A Layered Philosophy for Risk Classification, Low Cost (Class D & below) Mission Development, and Risk-based SMA

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

October 21, 2014

Agenda

- Risk Classification and Class D
- Layered risk reduction efforts to eliminate defects
- GPR 8705.4 introduction
- Low cost mission categories
- Center challenges
- Approaches for EEE parts for low cost projects
- What is risk-based SMA?

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**
  - 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**
  - 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 (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

Risk Classification
(Non-NPR 7120.5 Projects)

- **NPR 7120.8 "class" – 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 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

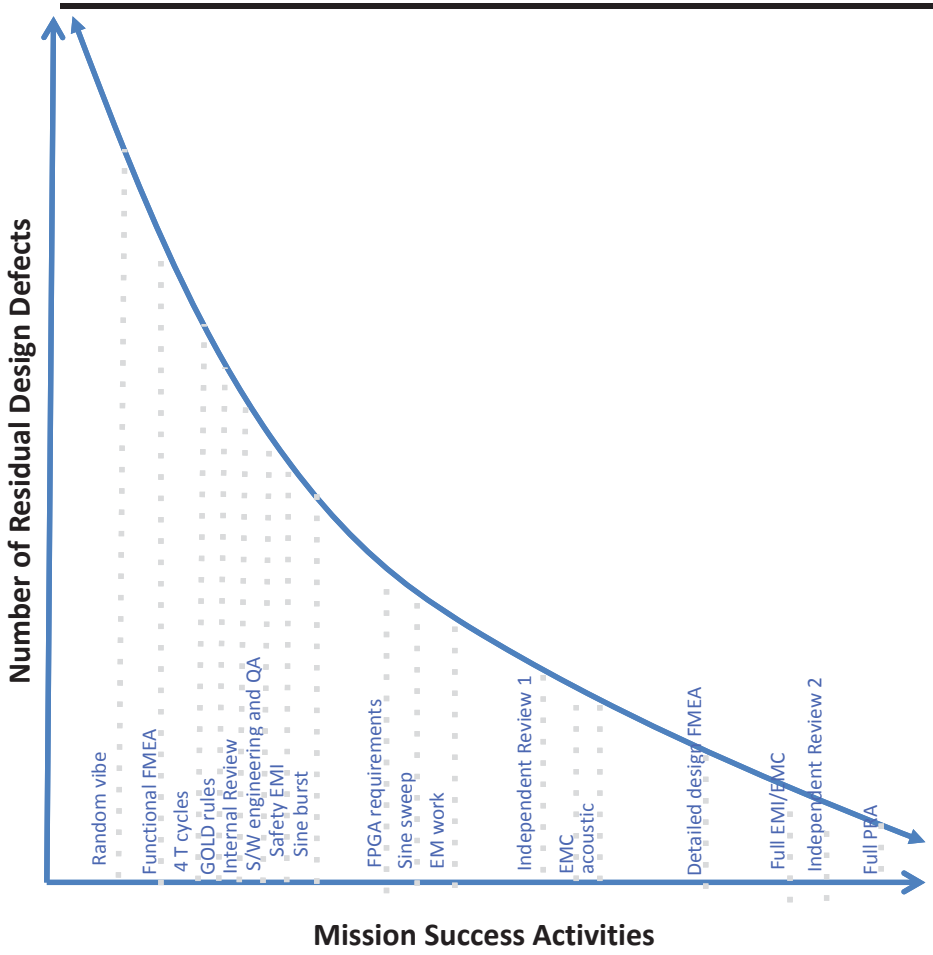
Class D at GSFC

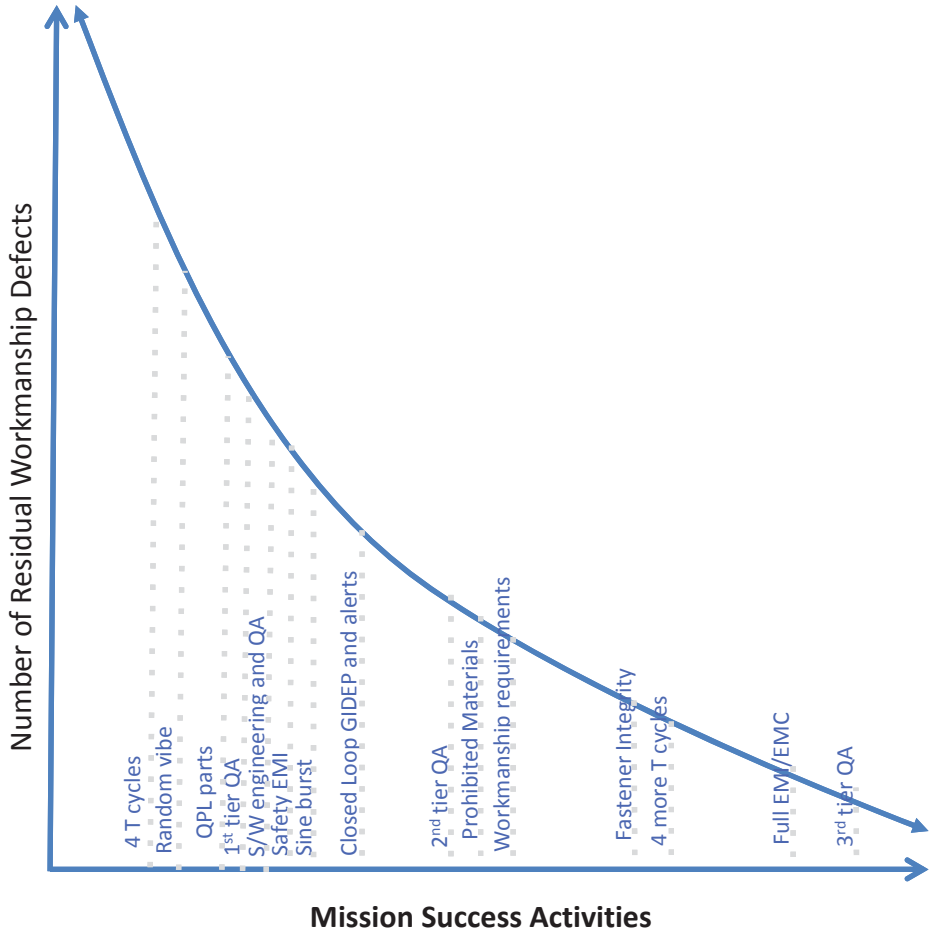
- **What is Class D? =** Highest risk posture for missions governed by NPR 7120.5
- **What is Class D not? –** A catch-all for projects that are not NPR 7120.5 Classes A-C
- ***Is there a problem unique to Class D at GSFC?***
  - **No**
    - There is an unbalanced approach to risk that affects Class D more than others
    - There is a lack of definition of how key processes for mitigating risk vary across all risk classifications
    - These problems even affect Class A
- GSFC Class D Constitution addresses some of the programmatic processes such as management structure, waivers, etc
- GPR 8705.4 effort and new organizational structure addresses the technical processes
- Organizational changes in 300 will provide the infrastructure for implementation
  - Implementation has already begun

Class D (and below) Dos & Don'ts

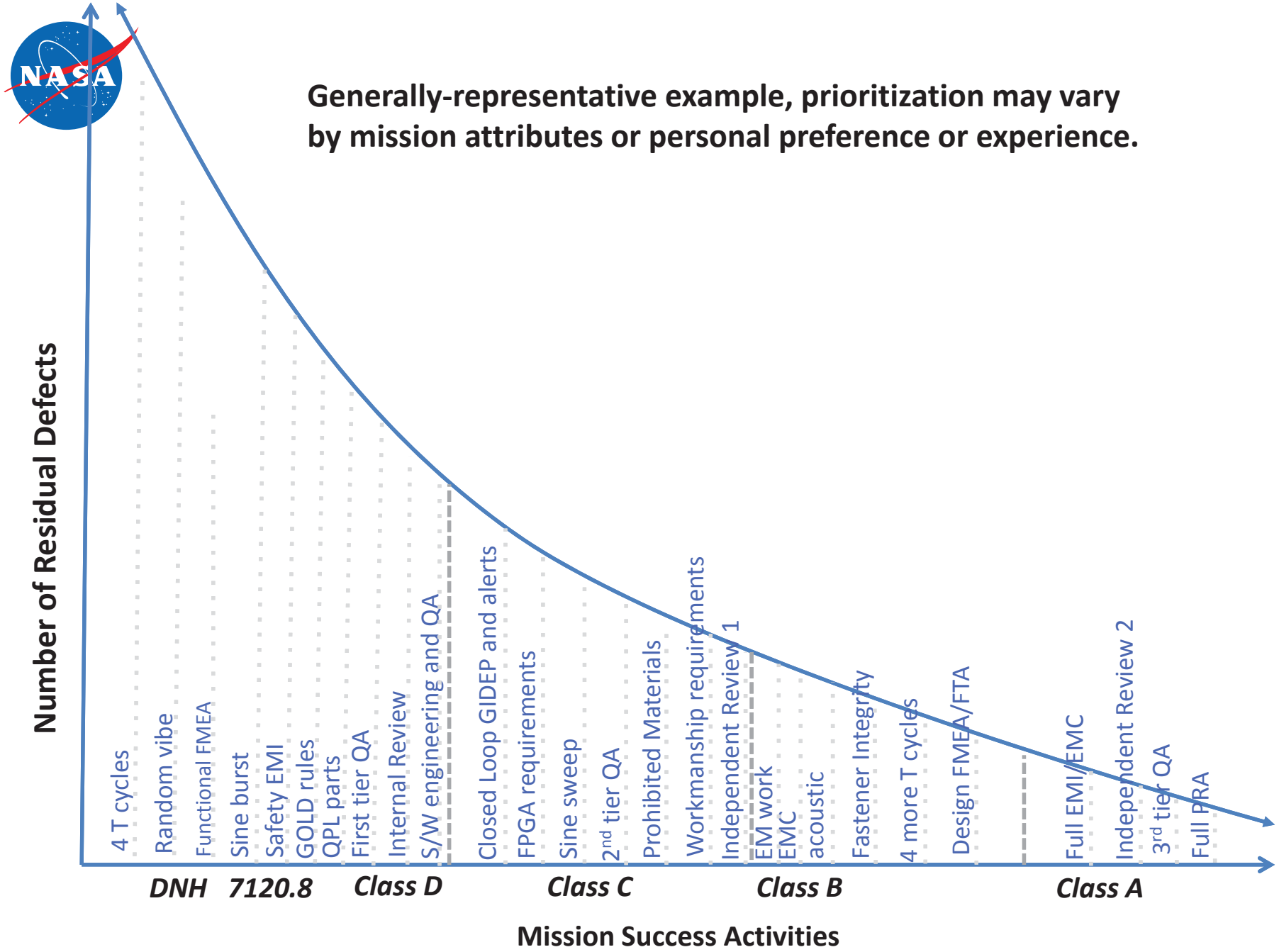
- ***Do:***
  - Streamline processes (less formal documentation, e.g., spreadsheet vs. formal software system for waivers, etc.)
  - Focus on tall poles and critical items from a focused reliability analysis
  - Tolerate more risk than A, B, or C (particularly schedule risk)
  - Capture and communicate 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

Risk can be characterized by number of defects 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

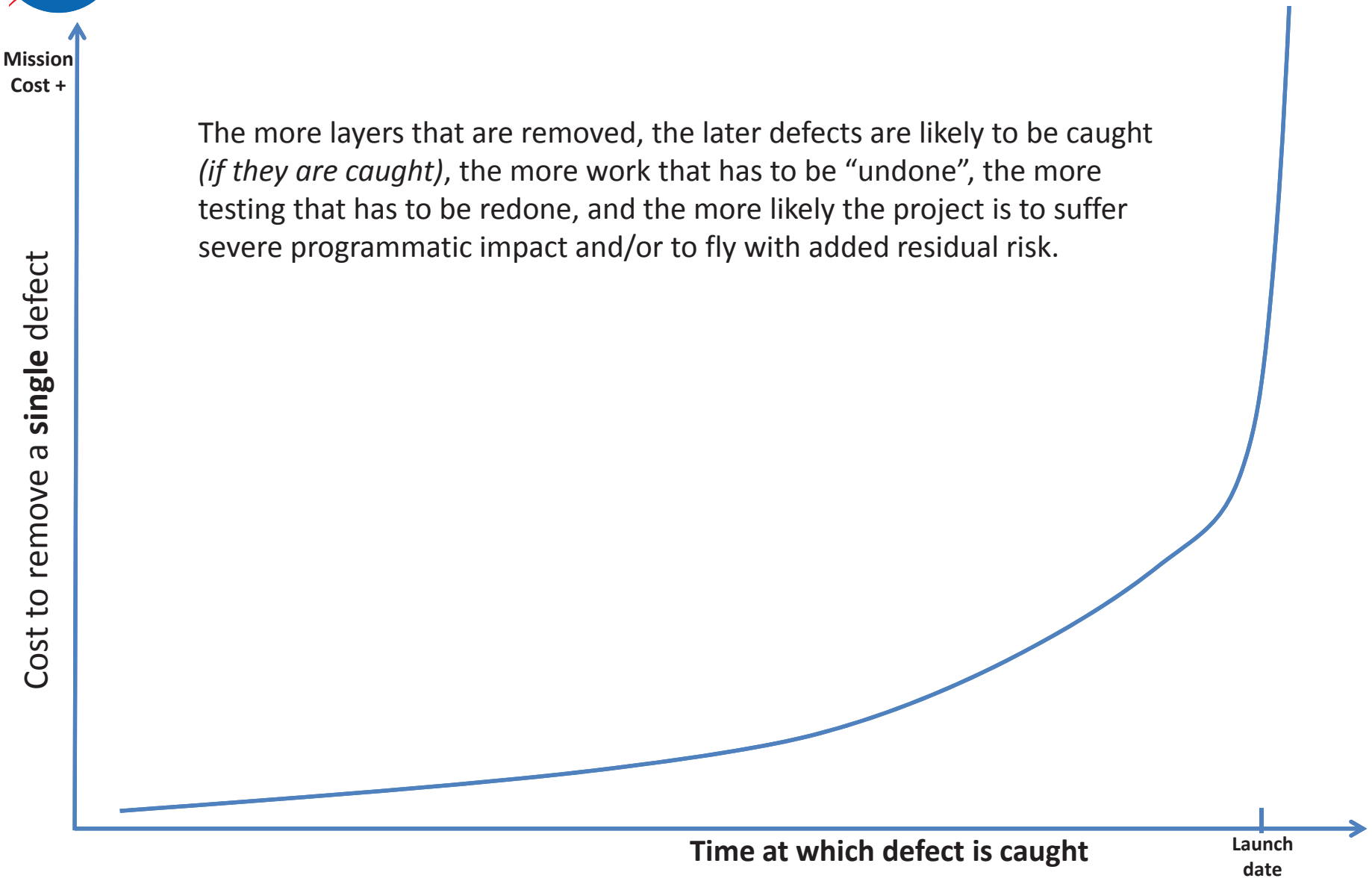

Generally-representative example, prioritization may vary by mission attributes or personal preference or experience.
Number of Residual Defects
4 T cycles
Random vibe
Functional FMEA
Sine burst
Safety EMI
GOLD rules
QPL parts
First tier QA
Internal Review
S/W engineering and QA
Closed Loop GIDEP and alerts
FPGA requirements
Sine sweep
2nd tier QA
Prohibited Materials
Workmanship requirements
Independent Review 1
EM work
EMC
acoustic
Fastener Integrity
4 more T cycles
Design FMEA/FTA
Full EMI/EMC
Independent Review 2
3rd tier QA
Full PRA
DNH
7120.8
Class D
Class C
Class B
Class A
Mission Success Activities

Other Activities with Cost & Risk Reduction Implications

- **Nonconformance handling**
  - Is the requirement that is *not* met important for the current project in its environment?
  - Is the nonconforming item critical?
  - What is the risk for this project of the nonconformance?
    - Cost/schedule
    - Technical
- **Work orders and procedures**
- **Anomaly resolution**
  - Documentation
  - Root cause analysis
  - Lessons learned for same project or others

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

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.



Mission Success Activities vs. Risk Posture
(example elements in draft)

	A	B	C	D	GS	7120.8 class	DNH	Hosted payload (host requirements)
Printed Circuit Boards	IPC 6012B 3/A for rigid PCBs, independent coupon verification	IPC 6012 B 3/A or IPC 6012 C 3/A – negative etchback and 1 mil IARs allowed based on significant heritage and modern cleaning processes	IPC 6012B 3/A, with one mil ARs and negative etchback approved based on heritage, allow vendor to perform their own PCB verifications	IPC 6012B 3, 3/A, or MIL-P-55110 for rigid PCBs, vendor can perform their own PCB verifications	Commercial practice	Best effort, as tailored in project documentation	Best effort	Host practices
Materials And Processes	NASA STD 6016, 541-PG-8072.1, Lot testing of EEE parts for > 3% Pb	NASA STD 6016, 541-PG-8072.1, Lot testing of EEE parts for > 3% Pb	Tailored NASA STD 6016, supply chain and counterfeit controls from 541-PG-8072.1, > 3% Pb for EEE parts, but no lot testing required	Tailored NASA STD 6016, Supply chain and counterfeit controls from 541-PG-8072.1, whisker prevention based on mission duration	Whisker prevention (min 3% lead content or conformal coating). A parts and material review board is needed for custom designed modules	Supply chain and counterfeit controls from 541-PG-8072.1	Supply chain and counterfeit controls from 541-PG-8072.1	Host practices
EEE Parts	Level 1 parts, GSFC S-311-M-70, 500-PG-4520.2.1, EEE-INST-002.	Level 2 parts from EEE-INST-002, except Level 1 & DPA for single point failures.	Level 3 parts from EEE-INST-002, except level 2 parts for single point failures, DPA or pre-cap inspection for hybrids.	Level 3 parts, 500 PG-4520.2.1, DPA or pre-cap inspection on hybrids.	For custom designed module, quality level of parts selected needs to be consistent with the criticality of the module.	Best commercial practices, advise on part selection & derating. ISO certified facilities preferred.	Best commercial practices, ISO certified facilities preferred.	Host practices. Advise on part selection & derating.
GIDEP and other alerts	Full closed loop for all systems	Full closed loop for all elements	Full closed loop for all elements	Full closed loop for all safety critical elements	Full closed loop for safety critical elements and for	Per project documentation	Project	Full closed loop

**Excerpt from current draft of GPR 8705.4*

Risk Classification – All Levels

- **Class A missions can have Class D elements**
  - Non-critical
  - Highly redundant
  - Deliveries with acceptable “defects”
- **Class D mission can have Class A elements**
  - Critical elements
  - Only available
  - Spares from other projects

Class D (and below) Categories

Science Mission (NPR 7120.5)	Research/Technology (NPR 7120.8)	Do No Harm
• Cost > = mission success • Schedule flexible (low priority) • ~6 mo – 2 yr life • Project failure = mishap • Medium technical risks (may fly with many yellow risks)	• Very low cost individual projects • Schedule flexible (low priority) • High technical risk • Very short lifetime (< ~3 months) • Success is determined over multiple projects, e.g., 85% success over one year's worth • Project failure is not a mishap	• Only requirement – do no harm to personnel or other property (e.g. ISS) • Schedule flexible (low priority) • Very high technical risk • Lifetime is best effort • Project failure is not a mishap

Best Applicability of a Streamlined Class D Approach

- **Simple design** (few critical elements)
- **Short mission life**
- **Clear and static science objectives and goals**
  - Sufficient, but not overreaching
- **Robust design** (tolerant to variance in workmanship)
- **Stable and repeatable manufacturing processes** (with known process variances)
- **High Margins** (to allow more design flexibility)
  - Mass
  - Power
  - Volume
  - Specifications: Dimensions, Materials
- **Prior flight experience** (with critical components in the same environment)

Center Challenges and Perceived Challenges for Low Cost Implementation In-house at GSFC

- **GSFC Directives and standards** (more detail in backup)
  - A dozen or so GPRs, centerwide PGs, and standards for workmanship, environmental test, and GOLD rules
  - Mostly handled by common practices
  - Risk classification is not handled well for those that have significant impact
  - Software requirements are the biggest burden, without particular basis in risk
- **NASA directives and standards**
  - Numerous NPRs, NPDs, and standards
  - Similar statement to above applies
- **Engineering resource budgeting** – Not closely tuned to streamlined implementation

EEE Parts Approaches – Class D Science Missions

High Quality Parts (~Level 2) (parts-focused fault-tolerance)	"COTS" Parts (architecture-focused fault-tolerance)
- Very selective redundancy - Radiation-tolerance/hardness dependent on environment, usage based on heritage - Closed-loop GIDEP for critical applications - Counterfeit controls	- Life testing dependent on mission life - Use and test multiple "lots" - Avoid SPFs at part level - Maximize graceful degradation due to part loss - Radiation tolerance/hardness dependent on environment, testing as required - Factor in prior experience with specific parts - Expect failures in test and on-orbit - Counterfeit controls

EEE Parts Approach – R&T (7120.8) Missions

- COTS parts for most from reputable manufacturers
- Level 2 for SPFs where affordable
- Very selective redundancy to avoid high likelihood SPFs
- Focused radiation analysis
- Use and test multiple “lots”
- Expect failures
- Perform “tall pole” reliability analysis
- Counterfeit controls

EEE Parts Approach – DNH

- COTS parts
- Use and test multiple lots
- Very selective redundancy
- Expect failures
- Counterfeit control or “sequestration”

What is Risk-Based SMA?

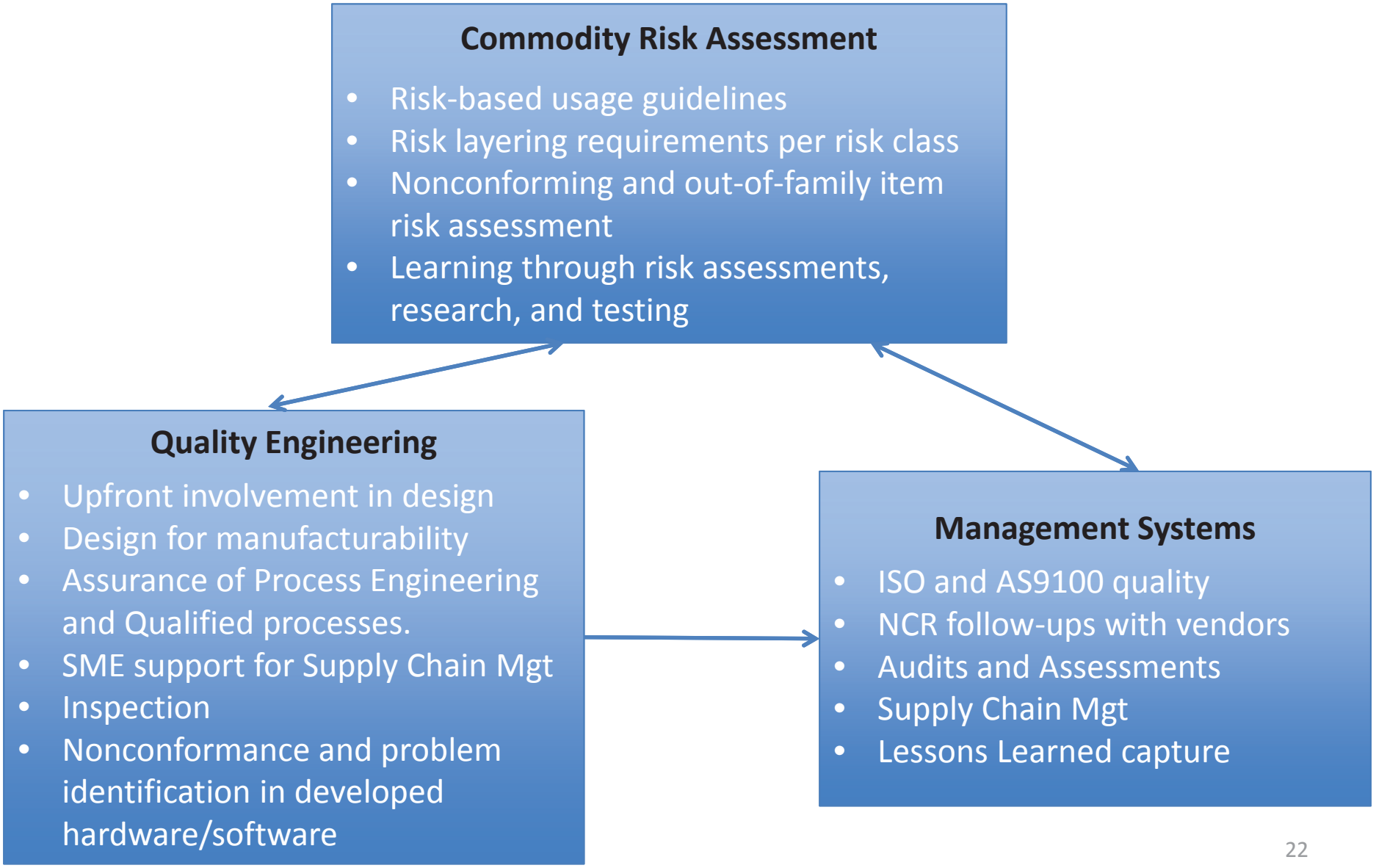
The process of applying limited resources to maximize the chance for safety & mission success by focusing on mitigating specific risks that are applicable to the project vs. simply enforcing a set of requirements because they have always worked

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

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

The GSFC Quality Triangle



CRAE: Commodity Risk Assessment Engineer

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

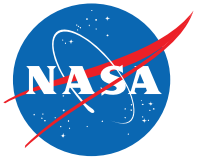
- Expert in key discipline area with background and experience with reliability and risk
  - Responsible and empowered to assign risks based on warnings, alerts, environments, and "what we are stuck with"
    - Establishes testing programs and protocols to keep up with current design practices and common 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 (ownership of GPR 8705.4)
          - 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

Commodity Areas

- Standard Spacecraft Components
- Printed Circuit Boards
- Digital Electronics (esp FPGAs and ASICs)
- Power Systems
- Capacitors/inductors
- Transistors
- Resistors
- Hybrid microcircuits
- Optocouplers
- On-board processors
- Workmanship/Printed Wiring Assemblies/Packaging/Components
- Software
- Materials
- Radiation
- Environmental testing
- Contamination
- Connectors
- ESD

Conclusion

- There are many appropriate solutions to enable mission success for any mission classification
- It would be shortsighted to prescribe a single solution for mission success approaches for Class D, or any other classification
- The context (environment, criticality, lifetime, etc.) is essential to make intelligent decisions
- Guidelines provide a helpful starting point but they cannot replace good engineering practice



Back-Up

Most Broadly Applicable Project-specific Directives and Standards

- **NPR:** 7120.5, 7123.1, 7150.2, 8621.1B, 8715.3C, 8735.1C
- **NPD:** 8730.2C, 8730.5B
- **NASA STDs** (most broadly applicable): 8719.13, 8719.14, 8719.9, 8739.1, 8739.4, 8739.5, 8739.8
- **GPR:** 5340.3, 5340.4, 7120.4, 7120.7, 7120.9, 7123, 7150.1, 7150.2, 7150.3, 7150.4, 8070.2, 8700.4, 8700.6, 8700.7
- **PG:** 500-PG-4520.2.1, 500-PG-8700.2.7, 500-PG-8700.2.8, 541-PG-8072.1.2

Before we get started…….

1. **Constitution Changes to the Preamble – effective now**

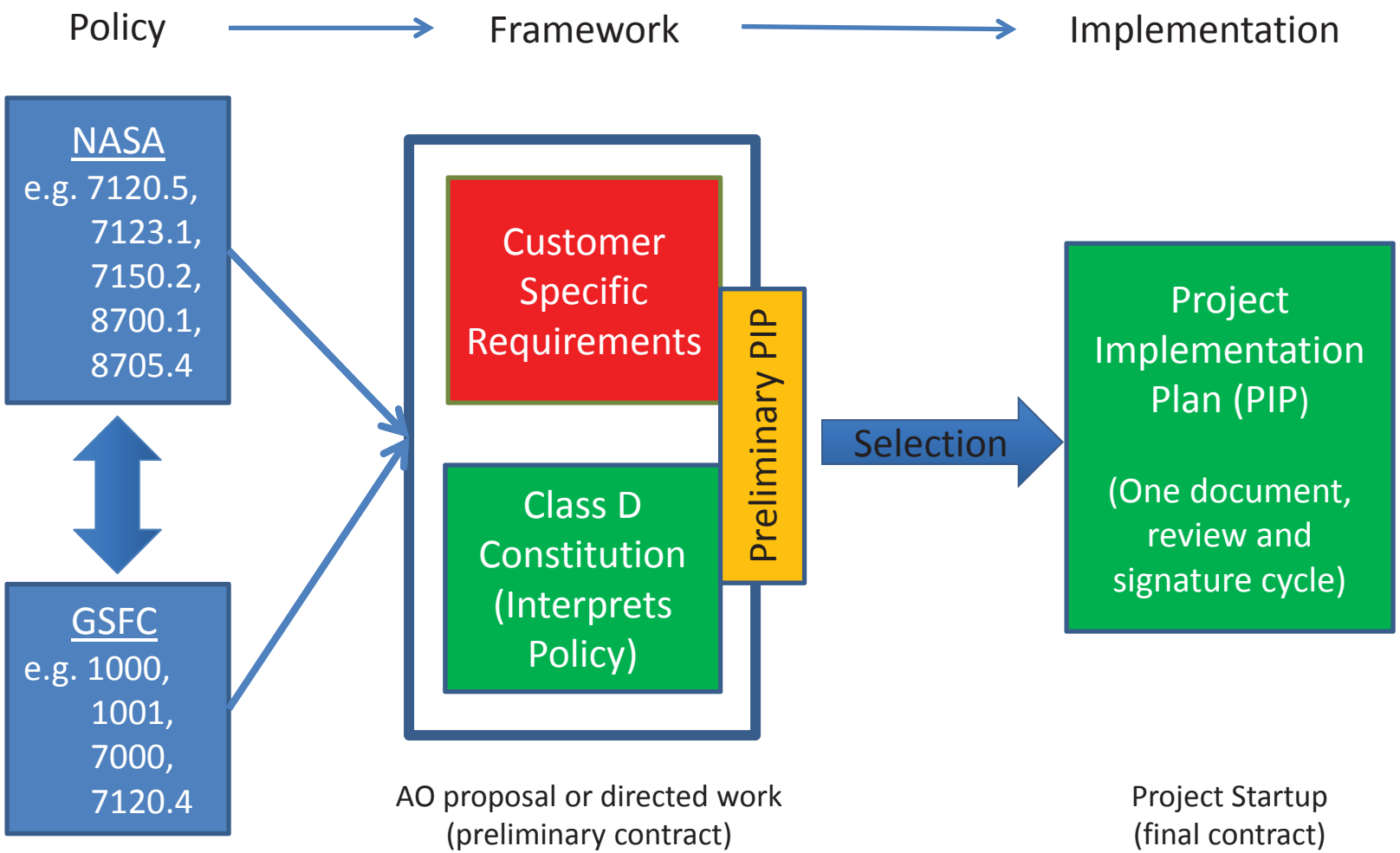
~~Projects operating under this Class D paradigm will benefit from a general waiver of Goddard Procedural Requirements (GPR's), these being much more prescriptive and restrictive than their NASA counterparts.~~ Class D missions will be tailored by applying only the specifications and standards necessary to meet mission requirements. Those GPR's that are considered to be relevant to the project will be highlighted by the champion and will be brought to the attention of the PI/PM team. This input will guide the PI/PM team during project execution. ~~The Class D Projects will follow the spirit of the GPR's while reducing or eliminating the formal processes associated with them, leading to more flexibility, a significant savings in time, and savings in overhead costs.~~

Before we get started…….

2. Key Constitution Take-Aways from an SMA perspective

- NPR 8705.4 Class Definitions do not change - vi
- This document does not redefine or rewrite any standard NASA Procedural Requirements (NPR) - vi
- Focus on schedule and budget - vi
- GSFC shall not impose requirements on a Project that are not clearly stated in the PPIP/PIP - vi
- The PPIP will contain sufficient detail to enable the Center to fully understand the resources needed to perform the proposed work before making a commitment to do so - vi
- It is essential that SMA personnel be included in discussions and planning early in the Project formulation stage ……. SMA personnel will be involved during the development of the PPIP - 8
- PI/PM will be accountable for creating an environment in which the Project team members (whether contractor or civil servants) feel empowered to bring up issues or risks openly to them for proper consideration and disposition - 2
- ITA remains intact – 2, 8

Class D In-House Approach



Constitution Underpinnings

- **Greater attention upfront to the credibility of proposals** - well before submission of a proposal - of a Preliminary Project Implementation Plan (PPIP) containing sufficient detail to enable reasonable and credible resource, cost, and schedule estimates that are consistent with the customer's Class D project definition; the PPIP will also contain a well defined performance floor.
- **Clear and focused lines of accountability** within the team with technical and programmatic authority residing at the Project level wherever feasible
- **Short reporting and communication channels** within the Project and between the Project and Center decision makers to support timely decisions, with an urgency to protect the schedule using a design- and build-to-cost approach
- **Ownership by the team** of a product-oriented approach, streamlined processes, minimum distractions, and low overhead
- **Expert advice and stewardship** to be identified and made available to advise management and Project on the approaches to design- and execution-to-cost

Changes from Business as Usual

Change	Rationale	Benefit	Impact
Preserving the schedule while maintaining the science floor is first priority	Early adherence to schedule reduces risk later on in a program.	Allows PM to establish and maintain control over work content and pacing. Higher likelihood to deliver on schedule	No negative impact
Simplify level 1 requirements	Level 1 should state succintly what the mission must accomplish and impose no further constraints.	Allows PI/PM to trade lower-level requirements against cost and schedule.	Must be perceived as less attractive science and fair worse in competitions.
In a timely, early and often way, establish descope plan for science requirements	Establish and reach agreement on threshhold below which mission is not worth doing.	Allows PI and PM to trade against cost and schedule.	May have to fly with only threshold science capabilities. The Center Director is taking responsibility for canceling a mission that gets out of control
Independently estimate cost and schedule at initiation	Determine whether project can be executed successfully.	Together with above, reduce overruns	No negative impact
Perform full risk assessment, but knowingly accept some risks	Full mitigation of risks is not compatible with keeping cost low; however a full assessment is necessary to allow a rational assumption of risk.	Allows PM to tailor the scope of the development and testing program.	May have to fly with known unmitigated risks
Streamline reviews SRR, PDR/CDR, PSR, MRR	Many reviews without benefit, but costing many man-hours, mainly due to involvement of many layers of management in pre-reviews.	Reduce burden on project team	Problems may go unnoticed
Schedule and Cost Reserve flexibility	Cost and schedule reserve needs vary significantly based on mission risk posture and Level 1 requirements.	Allows Project unique tailoring	Lack of historical basis at the onset of this new Class D process
PM/PI, Engineering, and SMA Implementation flexibility	One size does not fit all. Each project is unique in terms of its needs and development priorities	Allows PM to tailor the scope of the development and testing program.	Lack of historical basis at the onset of this new Class D process