



SMD Class D standard MAR

Jesse Leitner, Chief SMA
Engineer, GSFC



SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300



Outline

- Background
- Class D principles
- Significant departures from common practices
- Other highlights
- Summary

Background

- Numerous activities have taken place over the past several years to address the fact that Class D practices across the agency have differed little from those for Class A, B, or C missions
- Most of these activities have not resulted in substantial efforts to tangibly change how we perform Class D developments
- The result is that we have been limited in our ability to push the boundaries for moderate-risk/high-payoff missions
- This development effort has taken a very detailed view of the practices that are in place to ensure safety and mission success, and tunes them into risk-driven activities that accept developers' approaches in contrast to the current "do it the way we always have" approaches that have been difficult to depart from.
- This approach emphasizes the processes that provide the most risk reduction payoff and avoids the "feel-good" types of requirements that are abundant for Class A and Class B missions, where there is significant tolerance for overrun.
- This approach further emphasizes developer standard practices as opposed to prescriptive "do it our way" practices.
- At this point, there will be no choice, no matter what the risk posture, but to implement a "true Class D" for the new wave of highly resource-constrained missions that are abundantly emerging

Agency Team

- GSFC: Jesse Leitner (lead), Ron Perison
- LaRC: Joey Patterson, Don Porter
- JPL: Tom Ramsey, Sammy Kayali, Naomi Palmer
- Glenn: Cynthia Calhoun
- MSFC: Rodney Key, Kelly Bellamy, Michael Giuntini, James Kissell, Keith Dill
- ARC: Steve Jara, Don Mendoza
- APL: Steve Pereira, Rick Pfisterer
- SWRI: Joerg Gerhardus, John Stone

Class D Principles: Dos & Don'ts

- **Do:**

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

- **Don't:**

- **Ignore risks!**
- Reduce reliability efforts (but do be more focused and less formal)
- Assume nonconforming means unacceptable or risky
- Blindly eliminate processes

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

Significant departures from common practices (1/3)

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

Inherited items process principles

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

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

Significant departures from common practices (2/3)

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

Significant departures from common practices (3/3)

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

Minor departures from common practices

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

Other elements

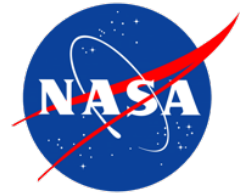
- Lifting
 - Vendor practices if command media exist
 - NASA-STD-8719.9 for all others
- ESD: ANSI/ESD S20.20-2007
- Lead-free and whisker controls required
- Assurance Plan for new digital electronic designs (FPGAs, ASICs, etc)
- Planetary Protection for outside of earth orbit
- Cybersecurity and Command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

What kinds of risks are acceptable?

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

Summary

- A Standard Mission Assurance Requirements document has been produced to represent the general set of requirements to impose on SMD Class D missions
- This is the first such document that truly addresses significant costs and programmatic risks that were not really addressed in the past.
- The document has now been baselined as a formal SMD document



Backup materials



SAFETY and MISSION ASSURANCE¹⁴
DIRECTORATE Code 300

