Risk-Based Safety and Mission Assurance: Approach and Experiences

Rich Barney

Safety and Mission Assurance Directorate

Goddard Space Flight Center

ESA-JAXA-NASA S&MA TRISMAC Meeting

June 4-6, 2018

NASA Goddard SPACE FLIGHT CENTER

www.nasa.gov/goddard

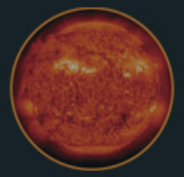
Can we answer the Big Questions?

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?

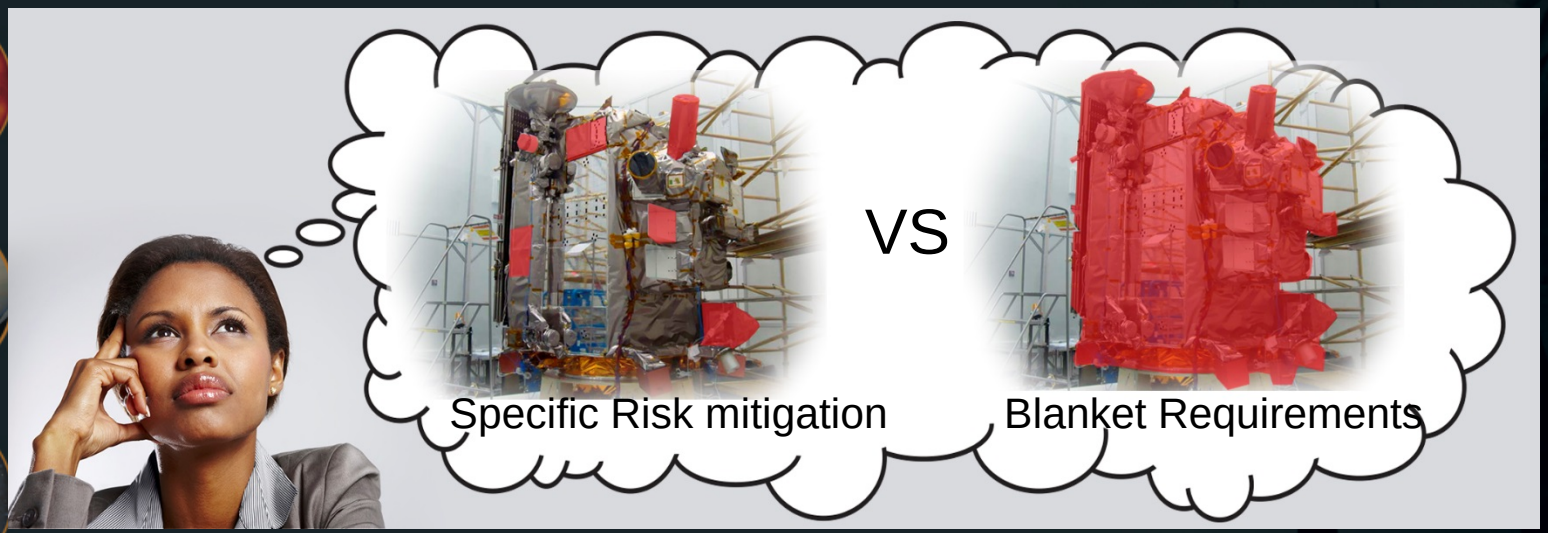
- Definition: The combination of
  - a) the probability that an undesired event will occur
  - b) the consequence or impact of the undesired event
  - In short, Risk is an expectation of loss in statistical terms



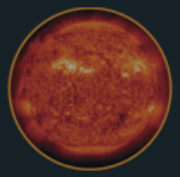
- Flavors of risk (consequences)
  - Technical (failure or performance degradation on-orbit)
  - Cost ($ it will take to fix the problem)
  - Schedule (time to fix the problem)
  - Safety (injury, death, or collateral damage)

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



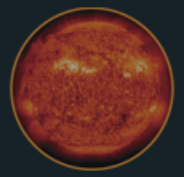
Risk Experience: Launch Operations



NASA Risk Classification

- **Class A: Lowest risk posture by design**
  - Failure would have extreme consequences to public safety or high priority national science objectives.
  - May launch with low to medium risks

- **Class B: Low risk posture**
  - Represents a high priority National asset whose loss would constitute a high impact to public safety or national science objectives.



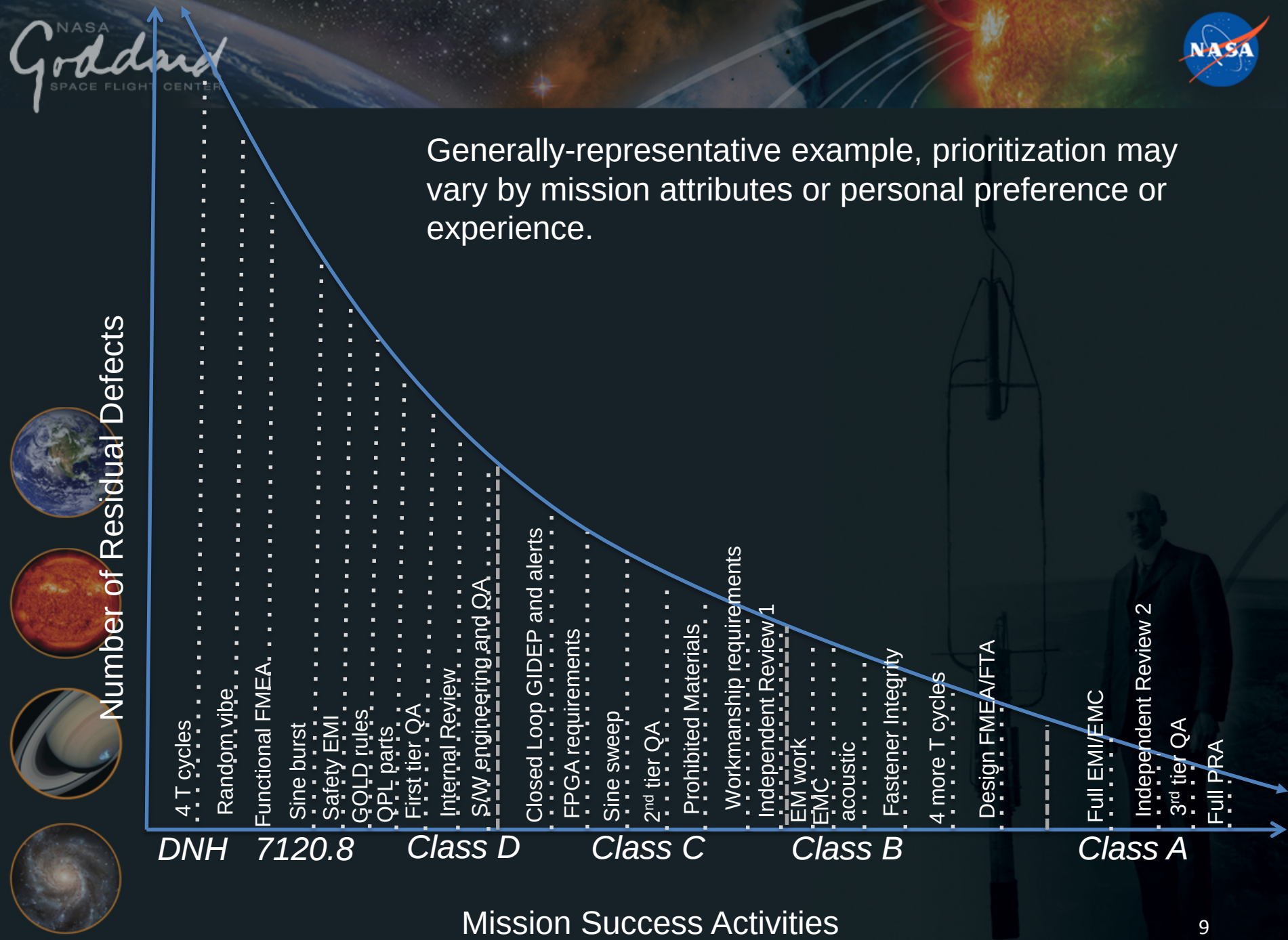
- **Class C: Moderate risk posture**
  - Represents an instrument or spacecraft whose loss would result in a loss or delay of some key national science objectives.

- **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 exist.

Mission Success Activities vs. Risk Posture
(example elements)

Technical Categories	Class A	Class B	Class C	Class D	Ground System (GS)	7120.8 Class	Do No Harm (DNH)	Hosted Payload Class (host requirements)
Single point failures (SPF)	Any SPF against Level 1 requirements necessitates a specific waiver, SPF analysis expected per GPR 7123.1	Particular attention to avoidance, tracking, and mitigation, SPF analysis expected per GPR 7123.1. Highly fault-tolerant, through redundancy and other means.	Selective redundancy for tall pole items, tracking, and communication, tall pole, critical item, or SPF analysis	SPF, critical item, or tall pole analysis up front, communication of results. Selective redundancy where cost effective.	N/A	Project best effort. Tracked in project documen-tation.	Project best effort	NASA review of design history
EEE Parts	Level 1 parts per EEE-INST-002; DPA performed per S-311-M-70; Counterfeit Avoidance requirements per 500-PG-4520. 2.1;	Level 2 parts per EEE-INST-002 except Level 1 parts for single point failures and hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance	Level 2 parts per EEE-INST-002 for missions greater than 2 years except Level 1 parts for hybrids containing active components and Level 3 parts may be used for fault tolerant, non-critical	Level 3 parts per EEE-INST-002 except Level 2 parts for hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance requirements	For custom designed module, quality level of parts selected needs to be consistent with the criticality of the module.	Best commer-cial practices, advise on part selection & derating. ISO certified facilities preferred.	Best commer-cial practices, ISO certified facilities preferred.	Host practices. Advise on part selection & derating.

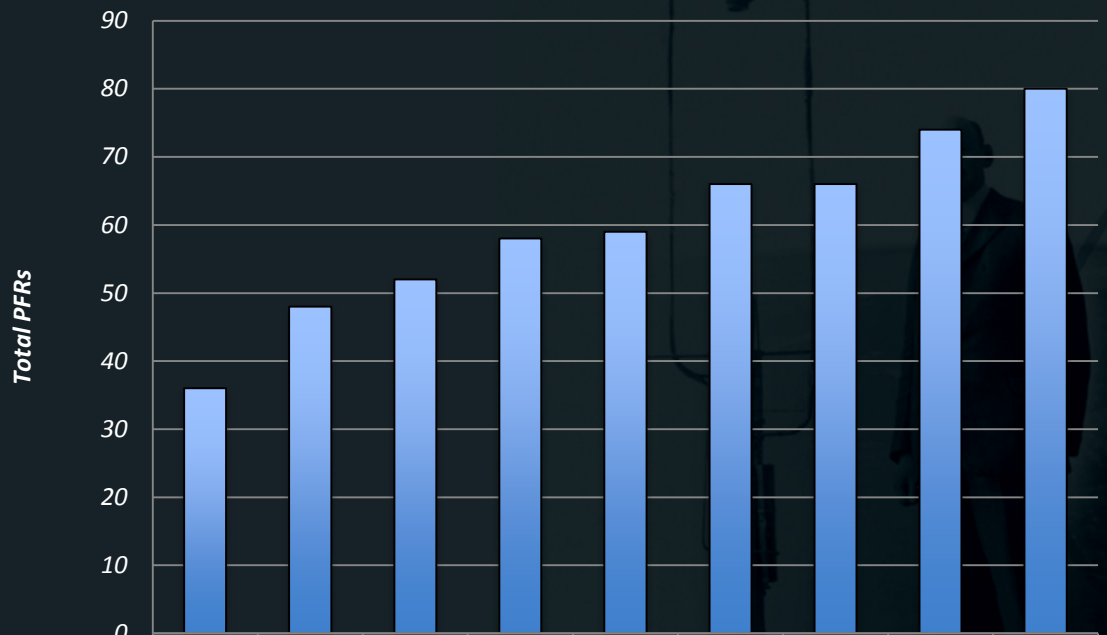
Generally-representative example, prioritization may vary by mission attributes or personal preference or experience.



Risk Experience: Thermal Cycling

- SMA reviewed the Problem Failure Report (PFR) database to isolate multi project failures associated with thermal cycling.
- The data shows that multiple thermal cycles do uncover issues after the first few cycles.
- About 45% of PFRs were written after failures on thermal cycles >3.
- The Magnetospheric Multiscale mission showed 8 PFRs in the database associated to thermal cycling and 5 occurred during cycle >3.

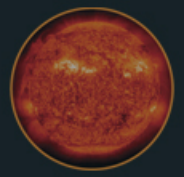
Multi Project Problem Failure Reports (PFRs) vs Thermal Cycle Failure #



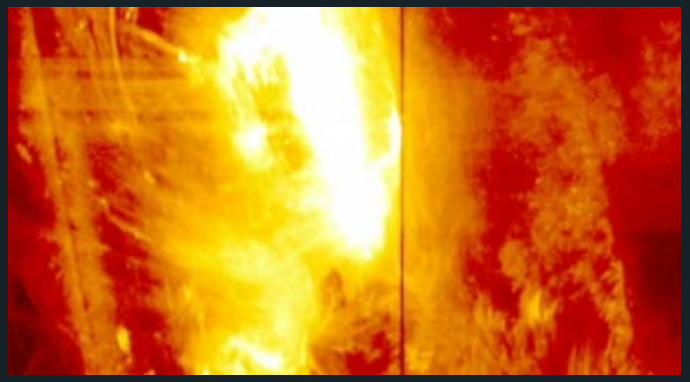
	1	2	3	4	5	6	7	8	>8
# of PFRs	36	48	52	58	59	66	66	74	80

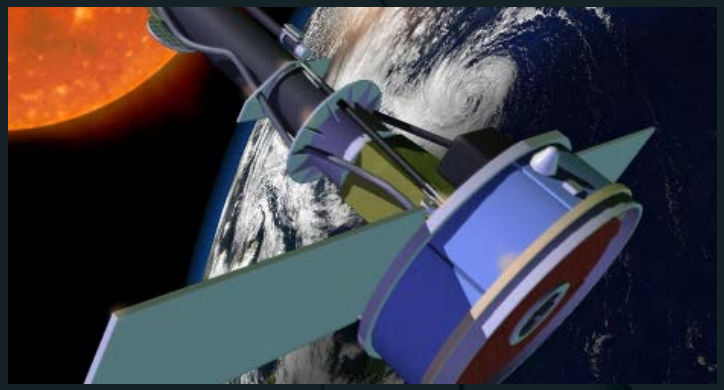
Attributes of risk-based SMA

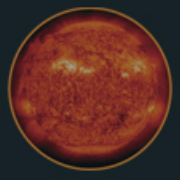
- Upfront assessment of reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied
- Early discussions with developer on their approach for ensuring mission success (e.g., use of high-quality parts for critical items and lower grade parts where design is fault-tolerant)
- Judicious application of requirements based on learning from previous projects and the results from the reliability/risk assessments
- 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.

Risk Experience: Learning from Previous Projects







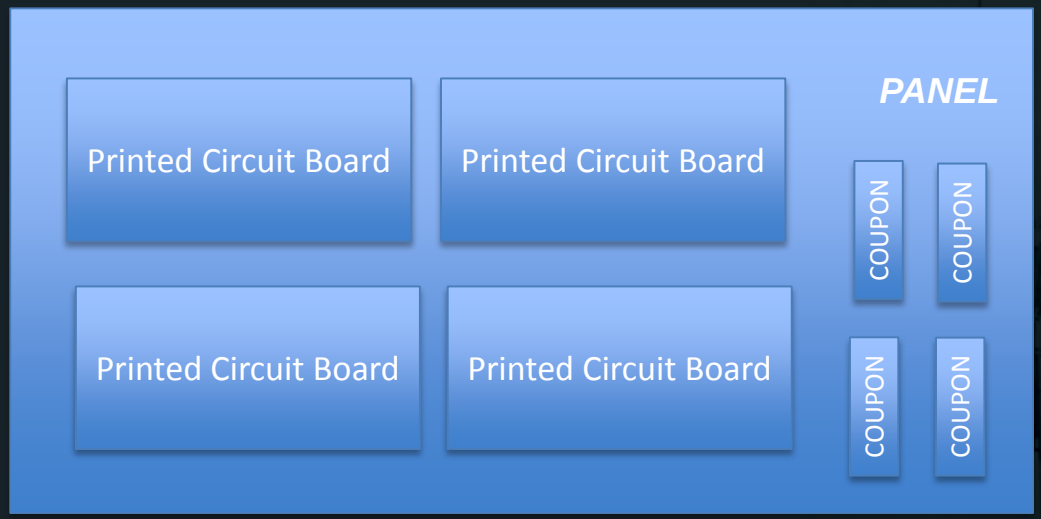
On Oct. 31, 2013, NASA's most recent addition to its solar-observing fleet began sharing its data and imagery with the world.

A mission that almost wasn't…….

Risk Experience: Nonconforming Printed Circuit Board Acceptance

- PCB coupons are evaluated for compliance on each panel. Each panel may have several PCBs and several coupons.

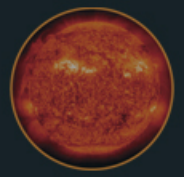
- GSFC projects develop dozens to hundreds of printed circuit boards (PCBs).



Risk Experience: Nonconforming Printed Circuit Board Acceptance Problem

- In the past, 30% of all printed circuit board coupons had been rejected due to nonconformance.
  - Solely based on the coupon not meeting the requirements to which they were evaluated.
  - Without any basis of risk or flightworthiness.

- Projects were choosing two vendors for most boards to mitigate the risk of coupon rejections.

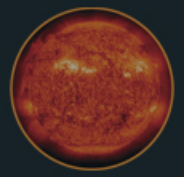


- The time and resources wasted on respins were reducing more important risk mitigation activities.

- Respins frequently resulted in boards that had bigger concerns than the first build.

Risk Experience: Nonconforming Printed Circuit Board Acceptance Risk-based Solution

- Risk assessments are performed by a central working group when coupons are nonconforming.
- Initial assessments took weeks to perform. Now they take a day.
- Out of the 231 risk assessments, boards from 33 panels were determined to be of elevated risk and scrapped (14% rejection).
- Cost savings of scrapped boards is between ~ $1M and $4M, schedule savings is on the order of years. Does not account for frequent re-attempts to build the same board without knowing the cause of the nonconformance or cost of microsection analysis labor.

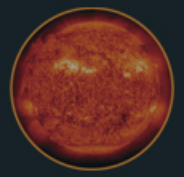
Continuous improvement and learning are at the core of this approach.

Risk Experience: Nonconforming Printed Circuit Board Acceptance Corrective Action

- Some requirements frequently reappear in risk assessments

- Requirements that frequently are violated and rarely entail risk raise red flags and demand continuing actions:
  - Industry survey
  - In-house testing
  - Follow-up with requirements body

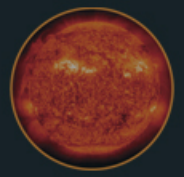
- Example: copper wrap requirement in IPC 6012 3/A for buried/hidden vias
  - Frequently violated (especially for European products since requirement not included in European spec)
  - Can be very difficult to achieve
  - Uniformity across the board is ambiguous

Summary

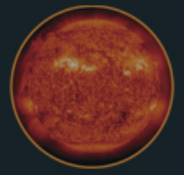
- Goddard Space Flight Center has implemented a risk-based SMA framework that prioritizes understanding all sides of risk for a given problem as opposed to applying a bias toward compliance with quality requirements after a problem has occurred.

- The Risk-Based SMA approach and experiences presented show that once noncompliance has occurred, careful analysis and risk management should be prioritized along with requirements compliance.



- The experiences presented demonstrate that the risk-based approach is effective at saving cost and schedule resources while establishing a risk posture commensurate with mission requirements and constraints.

NASA Goddard SPACE FLIGHT CENTER



www.nasa.gov/goddard