


# Risk Based Approaches to Electronics Hardware Assurance at NASA Goddard

**Bhanu Sood, PhD**

**Risk and Reliability Branch**

**Quality and Reliability Division**

**NASA Goddard Space Flight Center**

August 6, 2020

# One World-Class Organization

## *What makes Goddard one-of-a-kind?*



*NASA's* ***leading science center****, with* ***cross-disciplinary, end-to-end*** *capabilities*

Goddard
SPACE FLIGHT CENTER

Executing NASA's **most complex missions**



*World leader in* ***understanding the Sun's impact on Earth***



***Communications backbone*** *– 98% of NASA's data is transmitted via Goddard infrastructure*

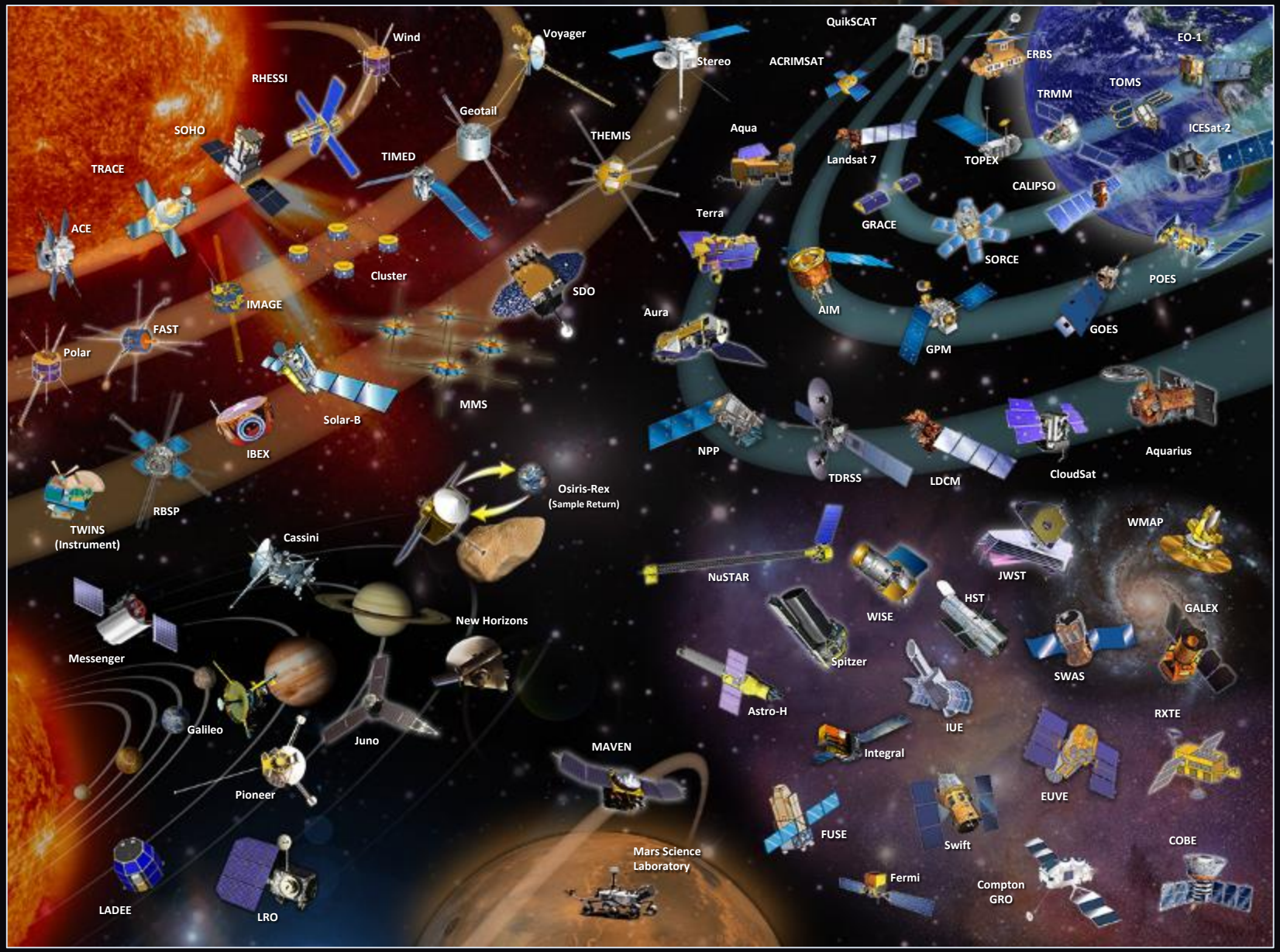


***1 of 2 US routes for ISS cargo;*** *1 of 4 US orbital launch facilities*



*Independent Verification and Validation Facility* ***assures NASA's most complex software functions as planned***

# GSFC: A Diverse Mission Portfolio

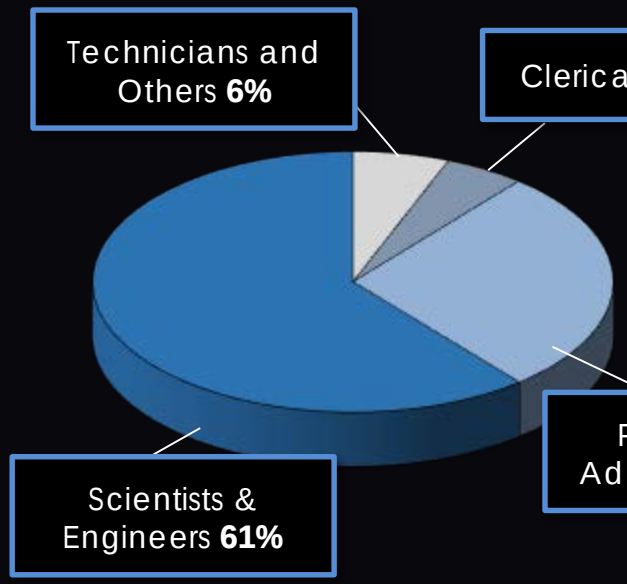


# Who We Are



## THE GODDARD COMMUNITY

More than 10,000 People




**GSFC Workforce**

3,000+ Civil Servants
6,000+ Contractors
1,000s of Others*

The Nation's largest community of

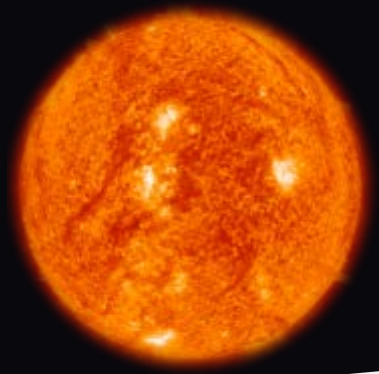
**scientists, engineers, and technologists**

**Including off-site contractors, interns, and Emeritus*

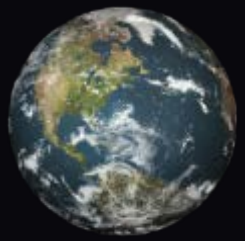
# A Place for Science

## TRANSFORMATIONAL DISCOVERIES in…

**Heliophysics**



**Earth Science**



**Planetary Science**



**Astrophysics**



**enabled by our…**



**End-to-End Capabilities**



**Exceptional Human Capital**



**World Class Facilities**



**Expertise in Core Science and Cross-Cutting Disciplines**



**Diverse Partnerships**

# What is Risk?

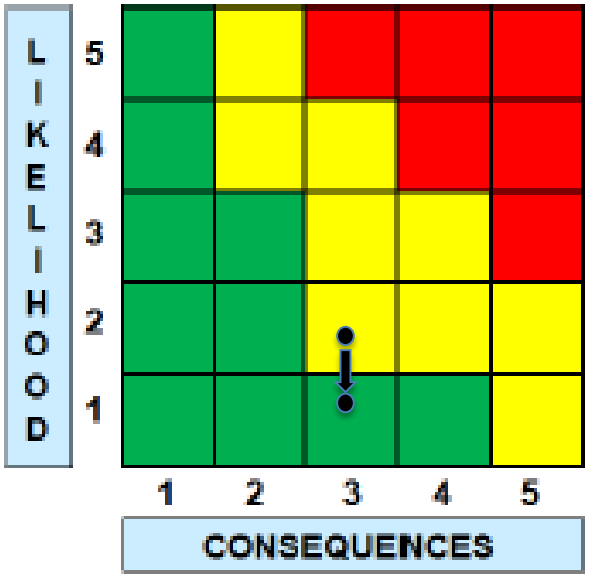
Risk is an expectation of loss in statistical terms.

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

- 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)




**Communicating risk is key to portraying the status of a new technology and project in development.**

# Why Do We Worry About Risk?

- **We don't want bad things** to happen

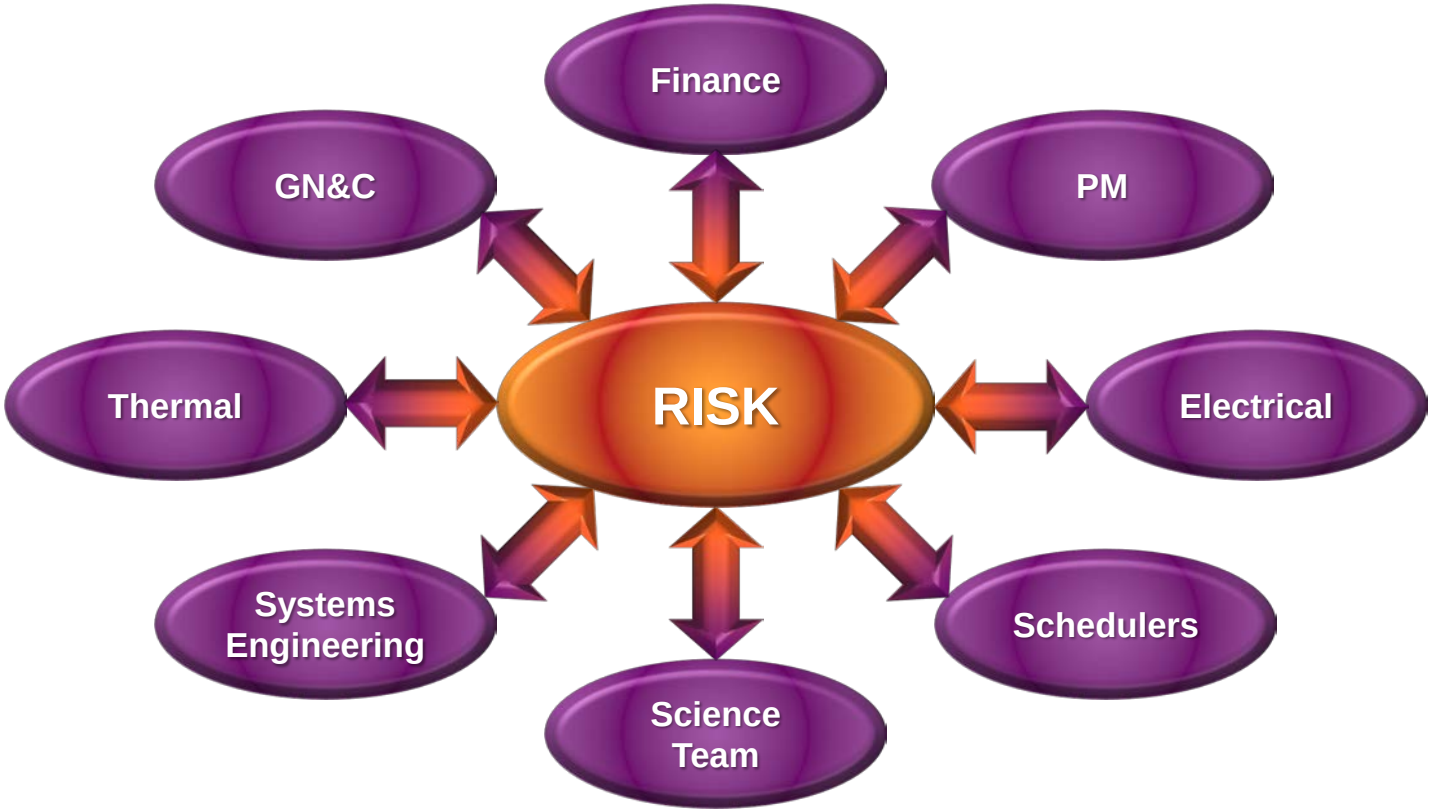
- The only way to avoid risk is to avoid doing anything
- Understanding risk is key to engineering the system
  - Establishing requirements
  - Responding to undesired or unexpected events
  - Choosing between different options
- Communicating risk is key to portraying the status of a project in development




Proton Failure

# Risk as a Common Language

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



# 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

- ***Upfront assessment*** of reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied
- ***Evaluating all risk categories*** (safety, technical, and programmatic) together to assure all factors are considered
- ***Early discussions*** with developer on their approach 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
- ***Judicious application*** of requirements based on learning from previous projects and the results from the reliability/risk assessment, and the operating environment (Lessons Learned—multiple sources, Cross-cutting risk assessments etc.)
- ***Careful consideration*** of the approach recommended by the developer
- ***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 nonconformance's**

# 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***



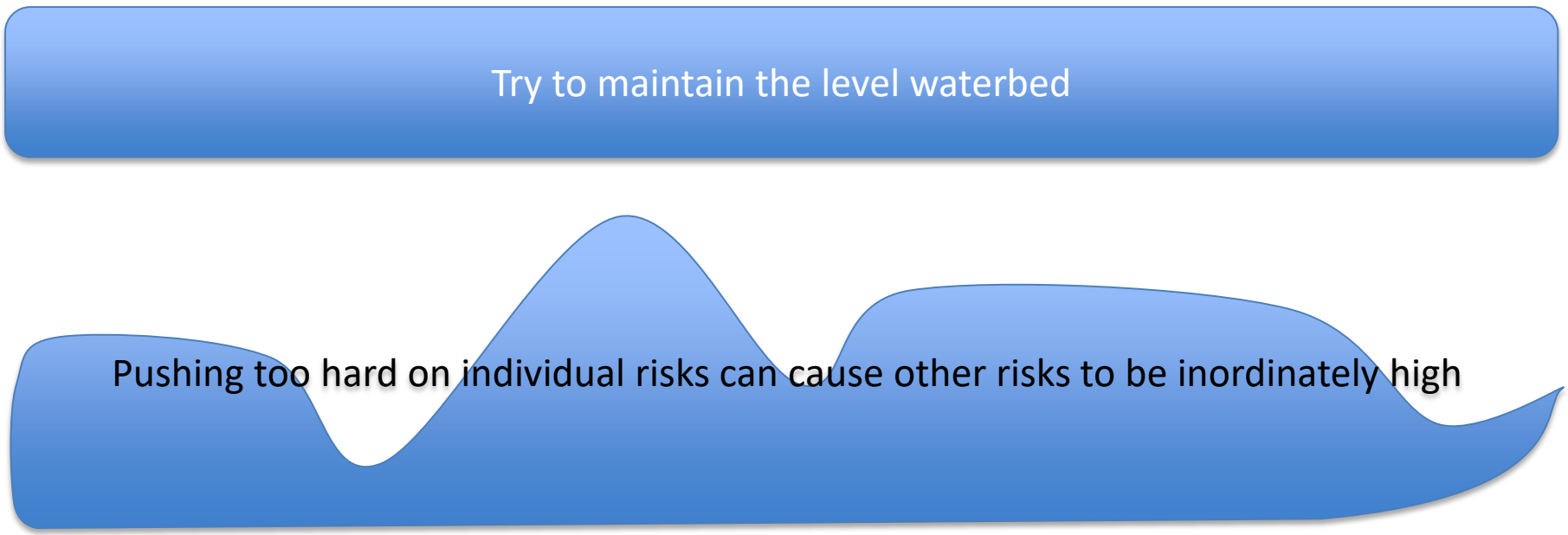
- There is a tendency to take action to eliminate severe consequences regardless of the probability of occurrence
- When a possibility is combined with an environment, an operating regime, and supporting data, a risk can be established.
- Lack of careful and reasoned analysis of each possibility in terms of the conditions that results in the consequence and the probability of occurrence **will** result in excessive cost and **may** increase the overall risk

# 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

# 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

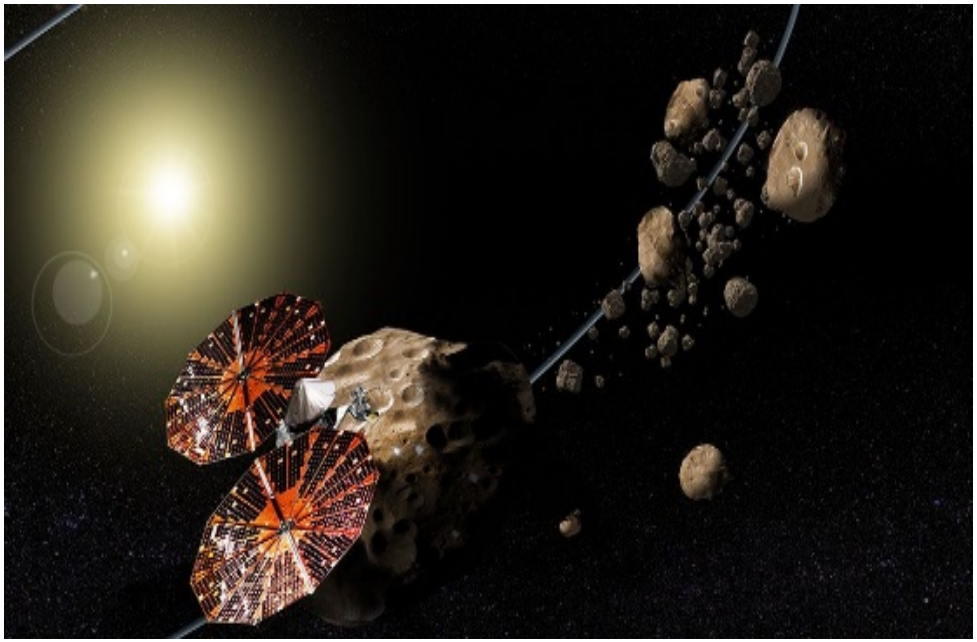


# Risk Acceptance at Different Levels and Times

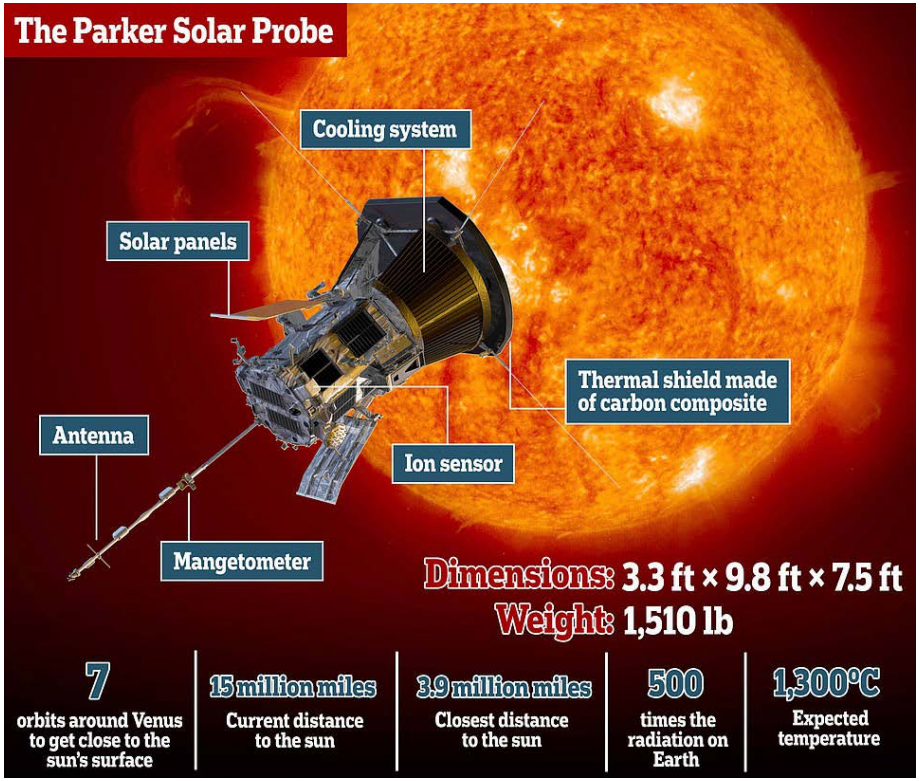
- The primary stakeholder(s) (MDAA, Center Director, NOAA, user community, etc.) accept(s) risks for project mission success
- Risk acceptance is delegated to the project to manage real-time, day-to-day development
  - Stakeholder has right of refusal through risk communication
- Safety and Mission Assurance 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?

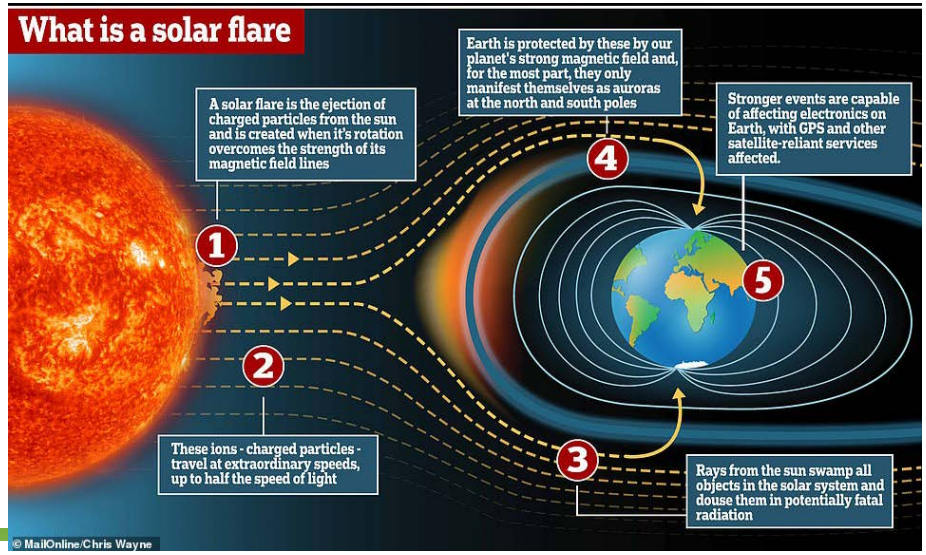
- Establishment of the level of risk tolerance from the stakeholder, with some independence from the cost
  - Cost is covered through NPR 7120.5 Categories
- If we were to try to quantify the risk classification, it would be based on a ratio of programmatic risk tolerance to technical risk tolerance.
  - 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.

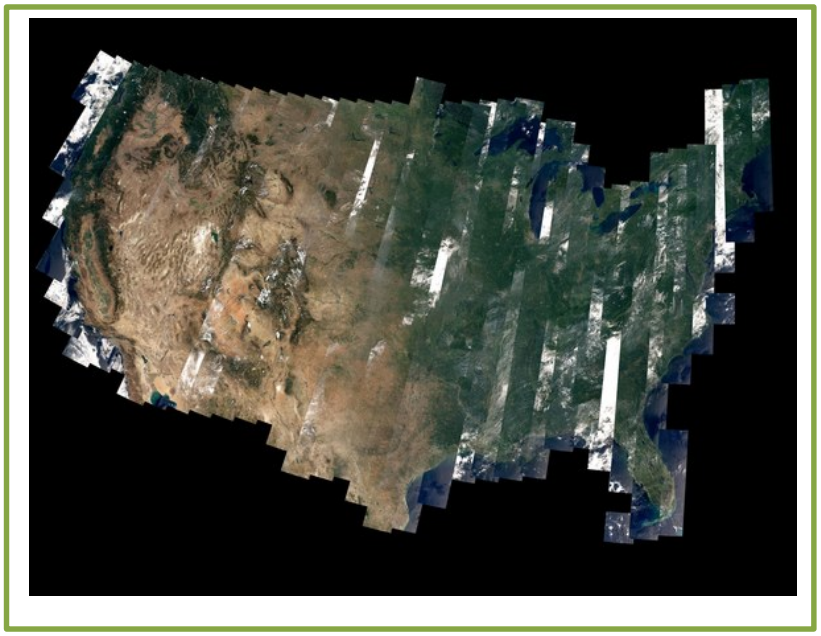


Lucy is a planned NASA space probe that will tour five Jupiter trojans, asteroids which share Jupiter's orbit around the Sun, orbiting either ahead of or behind the planet and one main belt asteroid. All target encounters will be fly-by encounters



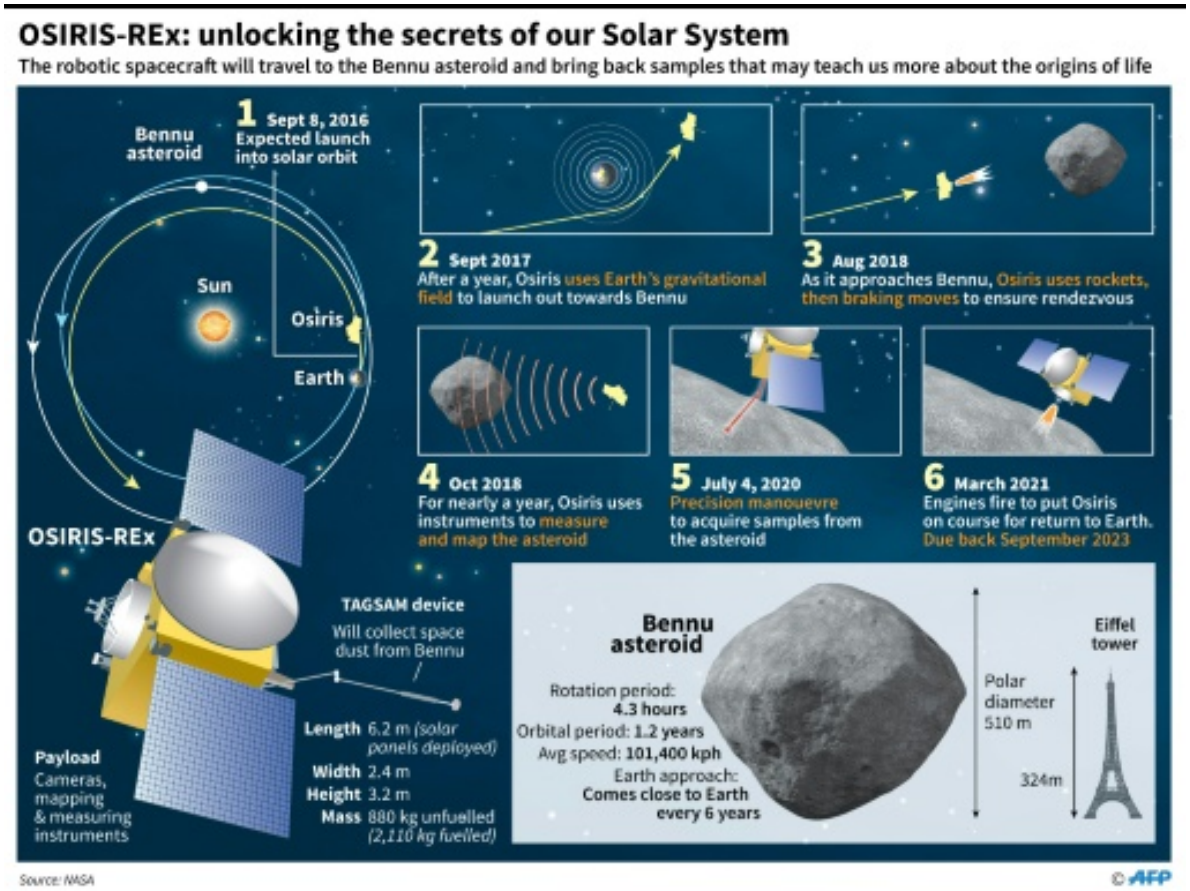

The Parker Solar Probe is a NASA robotic spacecraft launched in 2018 with the mission of making observations of the outer corona of the Sun. It will approach to within 9.86 solar radii from the center of the Sun, and by 2025 will travel, at closest approach, as fast as 690,000 km/h, or 0.064% the speed of light



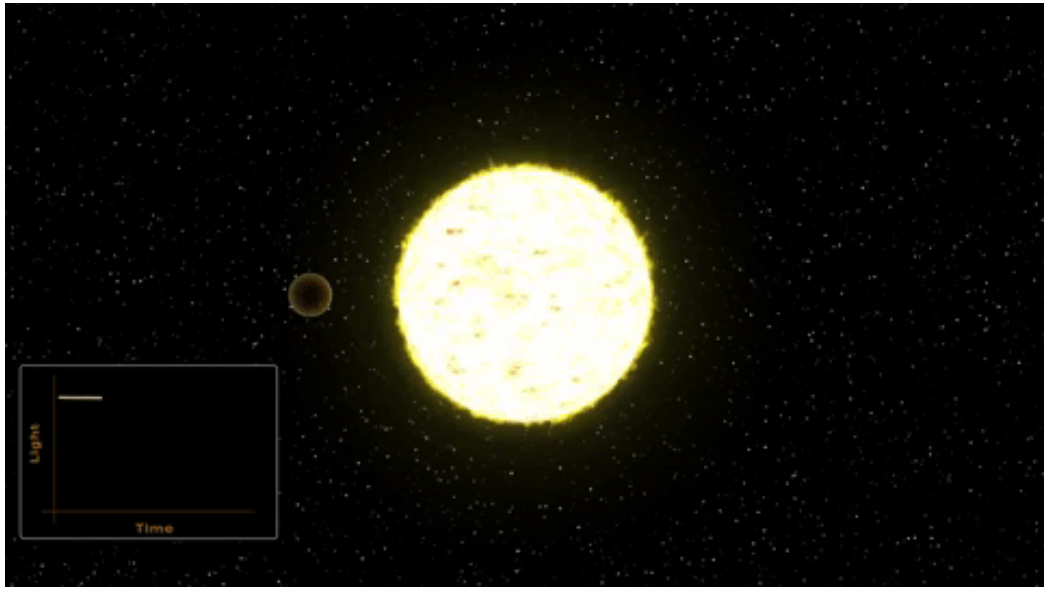


Landsat 9 is a planned Earth observation satellite, scheduled for launch on 8 April 2021. NASA is in charge of building, launching, and testing the system, while the United States Geological Survey will process, archive, and distribute its data.

The OSIRIS-REx is a NASA asteroid study and sample-return mission. The mission's primary goal is to obtain a sample of at least 60 grams from 101955 Bennu, a carbonaceous near-Earth asteroid, and return the sample to Earth for a detailed analysis






The Transiting Exoplanet Survey Satellite (TESS) is the next step in the search for planets outside of our solar system, including those that could support life. The mission will find exoplanets that periodically block part of the light from their host stars, events called transits. TESS will survey 200,000 of the brightest stars near the sun to search for transiting exoplanets. TESS launched on April 18, 2018, aboard a SpaceX Falcon 9 rocket.

# 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: LUCY, 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**

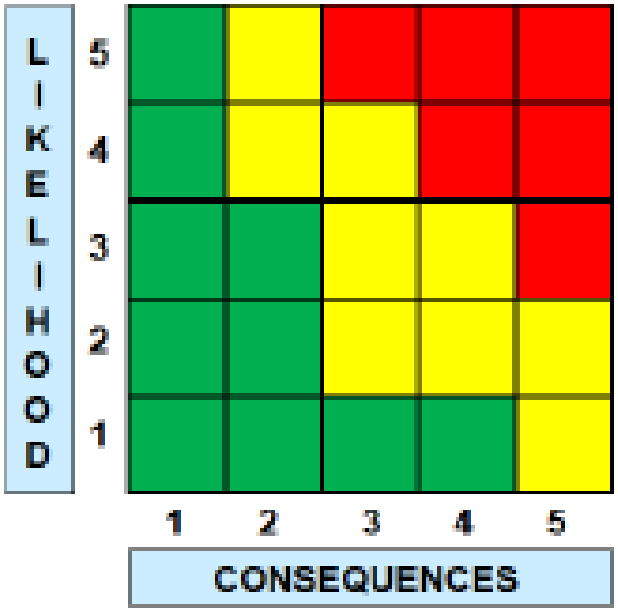
# Risk of Conformance vs. Risk of Nonconformance

- 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

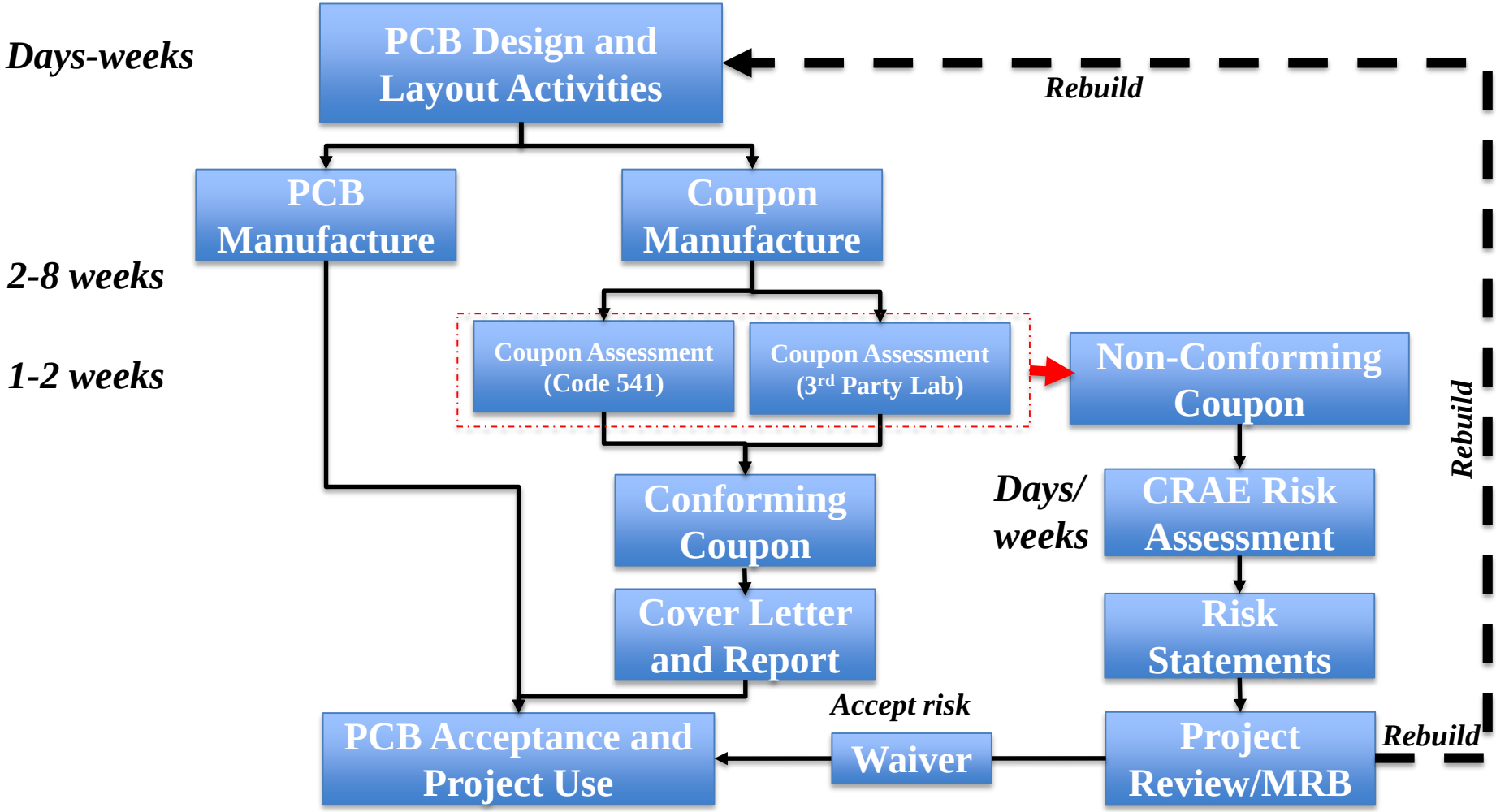
**Do not reject a nonconforming item without understanding the risk.**
**Determine the cause of NC before reproducing the item.**

# Impact of Non-conformances

- Bare boards cost $$ and build schedules – expensive!!
- But failures are even more expensive!
- Test sample nonconformance is not the same as PCB failure.
- Risk-based decisions are used for disposition of non-conformances.
- Non-conformances may have little to no impact per application.
- Began to explore origins and merit of requirements (more later).

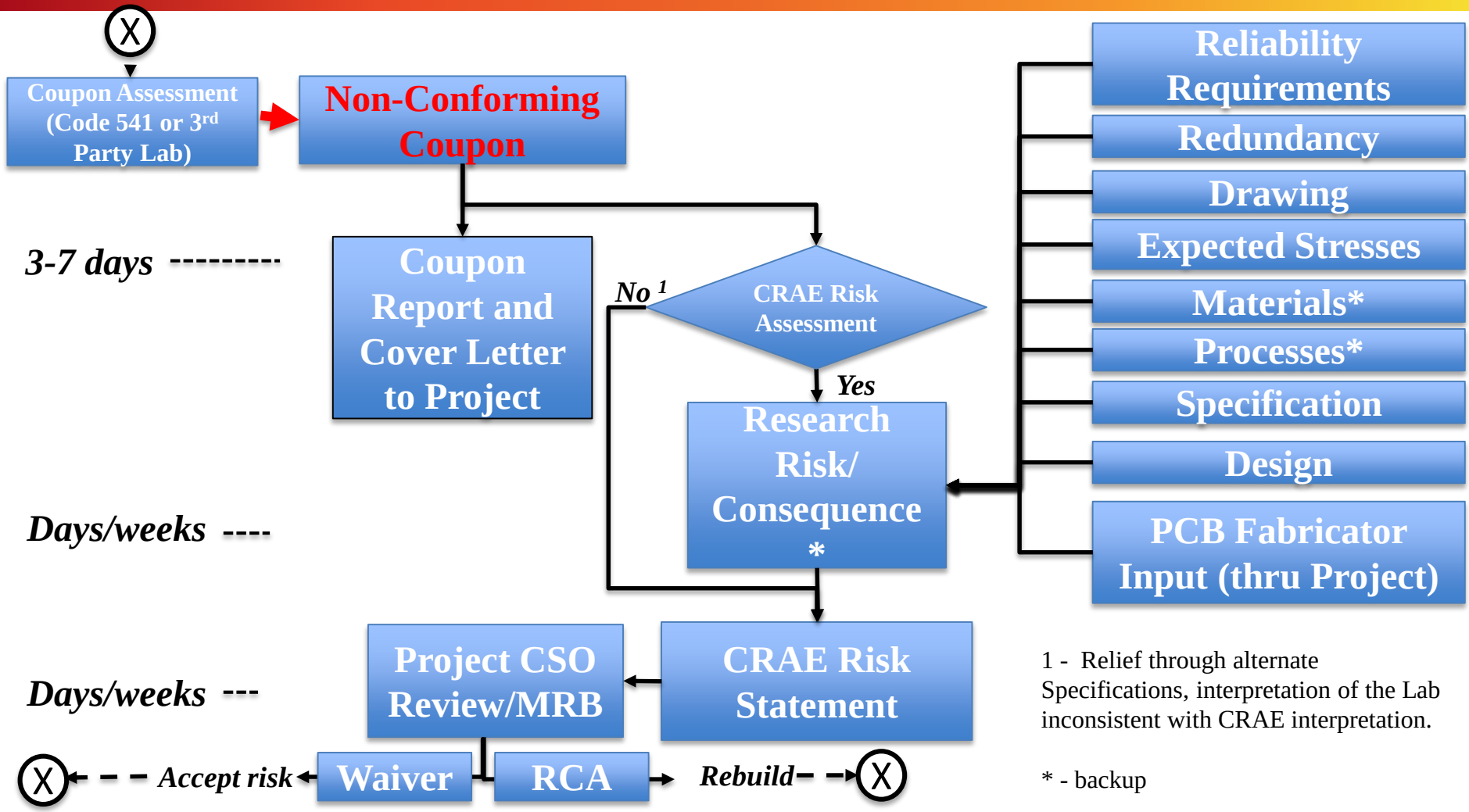


# PCB Assurance At NASA Goddard




Code 300 determines the risk, project decides whether to accept the risk.

# Risk Assessment Approach

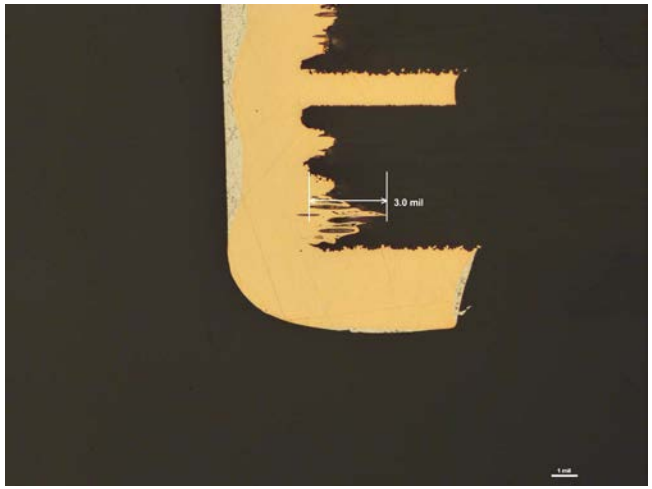



1 - Relief through alternate Specifications, interpretation of the Lab inconsistent with CRAE interpretation.

* - backup

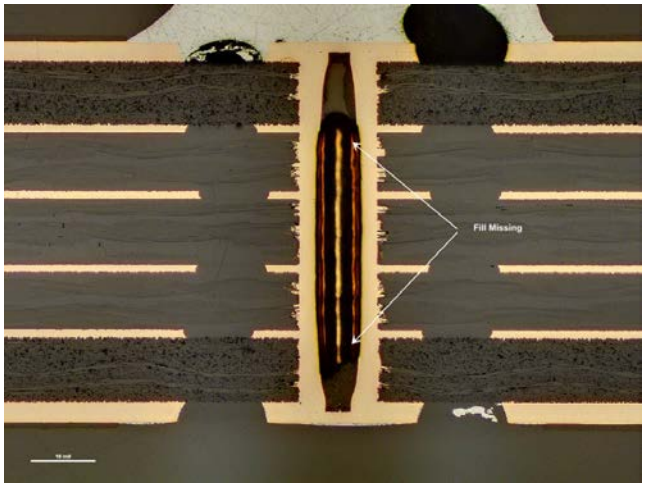
# Sampling of Risk Assessments – 1

Copper wicking in excess of 2.0 mil




The wicking is well-enclosed within the annular rings with significant margin, and should not violate electrical spacing. When inspected with IPC-6012 DS, these boards would be compliant (max 3.5 mil wicking + etchback).

Capped via with fill less than 75%




Voiding is contained and enclosed within the fill material (with matches in CTE with the PCB laminate), and does not appear to have an interface with the cap where contaminants could potentially trap.

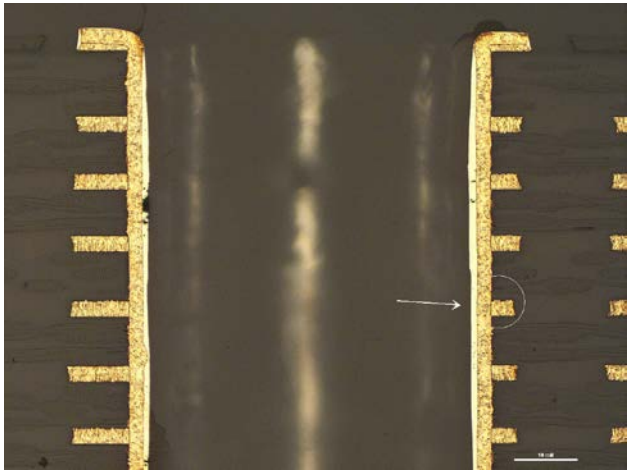
# Sampling of Risk Assessments – 2

Dielectric layer less than 3.0 mil



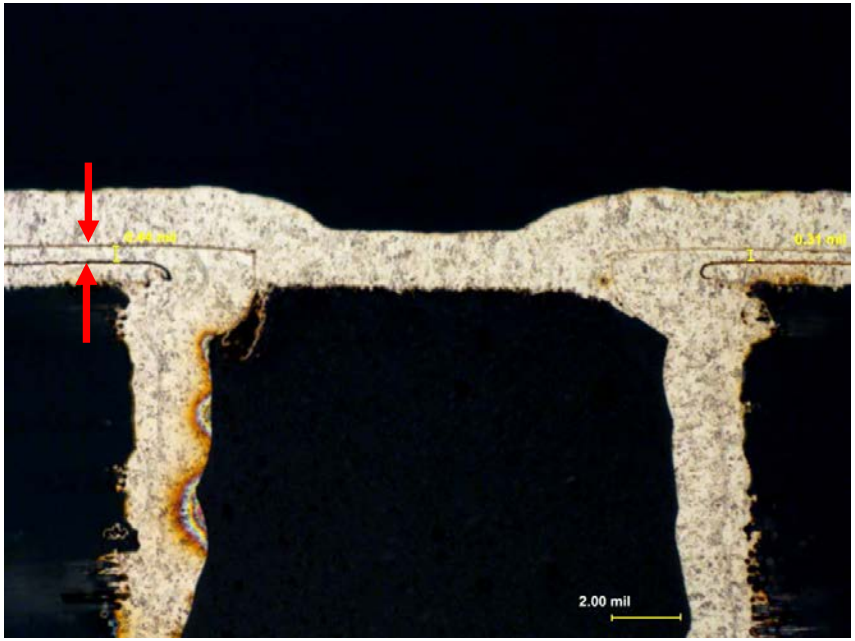

A 40kV dielectric breakdown strength, combined with a 28V service voltage provides a sufficient dielectric clearance at 2.8mil. There are at least two layers of dielectric material present.

IAR less than the minimum 5.0 mil



Out of date drawing notes containing a minimum 5.0mil annular ring and other requirements.

# PTH Copper Wrap Thickness Requirement




Per IPC-6012D for through-holes:

| | |
|---|---|
| Class 1 | AABUS |
| Class 2 | 5 µm [197 µin] |
| Class 3 & 3/A | 12 µm [472 µin] |

AABUS = As Agreed Between User and Supplier

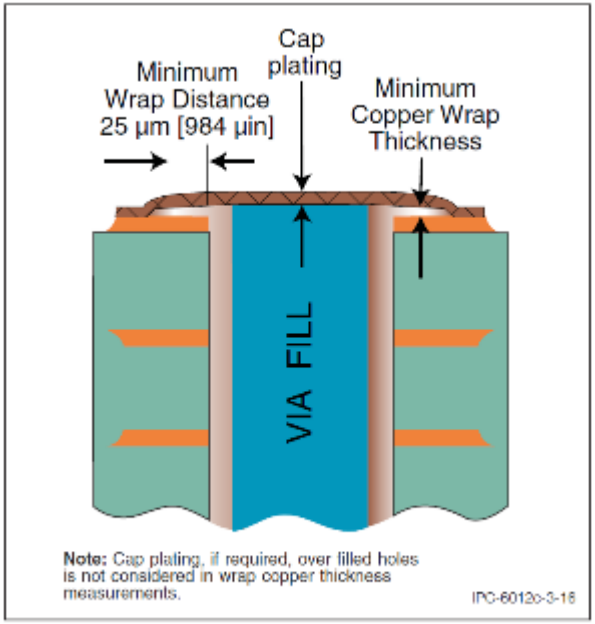



**Figure 3-16 Surface Copper Wrap Measurement (Applicable to all filled PTHs)**



- Thermal cycle stresses act on interfaces, outer layers experience the greatest stress.
- Reason: materials selection and geometry.

# PTH Copper Wrap Thickness: Disposition

- GSFC Mission had populated and integrated board with zero wrap, wrap planarization can cause 0.3mil or more variance in panel; manufacturers must target more wrap.
  - Wrap cannot be achieved at required thickness for designs with tight line-width spacing and/or with multiple lamination/plating steps
- Requirement was introduced to IPC with minimal data
  - Reliability reported to be better with wrap vs. butt joint
  - Half of barrel plating thought to be “good enough”
  - Higher quality limit used as safety margin against manufacturing variation during planarization
- **GSFC Studies:** Determined the impact of copper wrap plating thickness on PCB reliability, as characterized by thermal cycles to failure.
  - Able to determine acceptability of wrap defect based on reliability testing and analysis in context of mission environment and duration.
  - IPC voted to change the requirement (amendment in Rev. D and revisions in Rev. E).

# Concerns with IST Specifications

- High density interconnect (HDI) testing is performed with interconnect stress testing (IST) using a methodology documented in the IPC test methods manual TM650, Method 2.6.26.
- Elevated temperatures exceeding 220°C are sometimes used to cause HDI failures.

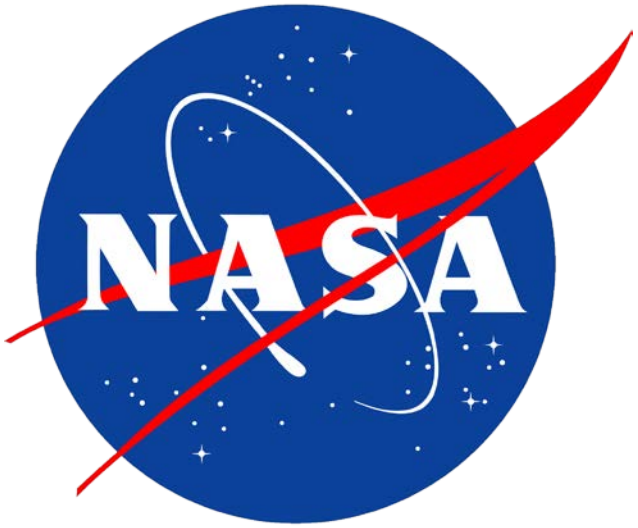
- Although IST can be an effective screen for process, materials, design and workmanship, it is not recommended as a predictor of reliability.
- Increasingly, IST test results that are generated at elevated and highly accelerated test condition are being used for predicting operational reliability of HDI PCBs.

# Summary

- Risk is a central element of space system development
- Understanding of risk is key to effectively engineering the system
- Lessons learned are at the core of the methodology
- 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.

# Acknowledgements






**Bhanu Sood, PhD**

**Risk and Reliability Branch**
**Quality and Reliability Division**
**NASA Goddard Space Flight Center**

**+1 (301) 286 5584**
**bhanu.sood@nasa.gov**