National Aeronautics and Space Administration

Perspectives on Risk in Space System Development

Jesse Leitner

Chief SMA Engineer, NASA GSFC

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

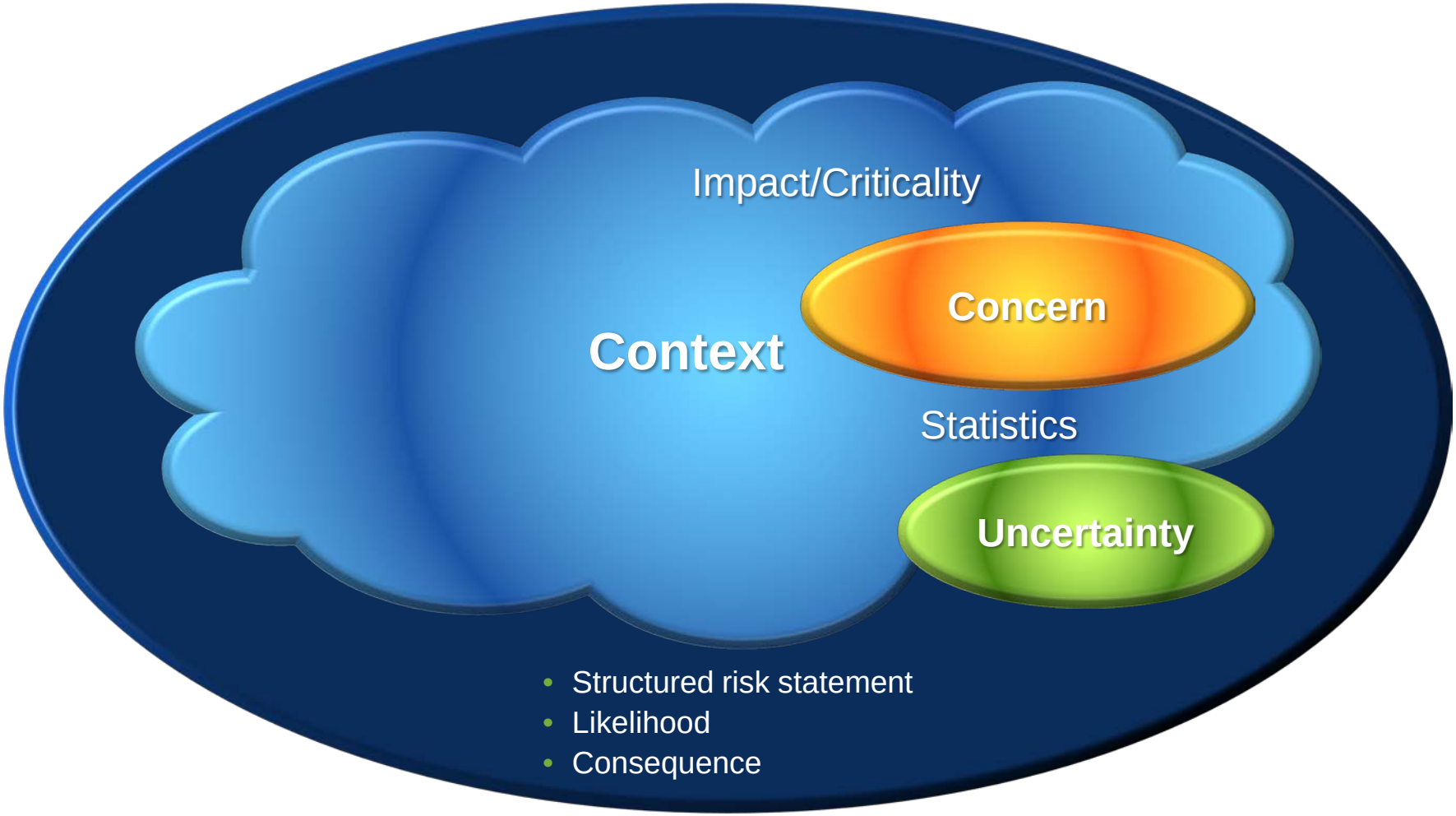
- What is Risk?
- Risk Terms in NASA
- Why Do We Worry About Risk?
- Risk vs. Possibility
- Balanced Risk
- Perspectives of Risk (Stakeholder, Developer)
- Risk as a Development Tool
- Acceptance of Risk at Different Levels and Times
- Risk Classification
- What is Risk-based SMA?
- Ugly vs. Risky
- Risks of Conformance and Nonconformance

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
  - In short, risk is an expectation of loss in statistical terms

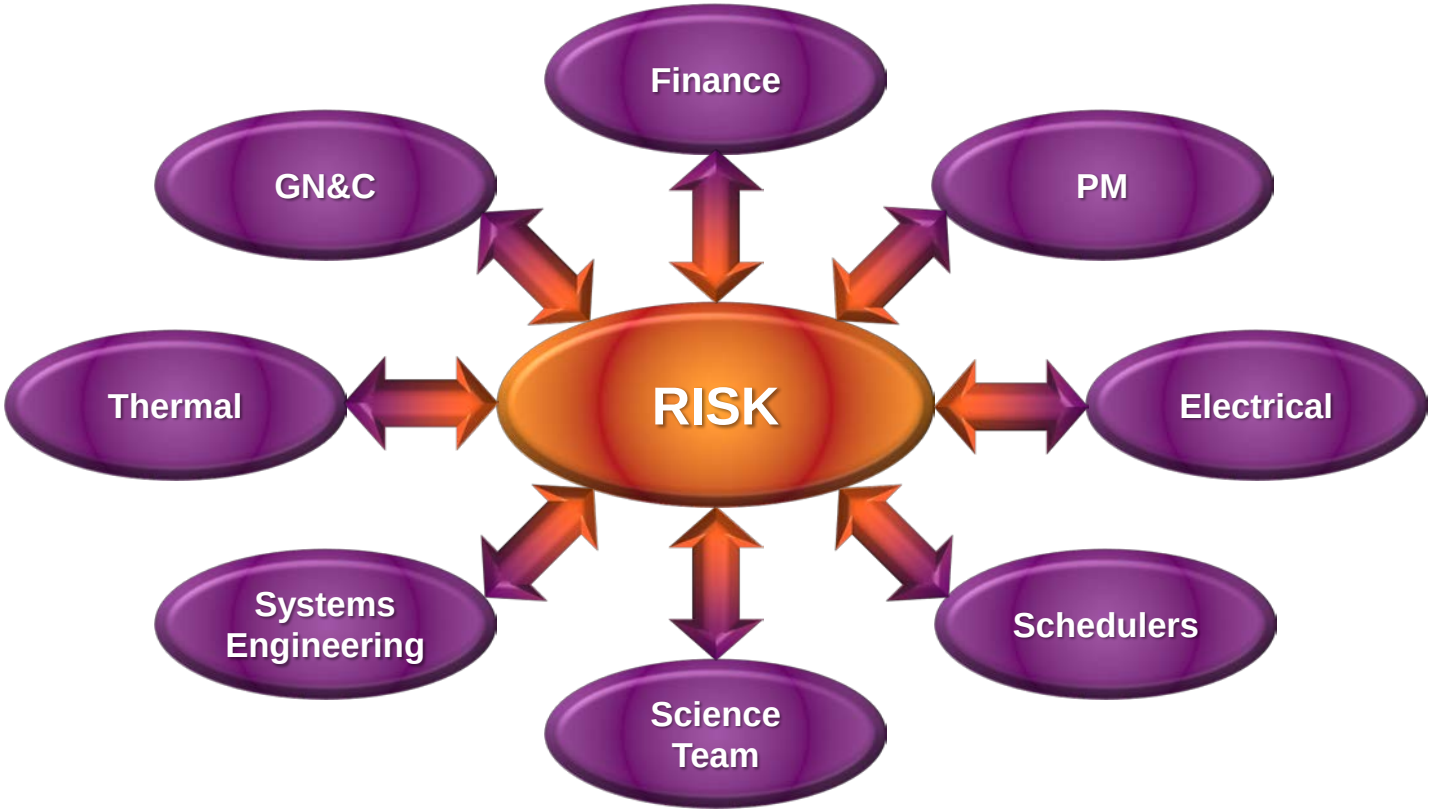
- Flavors of risk (consequences)
  - Technical (failure or performance degradation on-orbit)
  - Cost ($ it will take to fix the problem)
  - Schedule (time to fix the problem)
  - Safety (injury, death, or collateral damage)

Anatomy of a Risk



Risk as a Common Language

- Risk is the common communication language between all of the technical and nontechnical disciplines in a project



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.

Why Do We Worry About Risk?

- **We don't want bad things** to happen
- The only way to avoid risk is to avoid doing anything
- Understanding risk is key to engineering the system
  - Establishing requirements
  - Responding to undesired or unexpected events
  - Choosing between different options
- Communicating risk is key to portraying the status of a project in development

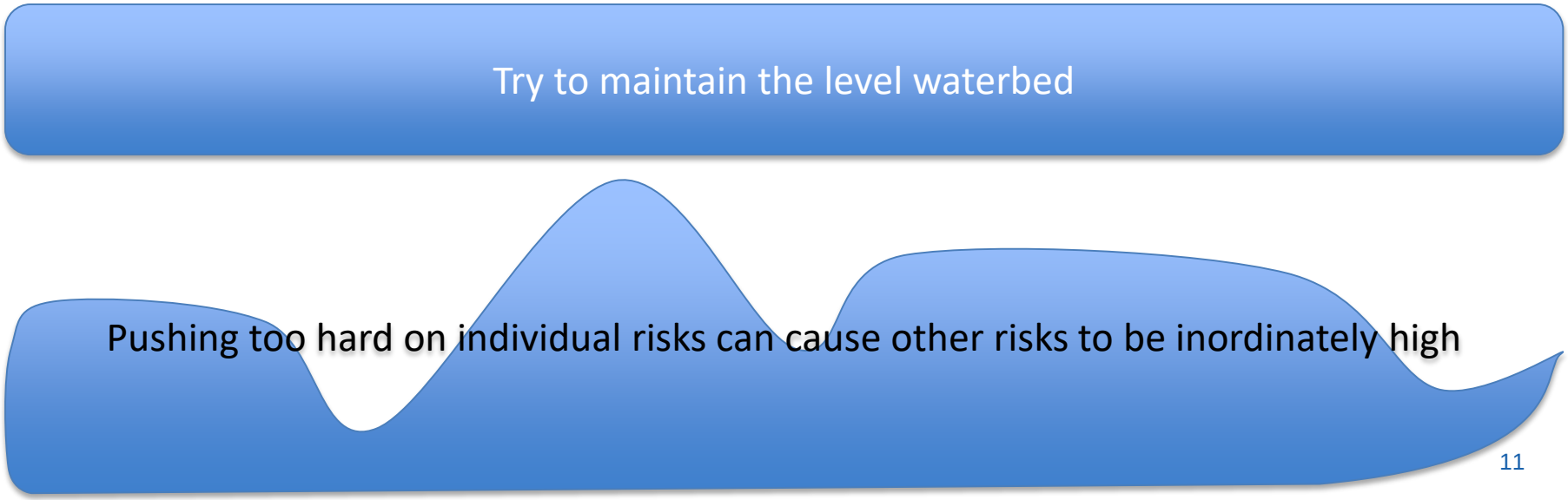
Proton Failure

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

Balanced Risk (maintaining a level waterbed)

- A systems approach of looking across all options to ensure that mitigating or eliminating a particular risk does not cause much greater risk somewhere in the system



Unbalanced Risk Example

- General safety requirements dictate that anything considered "safety" requires 3 inhibits.
- Unfortunately, many elements prior to launch vehicle separation that are tied solely to mission success are put under the safety umbrella.
- This means that by default, many items such as premature deployment of solar arrays or other appendages are considered a safety issue for the on-orbit portion, even if they have no range safety effect, and they prompt a decision that it is always better to have more inhibits even if such a design prompts an even greater risk of mission failure due to one of the inhibits not releasing.
- Ultimately, under the guise of “safety” we may end up with a less reliable system that is not more safe if we are not diligent with system-level thinking

A common occurrence: The Battle of Wills

- Each of two or more sides has a perspective, philosophy, or, in the worst case principle
- All are conflicting, and generally based on past experience in some context
- The heels dig in, and personalities take over
- It's time to frame the risk on both sides of each perspective

Perspectives of Risk—What Attributes are Used to Paint the Risk Picture?

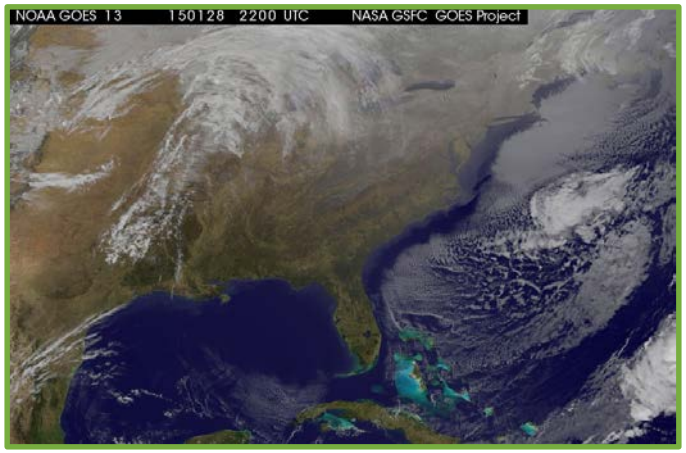
Stakeholder

- Well-established requirements and processes followed
- Assessment from independent review team
- Project risks presented
- Problem records
- Waivers

What do you mean you're not following the NASA Lifting Standard?

Developer

- Experiences in integration and test
- Project risks tracked
- Team internal dynamics and confidence
- PI/PM/systems engineer confidence



We know how to do this—we've done it before.

Risk Acceptance at Different Levels and Times

- The primary stakeholder(s) (MDAA, Center Director, NOAA, user community, etc.) accept(s) risks for project mission success
- Risk acceptance is delegated to the project to manage real-time, day-to-day development
  - Stakeholder has right of refusal through risk communication
- Safety and Mission Assurance ensures the risks are properly captured and communicated
- Many risks based on programmatic concerns are accepted from day one
- Most technical risks need not be accepted until launch
  - Many risks involve items that are buried into a system or core to the system design such that removal will be very painful and are for all intents and purposes accepted early on
- Programmatic risks based on technical concerns that have not been fully mitigated will frequently become technical risks, i.e., there may be a latent defect that survived through I&T

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.
- There is one technical requirement from HQ associated with risk classification: single point failures on Class A missions require waiver.
- There will be changes in the new NPR 8705.4

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 (may be dominated by yellow risks).
  - Many credible mission failure mechanisms may exist. A failure to meet Level 1 requirements prior to minimum lifetime would be treated as a mishap.
  - Examples: LADEE, IRIS, NICER, and DSCOVR

Risk Classification—(Non-NPR 7120.5 Projects)

- **NPR 7120.8 "class"—Technical risk tolerance 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

What is Risk-Based SMA?

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

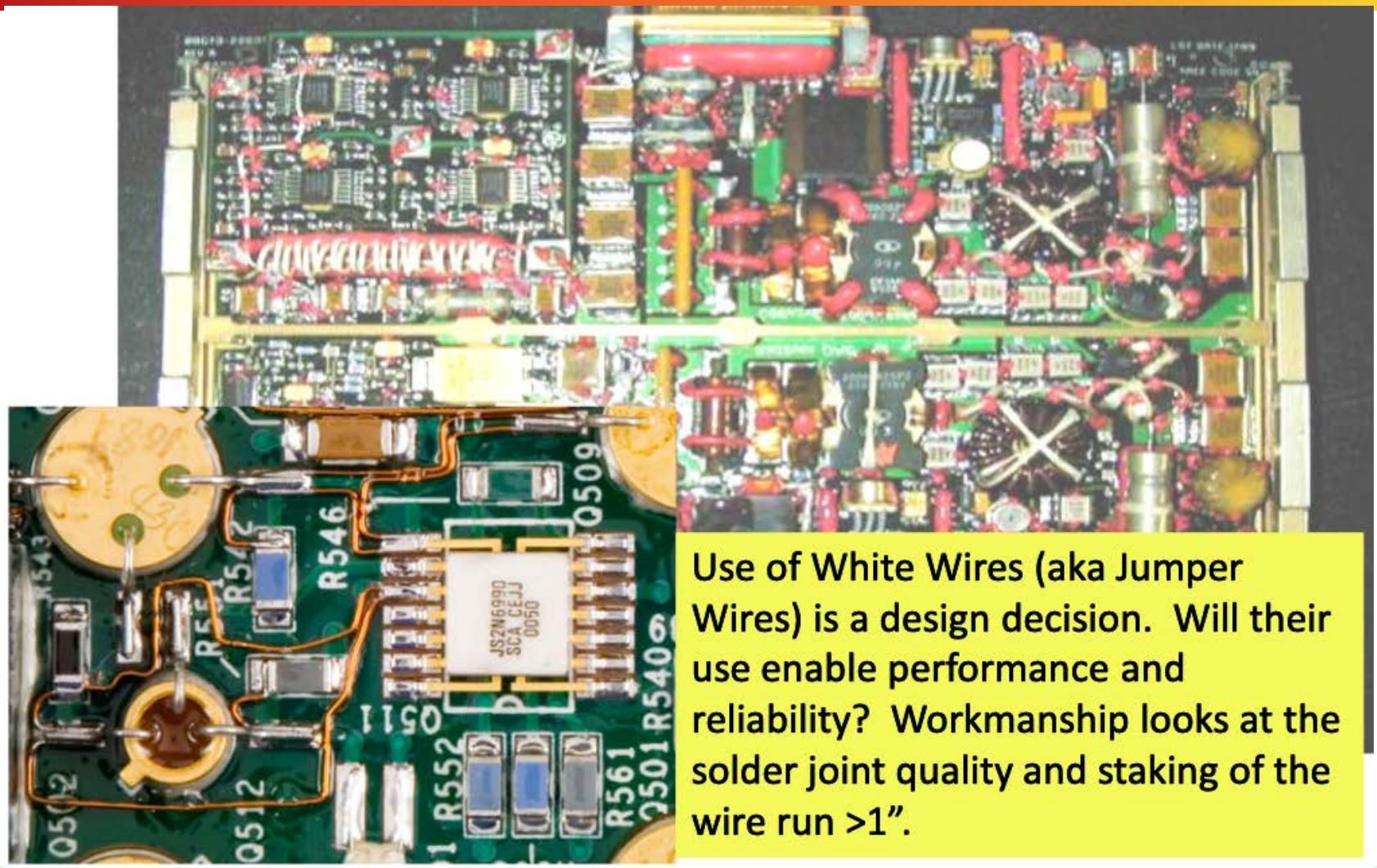
Risk-based SMA is now GSFC policy—GPR 8705.4

Attributes of Risk-Based SMA

- ***Early discussions*** with developer on their criteria and approaches for ensuring mission success (e.g., use of high-quality parts for critical items and lower grade parts where design is fault-tolerant) and responsiveness to feedback
- ***Upfront assessment*** of design, operations, reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied
- ***Judicious application*** of requirements based on learning from previous projects, the results from the reliability/risk assessment, and the operating environment (Lessons Learned—multiple sources, Cross-cutting risk assessments etc.)
- ***Continuous assessment*** of risks (safety, technical, and programmatic together to assure all factors are considered) to design performance, availability, manufacturability, operations/testing, and robustness in response to testing, revision, rusk mitigations, and remediation.
- ***Characterization of risk*** for nonconforming items to determine suitability for use—project makes determination whether to accept, not accept, or mitigate risks based on consideration of all risks
- ***Continuous review*** of requirements for suitability based on current processes, technologies, and recent experiences
- ***Consideration*** of the risk of implementing a requirement and the risk of not implementing the requirement.

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

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.

Summary

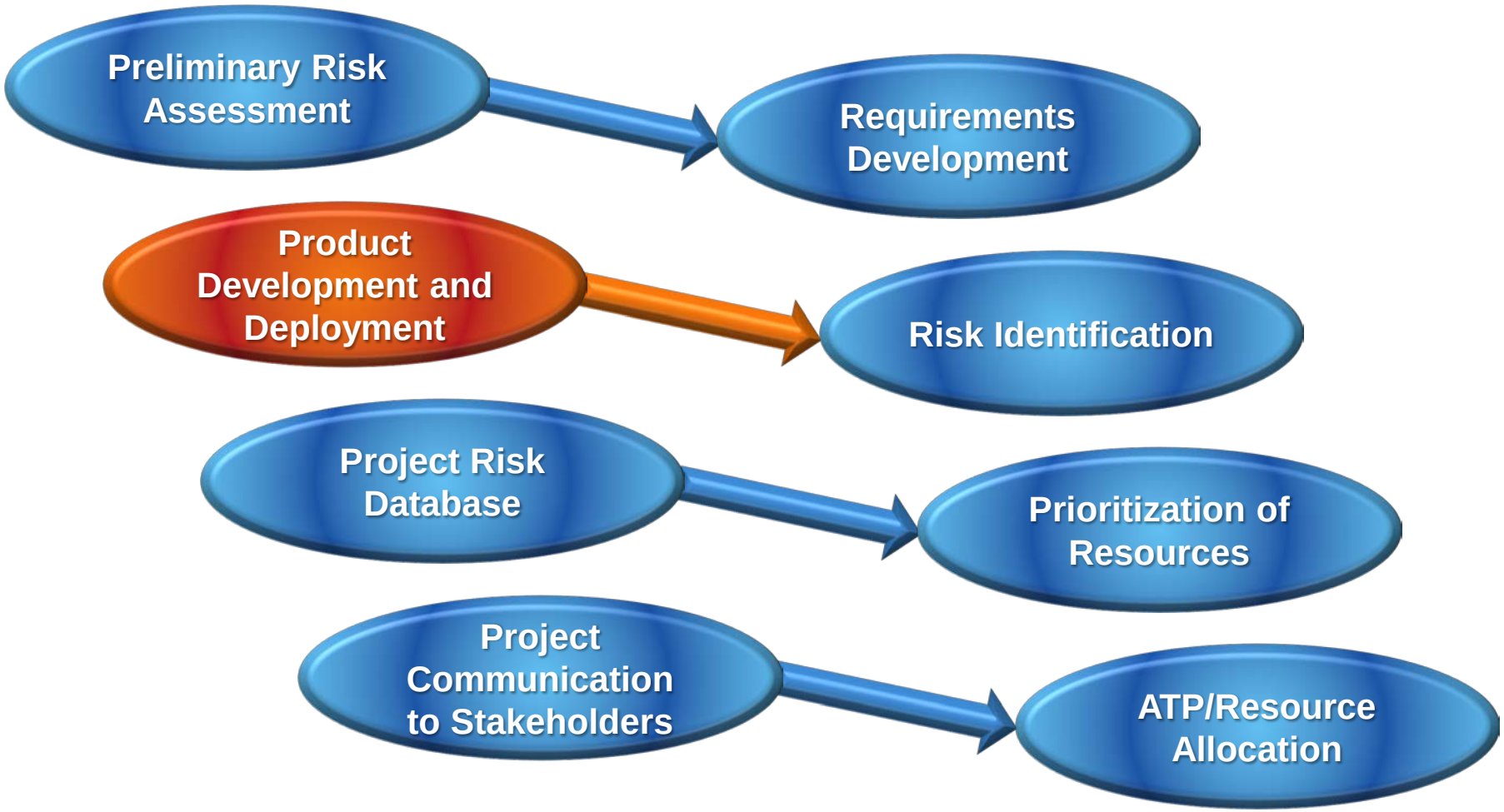
- Risk is a central element of space system development
- Understanding of risk is key to effectively engineering the system
- This understanding is used to prioritize resources in development and to convey the status to the project stakeholders
- Confusion between severity of consequence, scenarios, probability and relationship to other categories (safety, technical, and programmatic) can lead to unnecessarily high costs, unbalanced risk, and an overall higher risk posture for a project.

Additional Information

- **Link to GSFC Risk Assessment handbook:** https://standards.nasa.gov/center-specific-standards
  - Then select GSFC-HDBK-8005
- **Link to download GPR 8705.4:** https://elibrary.gsfc.nasa.gov/_assets/doclibBidder/tech_docs/GPR%208705.4-Signed%20Copy%20-%20Copy.pdf
- **Link to download Risk-based Safety and Mission Assurance article in *Quality Engineering:*** *https://www.tandfonline.com/doi/full/10.1080/08982112.2018.1473584*
- **Contact Info:**
  - Jesse Leitner: jesse.leitner@nasa.gov

Backups to Draw From

Risk as a Development Tool



Risk Classification Trends

- **Stepping from A, B, … "Do No Harm" results in:**
  - More control of development activities at lower levels; people actually doing the work
  - Less control by people who are removed from the development process
  - Less burden by requirements that may not affect the actual risks for the project
  - More engineering judgment required
  - Less formal documentation (does not relax need to capture risks nor does it indicate that processes should be blindly discarded)
  - Greater understanding required for reliability and risk areas to ensure that requirements are properly focused, risk is balanced to enable effective use of limited resources, and that good engineering decisions are made in response to events that occur in development
  - Emphasis on Testing/Test results to get desired operational confidence
  - Greater sensitivity to decisions made on the floor

Class D at GSFC

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

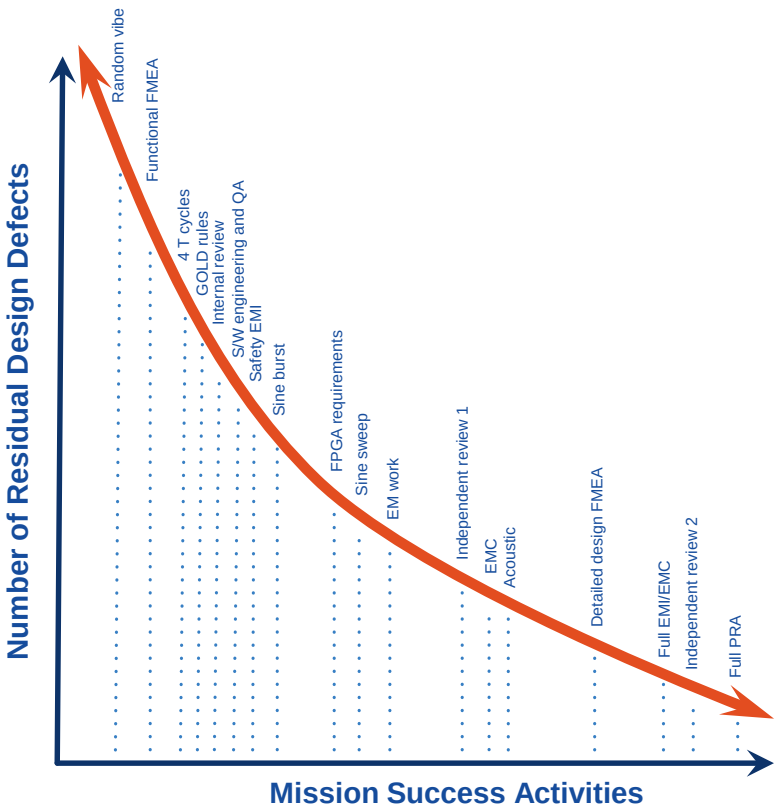
Class D (*and below*)—Dos & Don'ts

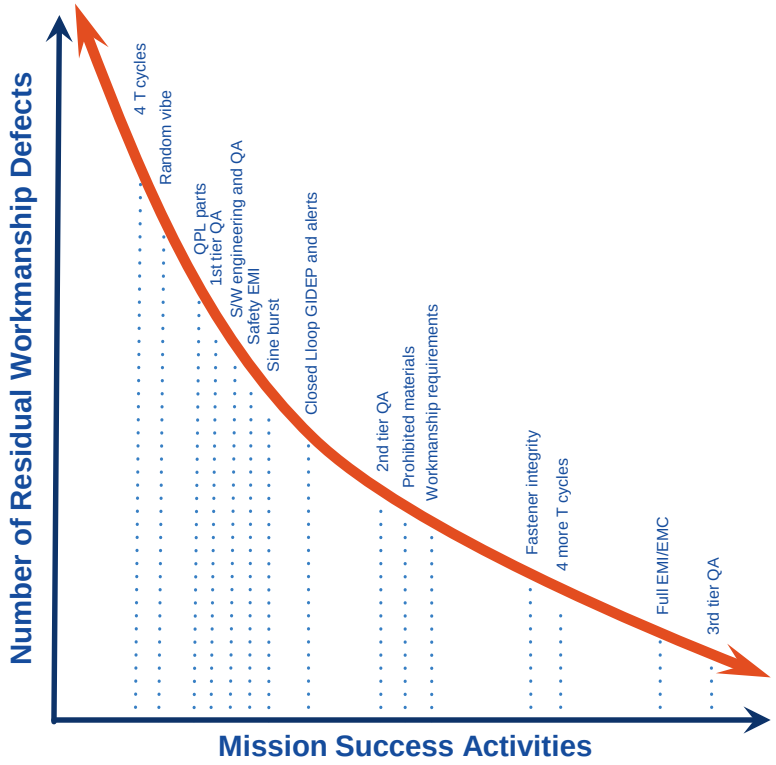
- **Do:**
  - Streamline processes (less formal documentation, e.g., spreadsheet vs. formal software system for waivers, etc.)
  - Focus on tall poles and critical items from a focused reliability analysis
  - **Tolerate more risk than A, B, or C (particularly schedule risk)**
  - **Capture and communicate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

- **Don't:**
  - **Ignore risks!**
  - Reduce reliability efforts (but do be more focused and less formal)
  - Assume nonconforming means unacceptable or risky
  - Blindly eliminate processes

Defects vs Mission Success

Risk can be characterized by number of defects that affect performance or reliability and the impact of each. Defects are generally of design or workmanship.

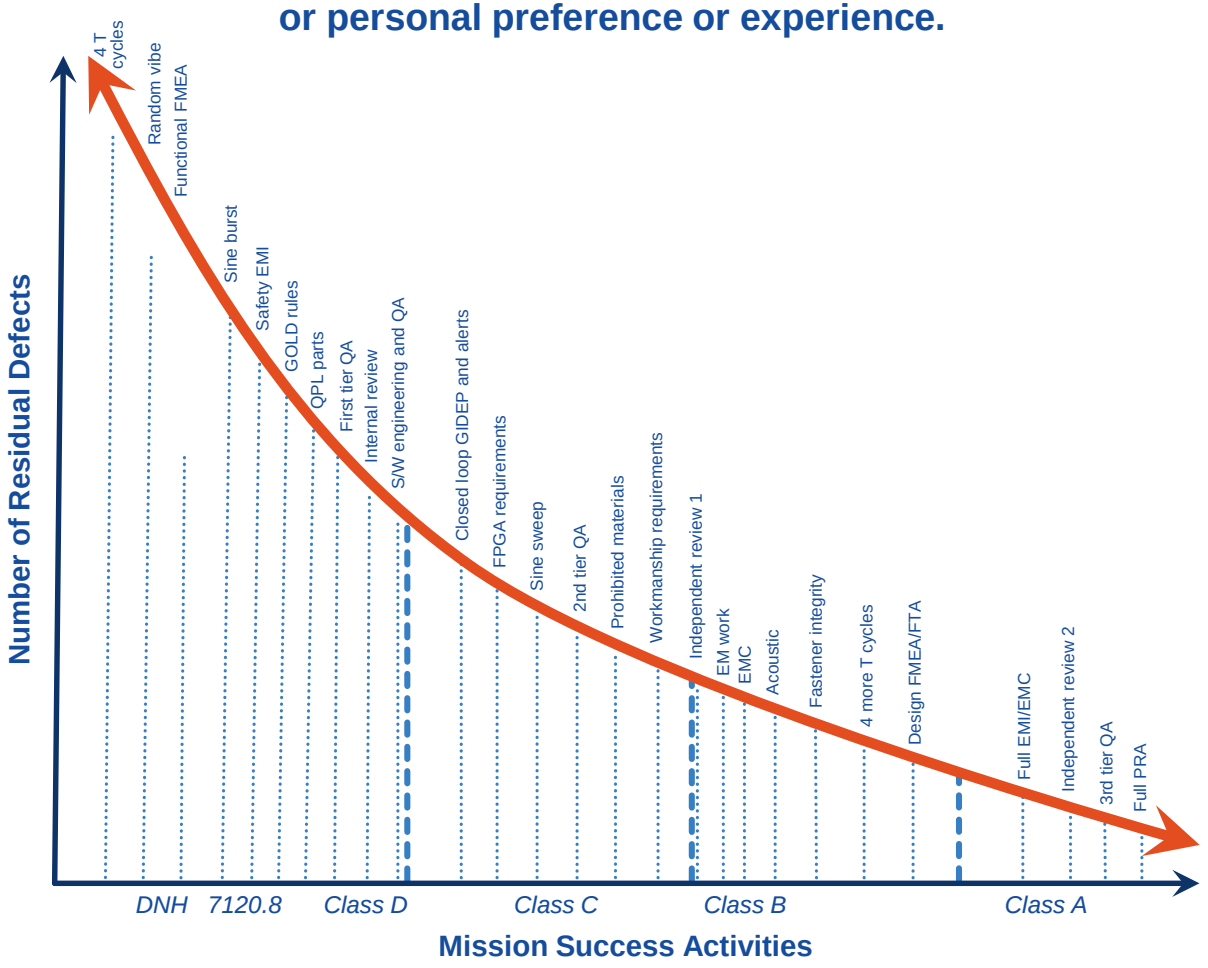




Note: A thorough environmental test program will ensure most risks are programmatic (cost/schedule) until very late, when time and money run out.

Defects vs Mission Success as a function of risk classification

Generally-representative example, prioritization may vary by mission attributes or personal preference or experience.

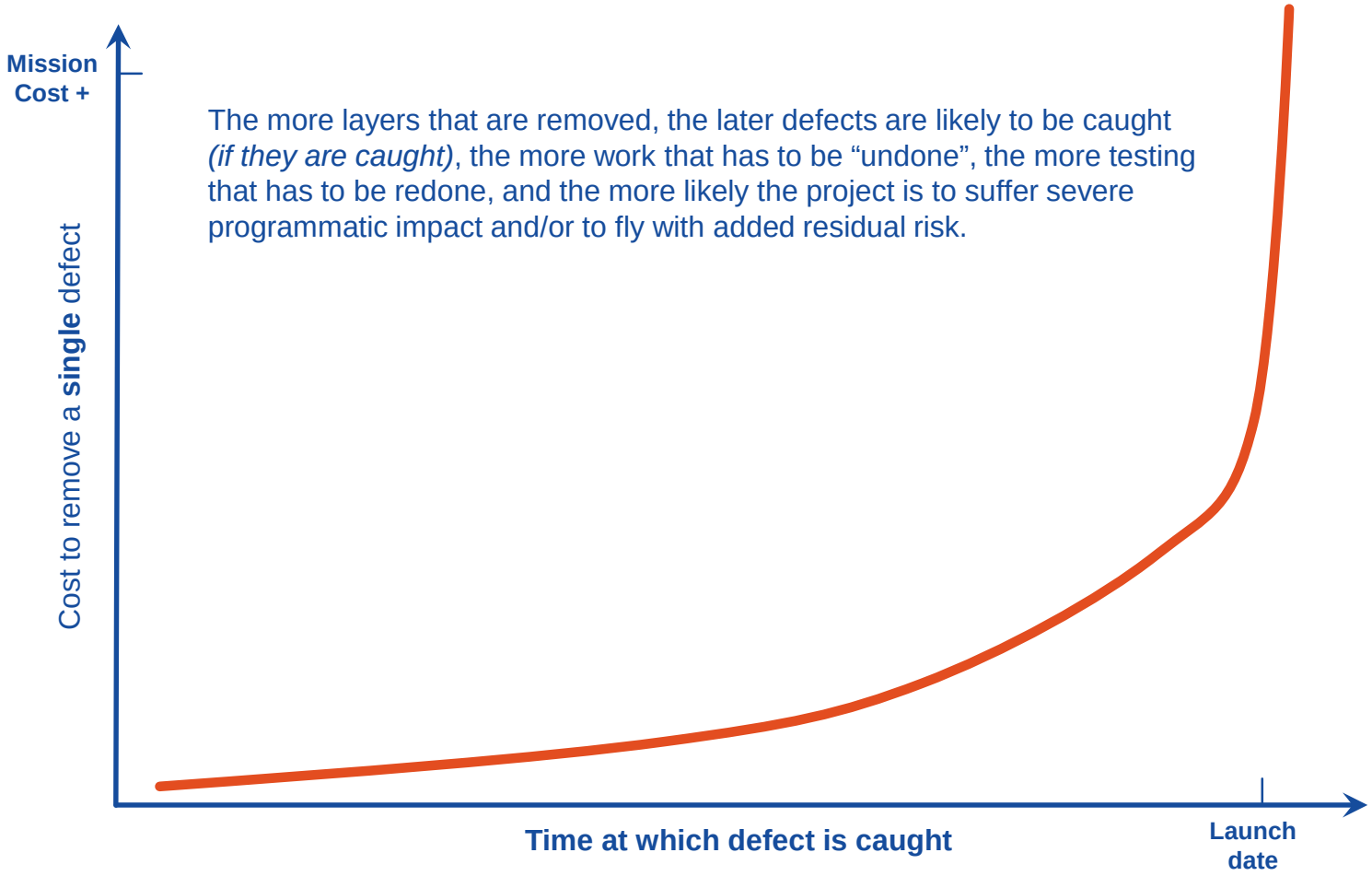


Other Activities With Cost & Risk Reduction Implications

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

Cost vs Time to eliminate a defect

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



GPR 8705.4

- GSFC implementation of NPR 8705.4
- Establishment of Risk-based SMA as policy for GSFC
- Risk Classification Definitions
- Nonconformance handling
  - Do not reject without understanding the risk
  - Determine cause of NC before reproducing the item (even from different vendor)
- Guidelines for activities vs mission class
- Ultimately will be one element used to develop project Mission Assurance Requirements vs mission class
- How does a project demonstrate that they are developing a Class “X” product?
- How do we convey to a vendor what we expect for Class “X”?

Risk Classification—All Levels

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

Class D (*and below*) Categories

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

Best Applicability of a Streamlined Class D Approach

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

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

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

The GSFC Quality Triangle

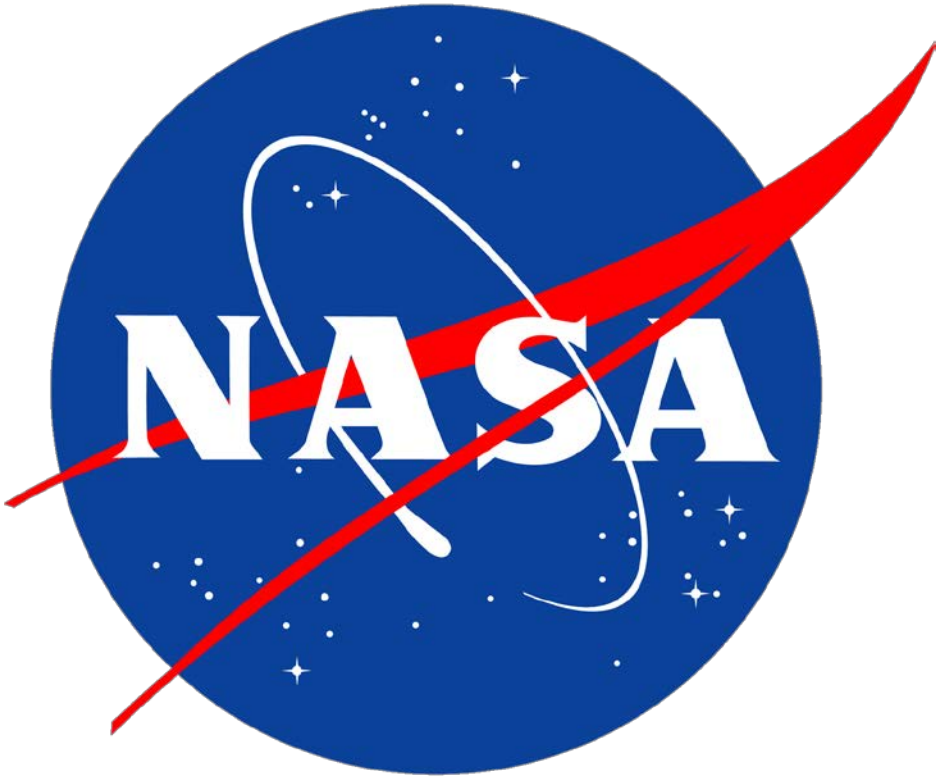
CRAE: Commodity Risk Assessment Engineer

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

- Expert in key discipline area with background and experience with reliability and risk
- Responsible and empowered to assign risks based on warnings, alerts, environments, and “what we are stuck with”
- Establishes testing programs and protocols to keep up with current design practices and common parts and components
- Sets the policies for the risk-based decisions on use of parts, components, and processes
- Establishes layers of risk reduction based on risk classification (ownership of GPR 8705.4)
- Determines the acceptability and risk of alternate standards or requirements, or deviations and non-conformances
- Answers, “are we okay?”, “why are we okay?”, “how okay are we?”
- Provides risk assessment to the project for the project to decide how they want to disposition

Commodity Areas

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


NASA