Challenges in Implementing Medium & High Risk NASA Payloads

Kim Plourde
JPL/Caltech
October 21, 2010

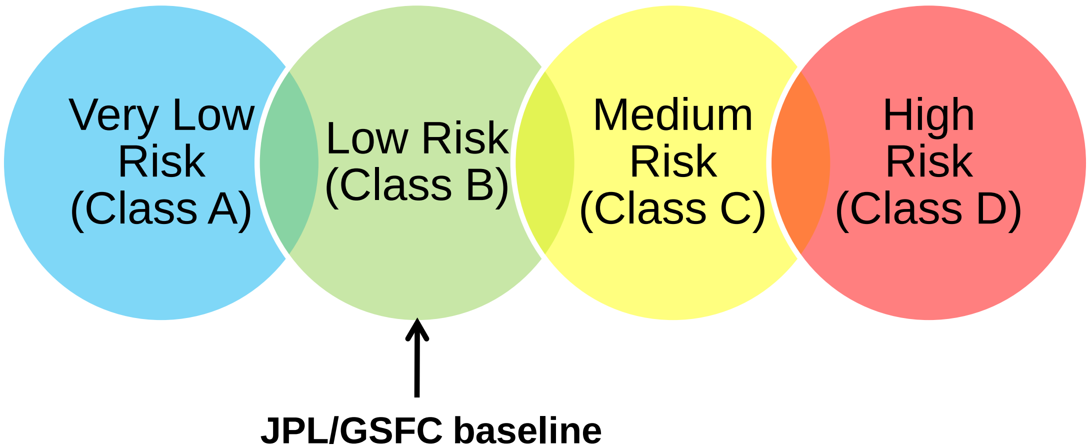
Agenda

- Review the NASA process for determining payload* risk classification
- Examine the implications of payload risk classification
- Discuss typical challenges at JPL with implementing payloads of varying risk classifications
- Observations/suggestions going forward

***- Payload- Any airborne or space equipment or material that is not an integral part of the carrier vehicle**

View From the Top

- NASA* divides all airborne/space equipment into one of four risk classifications-



- Determining the risk classification for a particular payload is an *inexact,* iterative process
  - Classification is finalized prior to Preliminary Design Review through a combination of various NASA offices/organizations/councils

*- NPR 8705.4, "Risk Classifications for NASA Payloads"

Risk Classification Considerations*

	Class A (Very Low Risk)	Class B (Low Risk)	Class C (Medium Risk)	Class D (High Risk)
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National Significance	Very high	High	Medium	Low-to-medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long >5yrs	Medium 2-5 yrs	Short	Short (<2 yrs)
Cost	High	High to Medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to None
In-flight Maintenance	N/A	Not feasible or difficult	May be feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

*-NPR 8705.4

Example- Deep Space Mission

	Class A (Very Low Risk)	Class B (Low Risk)	Class C (Medium Risk)	Class D (High Risk)
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National Significance	Very high	High	Medium	Low-to-medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long >5yrs	Medium 2-5 yrs	Short	Short (<2 yrs)
Cost	High	High to Medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to None
In-flight Maintenance	N/A	Not feasible or difficult	May be feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Example- Earth Orbiter (3 yr mission)

	Class A (Very Low Risk)	Class B (Low Risk)	Class C (Medium Risk)	Class D (High Risk)
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National Significance	Very high	High	Medium	Low-to-medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long >5yrs	Medium 2-5 yrs	Short	Short (<2 yrs)
Cost	High	High to Medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to None
In-flight Maintenance	N/A	Not feasible or difficult	May be feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Example- Instrument for Mars Lander

	Class A (Very Low Risk)	Class B (Low Risk)	Class C (Medium Risk)	Class D (High Risk)
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National Significance	Very high	High	Medium	Low-to-medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long >5yrs	Medium 2-5 yrs	Short	Short (<2 yrs)
Cost	High	High to Medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to None
In-flight Maintenance	N/A	Not feasible or difficult	May be feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Example- Space Station Tech Demo

	Class A (Very Low Risk)	Class B (Low Risk)	Class C (Medium Risk)	Class D (High Risk)
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National Significance	Very high	High	Medium	Low-to-medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission)	Long >5yrs	Medium 2-5 yrs	Short	Short (<2 yrs) 3 yr goal
Cost	High	High to Medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to None
In-flight Maintenance	N/A	Not feasible or difficult	May be feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Risk Classification Implications

- For each of NASA's four risk classes, there are companion guidelines/requirements in each of the following areas*-

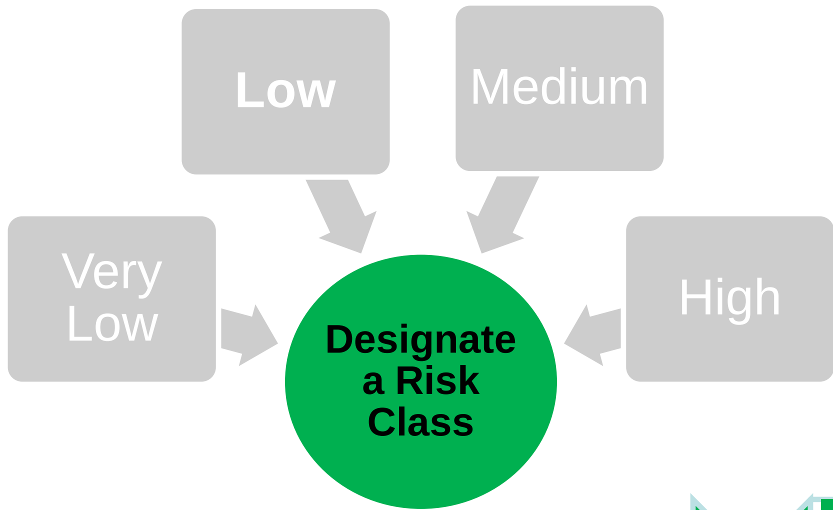
Single Point Failures	**Safety**	Maintainability
Hardware (EM, Flight, Spares)	Materials	Quality Assurance
Test program (Qual, ProtoFlight, Acceptance)	Reliability	Software (assurance)
EEE Parts	Fault Tree Analysis	**Risk Management**
Reviews	Probabilistic Risk Assessment	**Telemetry Coverage**

- With a few exceptions (noted in blue), the level of rigor and penetration required in each of these areas varies with classification, i.e. the expectations for low risk payload electronic parts are much greater than for a high risk payload

*- NPR 8705.4

Recap- It's a Two Step Process

STEP 1



STEP 2

Evaluate requirements associated with the designated risk classification*

EEE Parts
- Class A- NPSL Level 1
- Class B- NPSL Level 1/2
- Class C- NPSL Level 1/2/3
- Class D- NPSL Level 1/2/3

Reliability
- Class A- FMEA, Worst Case, Parts Stress Analysis
- Class B- Box level FMEA, Worst Case, Parts Stress
- Class C- Interface FMEA, Parts Stress
- Class D- Based on safety requirements

Etc
- Class A
- Class B
- Class C
- Class D

*- per NPR 8705.4

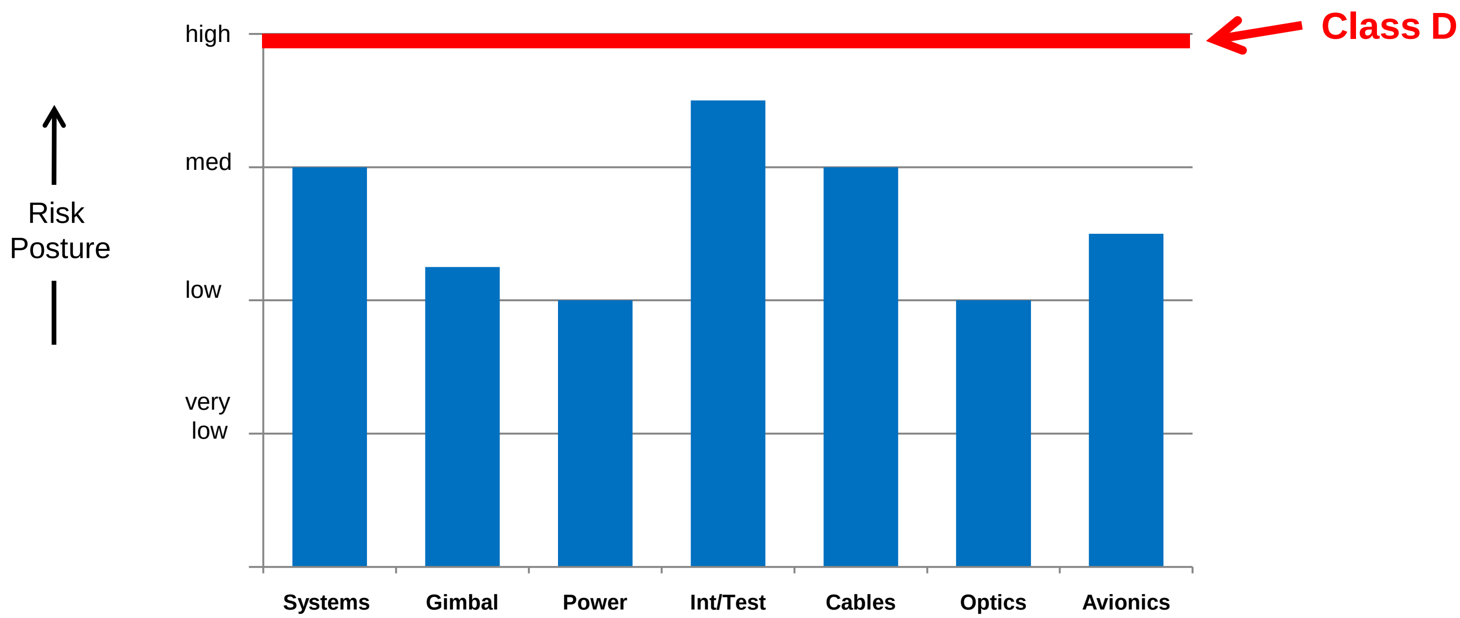
IMPLEMENTATION CHALLENGES

Main Challenges

- At JPL, there are generally two challenges in dealing with NASA's multiple payload risk classifications-
  1) Payloads with a lower risk posture than the JPL "low risk" Institutional baseline- i.e., "very low" risk missions
     - Meeting these guidelines requires a few add-ons to the way JPL typically performs work
       – Impact is largely programmatic- increases in cost and cycle time (full qualification & acceptance test programs, separate prototype and flight models, etc)
  2) Payloads that adopt a higher risk posture than the JPL "low risk" Institutional baseline- "medium/high" risk missions
     - In our experience, more effort (than expected) is required to actually execute a payload with less than traditional rigor and penetration

Medium/High Risk Payload Challenges

- The willingness to assume "additional" risk, versus normal practice(s), is typically uneven throughout an organization



Recent JPL Class D (high risk) Mission at PDR

- "Medium/high risk is OK in other areas, but not mine"

Medium/High Risk Payload Challenges

- In some areas, there is no clear line of demarcation (based on current guidelines) between various risk postures- which leads to differences in interpretation
  - Examples

Spares*

Low Risk	Medium Risk	High Risk
"..Spare hardware as needed to avoid major program impact."	"..Limited flight spare hardware (for long lead flight units)."	"..Limited engineering model and flight spare hardware."

Quality Assurance*

Low Risk	Medium Risk	High Risk
"… moderate surveillance"	"… tailored surveillance"	"… Based on applicable safety requirements"

*- NPR 8705.4

Medium/High Risk Payload Challenges

- There are corollary, unstated risks which need to be understood and communicated
  - Example
    - Medium/high risk payload guidelines allow the use of NASA Parts Selection List (NPSL) Quality Level 3 parts
      - Unstated risk-The radiation tolerance/hardness of NPSL Level 3 parts is typically not easily quantifiable
        - » Little or no test data
        - » Lot variability
        - » Use of off-shore suppliers
      - Result- Projects choose between painful options, including-
        - » Accept risk of a radiation-induced unrecoverable event (with an undefined likelihood of occurrence)
        - » Spend funds to characterize the parts (typically considered an out-of-scope task)

High Risk Payload Challenges

- During implementation of high risk payloads, there is a tendency to stray from the guidelines and expand the boundaries of what is acceptable. Common signs of this trend include-
  - Best practices and lessons learned are overlooked/ omitted
  - Documentation rigor suffers
  - Success criteria becomes less well defined, leading to potential miscommunication/misunderstandings with the customer/sponsor

- Implementation of high risk payloads requires specialized, unique training.
  - For many, this seems to be counterintuitive
  - It is hard to clearly define the "dos" and "don'ts" for high risk baselines

High Risk Payload Challenges

- The human-rated safety requirements for International Space Station (ISS) payloads restrict “flexibility”-

	High Risk Approach*	Additional ISS Safety-related Requirement
Single Point Failures	“…single string approaches may be used.”	Critical SPFs may be permitted if there are no safety impacts (per NSTS 1700.7B)
Materials	“..based on applicable safety requirements”	All materials shall be verified as specified in ICDs, NSTS 14046 and NSTS 1700.7B/ SSP 50021
Test Program	“..only for verification of safety compliance and interface compatibility”	Payloads will be required to be proven structurally safe and compatible with the ISS for all expected flight environments. This process will include verification of payload structural strength and life integrity as well as strength verification for selected materials.

- These additional requirements complicate the costing/planning process for technology development payloads, which are typically viewed as high risk

*- NPR 8705.4

Summary

- The advantages of early identification of an acceptable project risk posture for a NASA payload include-
  - Serves to baseline expectations and enhances communication among participants, as well as with customers and suppliers
  - Reduces the amount of time/expense required to justify deviations to normal practices
- Medium/high risk implementation approaches tend to move people out of their comfort zone
  - In our experience, more effort (than expected) is required to actually execute a payload with less than traditional rigor and penetration
- When working on high risk projects, training and adherence to guidelines are (still) two keys to success

BACK-UP

Definitions

- Payload- Any airborne or space equipment or material that is not an integral part of the carrier vehicle (i.e. not part of the carrier aircraft, balloon, sounding rocket, expendable or recoverable launch vehicle). Included are items such as free-flying automated spacecraft, Space Shuttle payloads, Space Station payloads, Expendable Launch Vehicle payloads, flight hardware and instruments designed to conduct experiments, and payload support equipment

- NASA payload- Any payload for which NASA has design, development, test or operations responsibility

Example Missions

Class A	Class B	Class C	Class D
HST, Cassini, JWST	MER, MRO, Discovery payloads, ISS Facility Class Payloads, attached ISS Payloads	ESSP, Explorer Payloads, MIDEX, ISS complex subrack payloads	SPARTAN, GAS Can, technology demonstrators, simple ISS, express middeck and subrack payloads, SMEX

NASA Parts Selection List- Level 3

- Level 3 is the minimum product assurance class assigned to parts listed in this document. Level 3 contains many advanced electronic functions (from a space flight applications standpoint) and has been created to provide a technology insertion path into NASA flight projects. Parts listed are those produced by reputable manufacturers under a recognized quality assurance system (QML, QPL, ISO 9000) or their equivalent. Typically, only a limited amount of information is available to NEPAG for these parts and NASA has minimal visibility into the manufacturing and testing of Level 3 product. The parts are usually available commercially and have the capability to be used in space applications. The intent of Level 3 listings is to provide products that are newer, have greater functionality and enhanced performance characteristics, and provide higher levels of integration. Because the product has little or no heritage in space flight application and data is unavailable or scarce, these parts are considered higher risk than the Level 1 and Level 2 parts. While the price of these parts may be less than the traditional Levels, more engineering evaluation may be needed to qualify the part for the project's application. The overall reliability and cost of ownership should be considered when selecting these parts. The Level 3 criteria is summarized as follows:
- The manufacturer has supplied and qualified parts for several NASA space projects within the past 2 years.
- The parts and manufacturers have been recommended by one of the following NASA programs.
  - PSAP
  - ASAP
  - ET
  - AIT
- A NASA, DoD, or other space agency procurement specification (e.g. ESA SCC or JAXA QPL/QML) exists.
- Available data on the manufacturer shows no significant problem trends such as GIDEP Alerts or NASA Parts Advisories, a low DPA rejection rate for the manufacturer's products in general, and no significant failures attributable to product quality and/or reliability.