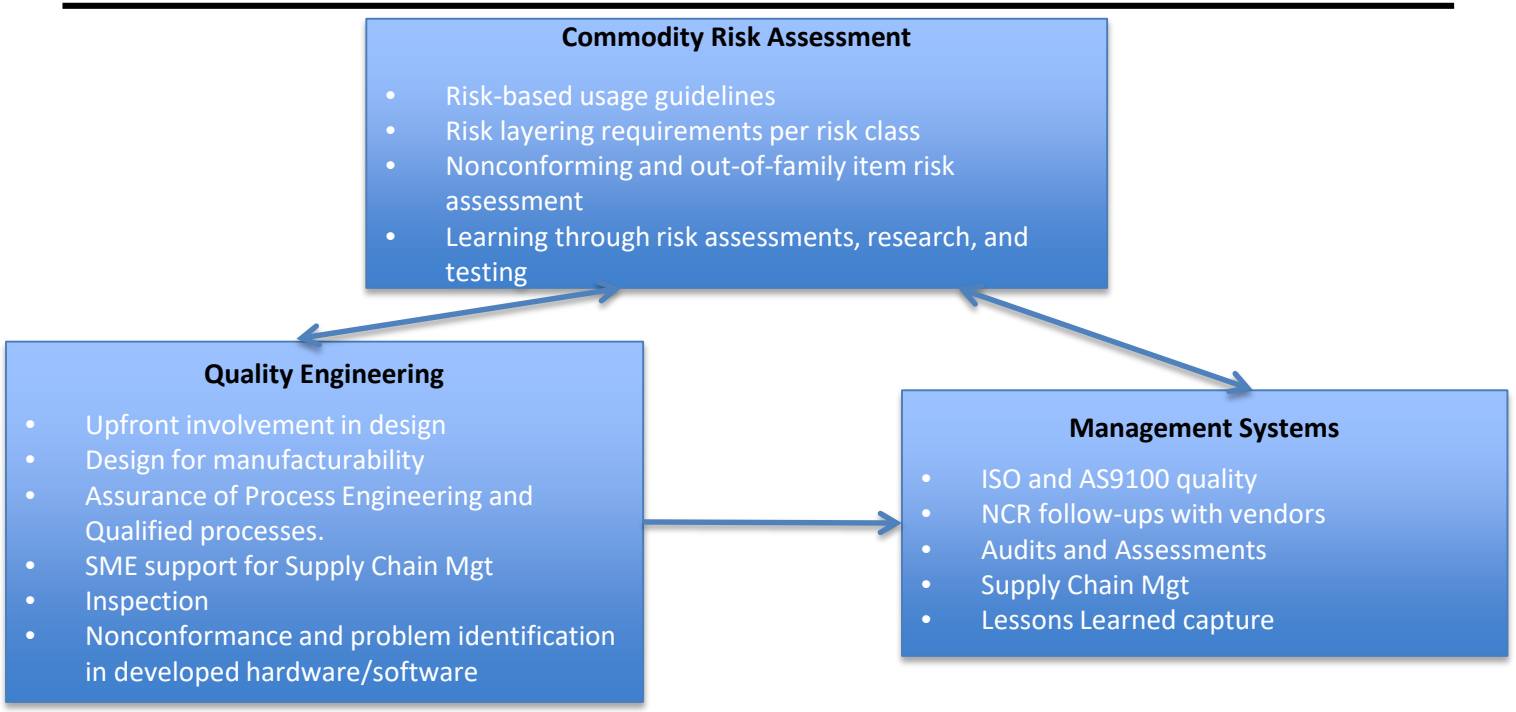
- General safety requirements dictate that anything considered a catastrophic hazard requires 3 inhibits.
- Unfortunately, many elements prior to launch vehicle separation that are tied solely to mission success are often captured under the safety umbrella.
- This means that by default, many items such as premature deployment of solar arrays or other appendages are considered a safety issue for the on-orbit portion, even if they have no range safety effect, and they prompt a decision that it is always better to have more inhibits even if such a design prompts an even greater risk of mission failure due to one of the inhibits not releasing.
- Ultimately, under the guise of “safety” we may end up with a less reliable system that is not more safe if we are not diligent with system-level thinking

Reliability under the safety umbrella



Reliability not under the safety umbrella

The GSFC Quality Triangle



Risk-based approach for capture of lessons learned

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Problems solved by risk-based lessons learned

- We unnecessarily repeat many things
- Lessons learned are not conveyed at all the right levels
- Lessons learned are not conveyed in an effective way
- Requirements do not appropriately account for our experiences
- We tend to do things because we've always done them
- Lessons learned are not considered in everyday practices
- Red herrings are running amok

Events to learn from

- Analyses performed
- Technical assessments
- Risk Assessments
- Failures
- Anomalies
- Mishaps
- Close calls
- Project conflicts
- Procurements
- Nonconformances and dispositions
- Cost overruns
- Schedule problems

Existing lessons learned artifacts

- Watchlist
- GIDEPs, NASA advisories, and MWARs
- SMA chief engineer's wiki

Handling Concepts, new and old

- Day-to-day responsibility within key positions
- Technical Activity Requirements Evaluation Group
  - Testing for reqmts evaluation
  - Requirements changes
- Close call monthly or quarterly briefing
- Wiki communication and discussion
- Risk boards in SMA, engineering, and flight projects
- MSR briefings
- Alert mechanisms
  - Watchlist
  - GIDEP
  - NASA advisory
- Entry into lessons learned system

People

- MPAEs (materials and processes assurance engineers)
- PRAEs (parts and radiation assurance engineers)
- CRAEs (commodity risk assessment engineers)
- QEs (quality engineers)
- REs (reliability engineers)
- Auditors

Introduction to the new positions

- CRAE: Commodity Risk Assessment Engineer
- PRAE: Parts and Radiation Assurance Engineer
- MPAE: Materials and Processes Assurance Engineer

What are these positions about?

- Risk
  - **Ensure that proactive and reactive actions are informed by risk in proper context of the project**
  - Operating at the lowest risk posture supersedes simply meeting lower level requirements
- Learning
  - **Ensure that lessons at all levels are applied from project to project and that subsequent assessments continuously improve in efficiency and effectiveness.**
  - Lessons learned are among everyone's job, but these positions are the leaders in applying the lessons learned in everyday activities.
  - Lessons learned are implemented in daily practices for continuous improvement

PRAE (373)
(Assigned directly to multiple projects)

- Ensure EEE parts requirements and guidelines reflect experiences
- Ensure that risk is the primary driver for parts-related decisions
- Ensure that parts entering the parts control board are prioritized by risk
  - Focus on high risk parts/high risk applications
  - Minimize efforts on low risk parts/applications
- Establish cross-cutting dispositions and processes for EEE parts-related alerts and advisories
- Maintain database of parts experiences
- Establish acceptability/risk of vendor parts practices

MPAE (373)
(Assigned directly to multiple projects)

- Ensure materials and processes requirements and guidelines reflect experiences
- Ensure that risk is the primary driver for materials-related decisions and acceptance/denial of material usage
- Ensure that materials approvals are prioritized by risk
  - Focus on high risk materials/high risk applications
  - Minimize efforts on low risk materials/applications
- Establish cross-cutting dispositions and processes for materials-related alerts and advisories
- Maintain database of materials experiences, e.g., where process problems cause major project issues
- Establish acceptability/risk of vendor materials practices

Specifics

- Review parts, materials, and processes lists
- Invited to all PCBs, MPCBs, etc. (not voting)
- Review or drive agendas for PCBs, MPCBs, MUA disposition
- Reach-out to vendors
- Review parts and materials related alerts for applicability and cross-cutting disposition
- Put parts and materials related decisions in project risk context
- Perform risk assessments when decisions cause problems in project or with vendors
- Document all issues encountered and risk assessments
- Ensure that vendor nonconformances and notable observations get to supply chain managers
- Act as a cross-cutting set of eyes
- Head off problems caused by requirements overreach and creep
- Focus overly broad prohibitions into proper context (e.g., press-fit connectors, RNC 90 resistors, table II and III materials, etc)
- Understand common vendor practices at all vendors

CRAE (371)
Senior Technical positions in 300

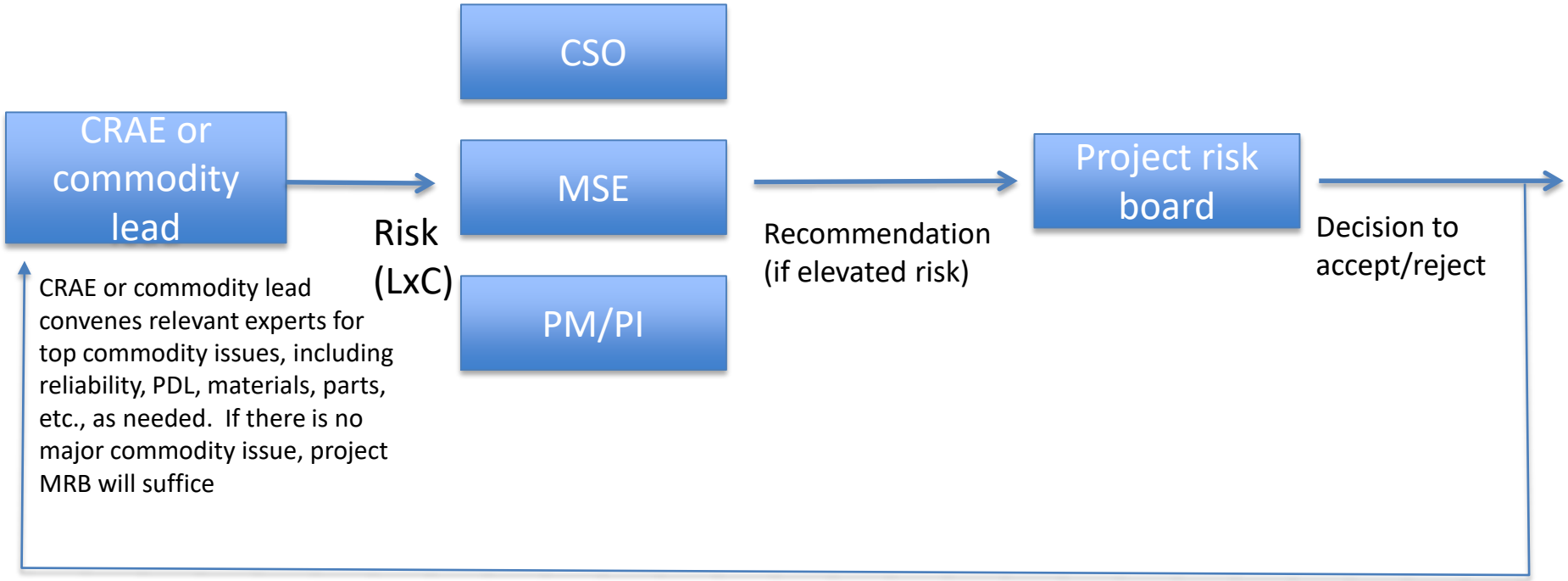
Commodity: Tangible or intangible entity that has a major impact on risk, cost or schedule for GSFC projects

- Expert in key discipline area with background and experience with reliability and risk
- Responsible and empowered to assign risks based on warnings, alerts, environments, and "what we are stuck with"
- Establishes testing programs and protocols to keep up with current design practices and common parts and components
- Sets the policies for the risk-based decisions on use of parts, components, and processes
- Establishes layers of risk reduction based on risk classification
- Determines the acceptability and risk of alternate standards or requirements, or deviations and non-conformances
- Answers, *"are we ok?" "why are we ok?" "how ok are we?"*
- Provides risk assessment to the project for the project to decide how they want to disposition
- Makes recommendations to projects on actions to take based on assessments performed
- Develops and maintains Commodity Usage Guidelines

Commodity Areas

- **Standard Spacecraft Components**
- **Printed Circuit Boards**
- **Electronic Packaging**
- Digital Electronics (esp FPGAs and ASICs)
- Power Systems (MOSFETS, power converters, high voltage, batteries, …)
- Capacitors/inductors
- Transistors
- Resistors
- Hybrid microcircuits
- Optocouplers
- On-board processors
- Additive Manufacturing
- Software
- Materials
- Radiation
- Environmental testing
- Contamination
- Connectors
- ESD

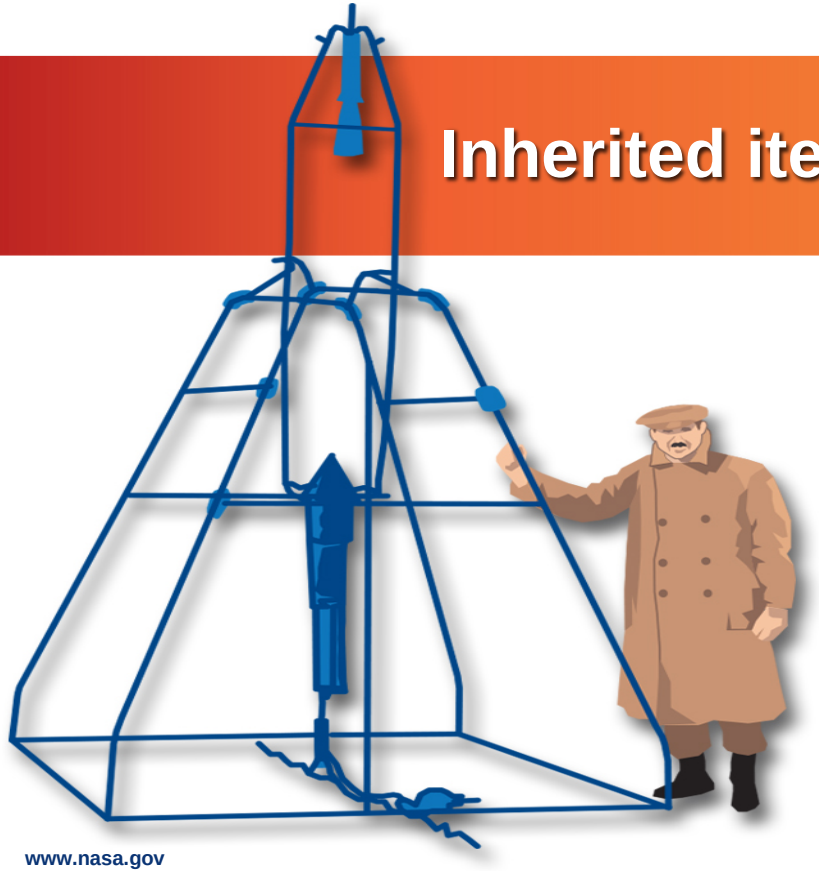
Decision-making process



Communication Mechanisms

- SMA monthly
- Project Monthly Status Reviews
- Lunch time seminars
- Systems engineering seminars
- Email distro to projects
- Code 300 all hands
- Safety awareness campaign
- Workshops
- 300/400/500 Board of Directors' meetings
- CSO learning sessions
- OAGS (on-orbit anomalies of GSFC spacecraft) reports
- MARs, SMA plans, etc

Inherited items process



SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

Inherited Items Process

- Now baselined: 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 data and analyses are used to the greatest extent
- Intend to bring in the more traditional heritage reviews to this process

Example Standard Components

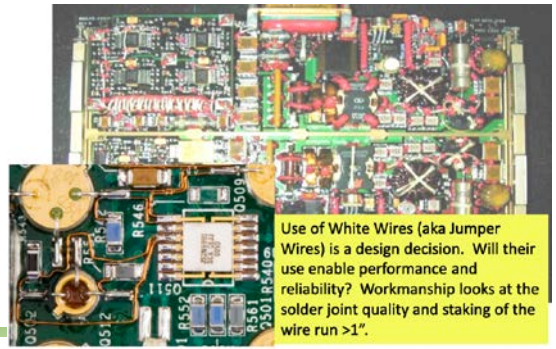
- Star Trackers
- Gyros/IMUs
- Reaction Wheel Assemblies
- Magnetometers
- Torquer bars
- Ground System Programmable Telemetry Processors
- Battery Relays
- High performance stepper motors and actuators
- Piezoelectric motors

“Traditional” GSFC SMA practices

- Strongly requirements-based
- Commercial practices only by exception
- Previously-developed and build-to-print items required to meet all (piece-part) 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 parts or commercially-screened 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/spare items

- Generally bottoms up approach for each project
  - Focus on piece parts
- 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 and appearance (i.e., ugliness vs riskiness)

Transition to Risk-based approach

- Early discussion about inherited items being brought to the table (but it is never too late)
- 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

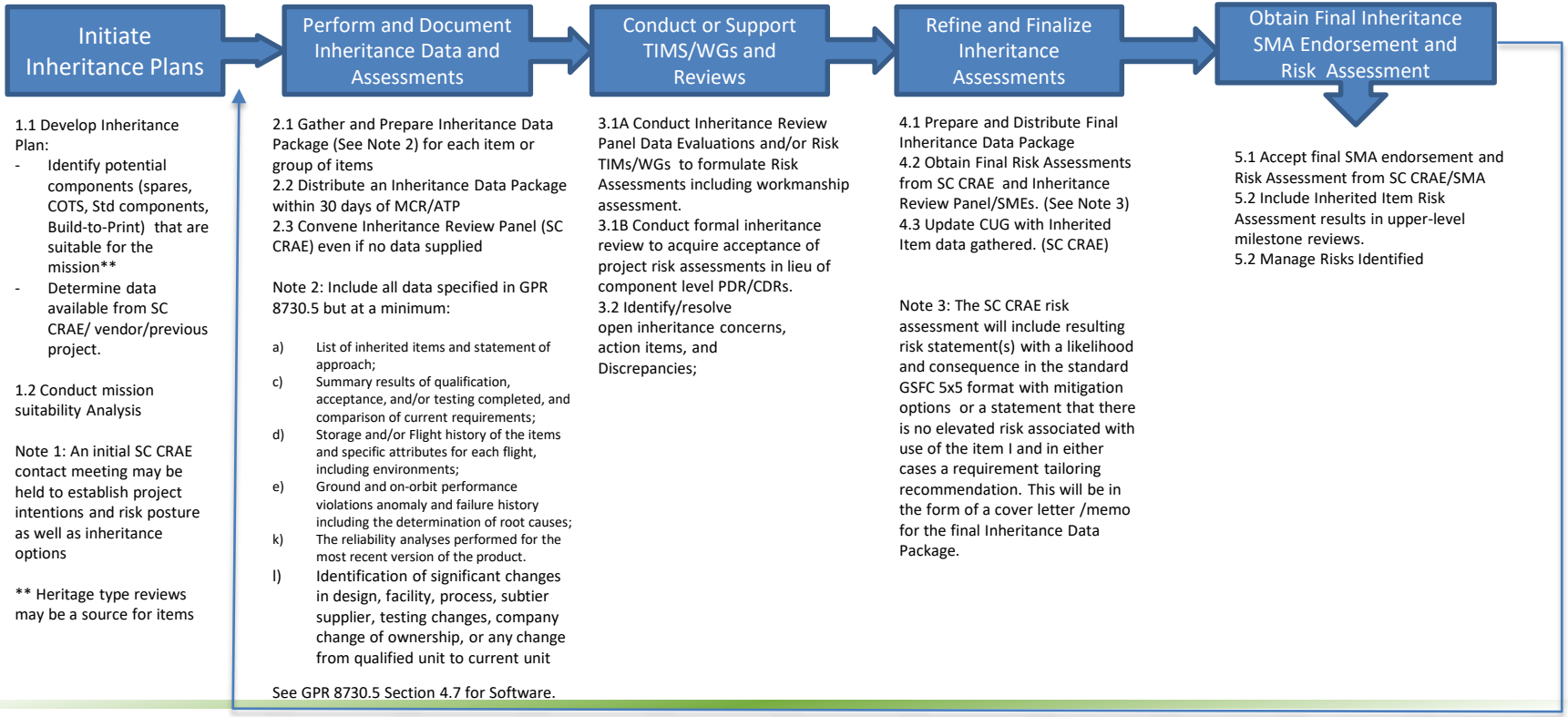
Standard Components Commodity Usage Guidelines

- 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
- On-orbit successful operating hours
- Failure rate updates (based on Bayesian experience)
- Prior risk assessments

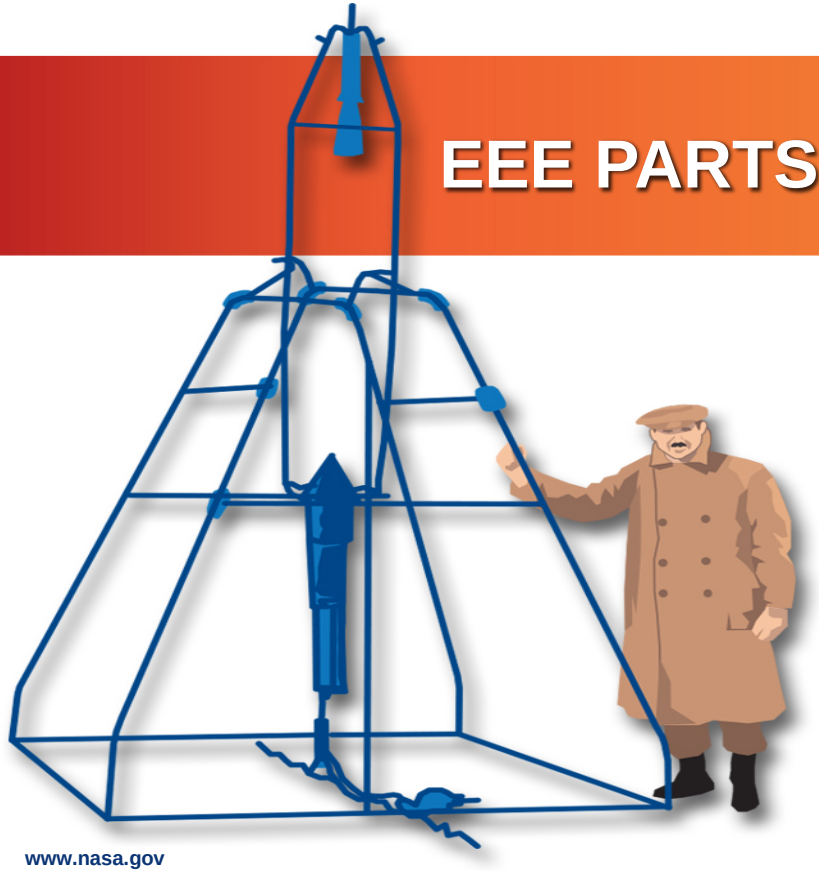
Acceptance of Inherited Items

- Information provided upfront
- Review and analysis
- Risk Assessment performed
- Risk LxC and statements 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



EEE PARTS



SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

Historical EEE parts approach

- Based on a time when long-term reliability and robustness were not commercially driven
- MIL-SPEC system cordoned off a “sample” of the parts manufacturing base
  - High scrutiny from an independent body
  - Reliability assessed by feedback and reporting
  - Tightly controlled quality processes
  - Screening over wide environmental ranges
  - Highly-controlled traceability
- Different degrees of screening and process controls in the system defined as “levels”
- COTS highly discouraged
- Preferred parts list supported by testing funded by Center resources
- Post full-cost accounting - MIL-SPEC processes translated over to screening levels for COTS and specialized parts
  - EEE-INST-002
- The term “risk” has been used to represent the degree of nonconformance of a part, not the likelihood and consequence of a problem in the system.
- Predicted lifetimes associated with screening levels only apply to MIL-SPEC parts used at or above rated values
- Screening levels are commonly (mis)equated to reliability levels or quality levels, and are often called grades
  - The equivalences of screening, reliability, quality, and grades only actually apply to MIL-SPEC parts within part classes, not general application to parts meeting the requirements

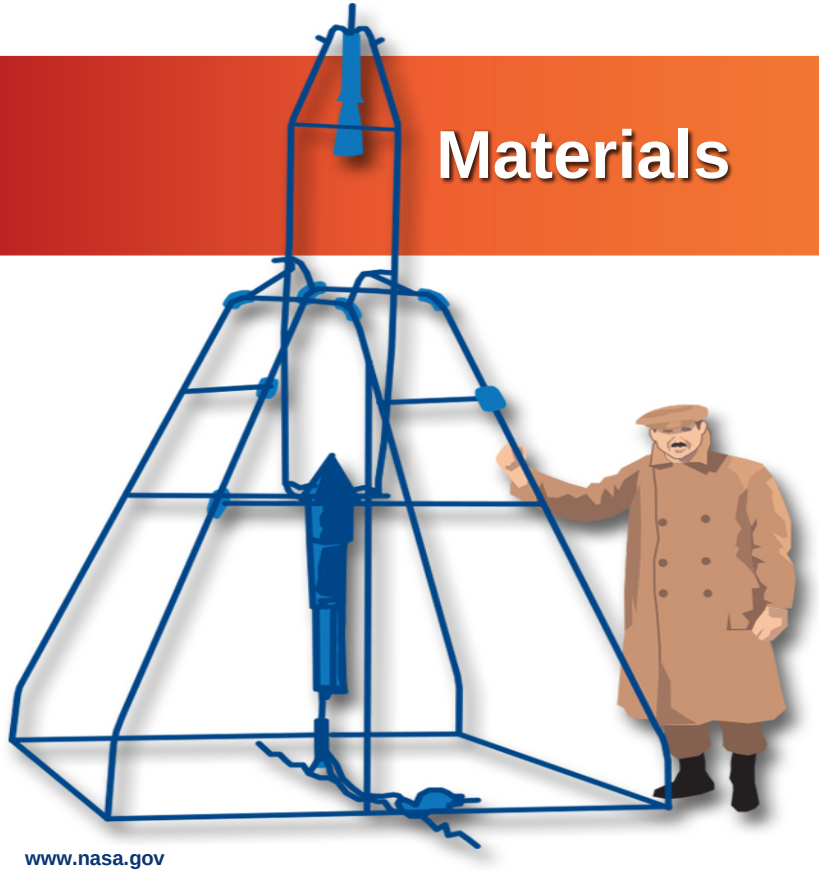
Transition to risk-based EEE parts

- Data being gathered on all parts failures, I&T and on-orbit
  - Failure distinguished from nonconformance
  - Mapped against screening level
  - Distinguish between parts that failed on their own vs those that were “murdered”
- Will be used to determine representative failure rates on which to base requirements
- Carefully reviewing reliability of automotive and other COTS classes vs MIL-SPEC (much larger volume, commercially-driven)
- COTS and specialized parts have become a reality for use in space applications as the commercial market (especially automotive) has grown to dominate the approaches for quality, reliability, and process control.
  - Has led to a large quantity of upscreened parts.
  - Upscreening parts to MIL-SPEC levels is not consistent with the design and construct of many COTS and specialized parts (in many instances we have damaged parts)
  - Need to move to a new approach for qualifying and accepting COTS and specialized parts
  - Requires reliability determination across the user community as opposed to MIL-SPEC monitoring
- Radiation should emphasize radiation-tolerant designs where rad-hardness/shielding is but one supporting approach
- There is still much work to be done to figure out how to establish reliability for COTS parts

Rework vs Use-as-is

- Rework entails credible risk that damage, including latent damage, may occur
  - Damage to the board itself (we've experienced damage to boards after 2-3 properly performed rework cycles)
  - Part damage is often credible as well (ceramic capacitors in particular)
- Tradition has been to always lean towards reworking boards if a parts concern has been raised
  - Qualitative parts risk has been considered to outweigh that of rework per SOP
  - Especially for out-of-house
  - Can be significant risk for damaging a fully environmentally tested satellite
    - Even worse, can result in latent defect
- PM or PI may have little choice
  - Don't replace parts and the blame is on you if something goes wrong
  - Replace parts and break something; it's the vendor's fault
  - We all lose if the parts are replaced at higher risk, especially if rework causes a latent defect
- Need to bring EEE parts risk assessment inline with other project risks for fair comparisons

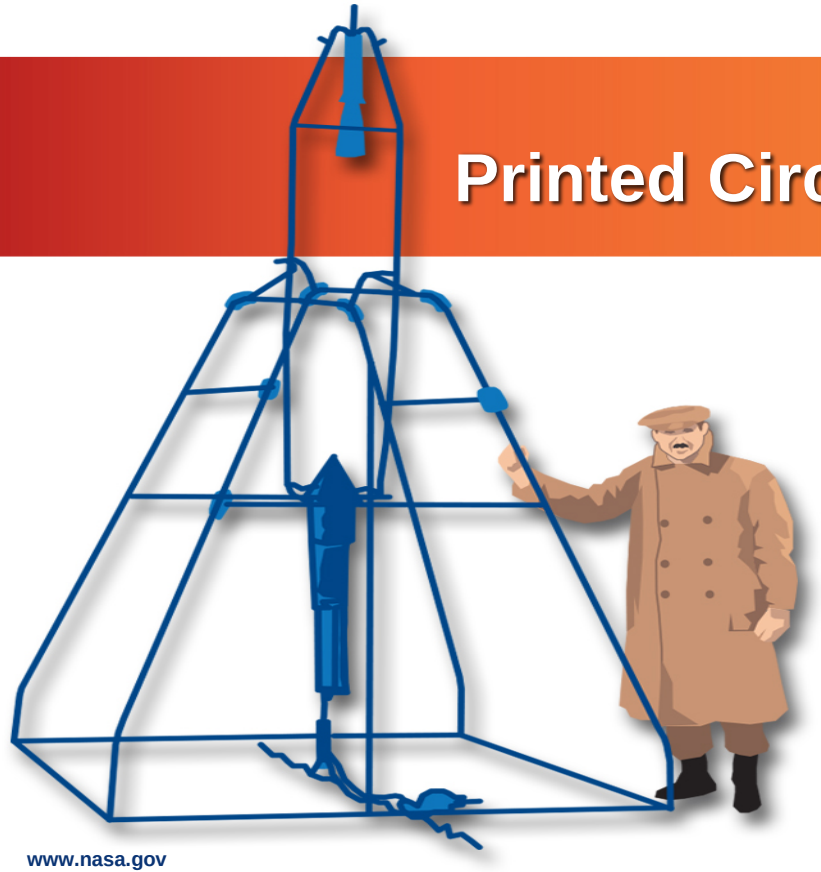
Materials



SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Streamlined MUA Process

- When an MUA process is driving up risk for a project or redefining the critical path, move immediately to a discussion of risk
- Use the project risk system to characterize risk from each nonconforming item (e.g., potential deviation, waiver, or Materials Usage Agreement (MUA)) under consideration
  - Materials and Processes Assurance Engineer (MPAE) completes a risk statement, working in conjunction with the Product Development Lead (PDL)
  - MPAE, PDL, and Instrument Manager assign likelihood and consequence levels based on available information and standard reliability methods
- Establishing likelihood and consequence levels
  - Compare environments that equivalent hardware have seen in relevant prior applications
  - Qualification comparison and relevant past experience serve as the primary means to establish likelihood
  - It is reasonable to make assumptions on the conservative, but realistic side
- Assessment may result in a risk that the project must capture or it is possible that the likelihood is low enough to make the risk not credible
  - If risk is credible (likelihood high enough to be on the scale), then CSO delivers to the project risk management board for disposition
  - Project will accept, mitigate, watch, or research the risk (if there is one)
- Projects make the determination about how to administratively handle the relief

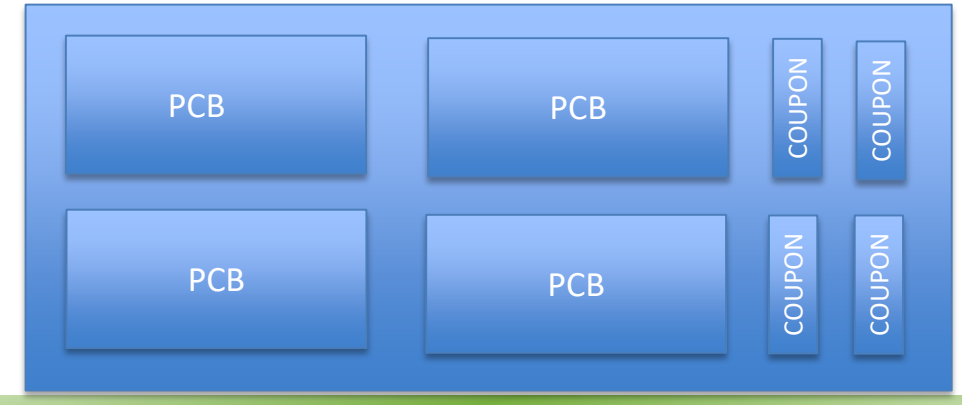


Printed Circuit Boards

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

Printed Circuit Boards

- Typical large projects develop dozens to hundreds of printed circuit boards (PCBs)
- 20-30% of all printed circuit board coupons had been historically rejected due to nonconformance against the imposed spec (usually IPC 6012 for rigid PCBs)
  - Solely based on the coupon not meeting the requirements to which they were evaluated
  - Without any basis of risk or flightworthiness (nonconformance was equated to flightworthiness)
- Projects were choosing two vendors for most boards simply to mitigate the risk of coupon rejections
- Time and resources wasted on respins were reducing more important risk mitigation activities
- Respins frequently resulted in boards that had bigger concerns than the first build



PCB risk assessments

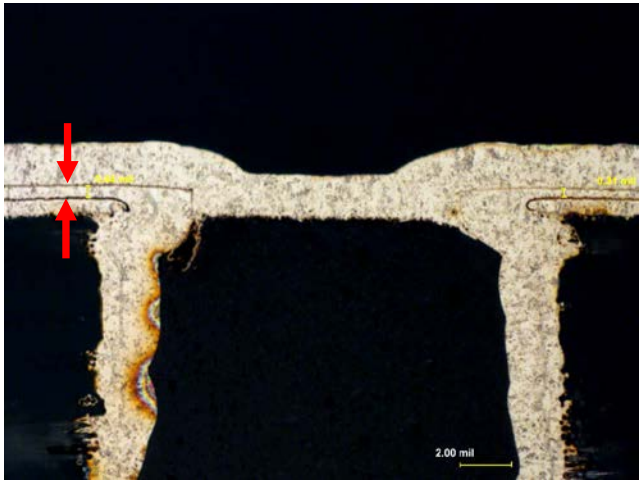
- Implemented an option initially, later a requirement, to perform risk assessments when coupons were nonconforming, prior to rebuilding
- Central working group led by PCB Commodity Risk Assessment Engineer performs all risk assessments (with specialized support from project as needed)
- Initial risk assessments took weeks to perform; after many now they take hours for repeated nonconformances
  - Continuous improvement and learning is inherent to the process
- Over 400 PCB lots with nonconforming coupons assessed for risk since Jan 2014, with approximately 80% entailing no elevated risk
- Each risk assessment is associated with one panel and each panel may have several boards (a recent example had 8). Each production run generally costs ~ $5k - $20k and takes between 2-8 weeks.
- Frequent reattempts to build same board without knowing cause of the NC or cost of microsection analysis labor added insult to injury.
  - Often the problem was on the government side, a requirements flowdown problem, or an incompatibility between the spec and the board design

Continuous improvement and learning are at the core of this approach

Corrective action

- Some requirements frequently reappear in risk assessments
- Requirements that frequently are violated and rarely entail risk raise red flags and demand follow-on actions:
  - Industry survey
  - In-house testing
  - Follow-up with requirements body
- Example: copper wrap requirement in IPC 6012 3/A for buried/hidden vias
  - Frequently violated (especially for European products since requirement not included in European spec)
  - Can be very difficult to achieve
  - Uniformity across the board is ambiguous
  - Prompted a major lien for ICESat-2
- Performed three independent lines of testing
  - Thermal cycled the ICESat-2 coupons through 50+equivalent lifetimes
  - Produced multiple board designs with variable levels of thickness for life tests
  - Performed highly stressing Interconnecting Stress Testing (IST) until failure
- Performed structural modeling in COMSOL™
- All testing and modeling concluded that wrap meeting requirement did not improve reliability
- We presented results at Quality Leadership Forum, then circled back to IPC with results
- Formed a committee in IPC to reevaluate the requirement.
- IPC produced an addendum accounting for our findings

PTH Copper Wrap Thickness Requirement



- Thermal cycle stresses act on interfaces, outer layers experience the greatest stress.
- Reason: materials selection and geometry.

Per IPC-6012D for through-holes:

Class 1	AABUS
Class 2	5 µm [197 µin]
Class 3 & 3/A	12 µm [472 µin]

AABUS = As Agreed Between User and Supplier

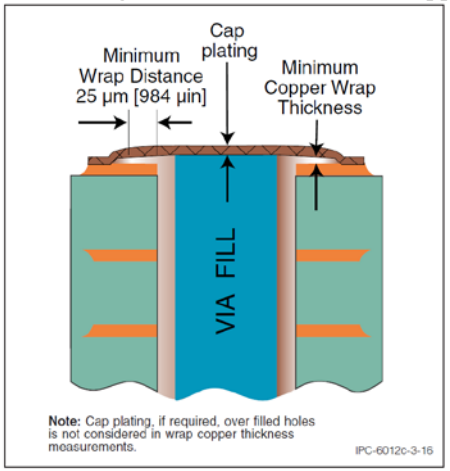


Figure 3-16 Surface Copper Wrap Measurement (Applicable to all filled PTHs)

Significance of Board Requirements

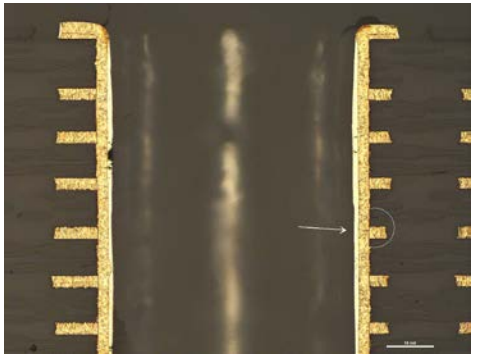
- Note that most board requirements are either in place for process control or are broad “conservative” requirements that can be determined applicable or inapplicable by direct analysis of board features.
- The requirements and coupons are a “front door”.
- Examples:
  - Internal Annular Ring:
    - egregious violations indicate there may have been a serious problem in development of the board
    - Minor violations don’t likely indicate any risk at all
  - Negative etchback:
    - With modern cleaning processes and flight experience can result in higher reliability with negative etchback
  - Wicking of copper:
    - Requirements are conservative based on broad statistics
    - A basic analysis of the board layout can indicate directly if there is risk or not, regardless of requirements violations

Sampling of Risk Assessments

Dielectric layer less than 3.0 mil

A 40kV dielectric breakdown strength, combined with a 28V service voltage provides a sufficient dielectric clearance at 2.8mil. There are at least two layers of dielectric material present.

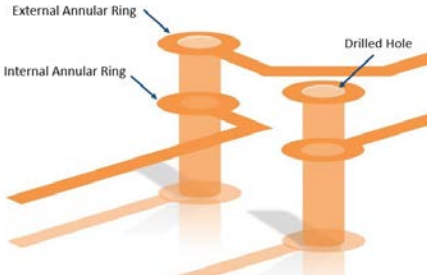
IAR less than the minimum 5.0 mil

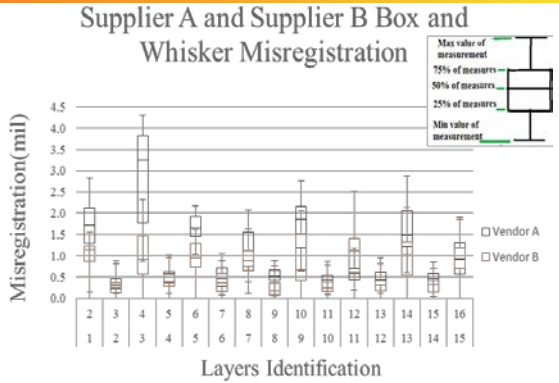


Out of date drawing notes containing a minimum 5.0mil annular ring and other requirements.

Internal Annular Ring (IAR) Assessments

- This work involved designing in variations in IAR geometries in printed circuit boards and correlating the effects of these variations as a source of risk for PCB failure in GSFC test and mission environments.
- Reliability tests such as temperature cycling and mechanical flexure are conducted on test samples constructed with control IAR widths, sub-optimal IAR widths and other configurations such as teardrops.





$$IAR\ size = \emptyset_{drill\ hole} + IAR_{min} + tol_{mfg}$$

tol_{mfg} = 8 mil Supplier A

tol_{mfg} - 10 mil Supplier B

- **Outcome:** On the basis of this work, it was determined that
  - IARs lower than 1 mil or in teardrop configurations offer a similar thermal fatigue reliability as 1 mil or larger IAR
    - Failure site due to thermal cycling is at the PTH barrel
  - Manufacturer's drill tolerance for a given hole size has the largest contribution to hole registration

New technologies require rethinking

- High pin-density technologies (e.g. Virtex 5 and later FPGAs, RTG4, some SRAM technologies, others with grid arrays) are inherently incompatible with some of the most stringent board specs
  - Higher-end specs require more spacing, more copper, more margins, etc
  - In order to get the spacing an additional 10 layers are needed as a starting point, as well as “via in pad”
    - More layers substantially increases the risk, as does via in pad
    - No evidence the higher end board specs result in higher reliability for boards in our applications
      - Still studying this and performing testing
  - At 1 mm pin spacing, challenge for 3 or 3/A (DS) may be implementation when constraints are tight (Class C or D)
  - At 0.8 mm pin spacing, you have hit a point of incompatibility for 3 and 3/A (DS)
- Test, test, test, and collect industry data where available
- Cubesats could be a great learning tool

Interconnect Stress Testing in proper context

- High Density Interconnect (HDI) testing is often performed with IST using a methodology documented in the IPC test methods manual TM650, Method 2.6.26.
- Elevated temperatures exceeding 220°C are sometimes used to cause HDI failures.
- Although IST can be an effective but highly-conservative screen for process, materials, design and workmanship, it is not recommended as a predictor of reliability or as a means to reject a particular board.
- Increasingly, IST test results that are generated at elevated and highly accelerated test conditions are being used for predicting operational reliability of HDI PCBs.
- IST is a means to provide extremely high, accelerated stresses to a representative coupon; it is not a test that is representative of a typical flight environment

Risk-based Alert handling

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

Advisories

- Defined
  - Statements warning of problems experienced in the broad community
- Examples
  - GIDEP alert
  - GIDEP problem advisory
  - NASA advisory
  - Agency Action Notice
  - External warning (from MDA, Aerospace, etc)
  - Code 300 watchlist item
- Generally not written with “ease of closure” in mind
- Generally introduces “possibility” of a problem and the challenge is to get to “risk”

GSFC's historical approach to closure

- GIDEP alerts and advisories, NASA advisories, and AANs sent out to all projects after careful review of applicability from GIDEP coordinator/representative
- Projects individually need to prove
  - Beyond a reasonable doubt they are unaffected
    - Some include having to provide closeout photos
  - All affected stakeholders within the project understand the risk when there is an impact
- When projects have a direct hit
  - Provide all lot date codes
  - Answer 6 detailed questions (the questions generally center on the prospect that a particular part may fail, even if the warning does not involve part failure)
  - Get sign off from MSE, CSO, PDL in the project for use
  - Even if (1) there is no risk, (2) the questions are not relevant, (3) the lot date codes are not relevant
- Based on "verify", not on "trust"

What can make an advisory hard to close?

- Ubiquitous part (2N2222, CWR06, etc)
- Noncompliance to a lesser-used parameter in a spec
- Parts are installed
- Parts in a component purchased from a sub
- Difficulty in tracing the entire supply chain
- Lack of root cause for problem
- Complex technical details to describe the concern
- Problem sounds bad but may not pose risk to us at all in our context

Unintended Consequences

- Without careful thought and context in providing the warning, we can drive up risk
  - Laser hole problem
  - DC/DC converters
  - Transistor moisture
- A huge amount of resources can go towards buying down very low risk
  - Thin film resistors
  - Laser hole
  - Counterfeit parts warning
- There is a propensity to feel like you have to “do something” about a product that has a warning, before it is determined that there is risk in its use

Example: Laser-etching hole GIDEP

- Encountered on GSFC project
- The nonconformance is a *combination of having a laser hole that penetrates all the way into the part and falsely passing the leak tests*
- Failure requires presence of corrosive agent, pressure to have it enter the hole, and other conditions to cause corrosion
- Problem has existed in some form since at least as far back as 2004.
- Over time parts were collected from across the electronics community (ultimately ~1M) and we were seeing about 12 ppm exhibiting the nonconformance defined above.
- 10 ppm is an approximate threshold for JANS part *failures* where red flags are raised, so 12 ppm just for the nonconformance would result in a failure rate much lower => this problem does not cause an abnormally high failure rate

Laser-etching hole GIDEP cont'd

- Responding to this GIDEP was painful and costly for projects with many of these parts (ubiquitous part)
- Responding to this GIDEP drove up risk for several projects
  - Boards were pulled from boxes that had gone through environmental test, packaged up, shipped to GSFC, and inspected
  - Without intervention, some boards that had already gone through rework were going to be reworked
  - It is likely many risky events occurred that we were not aware of.
- It took almost a year of effort and a very detailed rigorous reliability assessment to prove that the potential for failure was well within that expected for MIL-SPEC parts.

The intent of alerts is often misinterpreted

- Some developers wait until parts are installed in hardware before responding, instead of using the warnings preventatively
- Some will pull parts out of hardware without a basis in risk, or they will ignore the risk of pulling the parts
- Some believe that when we ask to assess the risk of use-as-is, that there is always elevated risk.
- Advisory is sometimes meant only to be advisory, though the action may not be commensurate

How do we transition to risk-based?

- Review all advisories in a cross-cutting sense before providing to projects
  - Gather SME inputs
  - Determine if there is likely risk to GSFC projects
  - Make all efforts to disposition at the Center level
- In “stuck with” situations, ensure that risk is captured for all options
- Do not demand information that is not necessary to assess the risk
- Create two bins
  - Those that require approval from management based on proof
    - Where efforts to disposition are commensurate with risk-level
  - Those that report to management if the problem affects them
    - Where efforts to disposition are likely far greater than the risk-level

Cross-cutting disposition approach

- SME reviews advisory in the following attributes
  - Is the advisory descriptive enough to provide clear applicability and direction for our projects?
  - Is the advisory overcome by our normal practices?
  - Does the advisory represent a completed analysis (e.g., is there any question whether a part actually failed or if the author killed the part)?
- SME evaluates potential risks vs resources required and risks of mitigating actions (e.g., replacement or stress testing)
- SME works to identify broad recommendations
- SME works with projects individually as needed
- If project-specific tasks are left, then project will complete the closure

Goal of dispositioning advisories

- When possible use advisories preventively to avoid problems when procuring
- Eliminate or mitigate risks associated with advisories
- Avoid increasing risk in projects through unintended consequences
- Properly document closure

Risk-Based Examples

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

Examples

- Printed circuit board coupon NC process
  - Over 400 panels would have been rejected by previous process with no elevated risk (hundreds of weeks, $Ms)
- PCB bromine restriction
  - Requirement prompted vendors to change working processes, caused substantial increases in cracking, crazing, and wicking
- PCB copper wrap requirement
  - Requirement for blind and buried vias, costly and difficult to meet, testing proves no reliability improvement
- Bi-polar junction transistors
  - Overly conservative failure prediction of moisture alone prompts much riskier rework in fully tested system
- DC/DC converters
  - Warnings about common converters drive projects to much lower quality devices
- ELC reverse capacitors
  - Assessment did not properly consider moisture effects
- Laser-hole GIDEP
  - Low incidence concern leads to high risk rework

Specific Efforts

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Past and Current Efforts

- Correlation of parts failure rates (ground and on-orbit) against screening levels (1, 2, 3)
  - Requirements should be commensurate with actual experiences
  - No correlation determined
- Characterization of reverse capacitors
  - Moisture and temperature effects
- PCB reliability vs selected standard (IPC 6012, Class 2, Class 3, Class 3/A, MIL-55110)
  - Copper wrap testing complete, IEEE paper produced, IPC addendum produced
  - Internal annular ring testing completed
  - Etchback coming soon
- Compatibility between high-end PCB standards and high-pin-density parts
- BJT moisture testing – how much does elevated moisture increase the risk of failure?
  - Moisture alone is not sufficient to cause part failure
- Cracking ceramic capacitors
  - Is it installation/thermal shock or a lot problem
  - How to identify specific manufacturing problem that has lingered for years (internal cracks)
- Cubesat reliability
  - Inherited items process principles to cubesats and standard cubesat components

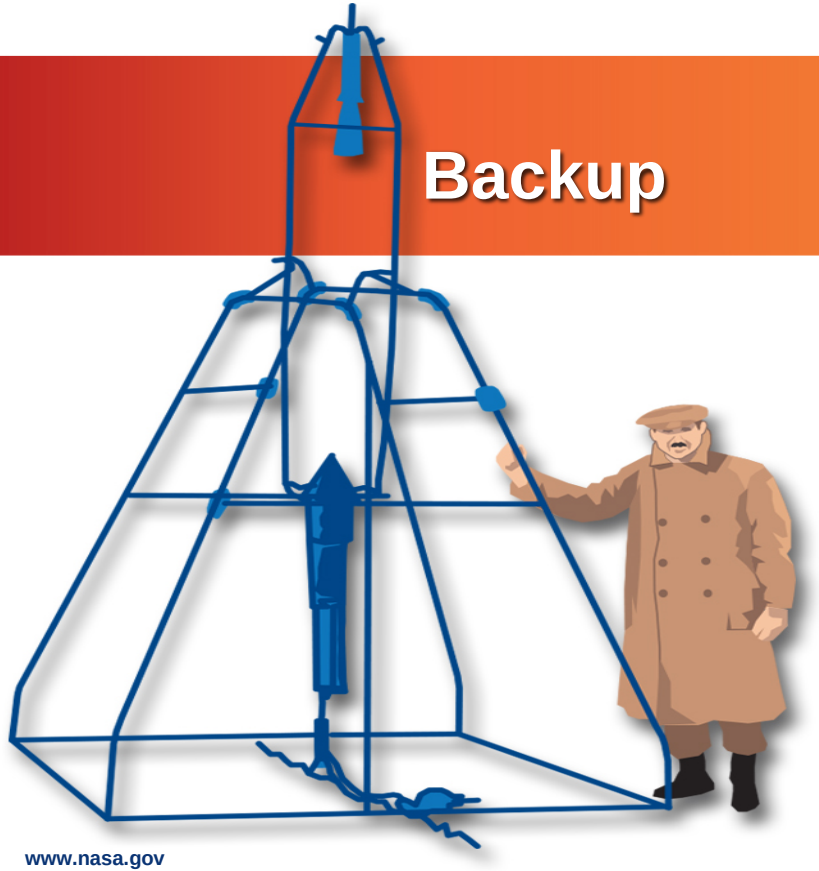
Summary

We talked about:

- Risk Classification
- Layered risk reduction efforts to eliminate defects
- GPR 8705.4
- Risk-based SMA attributes
- Lessons Learned and New Positions
- Inherited items process
- EEE parts
- Materials
- Printed Circuit Boards
- Alert and advisory handling

Additional Information

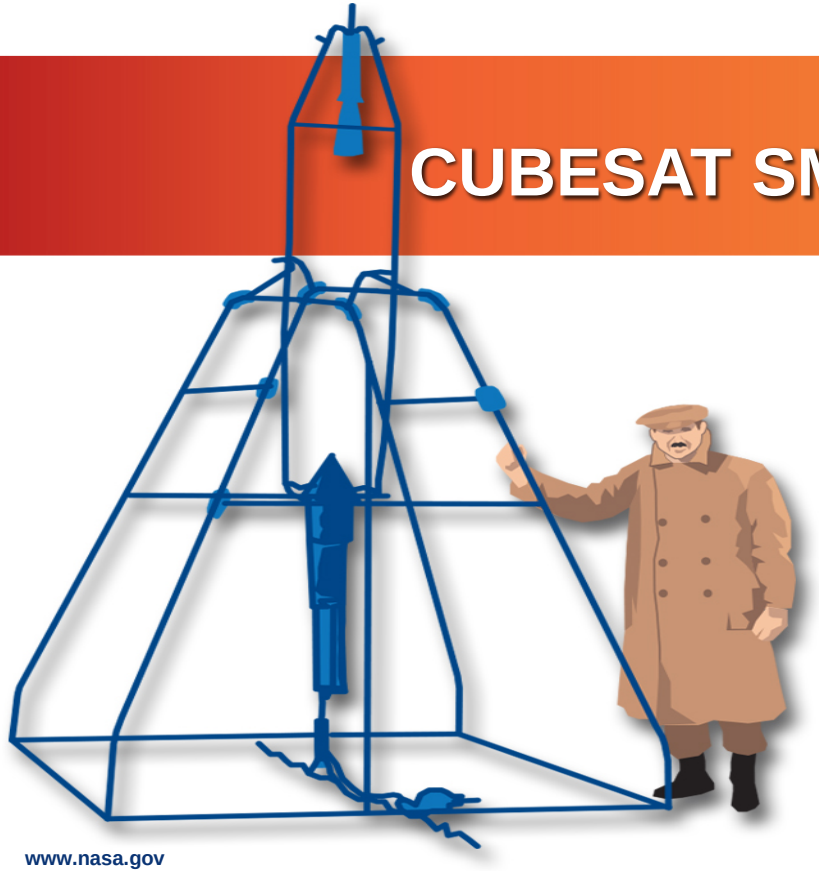
- **Link to GSFC Risk Assessment handbook:** https://standards.nasa.gov/center-specific-standards
  - Then select GSFC-HDBK-8005
- **Link to download GPR 8705.4:** https://elibrary.gsfc.nasa.gov/_assets/doclibBidder/tech_docs/GPR%208705.4-Signed%20Copy%20-%20Copy.pdf
- **Link to download GPR 8730.5:** https://elibrary.gsfc.nasa.gov/_assets/doclibBidder/tech_docs/GPR%208730%205_Signed%20Copy%20-%20Copy.pdf
- **Link to download Risk-based Safety and Mission Assurance article in *Quality Engineering:*** *https://www.tandfonline.com/doi/full/10.1080/08982112.2018.1473584*
- **Link to download IEEE paper on copper wrap study results for printed circuit boards** *https://doi.org/10.1109/TR.2018.2835140*
- **Contact Info:** Jesse Leitner: jesse.leitner@nasa.gov



Backup

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

CUBESAT SMA recommendations



SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

Cubesat
(M. Johnson 3 Nov 15)

- A miniaturized satellite consistent with standardized form factors used for space applications
  - Developed by Cal Poly and Stanford in 1999
  - Consists of any number of 10 cm x 10 cm x 10 cm units, or “U”s.
  - Each U has a mass around 1 kg, not to exceed 1.33 kg.

Risk posture for cubesats

- CubeSats can have any associated risk posture, depending on the importance
- Typically, the risk class would be D, NPR 7120.8, or Do No Harm
  - Lower importance missions using faster and more flexible options to obtain quick results at greater risk
- However, in some cases size may be the driver and risk tolerance will be lower
- There are SMA attributes tuned to the higher risk tolerance, and others that are tuned to the compact size or rapid development approach
  - No one-size-fits-all approach for cubesats in general

Special attributes

- Rigid size and mass limitations
  - Have to rethink connectors and wiring in general
  - Greater number of PCB layers
  - Thermal and EMI – more close neighbors
- Launch options will bring their own special constraints
  - New devices with hazards prompt new analyses
  - Significant uncertainty in the launch environment
- Trades for qual benefits for heritage devices vs constraints

SMA approach

- Driven more by risk classification vs fact that we have a cubesat (GPR 8705.4)
  - However, door must be opened to many past prohibited items (must “do no harm” to neighbors) even at lower risk postures
- Parts and materials – based on risk class
  - Connectors – think wireless or common commercial connectors
- Reliability
  - Focused more on how can we best apply our resources
  - Where to inspect
  - Fault tolerance in highly constrained space
- Design for manufacturability: Can we really build this under the constraints?
- Driven almost entirely by detailed engineering analysis instead of broad requirements
- Heritage items are great, but can constrain the design
- **No longer can count on the margins and barriers of protection we have always worked under**
  - Risk vs possibility
- We will have to scrutinize all broad requirements before applying them to a cubesat of any risk posture because most of the margins are not available to absorb excess
  - Must be risk-based
- Should strongly consider multi-cubesat architectures where loss of one or two cubesats minimally affect mission performance, but no potential increase in debris risk

Inherited items

- Many standard CubeSat components now exist
- Substantial reliability benefits of previously qualified items
- However, these give rise to constraints that will increase the system design challenge

Environmental Test

- The GSFC approach has always been to endure large amounts of programmatic risk in order to minimize technical risk (Class A/B approach)
  - This gap will have to narrow for any cubesat application or many will not make it to orbit
  - However, tight thermal control may not be nearly as achievable, therefore wide-range thermal testing may be necessary
  - Cubesat version of GEVS has been developed and baselined

Reliability

- Should we think about reliability for cubesats?
  - Absolutely, it's as important as for any other type of space system
  - Focus more on the tall poles and weak points than on long lifetime
  - Upfront reliability analysis helps focus requirements on critical areas
- Not much room for redundancy within a cubesat so fault-tolerance is best enabled through multi-cubesat architectures with redundancy or graceful degradation

Significance of Board Requirements

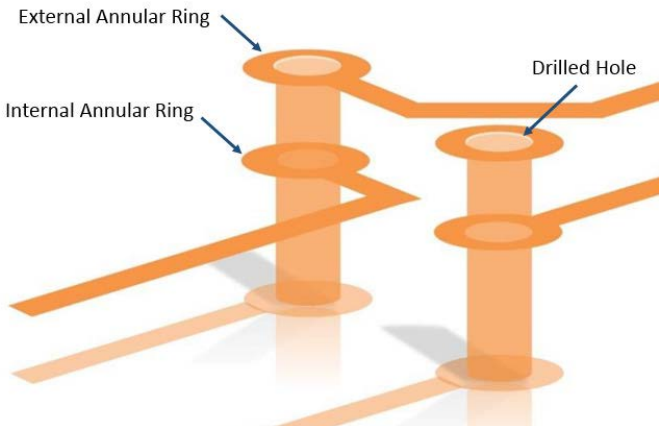
- The requirements and coupons are a “front door”.
- Examples:
  - Internal Annular Ring:
    - Egregious violations indicate there may have been a serious problem in development of the board.
    - Minor violations don’t likely indicate any risk at all (IPC-6012DS)
  - Negative etchback:
    - With modern cleaning processes and flight experience can result in higher reliability with negative etchback.
  - Wicking of copper:
    - Requirements are conservative based on broad statistics.
    - A basic analysis of the board layout can indicate directly if there is risk or not, regardless of requirements violations.

Re-evaluation/testing of requirements

- Regular nonconformances were common in copper wrap requirement in IPC 6012, especially on European products (Cu wrap reqmt was not in ECSS standard) caused significant cost and concern for multiple projects
- Risk assessment was difficult based on our capabilities at the time.
- Researched the problem and set up 3 independent testing activities
  - Thermal testing of coupons from affected project (over 50 project thermal lifetimes)
  - Aggressive thermal testing of many different board designs with varying wrap thicknesses
  - IST (Interconnect stress testing) of several representative designs
- Findings: insufficient wrap thickness does not affect reliability, failures seen were barrel cracks (unrelated to wrap thickness), earlier with more wrap
- Prompted group within IPC to re-evaluate the requirement

Internal Annular Ring (IAR) Assessments

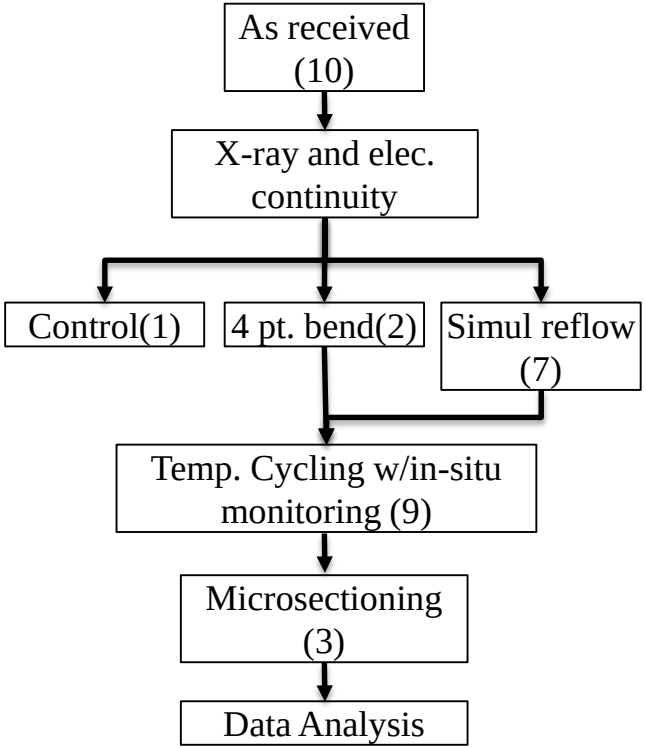
- Design in variations in the internal annular ring geometries in printed circuit board and correlate the effects of these variations as a source of risk for PCB failure in GSFC test and mission environments.
- Reliability tests such as temperature cycling and mechanical flexure conducted on test samples constructed with control IAR widths, sub-optimal IAR widths and other configurations such as teardrops.



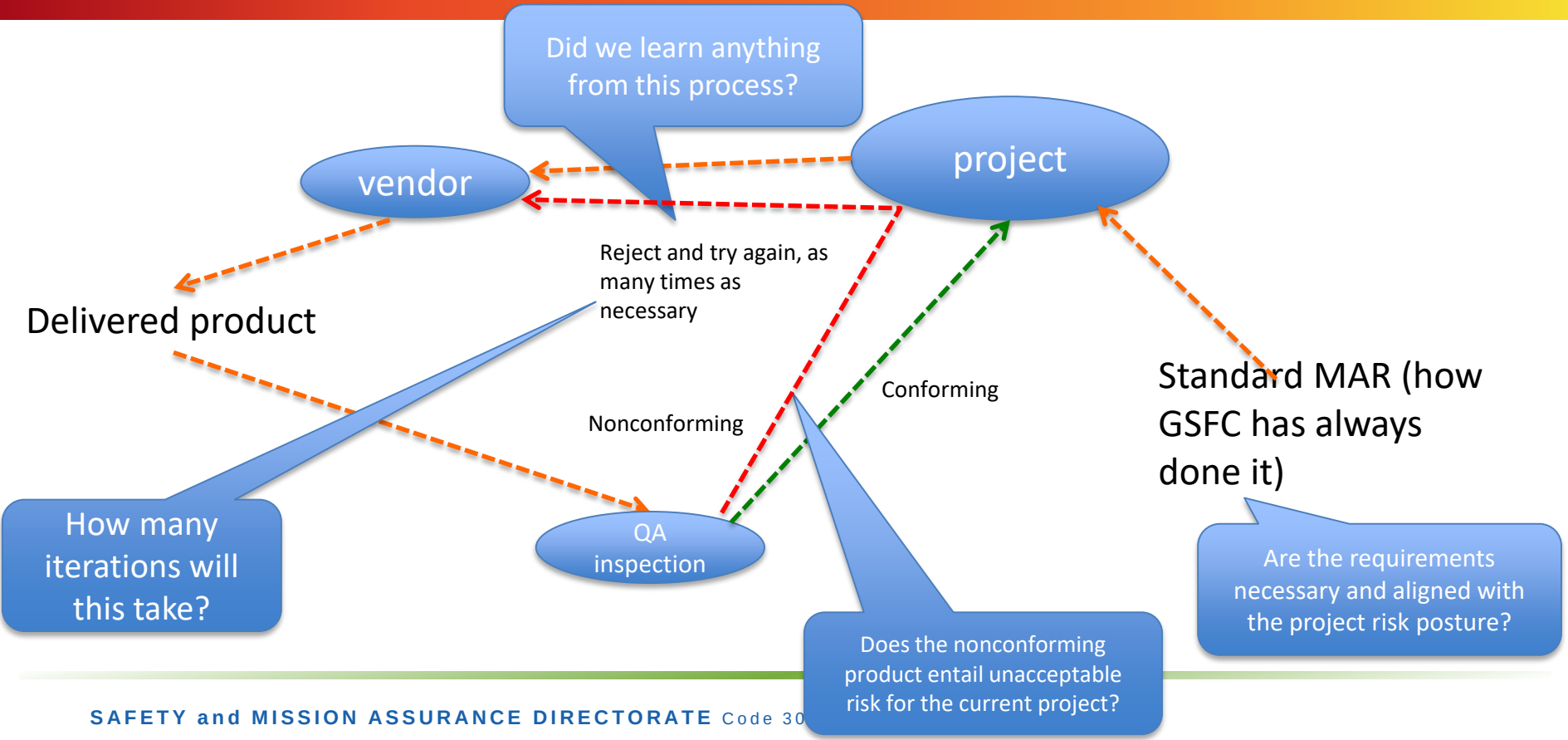
- **Outcome:** On the basis of this work, it may be determined that IAR should be between 1 mil and 2 mils, similar to IPC 6012C 3/A specifications, it can be lower than 1 mil (0.5mil) or in a teardrop configuration if it can be determined that minimum IAR size does not have an adverse effect on the reliability of PCBs and does not increase the risk of failure for GSFC missions.

IAR Experiments – Test Flow

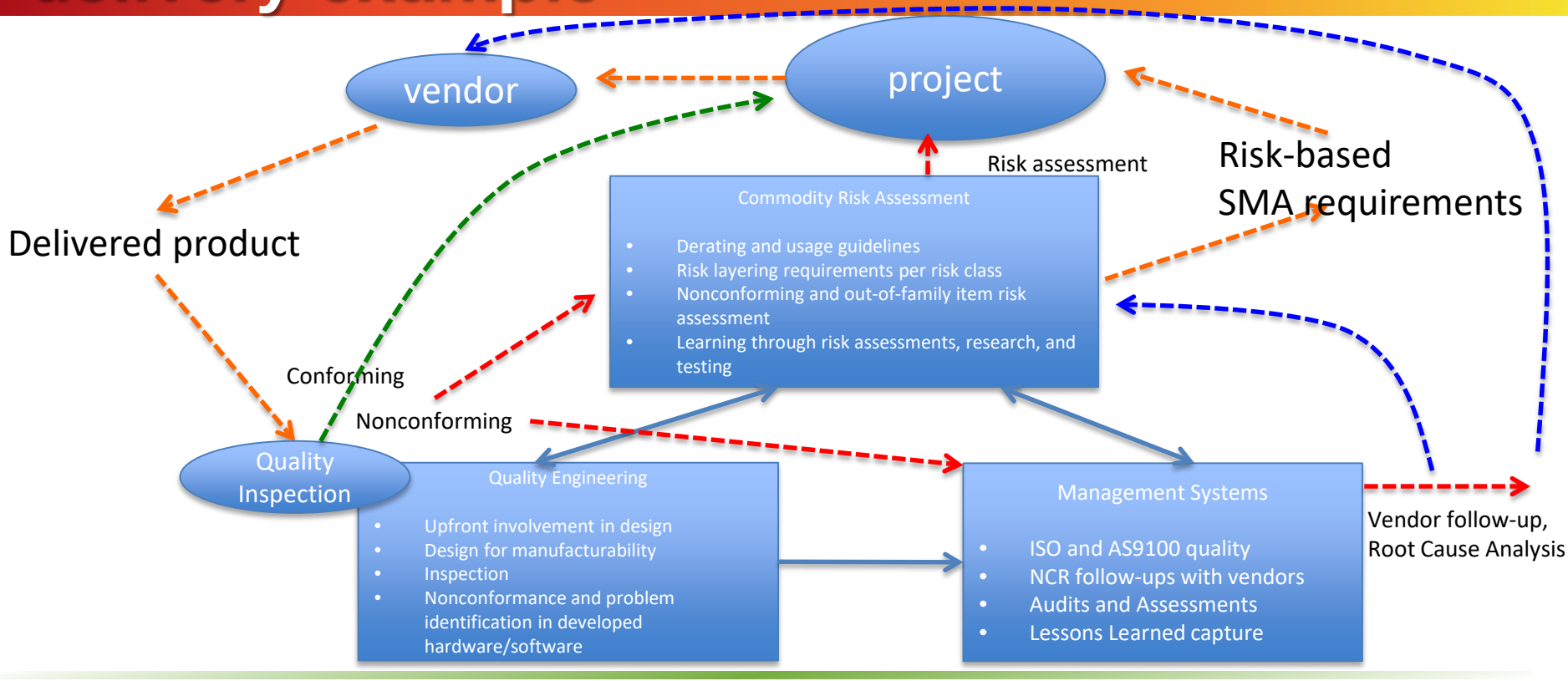
- Board x-ray inspection documents variations amongst facilities and effects of tolerance stacks within test boards fabricated with varying IAR configurations.
- AB/R design comprising donuts and circles from IPC-2221B replicated in whole or in part on four corners of each test board.
- The AB/R locations of each test board inspected in real-time 2D x-ray system and documented.
- These methods provide for 360° registration without the need for microsectioning at the receiving.
- Limited microsectioning performed after the accelerated tests were completed.
  - Results of the x-ray inspection correlated with micro-sectioned samples.



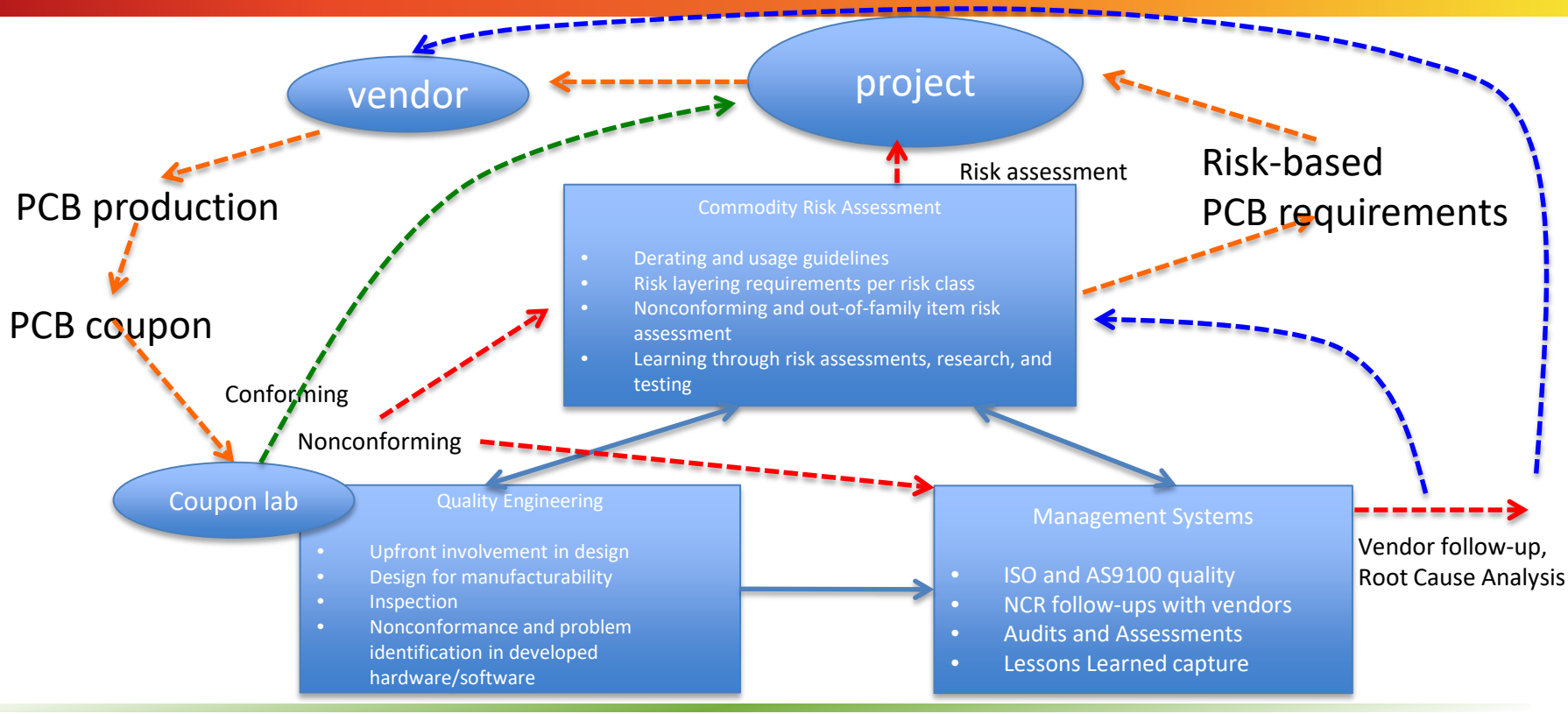
300 day in the life example - yesterday



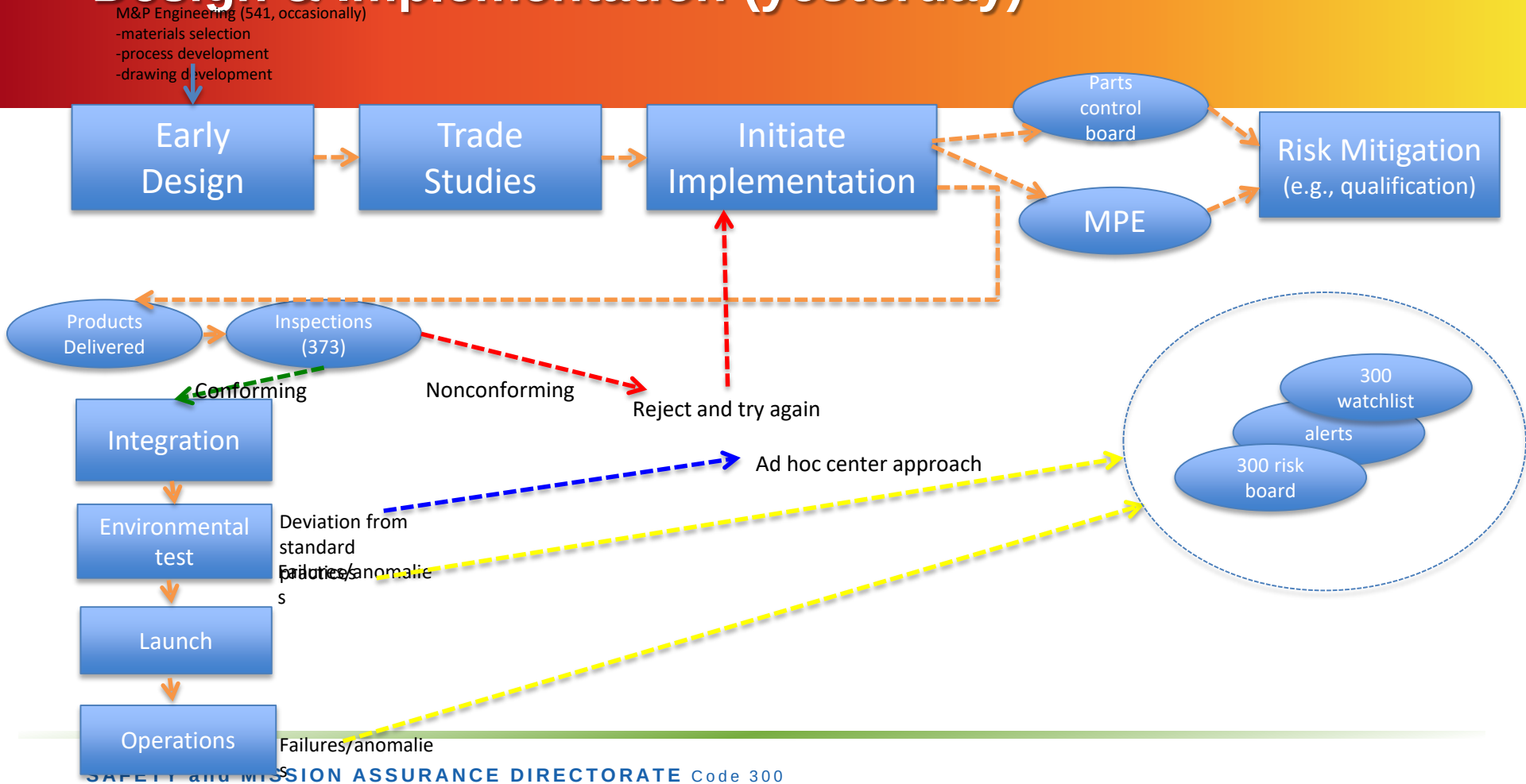
New 300 day in the life - generic product delivery example



New 300 day in the life PCB example



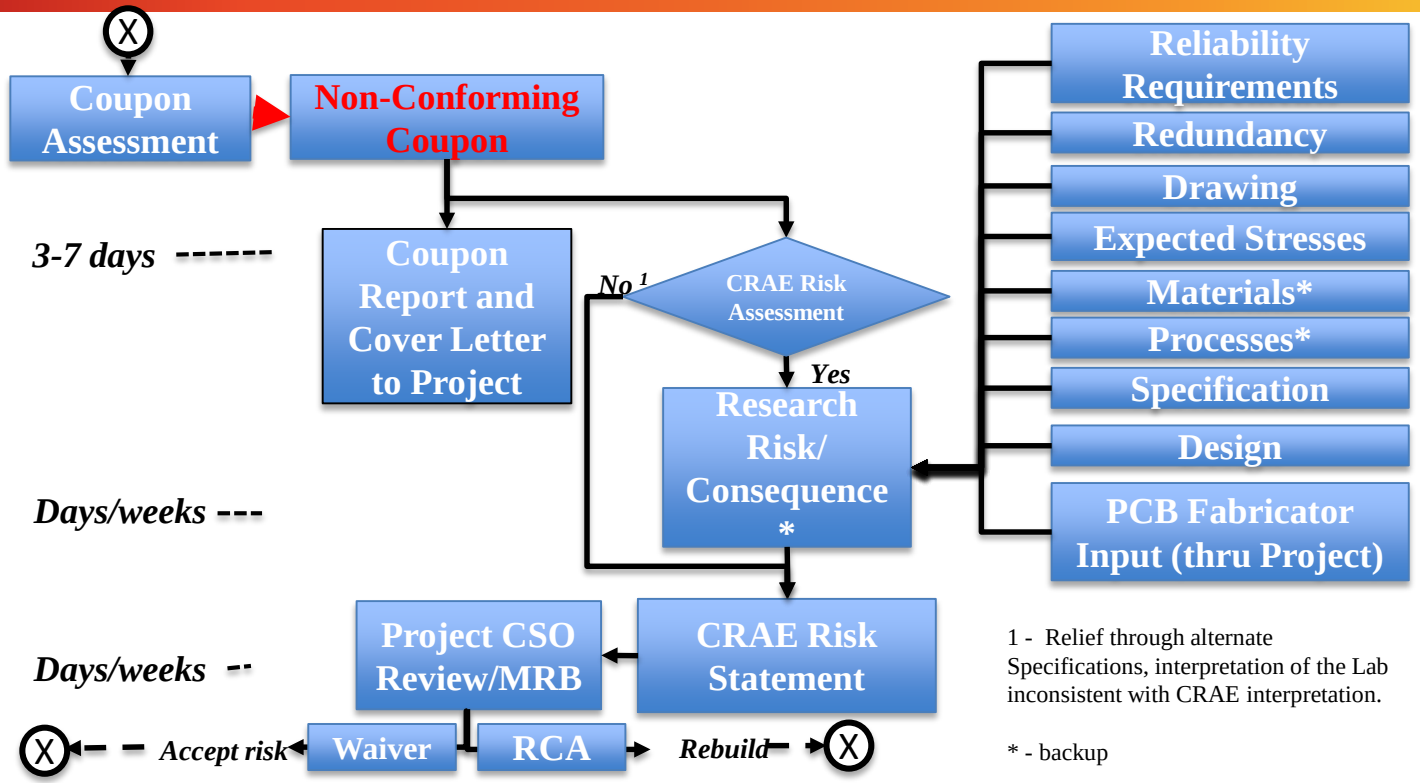
Design & Implementation (yesterday)



Risk Assessment

- Traceable PCB test coupons (designed per specs. such as IPC-2221B) are submitted to GSFC or to a GSFC-assessed laboratory.
- Reports that indicate nonconformance are dispositioned by risk assessment performed prior to refabricating or populating the PCB.
  - If risk assessment indicates elevated risk due to the nonconformance, then use is dispositioned by MRB.
- More than 400 PCB lots assessed for risk since 2014, with about 80% dispositioned as UAI, resulting in significant cost and schedule savings.
- Risk assessment process eliminates waste and saves money and schedule, lowers overall risk for the project

Risk Assessment Approach

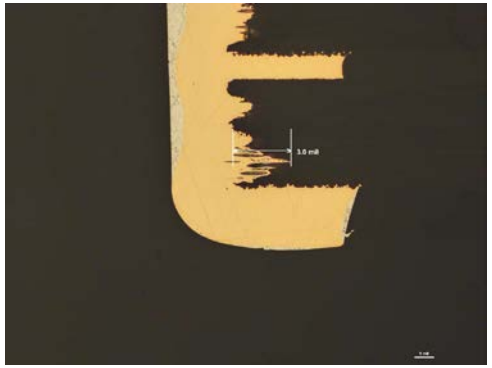


1 - Relief through alternate Specifications, interpretation of the Lab inconsistent with CRAE interpretation.

* - backup

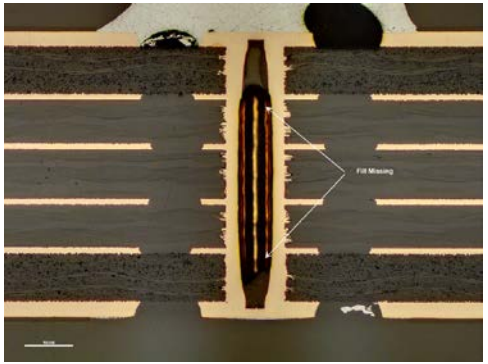
Sampling of Risk Assessments – 1

Copper wicking in excess of 2.0 mil



The wicking is well-enclosed within the annular rings with significant margin, and should not violate electrical spacing. When inspected with IPC-6012 DS, these boards would be compliant (max 3.5 mil wicking + etchback).

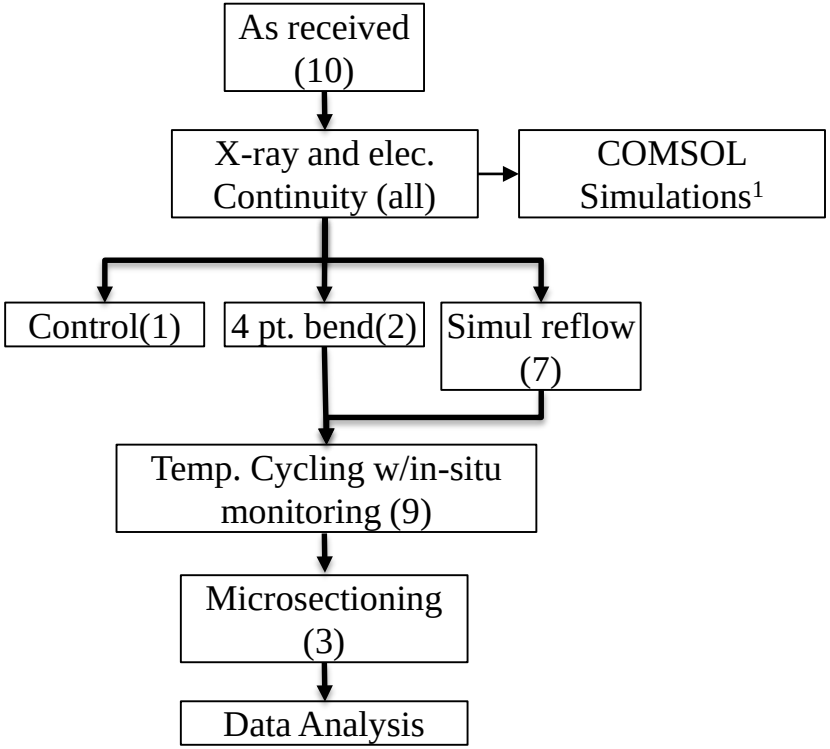
Capped via with fill less than 75%



Voiding is contained and enclosed within the fill material (with matches in CTE with the PCB laminate), and does not appear to have an interface with the cap where contaminants could potentially trap.

IAR Assessments – Test Flow

- Goal of board x-ray inspection is to document variations amongst facilities and effects of tolerance stacks within test boards fabricated with varying IAR configurations.
  - X-ray provides a method to assess 360° registration without the need for microsectioning.
  - Limited microsectioning will be performed after the accelerated tests are completed.
  - Results of the x-ray inspection are used for COMSOL simulations and correlated with micro-sectioned samples[1].
- Four-point bend and simulated reflow provide the necessary preconditioning stresses prior to thermal cycling.



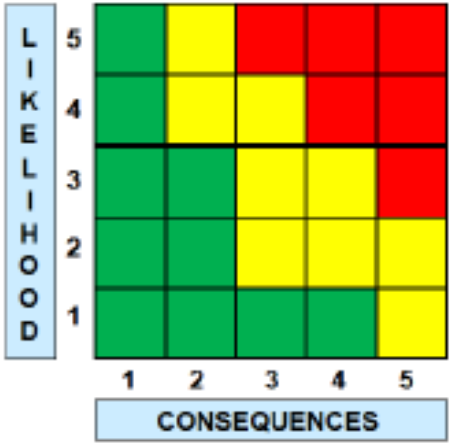
1- Comparison of Registration Errors Amongst Suppliers of Printed Circuit Boards, Bhanu Sood and Lionel-Nobel W Sindjui, IPC APEX Expo 2018, February 27 - March 1, 2018, San Diego, CA.

Process

- When coupons are nonconforming to the project spec (per project MAR), the report goes to the PCB CRAE
- The CRAE forms the PCB working group with project representative(s)
- Risk assessment is performed considering the nonconformance, criticality, environment, and lifetime.
  - If coupon is compliant to any of the approved specs for the mission risk class, then board is considered baseline risk
- Risk (if any elevated) is provided to project and project decides whether to accept, reject, or mitigate in other ways
- If projects choose to respin, they must determine the cause for the nonconformance before respinning.
- High NC rates with no elevated risk indicate requirements problem

Impact of Non-conformances

- Bare boards cost $$ and build schedules – expensive!!
- But failures are even more expensive!
- Test sample nonconformance is not the same as PCB failure.
- Risk-based decisions are used for disposition of non-conformances.
- Non-conformances may have little to no impact per application.
- Began to explore origins and merit of requirements (more later).

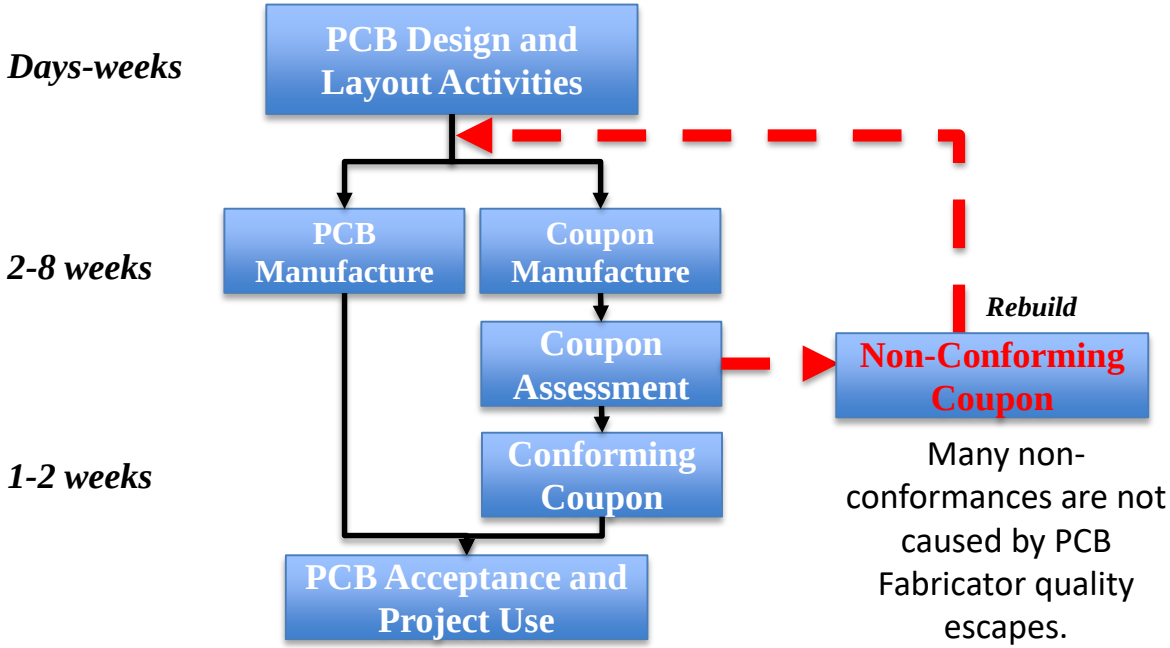


Microsectioning

- Suppliers perform microsectioning and inspect per specifications.
- Secondary GSFC independent microsection analysis yielded 20-30% inspection rejects, caused by:
  - Screening escapes:
    - Test sample quality not consistent
    - Supplier microsection process
  - Requirement interpretations
  - Requirements flow-down issues
    - Alternative specifications (MIL, ECSS)
    - Buying heritage and off-the-shelf designs

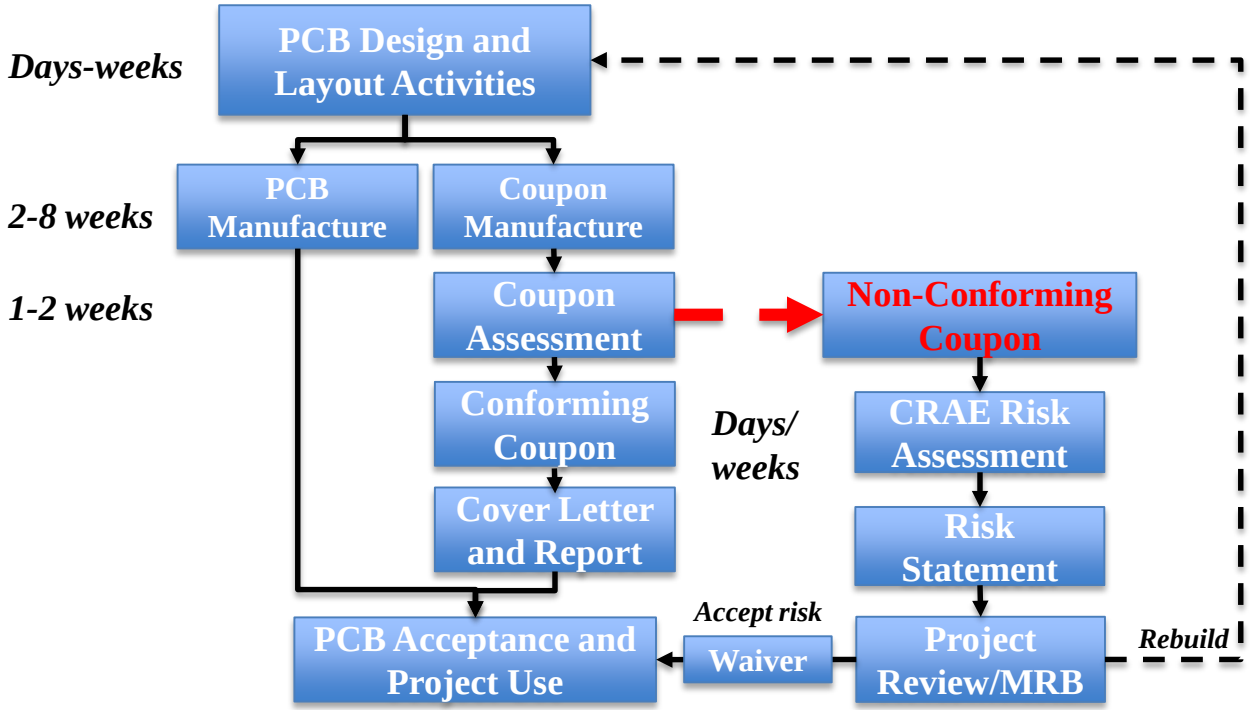
PCB Assurance – Historical Approach

We see a general 20-30% rate of non-conformance, a large portion is not a result of quality escapes.



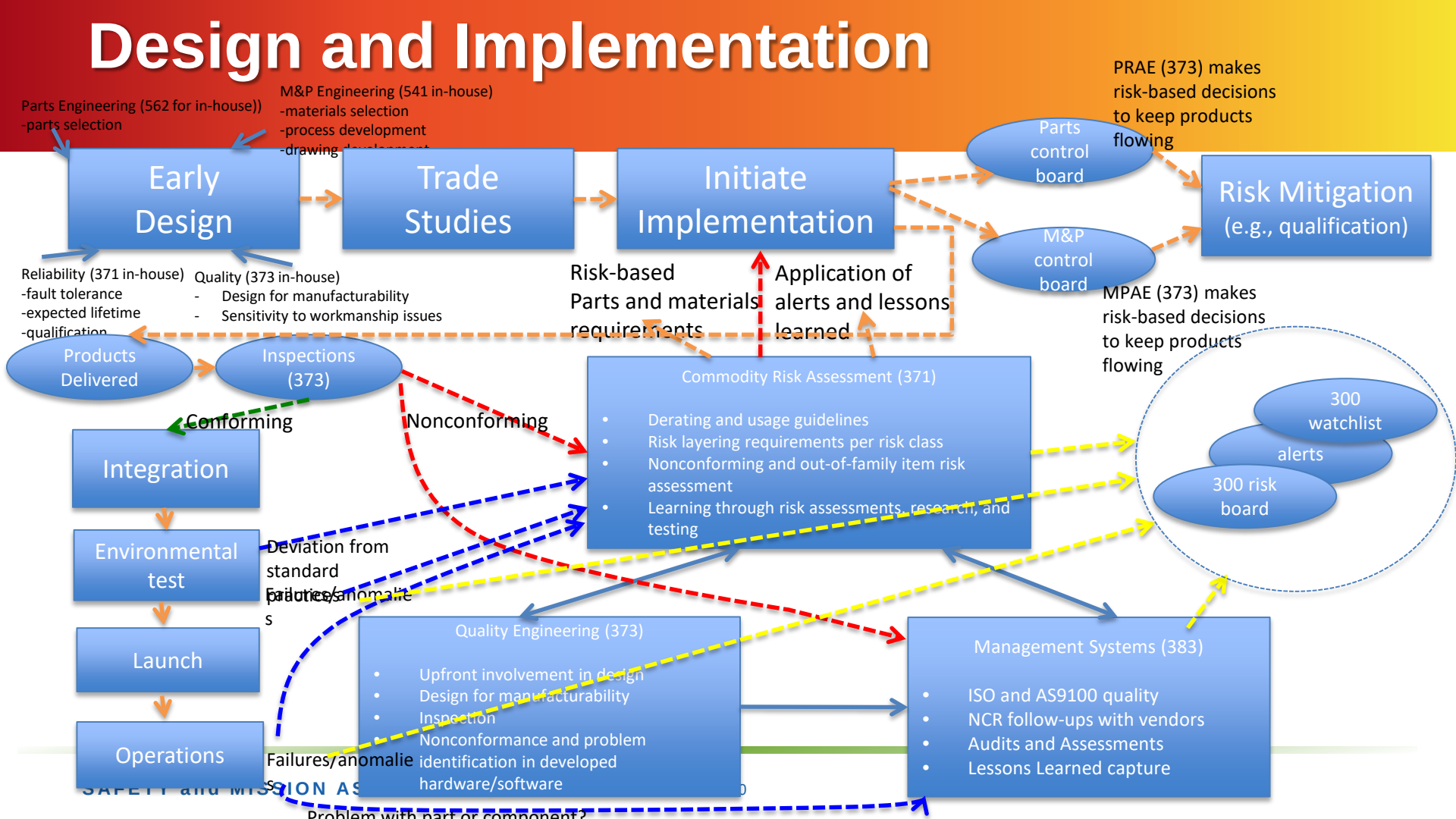
Inconsistencies between specifications, contract requirements, design drawings, production documentation, and coupon inspection lab submittals. Requirements were ambiguous. Voluntary consensus Standard requirements were interpreted conservatively, without a basis in risk.

PCB Assurance – Current Approach



Code 300 determines the risk, project decides whether to accept the risk.

Design and Implementation



How do a few weeks affect a project

Subsystem/Hardware	5/1/2016	6/1/2016	7/1/2016	8/1/2016	9/1/2016	10/1/2016	11/1/2016
Digitizer Unit (DU)	13 days	13 days	14 days	15 days			
Integrated Electronics Unit (IEU) to FSW	34 days	34 days	34 days	19 days			
Laser Electronics Unit (LEU)	9 days	9 days	18 days	18 days			
Harness	21 days	22 days	28 days	28 days			
Power Converter Unit (PCU)	24 days	25 days	31 days	31 days			
Primary Structure	9 days	9 days	29 days	29 days			
Optical Bench	6 days	6 days	40 days	40 days			
Thermal	21 days	21 days	20 days	20 days			
Optical (Receiver Telescope Assy)	44 days	44 days	29 days	29 days			
Optical (Transmitter Optical Assy)	3 days	3 days	12 days	9 days			
Optical (Detector Optical Assy)	6 days	7 days	14 days	14 days			
Optical (Rx Fiber & Fiber Array)	56 days	51 days	39 days	39 days			
Q-Switch Driver	2 days	2 days	4 days	6 days			
Laser (waiting on Q-Switch)	2 days	2 days	6 days	6 days			
Beam Dither Unit (BDU)	7 days	7 days	13 days	8 days			
Detectors	5 days	5 days	13 days	16 days			
Pointing Contr. Syst (PCS) GPS Recv.	13 days	13 days	13 days	13 days			
Pointing Contr. Syst (PCS) GPS Antenna	70 days	70 days	116 days	116 days			
Pointing Contr. Syst (PCS) Star Tracker	21 days	21 days	21 days	21 days			
Pointing Control Mech. (PCM/MCE)	23 days	23 days	23 days	23 days			
Flight Software (FSW) Build 2 (ETU IEU)	10 days	10 days	10 days	10 days			
Flight Software (FSW) Build 3	12 days	12 days	12 days	12 days			
Boresight Adjust. Mechanism (BAM)	20 days	20 days	20 days	20 days			
Aperature Cover Mechanism (ACM)	42 days	42 days	42 days	42 days			
Bench Checkout Equip (BCE)	43 days	57 days	44 days	20 days			

Slack Decrease ---------

Slack Increase ---------

Task 1: Initiate Inheritance Plans

- Project develops plan that can be in the form of project document or presentation (and must be kept up-to-date)
  - Project Inheritance Plan should include a list of potential inherited (heritage) items suitable for mission.
    - This can be list populated from project plans, vendor proposals and/or heritage reviews
    - Suitability and/or caveats should be attached or supplied with plan
  - Project with the assistance of SC CRAE and PDLs/Vendors assesses data availability

Example of Item List with Data Availability

Component	Testing Summary and Comparison	Storage / Flight History	Ground and On-orbit Performance	Reliability Analyses	Deviations from original design	Specifications and/or standards used to develop the item	Previous as-built parts list, including lot date codes, GIDEPs, and the differences for new inherited item	Known obsolete parts	Materials list and approved Material Usage Agreements (MUAs)	List of major electrical and mechanical analyses	Identification of significant changes in manufacturing
	Data Avail from Vendor										
		Data On Hand									
	Data Avail from PDL		Data Avail from Vendor/ Meta								
			Data avail from SC CRAE	Data On Hand but has Liens							

Task 2: Perform and Document Inheritance Data and Assessments

- Project/CSO gathers Inheritance Data Package for each item or group of items from SC CRAE and PDL/Vendor data stores
- Project/CSO prepares Inheritance Data Package for each item or group of items
- Project/CSO distributes an Inheritance Data Package within 30 days of MCR/ATP to SC CRAE/SMA
- SC CRAE convenes Inheritance Review Panel with experts consistent with inheritance items/plan

Task 3: Conduct or Support TIMS/WGs and Reviews

- SC CRAE manages the review of Inheritance Data Package(s).
  - Ensuring expert assessments are attained to support project deadlines
  - Arranging TIMs and WGs to facilitate data exchanges and clarifications to develop a proper risk assessment
- Project can request the SC CRAE convene a formal review for assessment (Note: this would still require the data package(s)).
- SC CRAE Identifies and ensure resolution of open inheritance concerns, action items, and discrepancies;

Task 4: Refine and Finalize Inheritance Assessments

- Project/CSO prepares final Inheritance Data Package for each item or group of items.
- SC CRAE manages the review of final Inheritance Data Package(s).
- SC CRAE supplies Project with a final Risk Assessment and Recommended Path forward (cover letter/memo for package acceptance)
  - Including requirement tailoring suggestions
  - And specific risks and mitigation options
- SC CRAE updates SC CUGs with data supplied for future projects.

Task 5: Obtain Final Inheritance SMA Endorsement and Risk Assessment

- Project accepts and releases final Inheritance Package with SMA Endorsement and Risk Assessment
  - This includes CM submittal and residual risk acceptance
- Project handles inherited item risk as manageable/residual risks and includes them in follow-on milestone reviews and risk management activities
- Project/CSO tailors requirements with SC CRAE assistance as needed

Inherited Items Summary

- Project Benefits:
  - Potential cost and schedule savings
  - Less waiver processing
  - Leverage off previous lessons learned
  - Knowledge sharing with previous missions
  - Use inherited and build-to-print hardware without introducing the additional risk of applying traditional piece part control approach to COTS/OTS/BTP

Objectives

- Minimize administrative burden from established SMA processes, but properly characterize, communicate, and address associated risks appropriately
- Streamline and accelerate processes to move to “use-as-is” disposition for a wide range of SMA-related concerns that the project is stuck with
- Meet the intent of risk-based SMA approach by applying resources primarily to address project risks as opposed to enforcing requirements that may not actually apply.