Risk classification modernization

Jesse Leitner
SMA Chief Engineer
NASA GSFC Code 300

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

What is risk classification?

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

Risk Classification
(NPR 7120.5 Projects)

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

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

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

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

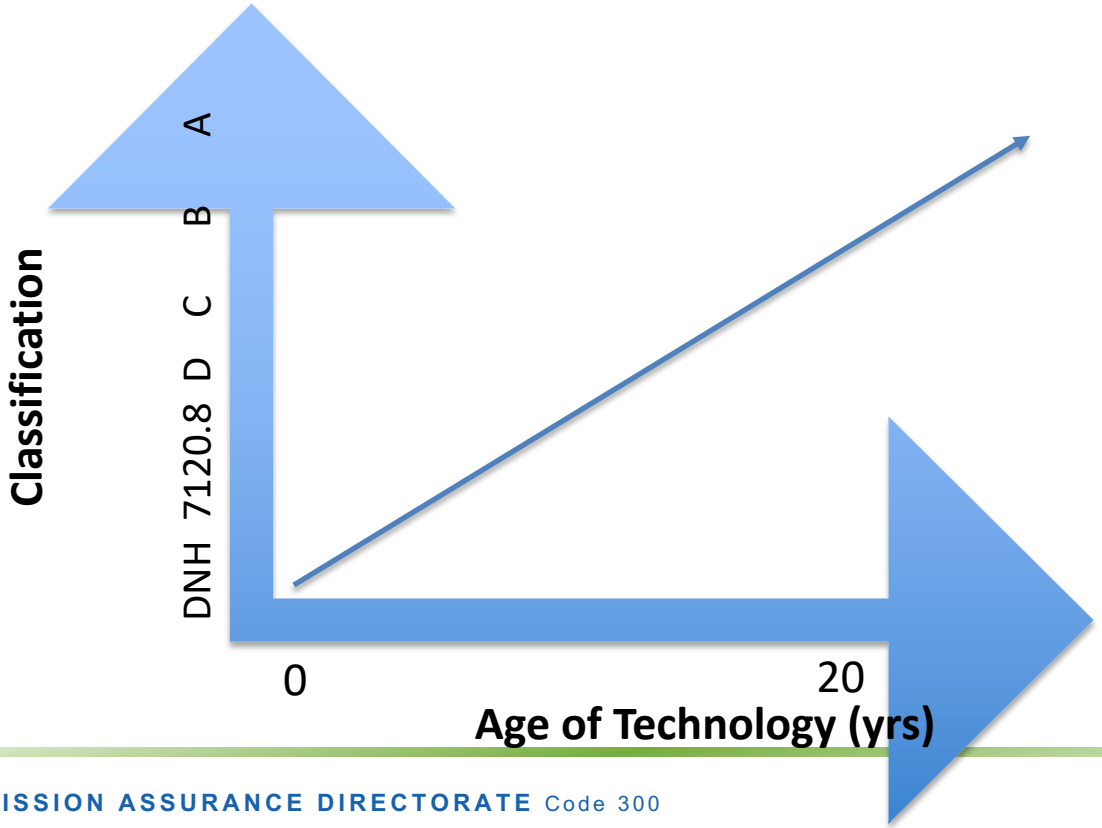
The left-hand-side vs right-hand-side

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

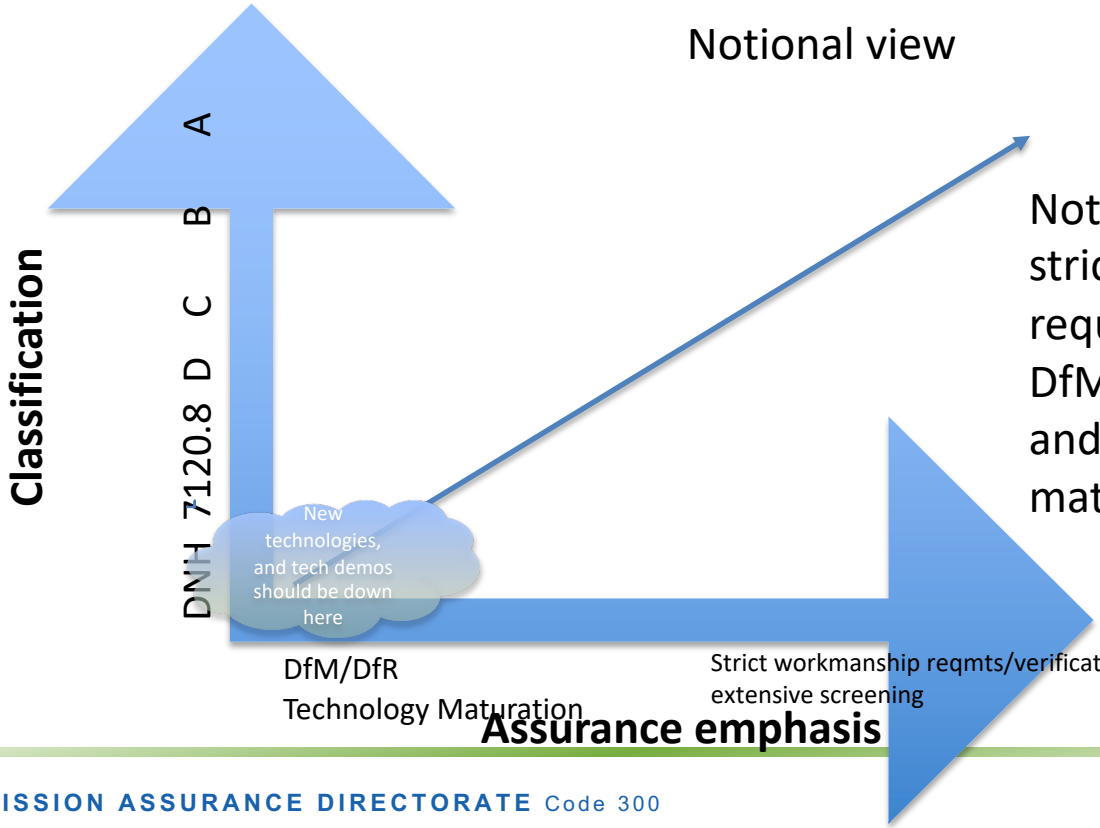
Risk Classification Notes (cont'd)

- 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 at the time of launch 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 vs Technology state of the art



Risk Classification vs Assurance Methodology Focus



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

Summary of expected assurance practices

Practice	A	B	C	D
GMIPs	Extensive	Extensive	Limited	Minimal
ARB/FRB/MRB voting	Voting on all	Voting on major	Participating	Participating
EEE parts	Level 1	Level 2	Level 3	COTS
PCB reqmts	DS, ES, 3/A	DS, ES, 3/A	D, E, 3	D, E, 3
PCB coupons[19]	Independent	Independent	Supplier only	Supplier only
Design redundancy	Fully redundant	Mostly redundant	Selective redundancy	Mostly single string
Workmanship	Space addendum	Space addendum	No space addendum	No space addendum flexible requirements
Radiation	Space-grade+rad-tol design + RDM 2.0	Radiation verified + rad-tol design + RDM 1.5	Rad-tol design, RDM 1.2	Rad-tol design
Lifting	Standard suite of 6 practices	Standard suite of 6 practices	Standard suite of 6 practices	Vendor practices

Oversight vs insight

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

Note on choosing elevated practices

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

Current Risk Classification limitations and shortfalls

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

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

New elements in GPR 8705.4A

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

Standard component classification in GPR 8705.4A

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

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

Collective classification of multiple identical standard products

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

Risk Class vs Design Lifetime vs Lifetime

Mission	Year	Risk Class	Planned Lifetime	Actual lifetime	Why ended
EO-1	2000	C	1	21	fuel expended
GOES-L	2000	A	10	10	outdated
TDRS-H	2000	B	11	22+	active
NOAA-L	2000	C	2	13	“critical anomaly”
GOES-M	2001	A	5	12	thruster issues
Aqua	2002	A	6	20+	active
NOAA-M	2002	C	2	11	two instruments failed
TDRS-I	2002	B	11	20+	Valve issue, took 6 months to get to GEO
RHESSI	2002	D	2	16	communication problems
TDRS-J	2002	B	11	19+	active
ICESat	2003	C	3	7	laser failure
Aura	2004	B	6	18+	active
Neil Gehrels Swift	2004	C	2	17+	active (thermoelectric cooler failed shortly into mission, but successful operational workaround was put in place)
NOAA-N	2005	C	2	17+	active
GOES-N	2006	B	10	16+	active (USSF now)
ST-5 (3 S/C)	2006	C	90 days	100 days	demo complete
Fermi (GLAST)	2008	C	5	14+	active
GOES-O	2009	B	10	10	replaced (now on-orbit spare)
NOAA-N’	2009	C	2	13+	active
LRO	2009	C	3	13+	active
GOES-P	2010	B	10	12+	active
SDO	2010	B	5	12+	active

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

Findings

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

*A thermoelectric cooler was DOA for undetermined causes

Conclusions

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

Origin of the space grade part

- There was a semi-conscious decision dating back to the 70's that all electronic parts flying in space must be rad-hard (by some definition),
  - radiation problem is best solved at the part level,
  - experiences in developing Skylab that concluded that given the immature manufacturing processes at the time it was much better to maximize part assurance practices at the time of manufacture then to add processes later or catch problems in testing.
- Class S part was born
  - Over time, "Class S" became conflated with other MIL-SPEC classifications and radiation hardness was subsequently conflated into the mix,
    - Trapped the community into the mantra that only "Class S" parts can be flown in space; anything else would be a disaster.
    - Had the unfortunate additional consequence that if a failure of a "Class S" part occurred, it was clear that all had been done, and there was no need to take things any farther to challenge whether part of the "Class S" mantra had contributed to the problem.
  - A "Class S vs COTS" notion would perpetuate. In parallel, commercial manufacturing processes were improving and far surpassing this MIL-STD-based control system, which was frozen in time at its inception and unaffected by commercial markets or improving technologies.

Radiation

- Radiation hardness (RH) is a multi-dimensional property of any part that describes intrinsic abilities to tolerate various radiation environments
  - Effects to be concerned with include total ionizing dose, total non-ionizing dose, and single-event effects – all of which depend on the mission, environment, application, and lifetime
- Radiation concerns are the same whether a part is COTS, MIL-SPEC, or NASA-screened COTS
- Overattention to radiation at the piece-part level has often supplanted the far more important concept of radiation-tolerant design (leading to a mission failure)
  - Note that some radiation effects can only be accurately characterized at the part-level, though that does not necessarily verify whole-of-system performance. In some cases, the fact that the radiation effects are only apparent at the part level is actually due to attenuation of the effect in the circuit. The understanding of this attenuation is one facet of radiation-tolerant design.
- All parts have a particular level of radiation susceptibility, but only some parts have details in their data sheets, and those details, when present, may be inadequate for a given mission, environment, application, and lifetime. Furthermore, piece part performance is often not indicative of circuit performance.
- Why is there less concern about radiation in MIL-SPEC parts?
  - Often in the space community, the MIL-SPEC term is used only to represent the small “space-grade” subset.
- Does RH of parts in one lot imply the same level of hardness in another lot?
  - Only if RH is in the datasheet (COTS or MIL-SPEC)
    - Any part without RH in the datasheet is not optimized or even controlled for RH, and thus requires further consideration for suitability
    - Furthermore, RH relative to some conditions (e.g., SEE) may provide no indication of RH to others (e.g., TID)
  - However, if it can be confirmed that the part has not changed, one can consider the attributes of the part and the environment to determine whether there are new risk factors in the different lot (COTS or MIL-SPEC). There is no valid reason to discard knowledge obtained from prior lots of the part of the same construct.
- Is past use of the exact same part in space in the same environment (MIL-SPEC or COTS) sufficient to guarantee its future use?
  - No, because the concern is overall radiation tolerance of the design, not radiation hardness of the parts. The previous design may have been radiation tolerant, while the current design may not be.

Radiation is a system-level problem that we have been traditionally (and unfortunately) largely addressing at the part level

Radiation FAQ

- What is a rad-hard part?
  - A part that has lot specific part-level radiation testing data from a radiation chamber for one or more types of radiation (typically TID at a minimum) and accompanying paperwork to demonstrate a specified level of tolerance to radiation effects
- What is a rad-tolerant part?
  - A part that by design or other measures has limited susceptibility to radiation, but not to a specific level, and not with paperwork to show
- Is a rad-hard part immune to radiation?
  - Only to the level specified of that specific part from that lot in a radiation chamber by itself
- Are rad-hard parts more protected against radiation than non-rad-hard parts?
  - No, they are tested and specified to specific levels, whereas non-rad-hard parts are not

What should be done about radiation?

- Using new parts and new technologies will demand a new approach for radiation
- Any expectation that all or most parts will be rad-hard or tested for radiation from their current lots will simply cause many to collapse under their own weight (including many that have been in space successfully for decades)
- Any expectation that radhard parts are necessary and sufficient for successful on-orbit operation will lead to disappointment (as in SMAP)
- Use good design practices
  - Protect and derate your MOSFET!
  - Implement TMR on FPGAs
  - Be sure your processor circuit is resettable
  - Employ EDAC and protect your memory
- Use familiar parts
  - New sensitive part types (CMOS, processors, MOSFETs, memory, etc) in critical applications should invoke testing or sufficient protection
- Use components that have flown in similar environments
- **Learn from on-orbit experiences! Do not use ground-testing as your primary means for radiation assurance – it will provide a hard barrier against moving forward for many mission concepts.**

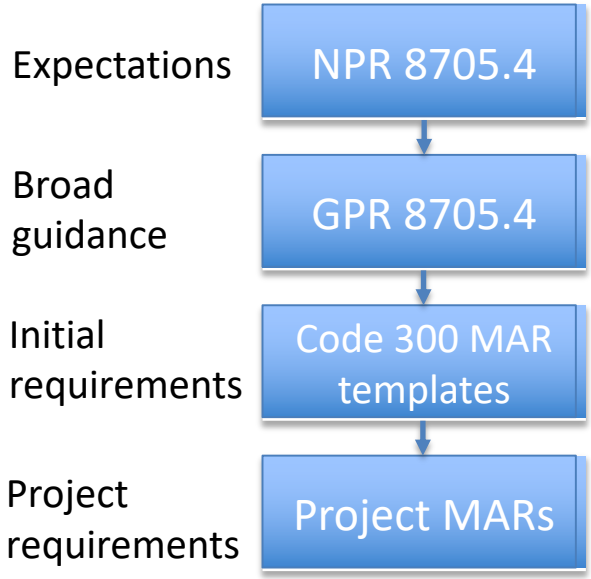
Why the resistance against using COTS components and spacecraft

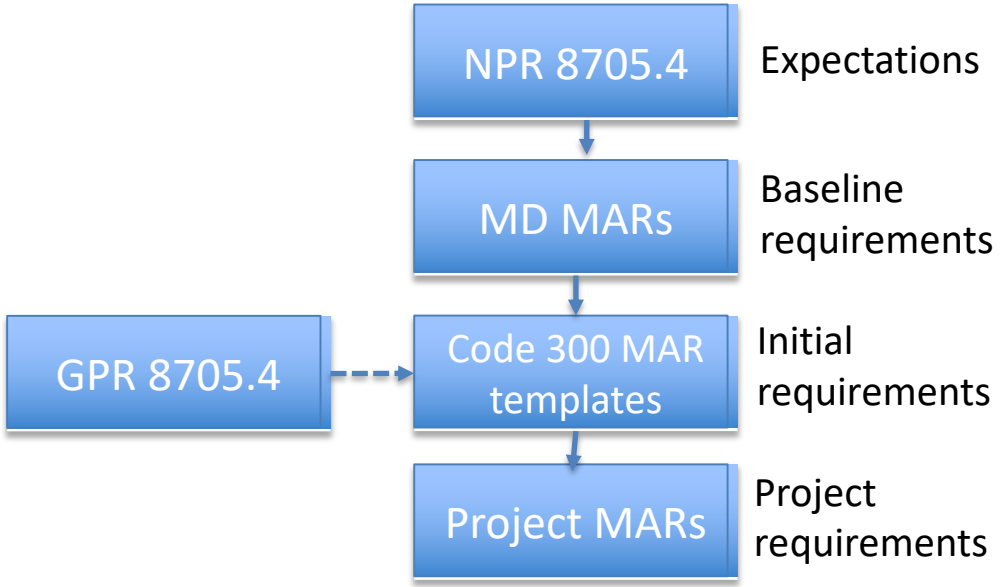
- The term COTS is unbounded – it is not descriptive enough on its own to assure quality or reliability
- NASA as a whole has not yet fully acknowledged that industry is capable of providing reliable hardware without assistance
- Conflation between quality and reliability within the agency and space community, combined with the retention of decades' old quality requirements
  - Our focus on traditional quality requirements has distracted many in the community from what actually makes a system reliable
- Past studies and lessons learned that concluded that COTS parts and components are "high risk" because they do not withstand our traditional screening processes
- Classification system itself is currently defined by higher classes being linked to maximum oversight (== minimum commercial practices)
  - Perception is that higher classification practices result in greater reliability and longer lifetime
- The "Skylab decision" that all parts flying in space must be space grade
  - Within a COTS product, you are not likely to have space grade parts, or even have information about the parts inside

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 requirements flowdown (GSFC-managed Projects)





Important notes (albeit repetitive)

- While this is a new concept to tie absolute recent reliability measures to classification of components, the approach does not center on a formal measure of reliability
  - Only recent flights are used
  - Design is considered, but not the fact that parts can change or operational regime may differ
  - Classification alone cannot be used to determine or establish reliability of an existing product or a product in development: “Classification is not equal to reliability”
  - Standard Ps calculations involve roll-ups of piece-part reliability estimates, rather than how well the design functions as a whole, and thus may not be used as absolute reliable measures for classification
- Large spacecraft of common designs that have flown in different applications (e.g., LS-8, LS-9, JPSS-2, etc) may be classified based on standard product calculations given their history, but not calculated Ps
- Since there is no measure of established reliability for a new development or non-standard design, the use of multiple non-standard spacecraft cannot change the classification of a single vehicle.
- This new approach incentivizes innovative approaches for cost-effective and reliable performance without historical perceived and real constraints