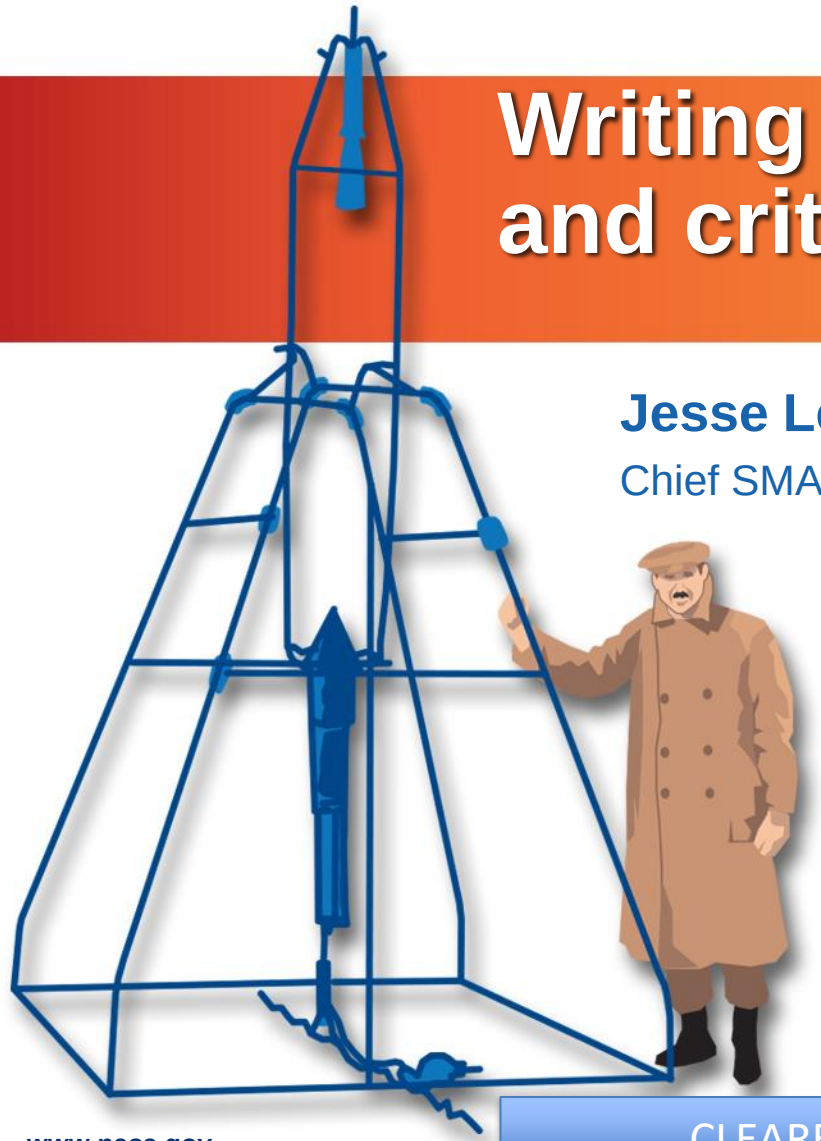
National Aeronautics and Space Administration



Writing good risk statements and critical thinking in risk

Jesse Leitner

Chief SMA Engineer, NASA GSFC

Aerospace Rethinking Risk Series

June 2024

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

Risk

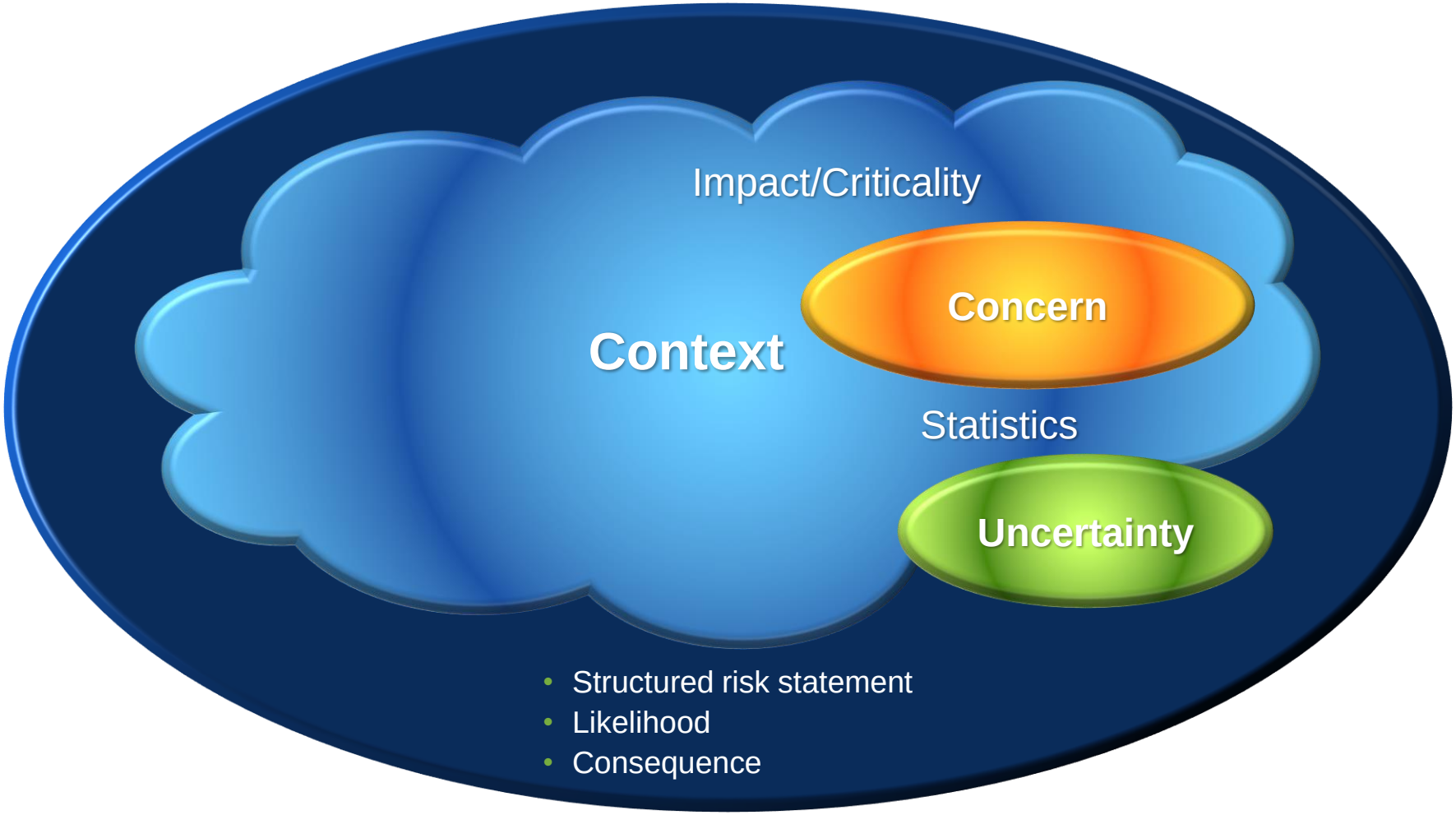
We'll take the house. Honey, the chances of another plane hitting this house are astronomical. It's been pre-disastered. We're going to be safe here.

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

Agenda Part 1: Formal risk processes

- Anatomy of a Risk
- Concern
- What is a Risk?
- Opportunities and Issues
- Risk Terms in NASA
- Risk vs. Possibility
- Ugly vs. Risky
- Risk of Conformance vs. Risk of Nonconformance

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)
  - Safety (injury, death, or collateral damage)

} programmatic

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

Opportunities and Issues

- Opportunity Definition: the combination of
  - a) the probability (qualitative or quantitative) that a positive gain or improvement will occur, and
  - b) the consequence or impact of the improved situation
  - c) a scenario that exists that may be exploited

- Issue: a problem that has occurred (an existing requirement is not being met)
  - This is a risk that has been realized, whether the risk was known beforehand or not

Handling strategies

- Research (Investigate): Consider and review all pertinent information sources to understand the risk.
- Mitigate – If “do nothing” is not acceptable, develop a mitigation strategy to measurably reduce the LxC. Specify the mitigation ECDs, resulting LxC score and rationale, and success criteria
- Watch: For risks where circumstances do not warrant immediate mitigation steps, define triggers that indicate the need for action. Include a timeframe for re-evaluation and active mitigation or alternate handling strategies.

Risk Terms in NASA

- Baseline risk: the normal level of risk in developing and assembling a product
  - This can be considered as risk that is accepted by a project at initiation without further tracking or debate
  - Generally we do not track risks within the baseline
  - Experienced developers mitigate baseline risks through standard processes

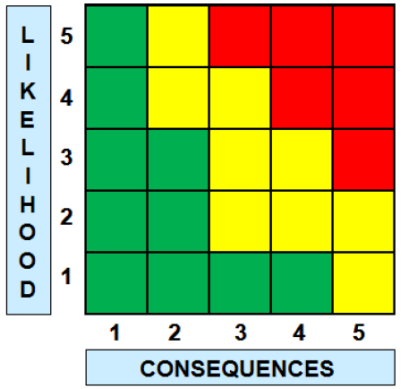
- Credible risk: risk having likelihood category of at least “1” on the pertinent risk scale (note that in GSFC’s risk scale there are 5 categories and 1 is the lowest risk category)
  - There are an infinite number of risks that are not credible for any project

Risk Terms in NASA (cont'd)

- Accept: Determine that the consequences of an identified risk, should they occur, are acceptable without further mitigation.
- Close: Determine that a risk is no longer credible and tracking may be discontinued
- Residual Risk: the remaining risk that exists after all mitigation actions have been implemented and/or exhausted in accordance with the RM process. Residual risks are often technical risks that are accepted at the time of launch. Often the term is used when an effort is complete to resolve a failure, anomaly, or nonconformance when resources are not available to completely resolve the concern or requirements shortfall.

Flight Project Risk Rating Scale (GSFC)

Likelihood	Safety Estimated likelihood of Safety event occurrence	Technical Estimated likelihood of not meeting performance requirements	Cost Schedule Estimated likelihood of not meeting cost or schedule commitment
5 Very High	$(P_{SE} > 10^{-1})$	$(P_T > 50\%)$	$(P_{CS} > 75\%)$
4 High	$(10^{-2} < P_{SE} \leq 10^{-1})$	$(25\% < P_T \leq 50\%)$	$(50\% < P_{CS} \leq 75\%)$
3 Moderate	$(10^{-3} < P_{SE} \leq 10^{-2})$	$(15\% < P_T \leq 25\%)$	$(25\% < P_{CS} \leq 50\%)$
2 Low	$(10^{-5} < P_{SE} \leq 10^{-3})$	$(2\% < P_T \leq 15\%)$	$(10\% < P_{CS} \leq 25\%)$
1 Very Low	$(10^{-6} < P_{SE} \leq 10^{-5})$	$(0.1\% < P_T \leq 2\%)$	$(2\% < P_{CS} \leq 10\%)$



Consequence Categories					
Risk	**1 Very Low**	**2 Low**	**3 Moderate**	**4 High**	**5 Very High**
Safety	Minor first aid treatment Required or collateral damage < $5k	Minor injury or occupational illness or collateral damage $5k - $20K	Major injury or occupational illness or collateral damage of $20k - $100k	Severe injury or occupational illness or collateral damage of $100k - $500k	Death or permanently disabling injury or collateral damage > $500k
Technical	Minor impact to lower priority full mission success criteria	Minor impact to higher priority full mission success criteria	Moderate impact to full mission success criteria. Minimum mission success criteria are achievable with margin	Major impact to full mission success criteria. Minimum mission success criteria are achievable	Minimum mission success criteria are not achievable
Schedule	Minor impact to schedule milestones; accommodates within funded schedule margin (FSM), no impact to critical path	Impact to schedule milestones; accommodates within FSM, slight impact to critical path	Substantive Impact to schedule milestones; accommodates within FSM, moderate impact to critical path	Major impact to schedule milestones; major impact to critical path anticipating replan of activities; FSM anticipated to fall below GPR requirements	Cannot meet schedule and program milestones; anticipate a re-baseline
Cost	0.5%-2% increase to the element ETC or 0.5%-1% impact on remaining project level development reserves through liens	≥2% but <5% increase to the element ETC or ≥1% but <5% impact on remaining project level development reserves through liens	≥5% but <7% increase to the element ETC or ≥5 but <20% impact on remaining project level development reserves through liens	≥7 but <10% increase to the element ETC or ≥20 but <50% impact on remaining project level development reserves through liens	≥10% increase to the element ETC or ≥50% impact on remaining project level development reserves through liens

HIGH RISK

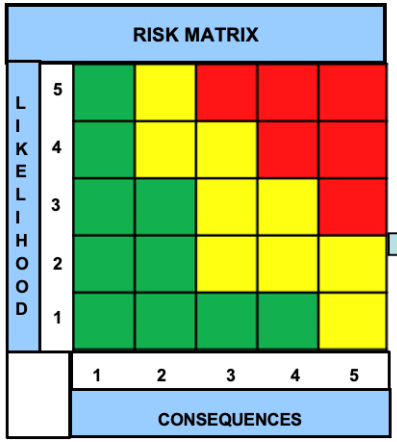
MODERATE RISK

LOW RISK

GSFC Institutional Risk Score Card

**For Likelihood rating, use Qualitative OR Quantitative analysis.*

LIKELIHOOD RATING			
5X5 Rating	Qualitative Likelihood	Quantitative (except Personnel injury/illness)	Quantitative - Personnel Injury/Illness
5	Very High	(P > 75%)	(Ps> 0.1)
4	High	(50% < P ≤ 75%)	(10^{-2}<Ps<10^{-1})
3	Moderate	(25% < P ≤ 50%)	(10^{-3}<Ps<10^{-2})
2	Low	(10% < P ≤ 25%)	(10^{-5}<Ps<10^{-3})
1	Very Low	(2% < P ≤ 10%)	(10^{-6}<Ps<10^{-5})



Time Frame	
Near-Term	6 months to 1 year
Mid-Term	1 to 2 years
Long-Term	> 2 years

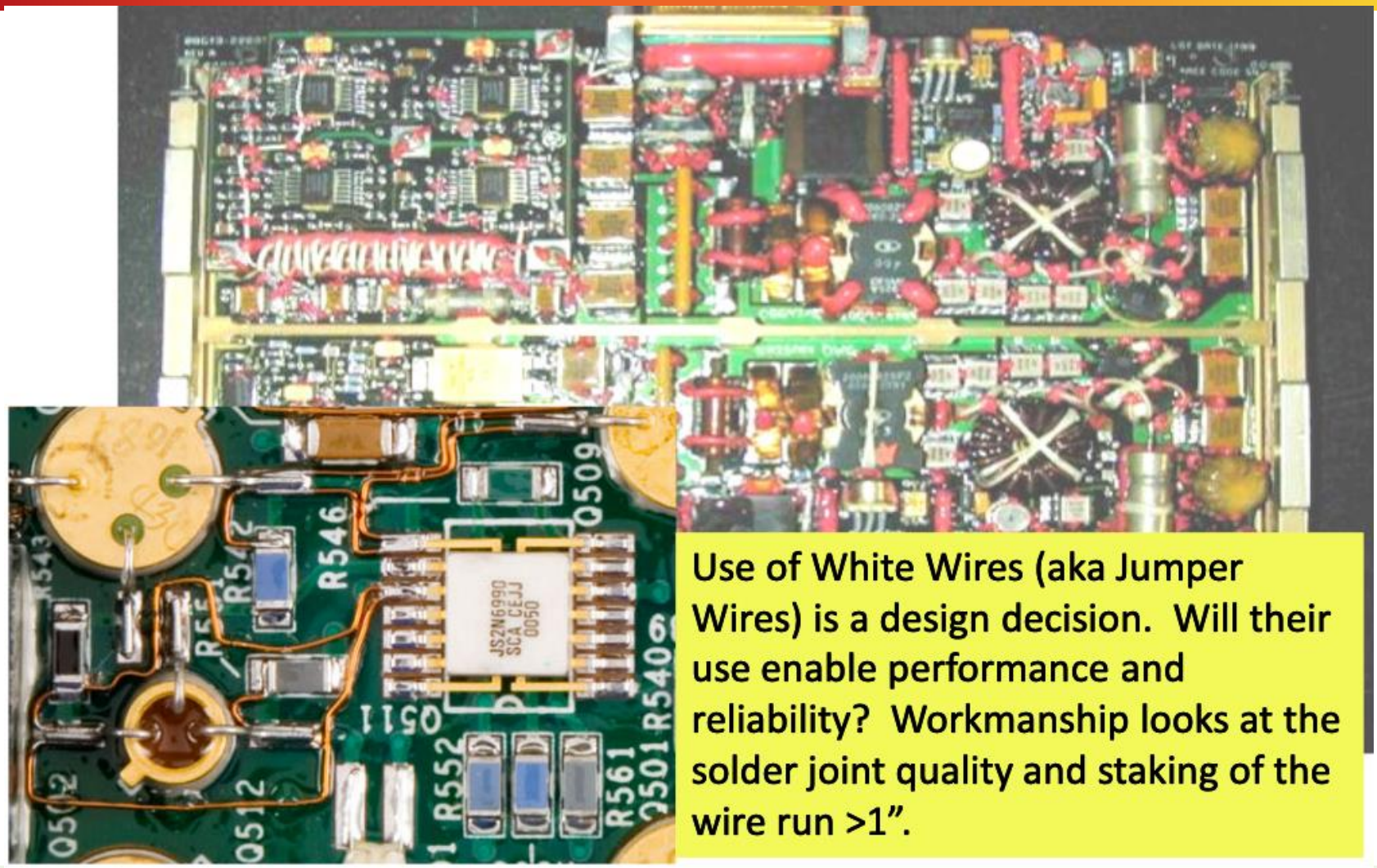
Risk Assessment Index (Possible Mitigation Strategies)	
	High (Mitigate)
	Moderate (Watch, Mitigate, Accept)
	Low (Watch, Mitigate, Accept)

		Very Low	Low	Moderate	High	Very High
Consequence	*Subcategories*	1	2	3	4	5
Health, Safety, Environment (HSE)	**Personnel injury/Illness**	Minor Injury	Short-term Injury or Illness	Injury or Illness Resulting in Days Away from Work OR Hospitalization	Injury or Illness Resulting in Permanent Partial Disability OR Hospitalization of 2+ People	Injury or Illness Resulting in a Fatality OR Permanent Total Disability
	Property Damage – **(Cost)**	$1K to $20K	$20K to $50K	>$50K to $500K	$500K to <$2M	≥$2M
	Compliance – OSHA Environment	De-minimis not compliance; or Minor or Non-Reportable Hazard or Incident	Minimal Impact to Compliance; or Administrative OSHA Violation	Moderate Hazard or Reportable Violation; or Minor OSHA Violation	Significant Threat to Regulatory Requirement; Event Requires Immediate Remediation	Cannot Comply with Regulatory Requirement; or Catastrophic Hazard
Technical Performance	**Infrastructure and Asset Impacts**	Minor Impact to Mission Support Infrastructure and/or Asset that can be immediately dispositioned.	Minor Impact to Mission Support Infrastructure and/or Asset	Significant Impact to Mission Support Infrastructure and/or Asset	Major Impact to Mission Support Infrastructure and/or Asset	Severe Impact or Loss of Mission Critical or Agency-Unique Infrastructure and/or Asset
	Organizational Objectives	Minimal Impact with immediate workarounds	Minimal Impacts	Moderate Impacts, workaround(s) available	Significant Threats, no feasible workaround(s)	Failure to Meet Critical Objectives
Agency Capabilities	Service Delivery Physical & Cybersecurity	Incidental Disruption of Institutional Services or Operational Support	Short-Term Disruption of Institutional Services or Operational Support	Significant Disruption of Institutional Services or Operational Support	Major Disruption of Key Institutional Services or Operational Support	Work Stoppage of Key Institutional Services or Operational Support
	Workforce (includes Technical Excellence)	Reduced Efficiency of Mission Support Resources	Minor Impact, Reduced Efficiency of Mission Support	Significant Impact, Reduced Efficiency of Operational Support	Major Impact to Effectiveness of Mission Operations Support	Severe Impact, Loss of Critical Skills or Capabilities
Cost	Organizational Budget Impacts	$5K to <$500K OR 0.5%-2% increase over allocated and negligible impact on reserve	$500K to <$1M OR 2% to 5% increase over allocated and can handle with reserve	$1M to <$2.5M OR 5% to 10% increase over allocated and cannot handle with reserve	$2.5M - <$5M OR 10% to 15% increase over allocated and exceeds reserves	>$5M OR >15% increase over allocated and exceeds reserves
Schedule	Project Timelines	1-3 days slip	Minimal Impact, Slip Is Within Schedule Dvell Time, No Impact to Milestones	Moderate Impact, Project Milestone Slip, No Impact to Budget	Significant impact, Project Milestone Slip Impacts Budget by <3 months	Major Impact, Project Milestone Slip Impacts Budget by >3 Months

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 severe consequences regardless of the probability of occurrence
- 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
- Lack of careful and reasoned analysis of each possibility in terms of the conditions that results in the consequence and the probability of occurrence **will** result in excessive cost and **may** increase the overall risk

Ugly vs. Risky—
Does Ugliness = Riskiness?



Use of White Wires (aka Jumper Wires) is a design decision. Will their use enable performance and reliability? Workmanship looks at the solder joint quality and staking of the wire run >1".

From: J. Plante, NSC Quality Engineering Seminar on Workmanship Standards., 2011

Risk of Conformance vs. Risk of Nonconformance

- Were requirements imposed based on an understanding of the risks within a project?
- What are the risks associated with the enforcement of requirements?
- What is the risk associated with a particular nonconformance?
- Should we immediately assume that a nonconforming item is risky for the application?
- In many cases there is a good reason why a product is nonconforming

Do not reject a nonconforming item without understanding the risk.
Determine the cause of NC before reproducing the item.

Agenda Part 2: Writing Risk Statements

- Key Rules To Follow
- Considerations
- Flight Project Risk Statements
- Institutional Risk Statements
- Examples
- Exercise

Risk Statement (GPR 7120.4)

- 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. 22
  - 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. 24)
  - 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
  - Caveat – if redundancy is required to continue mission, then it is effectively a level 1 reqmt
- 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.

Fundamentals (part 1)

- The GIVEN must substantively lead to the direct effect or INTERMEDIATE CONSEQUENCE:
  - (good example) Given a problem on other components that has caused failure, it is possible that we experience failure using the same components
  - (bad example) Given that we are using parts, it is possible that they will fail
  - (good example) Given that we are using parts that have a known failure history, it is possible that that they will fail
  - (bad example) Given that we are using COTS parts not screened by the government, it is possible that they will fail
    - if there is not a known history of failure, then the context does not lead to the INTERMEDIATE CONSEQUENCE
  - (good example) Given the use of high voltage optocouplers that have sustained a x% failure rate in applications at 5 kV, it is possible that the same optocouplers will fail in our 5 kV application
  - (good example) Given the use of “happy meal” COTS parts that fail in less than one year at 5% of the time, it is possible that two parts will fail in less than one year
  - (bad example) Given the use of a hybrid DC/DC converter that had a DPA unit from the lot fail a 5000g constant acceleration test, it is possible that one converter will fail in the mission
    - If the mission will never expose parts to greater than 50g, then there is no relevance of the test to cause elevated risk.

Fundamentals (part 2)

- The CONSEQUENCE must be an effect on mission performance (programmatic or technical, i.e., L1 requirements or mission success criteria), or safety (threats to people, the environment, collateral damage, etc); not to internal requirements
- (good example): it is possible that two parts will fail, resulting in mission failure
- (good example): it is possible that the star tracker will fail, resulting in substantial degradation to long wave science
- (bad example): it is possible that a part will fail, resulting in failure of the star tracker
  - What does failure of star tracker mean to mission performance
- (bad example): it is possible that a workmanship violation will occur, resulting in a degraded solder joint
- (good example): it is possible that a degraded solder joint will escape further environmental testing inspection but fail on-orbit, leading to box failure (non redundant box) on orbit, resulting in loss of ocean color measurements
- (bad example): it is possible that noncompliance to quality requirements will occur, resulting in mission failure

Considerations

- For programmatic risks (e.g., risks of loss of schedule and budget reserve from having to rework hardware to repair a failure), redundant elements increase risk likelihood because more opportunities for failure exist and, generally, a project will not launch with a nonfunctional or degraded side redundant element.
- For technical risks, redundancy reduces risk likelihood because at least two failures of less than 100% likelihood must occur and the likelihoods are multiplicative (when the failures are independent).
- Hardware safety almost always is associated with programmatic risks (commonly associated with lifting or the potential for overtest), but in some cases may involve a threat during pre-launch processing, launch, or commissioning.
- Be careful not to capture hardware safety risks as safety risks. Hardware safety risks are programmatic or technical. Otherwise, an unbalanced risk will result from prioritizing one risk over another that has the same outcome.
- Safety risks are not common at GSFC because generally the approach is to eliminate any elevated threat to personnel or collateral damage.

Risk example with corrections (1)

(first attempt) Given that TRW might deliver the avionics box late

It is possible that testing will not be completed on time

Resulting in slip in launch date

(corrected) Given the high turnover rate (approximately 20% of avionics project staff over last two months) at TRW

It is possible that the avionics box will be delivered late, affecting critical path

Resulting in slip in launch date

Other risk example with corrections (2a)

(first attempt) Given the use of dozens of parts directly affected by GIDEP H6-XXX-YYY

It is possible that a part failure will occur

Resulting in resources to recover or mission failure

(corrected – part 1) Given the use of dozens of parts directly affected by GIDEP H6-XXX-YYY (which warns of part failures during ground test)

It is possible that a part failure will occur in I&T

Resulting in resources required to recover

Other risk example with corrections (2b)

(first attempt) Given the use of dozens of parts directly affected by GIDEP H6-XXX-YYY

It is possible that a part failure will occur

Resulting in resources to recover or mission failure

(corrected – part 2) Given the use of dozens of parts directly affected by GIDEP H6-XXX-YYY

It is possible that a part failure will occur on-orbit without any sign of a problem in I&T

Resulting in loss of key science objectives

Other risk example with corrections (3)

Concern: relatively high volume of nonconforming product delivered

(initial proposed risk) Given the acceptance by the project of nonconforming product in the past

It is possible that nonconforming product will be accepted in the future

Resulting in mission failure

(corrected) Given the regular delivery of nonconforming product by McDonnell Douglas in the past

It is possible that multiple retries will be required to obtain acceptable product on upcoming builds

Resulting in significant schedule delays

Institutional Safety Risk Example

- An incident that occurred in an office at GSFC involved a smoke alarm that caught fire due to an internal short circuit.
- After analyzing the problem, it was discovered that there is a flaw in the circuitry for an affected class of units that would cause 1 failure per 7 years for 1% of the class of units.
- Between 200 and 400 of the offices and facilities at GSFC have a unit in the affected class.
- It is estimated that it would take a month to replace all affected units using the standard replacement process.
- It is necessary to determine the risks both to facilities and personnel of proceeding with the nominal (i.e., non-emergency) replacement process.

Institution risk example – programmatic facility risk

A facility assessment established that all smoke alarm installations of affected alarms are known to be within fire retardant ceiling tile, with a minimum of 1 ft radius of each other. In case of a characteristic fire, the probability of catching neighboring materials on fire, including sparks going to the carpet prior to self-extinguishing is determined to be 1/3 for "moderate" damage, consequence "3". A pertinent risk statement is:

Given the use of fire alarms affected by a systemic flaw, **it is possible that** one catches fire during the month it takes to replace them all, **resulting in** moderate damage to facilities

The likelihood is 0.01*(1/7)*(1/12)*(1/3)*400 = 1.58%, assuming all 400 offices are affected. The programmatic risk scale begins at 2%, so this risk is noncredible. Being close to the threshold may prompt an accelerated process. Next, we will consider the safety risk.

Institutional Risk Example – personnel safety risk

- The safety risk will build upon the previous programmatic risk, but safety becomes an issue prior to moderate damage, so a ½ is used as the probability of toxic smoke or other fire danger if the unit catches fire. The threats that the local area will catch fire without a functioning fire alarm include smoke inhalation, explosion, and trapped personnel. Furthermore, there is also a threat that toxic smoke will affect personnel prior to detection and warning by functional fire alarms.

- A pertinent personnel safety risk statement is:

- **Given** the use of fire alarms affected by a systemic flaw, **it is possible that** one catches fire during the month it takes to replace them all, **resulting in** in serious injuries to personnel due to fire

- The likelihood is 0.01*(1/7)*(1/12)(1/2)*400 = 2.38%. This results in a 4x4 safety risk using GSFC's risk scale. This red risk will prompt emergency action to replace the smoke detectors or perform other mitigations.

Software risk scenario

The software architecture for a polar-orbiting, three-axis stabilized spacecraft is compartmentalized with most of the primary spacecraft and instrument software being a COTS product with an interface for a custom software module. Mission success is defined by capturing three events over a two-year period for events that occur 25 times per year. The COTS software was largely aligned but not fully compliant with Class C software requirements. The primary software had two prior successful flights on gravity gradient stabilized LEO equatorial missions. Battery, propulsion, and electronics are capable of supporting a minimum of three-years of on-orbit operation. Mission Operations is funded for 18 months. On one prior flight, a software anomaly shut down spacecraft operations for 2 weeks to resolve the problem. A custom software module is interfaced, which includes the attitude control system software, communication link capability with the ground, ability to upload new software from the ground, full safe mode for the spacecraft, and the ability to boot up the primary software. The custom software module is also stored (redundantly) on a PROM.

Scenario cont'd

- The custom software is fully Class B compliant and is all deemed mission critical, and treated as safety critical software, with complete testing.
- Thorough tests were performed based on several injected faults into the primary software to verify the ability for the safe mode to take control, communicate with the ground, upload new software, and boot up the new software, both from the primary storage and from PROM.
- How can we characterize the risk picture? Let's look at a few risks.

SW risk 1 (technical)

- Given: the minimally tested COTS flight software with limited past usage and previous significant anomalies
- It is possible that: software will go into a frozen state, unable to perform any mission functions and losing control of the spacecraft
- Resulting In: end of mission
- In this case, we have provided sufficient testing to verify the “bullet-proof” safe mode, so we wouldn’t consider this a credible risk

SW risk 2 (technical)

- Given: the minimally tested COTS flight software with limited past usage and previous significant anomalies
- It is possible that: software will go into a frozen state, unable to perform any mission functions and losing control of the spacecraft, tripping into safe mode to troubleshoot software
- Resulting In: Excessive time required to develop and test new software and thus reduced science over 18-month period
- In this case, we acknowledge the possibility that we have limited capability to fix the COTS software and perform patches or redesign. However, the need for only 3 events, with 25 per year, over 18 months, gives much opportunity:

- A reasonable (and conservative) risk might be 1x4 (0.1-2% likelihood of major impact of full mission success criteria)

SW risk 3 (programmatic)

- Given: the minimally tested COTS flight software with limited past usage and previous significant anomalies
- It is possible that: software will go into a frozen state, unable to perform any mission functions and losing control of the spacecraft, tripping into safe mode to troubleshoot software
- Resulting In: Excessive time required to develop and test new software and thus extra cost and time

- A reasonable (and conservative) risk might be 4x3 (50-75% likelihood of 5-7% increase in cost)

Mechanical Example (1)

(T) Given that the vendor performs random vibe in lieu of sine vibe

There is a possibility that the amplitude of the 4 Hz response will be under-determined and the structure will be subsequently damaged in launch

Resulting in major mission degradation

Mechanical Example (2)

(T) Given the lack of a component level vibe

There is a possibility that inherent flaws remain and are not uncovered in observatory level vibe

Resulting in structural failure during launch and subsequently end of mission.

(P) Given the lack of a component level vibe

There is a possibility that model deficiencies are not identified until observatory level vibe

Resulting in excessive cost and schedule to redesign the structure

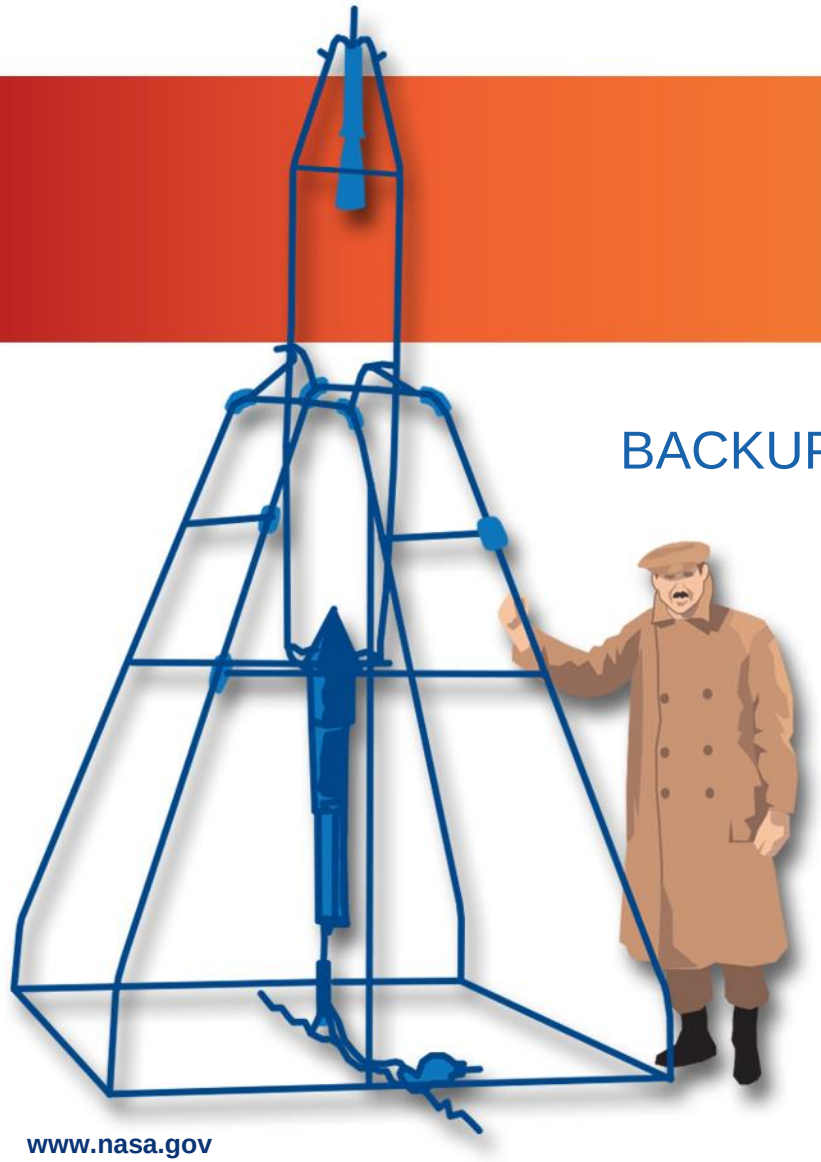
Summary

- Consistency and rigor in writing risk statements is key not only for communicating risks, but also to ensure proper risk trades can be performed
- Writing good risk statements will enable the most effective risk management

References

- GPR 7120.4E (GSFC risk management procedures)
- NPR 8000.4 (Agency risk management procedures)
- GSFC-HDBK-8005 (GSFC risk assessment handbook)
- NASA/SP-2011-3422 (Agency risk management handbook)

National Aeronautics and Space Administration

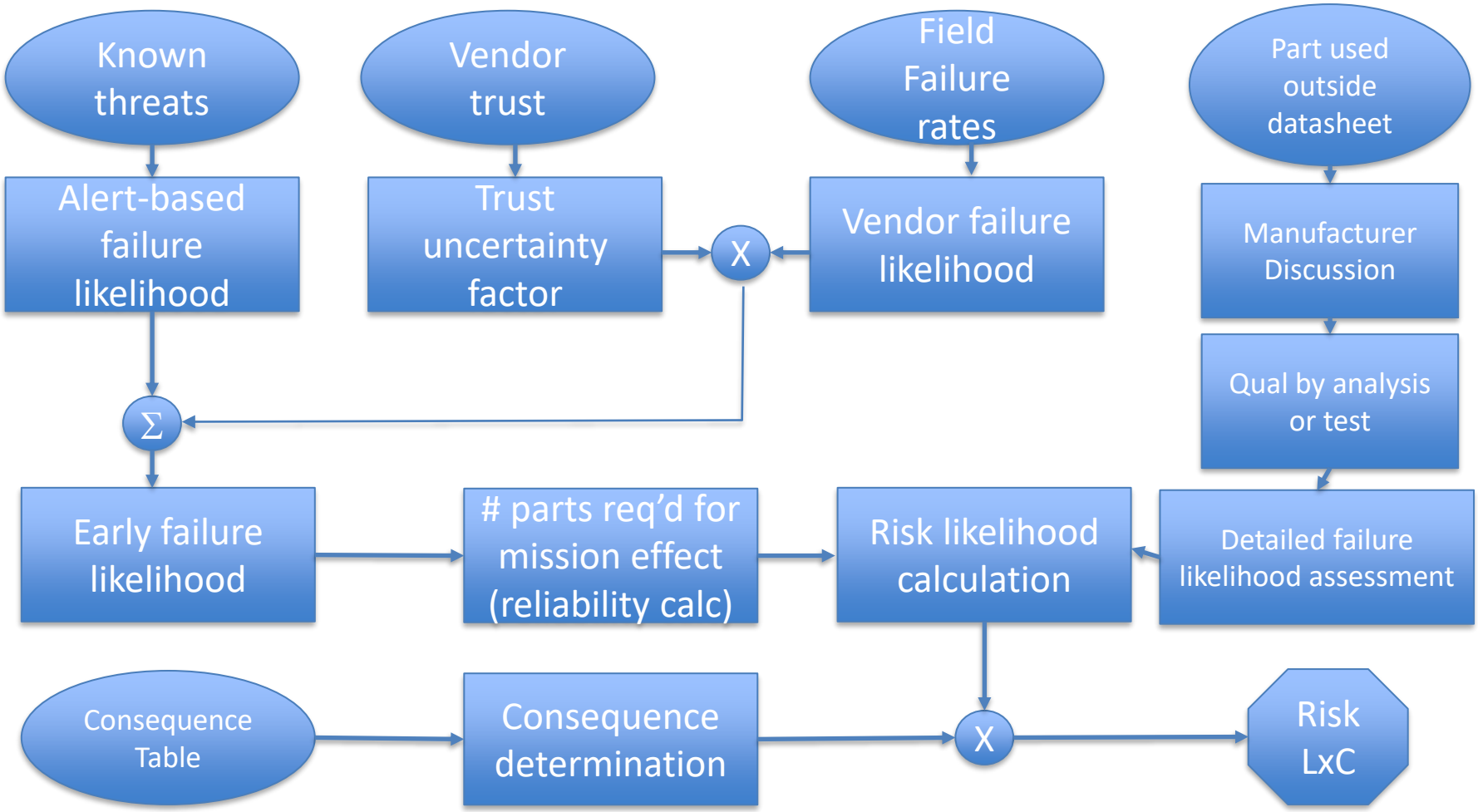


BACKUP

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

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

Known threats (examples)

- GIDEP warns that 1% of parts have been failing
- GIDEP warns that 5% of parts will experience intermittent open 1% of the time.
- 5% of parts from same LDC have failed at power-up on a different project's board, but worked otherwise
- GIDEP warns that 5% of LDCs have 10% of parts in lot experience ESR increase of up to 20%
- Parts are used over their rated values by 20%, 0.05% of the time

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

Parts 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

Parts 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.

Alert-driven examples (1)

(P) Given that the vendor will rework the board with encapsulated leads precluding further rework

There is a possibility that normal issues encountered during I&T will require replacement of a board late in the program

Resulting in significant cost and schedule expenditure

(T) Given that the vendor will rework the board with encapsulated leads with only 2 prior instances of performing similar work

There is a possibility that a latent defect will be present that is not exposed in environmental test

Resulting in on-orbit failure

Alert-driven examples (2)

(P) Given the use of 96 (opportunities for a part failure across both boards) BJTs in small TO cans affected by the reported laser etching concern

It is possible that one will fail in I&T

Resulting in significant resources to replace the part and regression test the board.

(T) Given the use of 2 redundant boards, with 48 BJTs each in small TO cans affected by the reported laser etching concern

It is possible that two parts will fail (loss of one each side is required to lose function) on orbit after making it through I&T successfully

Resulting in loss of mission

Ex. 2: one solution

- For this problem, it is a simple matter of establishing a local context for risk.
  - Are there tight cables? Is there adequate stress relief? Is there a known history of related problems or positive performance with this particular vendor and location?
    - Specific situations will lead to determination of specific areas of risk, and the overall context (including redundancy, testing done, testing yet to perform, etc) will lead to determination of project risks
  - Take note of jumper wires and see how they are actually implemented. If not staked, is there adequate integrity of the wires?
  - In either case, any off-nominal situation provide context for assessment of risk

Ex 3, one solution

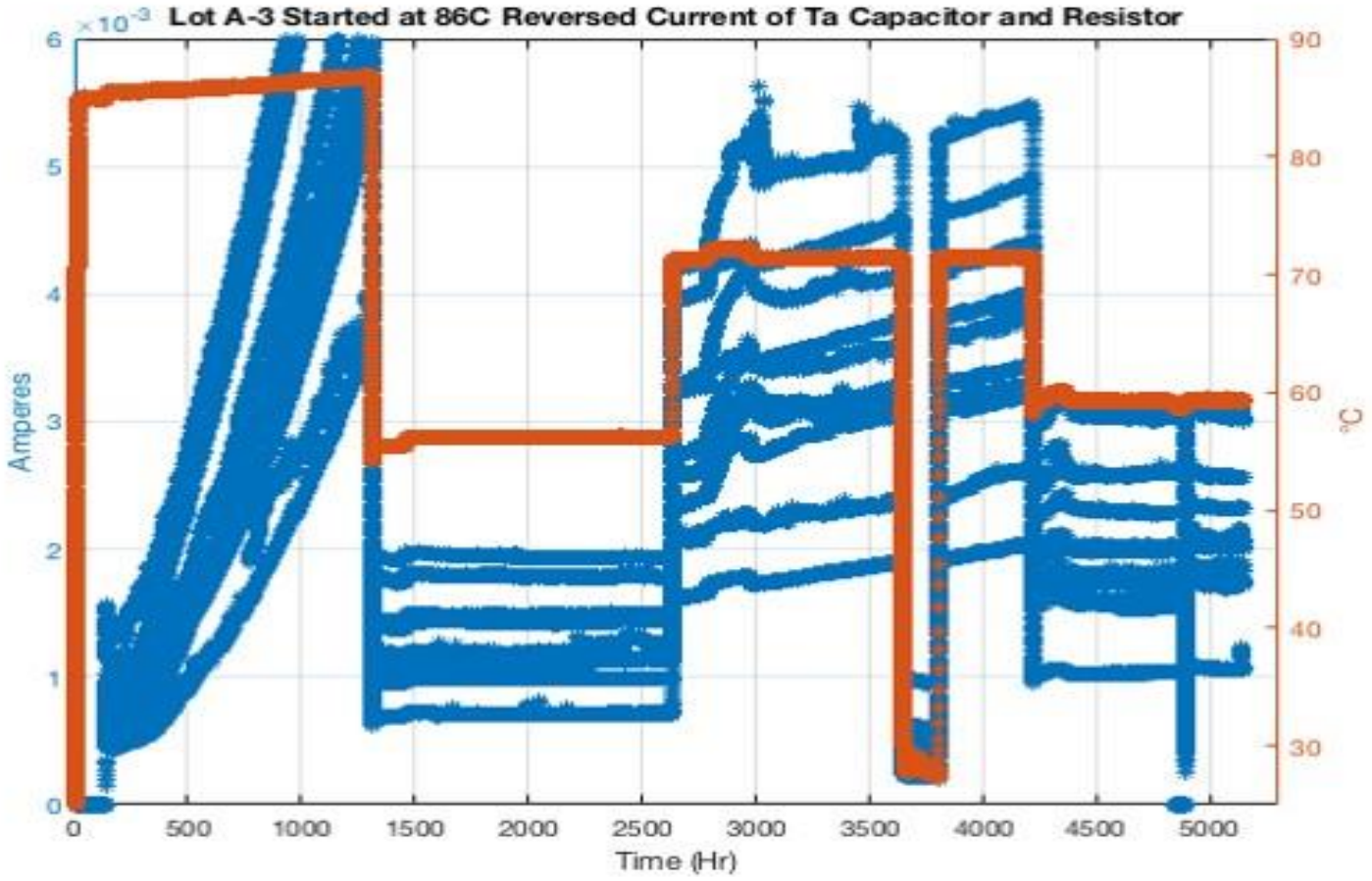
- Starting with the assumption that these are popular capacitors, the fact that there is only one reported failure, starts out with a very low context for risk. 1% of the parts are apparently affected by the delamination problem, but the delamination problem does not indicate that a part will fail. So early failure likelihood of a part can roughly be estimated by (.01)*(likelihood of failure given delamination)*(likelihood of having an affected lot). Given the fact that only one failure has occurred, it is apparent that the likelihood of failure is very low, unless we know for a fact that only a small number of lots are affected, in which case we need to determine if we have one of them. If the problem is very recent, for recent lot date codes, and we have a recent lot date code but don't know whether we are affected, then the likelihood of having an affected lot may be relatively high. If we assume that both of the likelihoods above are ~1, then we're still left with a .01 likelihood of early failure of one part, and 5 opportunities on the side. A redundant application indicates that two part failures are required for an on-orbit failure, and since we have already linked the failure likelihood given delamination and the fact that we have an affected lot, the two failures would be independent in terms of the .01 likelihood, and we end up with an early failure likelihood of .05*.05 = 0.0025, or 0.25%, which makes just above the floor of 1 on the technical risk scale. If the board is critical, then we would have a 1x5 risk. Redundancy penalizes us for programmatic risk, and we would get roughly 50*.01 = 0.5, or 50% chance of failure of any capacitor that would require replacement before launch, so in the case where we know the lot is affected and delamination leads to certain failure, the programmatic risk would be high, with a 50% chance likelihood of part failure (4 likelihood). Replacing a part depends on many factors, but in most cases a 2 is about right, so that would be a 4x2 risk. Note that in most cases, both of these likelihoods are going to be very low and most scenarios would have both risks to be noncredible. Context is critical here.

Parts 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

Parts risk example 3 cont'd



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

Parts 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.

Parts 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.

Parts 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.

Risk exercise 1

- The following risk was proposed that provides a perfect basis for discussion

- Given that the FPGA ESD suppression diodes are disabled
- There is a possibility that if it is determined that the PSU is ESD class 0 at the box level
- Resulting In an increased risk of a damaging ESD event

One Solution

- One revised form

Given that: the RTAX2000 FPGA ESD suppression diodes are disabled

There is a possibility that: the payload services unit will be damaged during a regular ESD event .

[what we are saying here is that ESD events will occur, so there is not another hidden likelihood here – the question is whether we can say that is a fact. This also assumes that all of the other ESD barriers of protection break down, such as wrist straps, mats, etc]

Resulting in: Severe mission degradation

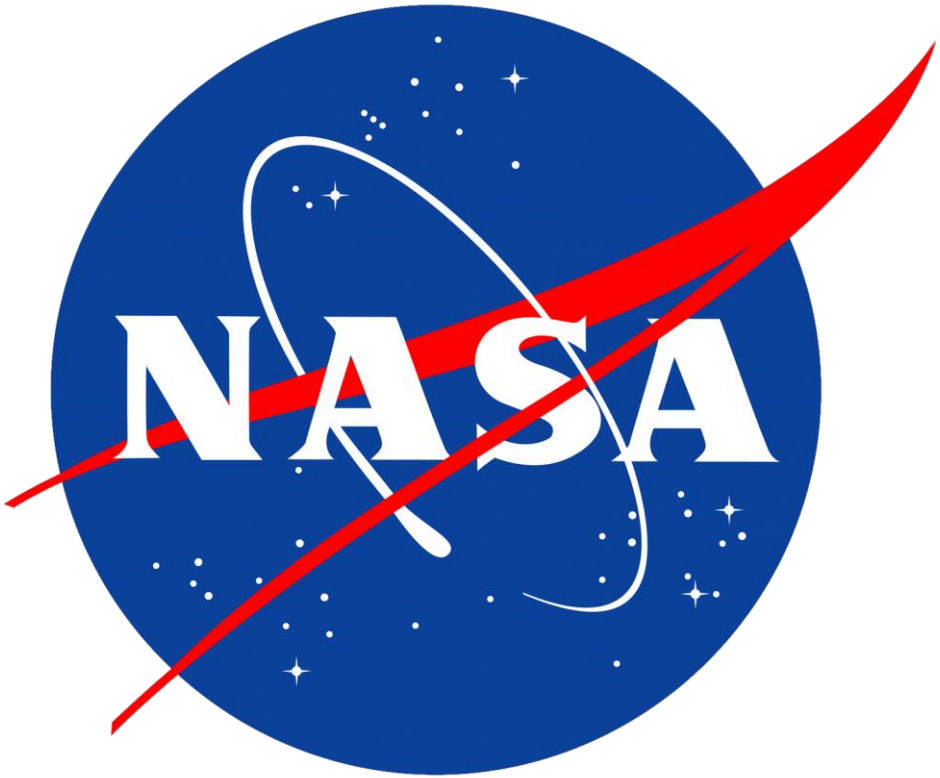
- The reality is that there are numerous barriers of protection against an ESD hit. These can either be used to make the risk noncredible or treated as a mitigation strategy if the diodes are not going to be enabled.

Risk Exercise 2

- McDonnell Douglas, the prime contractor, has indicated that now that all of their other customers (DoD, IC, and commercial) have accepted their own internal command media for workmanship and no longer are requiring their own standards. Hence, they have now stated that they are using their own standards from here on in for all customers, as it does not make sense to use a different standard for such a small part of their customer base.
- GSFC workmanship assessed their practices and found two primary areas where MD used less stringent practices:
  - There is no bend radius requirement for cabling
  - There is no staking requirement for jumper wires
- Does this situation indicate elevated risk to you? Write a risk statement to characterize the situation and estimate a likelihood and consequence

Risk Exercise 3

- Late in I&T it was discovered that one of the parts used in the power control unit has been identified in a new GIDEP problem advisory. The advisory states that 1% of the parts in several lot date codes of capacitors are affected by an internal delamination problem that appeared after the parts had been subjected to vacuum for at least 100 hours. The delamination problem was discovered in CSAM imaging of samples of parts, and delamination itself does not affect the function of the part. One part failure has occurred due to the problem and an exhaustive search has not revealed other instances. The power control unit has a primary and redundant side, each with 5 such capacitors that can take out the side if the capacitor were to short, and 20 such capacitors that have minimal impact to the performance.
- Is there elevated risk? How would you characterize it?


NASA