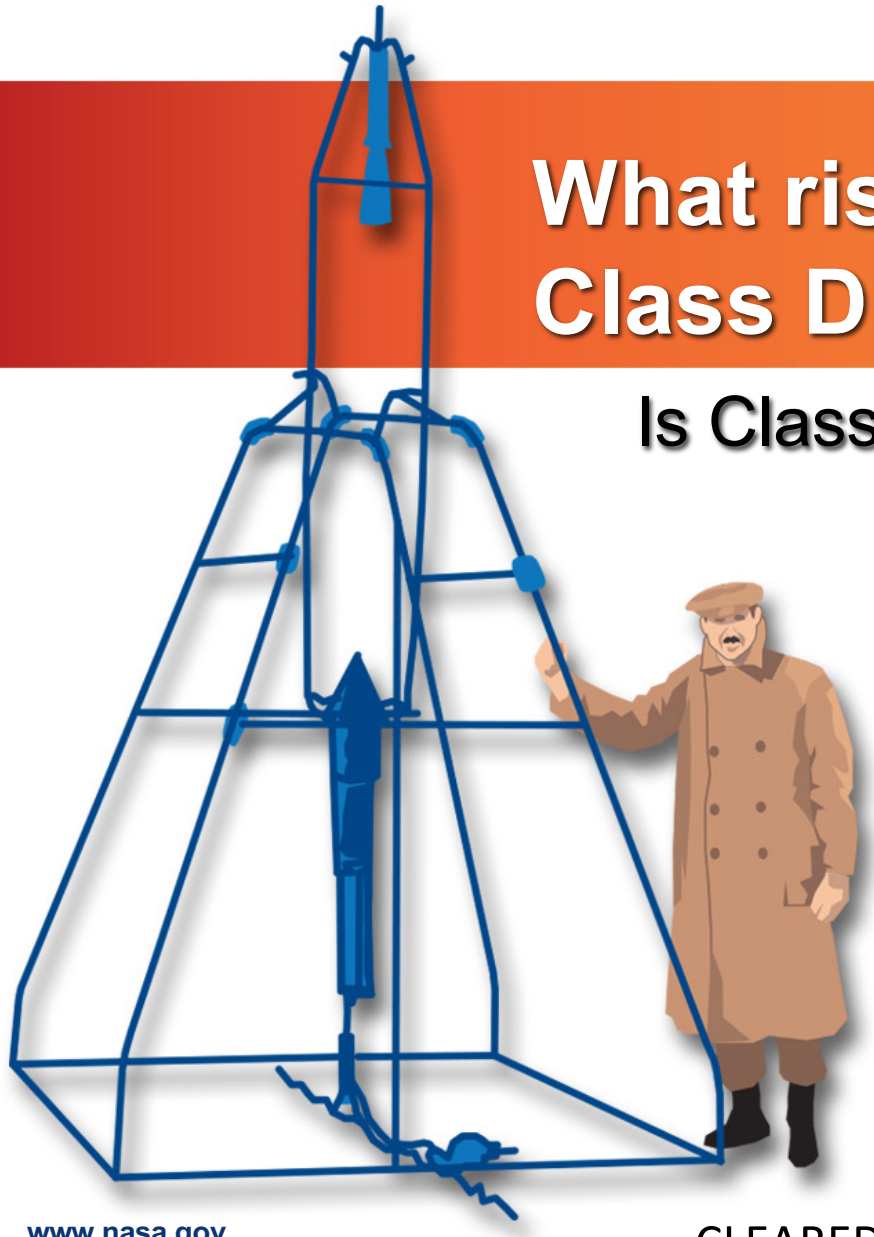
National Aeronautics and Space Administration



What risks are acceptable for a Class D mission?

Is Class D the wild west?

Jesse Leitner,
Chief SMA Engineer, GSFC
November 8, 2023

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

www.nasa.gov

Outline

- Class D principles
- What is risk?
- What risks are acceptable for Class D?
- Summary

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.

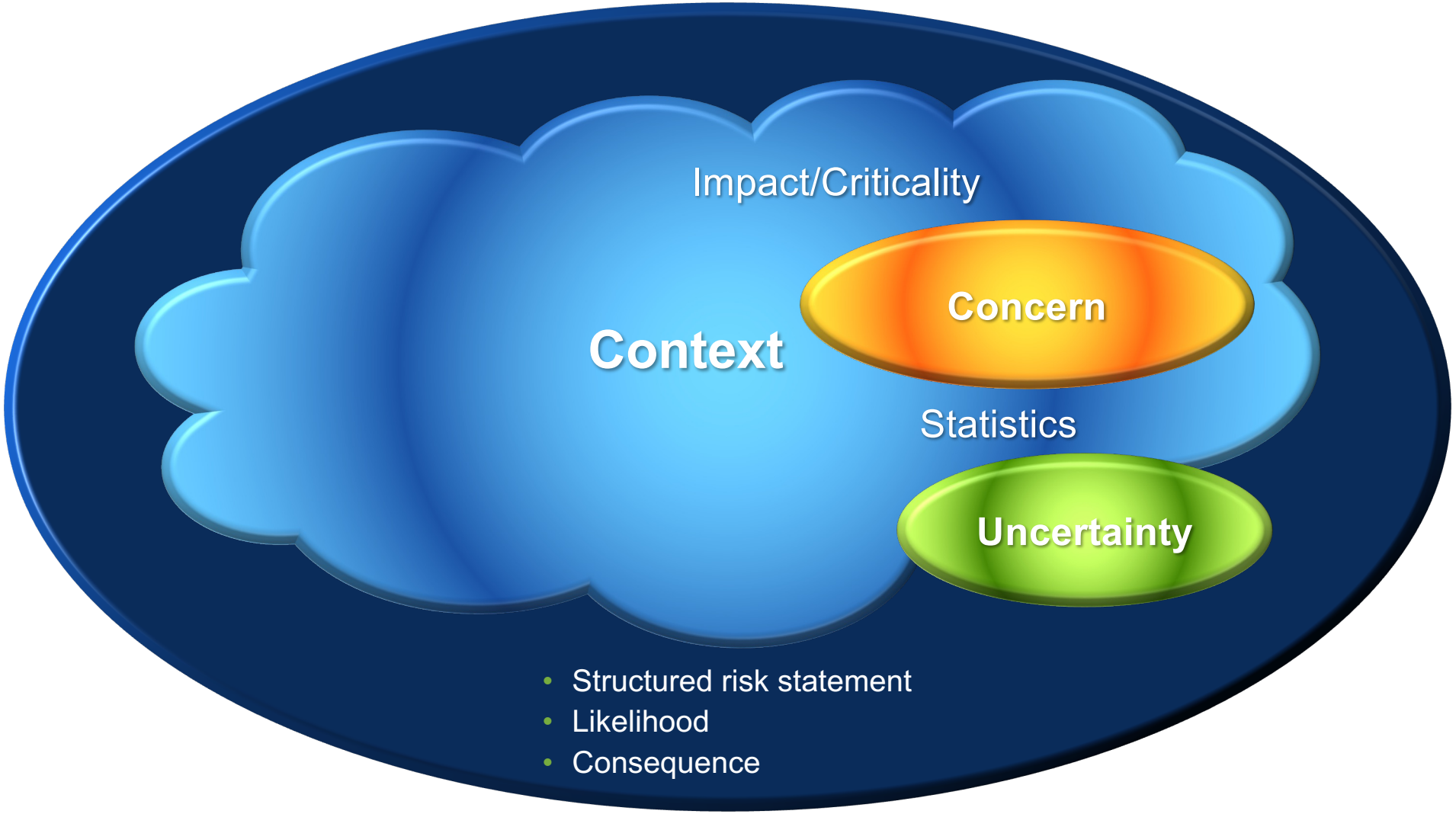
*outside scope of MAR

Risk

We'll take the house. Honey, the chances of another plane hitting this house are astronomical. It's been pre-disastered. We're going to be safe here.

From: The World According to Garp, Warner Bros., 1982

Anatomy of a Risk



Concern

- Definition: A logical determination that an undesired event may occur or that the protections against such an event may not be sufficiently well understood based on available data
- This is the core element upon which a risk is founded
- In some sense, it is the risk without the context, likelihood or consequence.
- Can come in the same “flavors” (categories) as risks
  - Technical
    - A part may fail
  - Cost
    - Cost of an item may grow
  - Schedule
    - Delivery may be delayed
  - Safety
    - The spacecraft may fall off the crane

What is Risk?

- Definition: the combination of
  - a) the probability (qualitative or quantitative) that an undesired event will occur, and
  - b) the consequence or impact of the undesired event
  - c) a factual context or scenario that exists to cause the risk to be present
  - In short, risk is an expectation of loss in statistical terms based an existing condition.

- Categories of risk (consequences)
  - Technical (failure or performance degradation on-orbit)
  - Cost ($ it will take to fix the problem)
  - Schedule (time to fix the problem) } programmatic
  - Safety (injury, death, or collateral damage)

- This is the substantive version of a concern
- The category may not match that of the concern
  - Common: programmatic risk based on technical concern

Risk Statement (GPR 7120.4D)

- Given the [CONDITION*]
  There is a possibility that [INTERMEDIATE CONSEQUENCE] will occur
  Resulting in [CONSEQUENCE]

  CONDITION: A factual statement that describes the context that elevates the likelihood of a failure or shortfall. A system being single string does not automatically indicate that a risk is above baseline risk. What is the condition that exists that elevates the likelihood of failure?
  - there is a part installed that is a GIDEP direct hit
  - the supplier is located in a war zone
  - the expert personnel have just retired

  INTERMEDIATE CONSEQUENCE: The immediate, direct effect from a concern being realized
  - a part will fail
  - an item will be delivered late

  CONSEQUENCE: Foreseeable, negative impact(s) to meeting performance, programmatic, or safety requirements at the level of a project that is tracking the associated risk. Project level risks are threats to mission requirements.
  - instrument will fail
  - mission will fail
  - launch will slip
  - a person will be injured

*[CAPITALIZED] terms will be called *fillable* items

Key Rules to follow

- The CONDITION must exist today and should be indisputable
- No conditional statements or risks should be in any of the fillable items (the condition is already included in the statement structure) – see example on p. 20
  - Rationale: Conditional statements within the risk will result in arbitrary likelihoods and “risk of a risk” scenarios.
- Avoid using multiple consequences in a single risk statement (see p. 21)
  - Especially if they are different flavors (common) as risk scales are different
- The CONSEQUENCE represents the category
- Safety of your own hardware is in the category of technical or programmatic risk
- Avoid using “loss of redundancy” as a risk consequence at the project level (project level risks should be threats to level 1 requirements)
  - Can result in unbalanced risk by comparing one risk of loss of function to another with no effect on mission performance
  - Loses the benefit of redundancy
- If possible, avoid risks that suggest that your own project team is going to make bad decisions – better to address those concerns directly within the project.

(aggregate) Risk Example

- *Given:* the massive size, complexity, development constraints, and one-of-a-kind nature (with no historical reliability) of the JWST observatory that prevent complete test as you fly verification and/or validation of complex models,
- *There is a possibility that:* a key interaction that impacts system performance is not identified,
- *With the result that:* mission performance will be moderately degraded.
- LxC: 2x3

Closure on performance verification of instruments after commissioning

Context for Risk in Parts

COTS

- Parts with special features that are difficult to manufacture consistently (never available on MIL-SPEC)
  - e.g., extra-low ESR and ESL ceramic capacitors
- Parts used in brutal operating regimes
  - High-voltage (particularly > 3 kV)
  - Cryo
- Low volume and hand-produced parts
  - Lack a basis for reliability and often do not have optimized manufacturing processes
- Parts used in extremely sensitive (poor) designs (based on variability of parameters not in part spec)
- Parts used in applications in which the environment is unknown
- Parts from unknown or poor-performing vendors (no recent examples)
- No "hi-rel" or automotive parts available

MIL-SPEC

- **All risk-contexts for COTS, plus:**
- Low-volume parts
- Lead time and costs can reduce system-testing resources
- Designed for old manufacturing processes and broad environments
- When used broadly, they can bring false hope and extensive problems may ensue
- Processes will miss new manufacturing flaws
- Performance and reliability not driven by the need to stay in business
- Performance limitations may lead to weak designs

NASA-screened COTS

- **All risk-contexts for COTS, plus:**
- Parts are often overtested since MIL-SPEC testing regimes are not related to actual usage and parts are often not designed or optimized for such regimes
- False hope that screening is relevant to operation
- False hope that screening, testing, and qualification increase reliability or quality
- The prospect for burying a problem or reduced lifetime into a part by the "overtest by design".

Note that the contexts for risk in COTS parts all arise from mission performance requirements that would be present no matter which parts approach is used, so they apply to all cases.

What kinds of risks are acceptable for Class D?

- Risks that the stakeholder has declared to be 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/assemblies 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

Will use of COTS cause a radiation nightmare?

- It certainly can if you're in a radiation environment and you pretend it's not there, but that has **nothing** to do with COTS.
- Typically, about 90% of the part count even for large missions are not radiation-hardness-assured (because they don't need to be).
  - The majority of places where COTS are really needed are for non-susceptible parts
- The problem is no different from that of using a 5962-XXX microcircuit or a JANS2NXXXX BJT (neither of which is radiation hardness assured)
- For reference, an IRHM58160 is a COTS part (and it is radiation hardness assured).

- No matter whether you use COTS, MIL-SPEC or "special drawing" parts, radiation should be addressed in the same way
- As we transition to newer technologies and higher performance, we will have to think about radiation mitigation in different ways because parts with RHA will almost always be multiple generations behind
  - However, some of the new technology parts will be less susceptible to radiation by the nature of their designs (thinner gate oxides, etc)

Summary

- Class D missions are an opportunity to move the space community forward and make use of new products and approaches
- Navigating the risks of a Class D development need not be representative of the wild west

Typical BOM excerpt from high-end mission (Class B GEO)

102	5962H0254301VXC	UT54ACS162245S	Microcircuit, Digital, CMOS, Radiation hardened, S	2			
103	5962F9674202VXC	HS9-508BRH	Microcircuit, Linear, 8-Bit Channel Analog Multipl	2			
104	5962F9563002VYC	HS9-1840ARH	Microcircuit, Linear, Radiation Hardened, Single 1	4			
106	311P407-5S-B-15	HD-22	Connector, Electrical, Rect., HD, D-Sub, Receptacl	1			
107	311P407-2S-B-15	HD-22	Connector, Electrical, Rect., HD, D-Sub, Receptacl	1			
108	311P409-1P-B-15	HD-20	Connector, Electrical, Rect, Standard Density, D-S	1			
109	5962-9689202VJA	AD565ATD/QMLV	Microcircuit, Linear, 12-Bit D/A Converter	1			
111	5962-8686103XA	AD580	Microcircuit, Linear, 2.5V Precision Voltage Refer	1			
112	5962R8776001S2A	54ACT244LMQB	Microcircuit,Digital,Advanced CMOS,Octal Buffer/Li	8			
113	D55342E07B10B0R	RM1206	Resistor, Fixed, Film, 10K**, 0.1%, 125mW, 25PPM	8			
114	D55342E07B10E0R	RM1206	Resistor, Fixed, Film, 10K**, 1%, 125mW, 25PPM	25			
116	D55342E07B68D1R	RM1206	Resistor, Fixed, Film, 68.1**, 1%, 125mW, 25PPM	4			
117	D55342E07B20E0R	RM1206	Resistor, Fixed, Film, 20K**, 1%, 125mW, 25PPM	12			
118	D55342E07B11B3R	RM1206	Resistor, Fixed, Film, 11.3K**, 0.1%, 125mW, 25PPM	1			
119	D55342E07B71B5R	RM1206	Resistor, Fixed, Film, 71.5K**, 0.1%, 125mW, 25PPM	2			
120	D55342E07B21B5R	RM1206	Resistor, Fixed, Film, 21.5K**, 0.1%, 125mW, 25PPM	1			
121	D55342E07B2E00R	RM1206	Resistor, Fixed, Film, 2K**, 1%, 125mW, 25PPM	2			
122	D55342E07B4B99R	RM1206	Resistor, Fixed, Film, 4.99K**, 0.1%, 125mW, 25PPM	28			
123	D55342E07B100DR	RM1206	Resistor, Fixed, Film, 100**, 1%, 125mW, 25PPM	4			
125	CWR06KC106KCA	CWR06	Capacitor,Tantalum,Solid,Chip, Fixed,10uF,25V,10%	2			
126	SR0805X7R103#011F	SR0805X7R	Capacitor, Ceramic, Chip 0805, 0.01**F, 25V	15			
127	SR0805X7R104#00VR	SR0805X7R	Capacitor, Ceramic, Chip 0805, 0.1**F, 25V	22			
128	CDR01BP101BKUS	CDR01	Capacitor, Ceramic, BP Dielectric, 100pF, 10%, 100	2			
129	CDR01BP100BKUS	CDR01	Capacitor, Ceramic, BP Dielectric, 10pF, 10%, 100V	10			
130	CDR33BX473AKUS	CDR33	Capacitor, Fixed, Ceramic, 47000pF, 50V, 10%	27			
131	TLW-101-05-G-S	TLW-101-05-G-S	Header, Low Profile, 0.025`` Square Post	25			
132	1-102972-0	1-102972-0	Header, 10 Positions, Breakaway, Single Row, 0.100	10			
133	M32159B06T	S0705CPX000	Resistor Chip, Fixed, Film, Electrical, Zero **, J	1			
134	CDR33BX273BKUS	CDR33	Capacitor, Fixed, Ceramic, 27000pF, 50V, 10%	1			
135	5-0085	BJ376	Connector, Receptacle, Twinax/Triax, TRB Rear Moun	2			
136	311P407-1S-B-15	HD-22	Connector, Electrical, Rect., HD, D-Sub, Receptacl	1			
137	CWR19MC106JCHA	CWR19	Capacitor, Tantalum, Chip, Fixed, 10uF, 5%, 35V	4			
138	CDR31BP680BKUS		Capacitor, Fixed, Ceramic, 68pF, 10%, 100V	12			
139	M55342K11B49D9R	RM0402	Resistor, Fixed, Film, 49.9**, 1.0%, 40mW, 100PPM	4			
140	M55342K11B30D1S	RM0402	Resistor, Fixed, Film, 30.1**, 1.0%, 40mW, 100PPM	1			
141	M55342K11B10D0R	RM0402	Resistor, Fixed, Film, 10**, 1.0%, 40mW, 100PPM	3			
142	D55342K07B499DS	RM1206	Resistor, Fixed, Film, 499**, 1.0%, 205mW, 100PPM	4			
143	M55342K11B10E0S	RM0402	Resistor, Fixed, Film, 10K**, 1.0%, 40mW, 100PPM	36			
144	M55342K11B33D2R	RM0402	Resistor, Fixed, Film, 33.2**, 1.0%, 40mW, 100PPM	56			
145	D55342K07B357DR	RM1206	Resistor, Fixed, Film, 357**, 1.0%, 250mW, 100PPM	1			
146	D55342K07B2E94S	RM1206	Resistor, Fixed, Film, 2.94K**, 1.0%, 250mW, 100PP	1			
147	D55342K07B2E43S	RM1206	Resistor, Fixed, Film, 2.43K**, 1.0%, 250mW, 100PP	1			
148	M55342K11B68D1S	RM0402	Resistor, Fixed, Film, 68.1**, 1.0%, 40mW, 100PPM	12			
149	M32159B11T	RCZ0402	Resistor Chip, Fixed, Film, Electrical, Zero Ohm,	9			
150	RH1499MW#50326	RH1499	Microcircuit,Linear,Precision Rail-to-Rail I/O, Qu	4			
151	5962F0151705VXA	UT28F256LVQLC-	Microcircuit, Digital, Radiation Hardened, PROM, 3	2			
				38		0.03646833	
				10		0.00959693	
				16		0.01535509	
			total parts count	1042			

Yellow highlight
MIL-SPEC FMRR

Orange highlight
COTS FMRR

Gray/purple highlight
Actives with no FMRR

Total parts count: 1042
Total MIL-SPEC FMRR: 3.6%
Total COTS FMRR: 10: 0.96%
Total non-FMRR and discrete semiconductors (requiring radiation testing or other forms of analysis: 16 (1.5%)

Common approaches for addressing radiation

- Avoidance: dormancy of sensitive electronic elements in high stress regions such as SAA or Van Allen Belts
- RHBD: Proven rad-hard by design approach, applied to circuits and/or parts
- Traditional parts-centric: Use of RHA* parts with radiation-tolerant design to accommodate high stress region operation
- Modern parts-centric: Use of familiar sensitive** parts along with proven circuit designs in comparable environment, normally combined with select strategic parts testing outside of specific projects to characterize variability or parts changes in general
- Radiation-tolerant design: Use radiation-tolerant circuit design techniques including features such as MOSFET protection and overcurrent detection with reset capability, resettable processors, EDAC, derating beyond EEE-INST-002 recommendations, etc.
- Risk-based approach combining past on-orbit experiences in similar stressing environments.
- System fault-tolerance (including redundancy): This may include new, unproven approaches, with backup proven systems.

* RHA = radiation-hardness assured, with lot-specific testing and accompanying paperwork

**Sensitive parts include memory, processors, CMOS devices, MOSFETs, etc.

Vendor trust (and established reliability basis)

- ILPM
- Established relationship
- DLA verified (MIL-SPEC)*
- QML manufacturer, not under DLA for part
- PPAP provided
- All vendor screening and qual data provided
- High-volume part
- 100% manufacturer screening across datasheet (possibly at single temp)
- Part in-service at least 1 year.

*while most MIL-SPEC parts will have a factor of 1 based on trust, some may not be established while being low-volume, requiring a higher factor

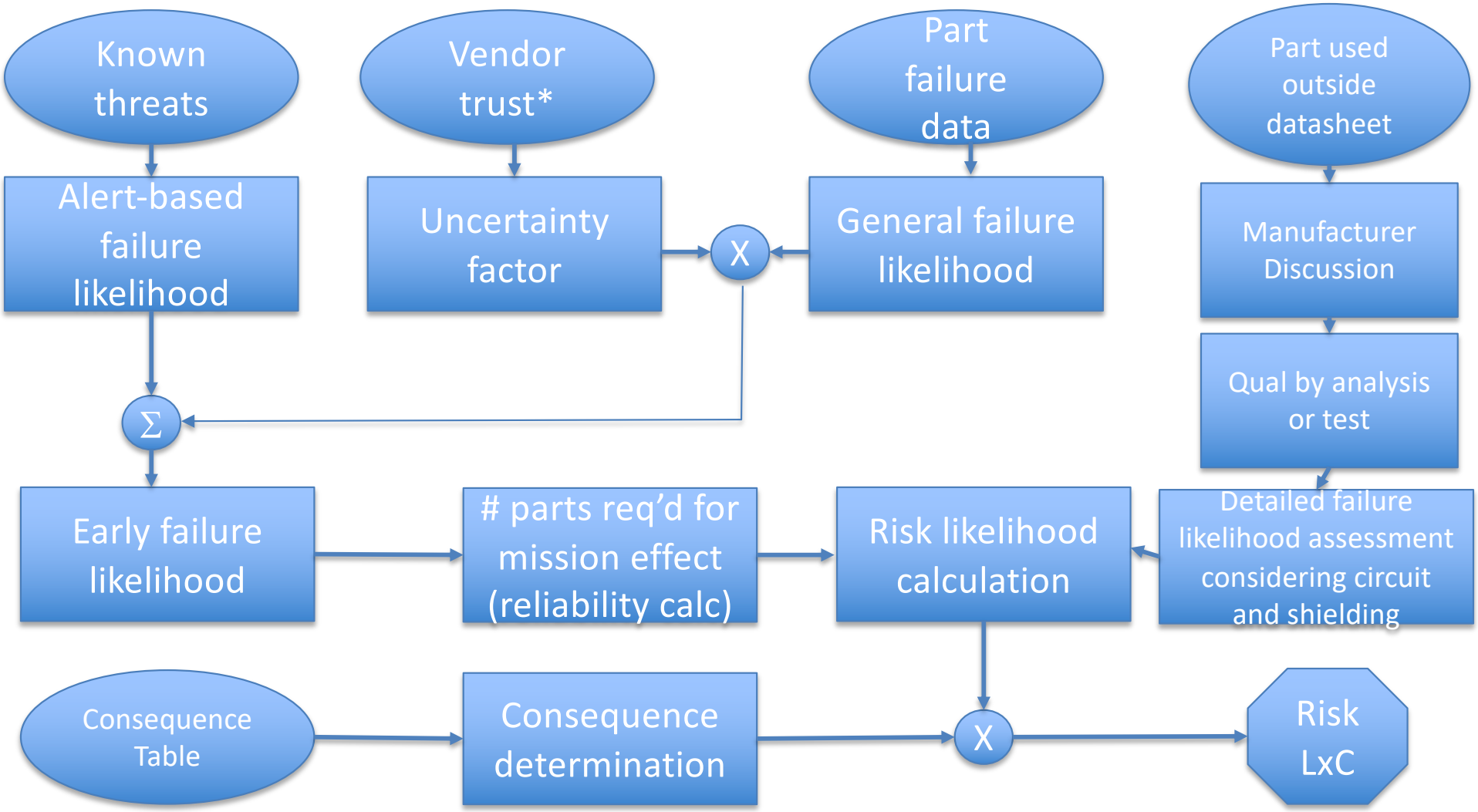
Intelligent use of COTS parts

- Always use parts within the limits of their datasheets
  - Respect the datasheet!
- AEC-qualified parts (not just “for automotive use”) from leading manufacturers, produced under IATF 16949 will maximize reliability
- Use familiar parts when possible
- Avoid an approach that prompts you to use more parts as often happens with capacitors
- Conservative derating is good practice, but excessive and forced derating may result in need for many extra parts, a mass or space problem, or a weaker design with less margins.
- Buy parts from authorized distributors
  - There is no purpose in MIL-SPEC distributor restrictions when buying COTS parts
- There are many great options for “enhanced space” COTS parts for microcircuits and discretes

Radiation and on-orbit non-RHA performance data sources

- Test data:
  - Traditional: radhome.gsfc.nasa.gov, transitioned to https://nepp.nasa.gov/pages/pubs.cfm
  - New: esarad.esa.int
  - New: pmpedia.space
- On-orbit experiences (“fact of” - some info available)
  - Spacecube data (LEO on-orbit – extensive non-RHA and COTS – 10+ yr)
  - Aerocube data (LEO on-orbit – 100% non-RHA COTS – 10+ yr) (Aerospace Corporation)
  - Swift data (585km x 604km, 20.6 deg - extensive COTS ~ 19 yrs)
  - Ascent (GEO cubesat – launched 12/2021) (AFRL)
  - Biosentinel (deep space cubesat – launched with Artemis)
  - Newspace – extensive, limited data availability

The path to part-driven mission risks



*vendor trust should also include established reliability basis for the part, driven by high-volume and at least a year in the field

Risk example 1

- **Given**: the use of a properly-derated, high-volume, established BME capacitor from a trusted-ILPM with 10 reported field failures due to manufacturing defects out of 12 million parts delivered
- **It is possible that** three capacitors will fail, taking out the (non-redundant) power supply, within mission lifetime
- **Resulting in** early mission failure

- In this case, all three of this type of capacitor must fail to cause a PS failure. Consequence would be 5.
- Let's assume the pool is actually 3 million parts to account for parts that are not actually used and to adjust for non-reporting (even if manufacturer is trusted). We will also freeze time for the mission and field reporting. So vendor failure likelihood is 10/3e6
- Uncertainty (Vendor trust) factor we will set at 1.5 (1 is complete trust) because we have no PPAP.
- Early failure likelihood of a single part is 1.5*10/3e6 = 5e-6
- Important quantity is failure of the PS, because that will end the mission. Three part failures are required, likelihood = (5e-6)^3 ~ 0 (well off of any risk scale)
- Risk is noncredible

Risk example 2

- **Given**: the use of a properly-derated, high-volume, established BME capacitor 50 reported field failures due to manufacturing defects out of 20 million parts delivered
- **It is possible that** one capacitor will fail, taking out the star tracker, within mission lifetime
- **Resulting in** severe mission degradation

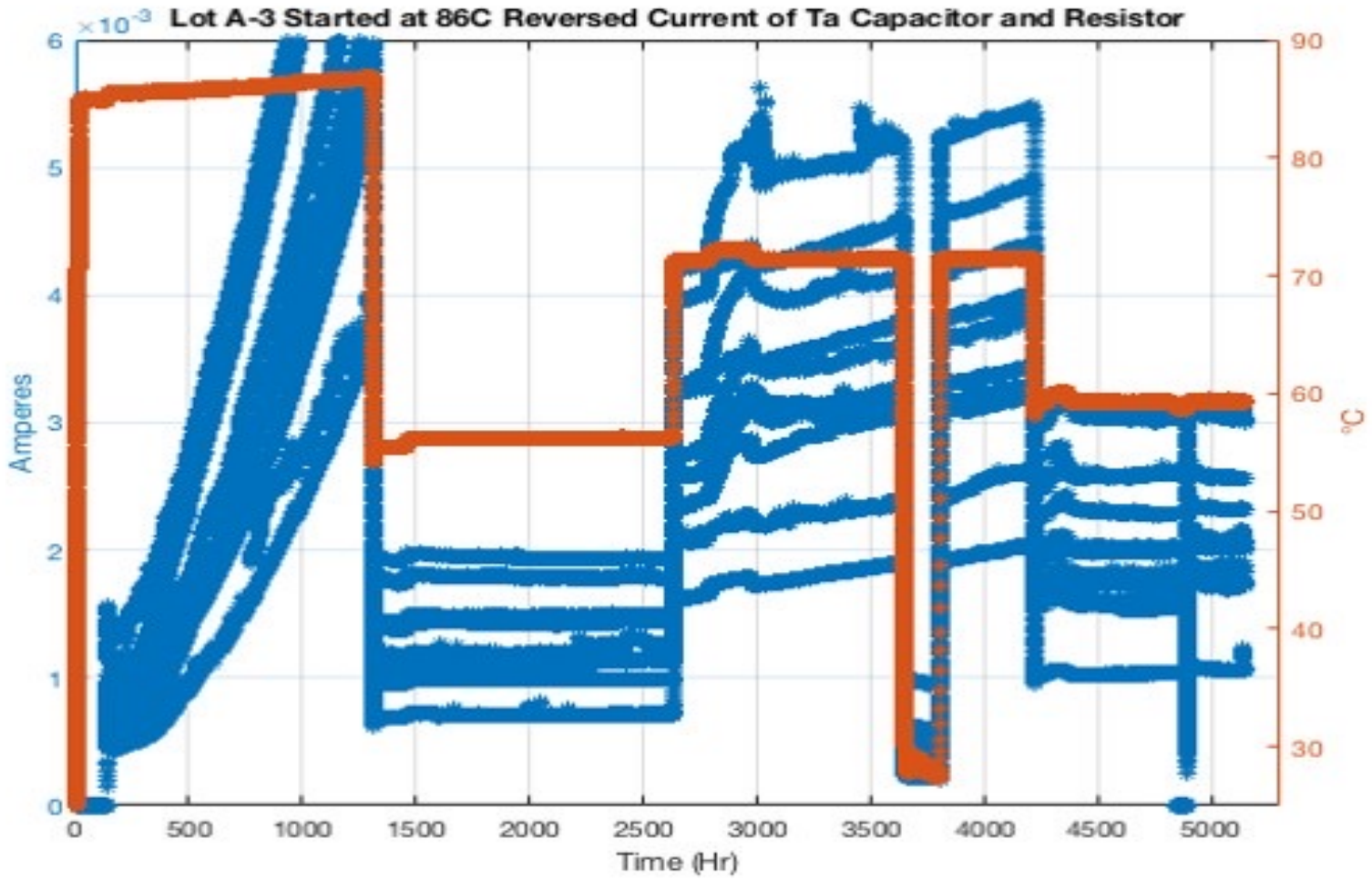
- In this case, one capacitor takes out the star tracker, and the loss of the tracker greatly reduces science value, consequence 4
- Let's assume the pool is actually 5 million parts to account for parts that are not actually used and to adjust for non-reporting. We will also freeze time for the mission and field reporting. So vendor failure likelihood is 50/5e6
- Uncertainty (Vendor trust) factor we will set at 100 (1 is complete trust) because vendor is not ILPM but there is past history with this vendor and no known part failures that have been to reported to us.
- Early failure likelihood of a single part is 100*50/5e6 = 1e-3 = 0.1%
- 0.1% is a "1" likelihood on GSFC's technical risk scale, so risk is 1x4.

Risk example 3

- On ELC on the ISS, the Tantalum capacitor for both main/aux feeds of the LVPS was installed in reverse polarity.
  - Additional Finding: All active ExPCAs on ELC1-4 and spare on ELC3 were built with same capacitor in reversed position
- This has resulted in 2 failures on the ground - one in initial ground testing of the ELC simulator (at KSC in 2011, resulting in replacement of parts without solving problem*), and another in 2012 in operation of the ELC simulator to support a customer, each after a few hundred hours of operation
- The primary sides of each ELC pallet have been operating continuously without any observed anomalies for many years; secondary sides have not been exercised on-orbit (with the possible exception of initial checkout).
- **The assertion from NESC & Aerospace Corp testing has been that temperature is the critical factor and that 25 deg C is the threshold above which there is a real threat to the capacitors and associated circuits**
  - This is based on temperature cycling that occurred in ambient pressure
  - This drives ISS to restrict Payloads' operations loading in the 120 to 28V converter above a particular beta angle
  - There have been no failures, leakage current excursions, or circuit issues to date in any operation in vacuum
  - No failures have occurred on-orbit in 4+ years of operation, albeit at temperatures mostly around 15 deg C with infrequent excursions up to about 30 deg C

*Since there was no resolution of PFR-ELC-003, there is not broad agreement that this failure is due to the reverse-bias capacitor

Risk example 3 cont'd



Testing profile of reverse caps from same lot in vacuum at operational V (-5.4V)

Risk example 3 cont'd

What is the risk of mission failure in the next 5 years of the temperature restriction is lifted from 40 deg C to 85 deg C and the temperature is maintained at a steady 85 deg C?

Given the reverse 25V Ta caps installed in the ELC LVPS (operating at -5.4V at 85 deg C) and the subsequent testing profile in the previous figure
It is possible that the leakage current will exceed 8 mA, taking out the MOSFET that regulates primary and secondary side power
Resulting in failure of the ELC pallet

The 85/86 deg C portion of the figure shows a parabolic profile of leakage current that would surpass 8 mA in < 2000 hrs, with almost complete certainty. This risk is a 5x5.

Risk example 3 cont'd

What is the risk of mission failure in the next 5 years of the temperature restriction is lifted from 40 deg C to 85 deg C and the temperature is less than 50 deg C 95% of the time, 60 deg C 5% of the time (but never for more than 24 hours) and spurious jumps to 85 deg C for no more than 2 hours each instance?

Given the reverse 25V Ta caps installed in the ELC LVPS (operating at -5.4V at the described temperatures conditions) and the subsequent testing profile in the previous figure
It is possible that the leakage current will exceed 8 mA, taking out the MOSFET that controls switching between primary and secondary side power
Resulting in failure of the ELC pallet

The majority time period of 50 deg C involves flat, stable leakage current. At 58 deg C, the leakage current remains flat as well. At 60 deg C, we can assume there is a very slight slope, but with no more than 24 hours time at 60 at any instance and maximum total hours of 2190, the leakage is insignificant. (note that at 70 deg C in figure, the continuous rise in leakage current would be around 1 mA over 2000 hrs). Furthermore, the brief periods of operation at 85 deg C also have insignificant effect on leakage current. Thus, the likelihood of exceeding 8 mA is insignificant (well below 0.1%) and the risk is noncredible.

Risk example 3 cont'd

- Note that for other conditions in between the two provided, the figure can be used to estimate cumulative leakage current, and by covering the ranges over the individual tested capacitors, the likelihood of exceeding 8 mA for the range of conditions can be predicted.
- In some cases, the data will be available to make reasonable predictions of risk, while in others testing will be required.
- In this example there were enough test data and accumulated time on-orbit to understand that under temperature restrictions, the hardware would be safe while extensive testing was performed.
- This case is extreme in that there should be no cases where you would want to so egregiously misuse a part when you have a choice.