Mission Operations Assurance - A Lesson Learned

Grant Faris
Jet Propulsion Laboratory
California Institute of Technology
15 October 2009

Mission Assurance During Mars Climate Orbiter Operations (1999)

Event Description

- Although a Mission Assurance Manager (MAM) was assigned to Mars Climate Orbiter (MCO) during project development, there was no independent mission assurance function established for the work performed at JPL following launch.

- Discrepancies between the delta-Vs expected by the Navigation Team and those produced by the Angular Momentum Desaturation (AMD) file from the Spacecraft Team were observed during mission operations.
  - No Incident/Surprise/Anomaly (ISA) or Problem/Failure Report (P/FR) was written on this issue.

Recommendations and implementations

1. Recommendation: Revise JPL mission assurance policies and procedures to require an independent Mission Assurance representative during the operational phase of every flight project. This individual should become familiar with and be integrated into the project during the latter phases of development, and possess independent responsibility to verify compliance with design and operational requirements.

   Implementation: FPP 7.7.1 “A mission operations assurance manager (MOAM) is assigned to each JPL-managed project or flight instrument prior to the start of operational readiness testing and continues through the end of mission, including extended missions.”

2. Recommendation: Require all flight projects to report and track post-launch anomalies on ISAs. Project management should rigidly enforce this requirement and maintain a disciplined disposition, tracking, and resolution process.

   Implementation: FPP 7.6.1 “Problem reporting at JPL is implemented using the Problem/Failure Reporting (PFR), Incident Surprise Anomaly (ISA), and other systems as appropriate. Contractors use equivalent systems as negotiated in the contract.

Mission Operations Assurance Vision

Integrate the mission operations assurance function into the flight team providing:

- value added support in identifying, mitigating, and communicating the project’s risks and,
- being an essential member of the team during the test activities, training exercises and critical flight operations.

Mission Operations Assurance Requirements

- Independently assess project risks throughout mission operations.
- Independently assess the project's operational readiness to support nominal and contingency mission scenarios.
- Implement the project's problem/failure reporting system to comply with JPL's Anomaly Resolution Standard.
- Provide training on problem reporting for the flight team.

Mission Operations Assurance Implementation

- Risk assessment
  - Captures the residual mission risks as the project transfers from the development to the operational phase of the mission.
  - Assesses residual risks throughout the post-launch risk review process and integrates them into an overall risk assessment.
  - Provides an independent risk assessment of the Project's risk posture in preparation for critical events.
- Operational Readiness
  - Participates in Operational Readiness Tests (ORTs) to assess if the test objectives were met; and that residual liens are identified, tracked, and resolved.
- Problem Reporting
  - Manages the problem failure reporting system for flight operations including the system setup; as well as the initiation, processing and closeout of Incidents, Surprises, Anomalies (ISAs).
- Operations Training
  - Oversees/conducts the problem/failure reporting function training to the flight team.
  - Assesses the adequacy of the flight team operations position training and overall system level flight team training program.

Mission Operations Assurance Implementation

- Operational Requirements
  - Works with the MAM, PSE, and MOS engineer to assure operational requirements are implemented into the flight hardware, software, and operations design.
  - Participates in operations peer reviews and the Operational Readiness Review (ORR) to assess resolution of integration issues between development and operations.
- Project Planning
  - Assesses Mission Change Requests (MCRs) to ensure appropriate review has been completed, and provides independent risk assessments, as appropriate.
- Flight Rules
  - Reviews waivers to flight rules and makes recommendations to the project.
- Reporting
  - Briefs independent risk assessments at Mission Management Reviews (MMRs), Project Status Reviews (PSRs), Quarterly Reviews, Office of Safety and Mission Success (OSMS) monthly reviews, and Critical Events Readiness Reviews (CERR).
- Interfacing with other Quality/Operations Assurance Function
  - Coordinates Software Quality Assurance support for in-flight software development, flight software modifications, and the resolution of flight software anomalies.
  - Coordinates with industry partners to assure an integrated mission operations assurance program is in place.

Example
Post-Launch
Residual Risk Assessment

Example Post-Launch Residual Risk Assessment

- Performed an independent review and assessment (JPL and Contractor) of the Project's pre-launch residual risk items with implications to earth return.
  - Reviewed and assessed all pre-launch residual risk items including single point failures, spacecraft design risks, mission design risks, red flag PFRs, unverified failures, and major waivers.

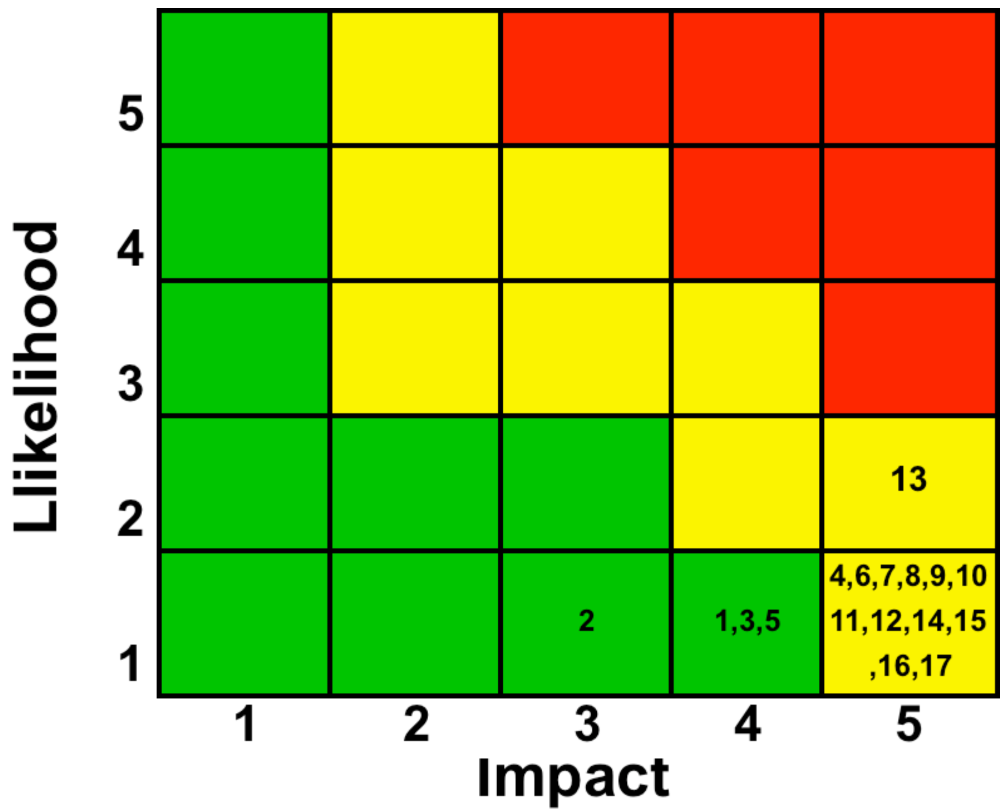
- Performed an independent review and assessment (JPL and Contractor) of the Project's ISAs and operational waivers with implications to earth return.
  - Reviewed all Criticality 1 and 2 ISAs
  - Reviewed all Spacecraft ISAs
  - Reviewed Remaining Criticality 3 & 4 ISAs

- Captured residual risks from the Project's post-launch risk review process.

- Participated in Flight team rehearsals and Operational Readiness Tests.

- Reporting on the risks with specific critical event applicability followed by generic risks applicable throughout the mission.

Example Post-Launch Residual Risk Assessment



Likelihood	
1	Very low - Very unlikely
2	Low - Unlikely
3	Moderate - Significant likelihood
4	High - More likely than not
5	Very high - Almost certain

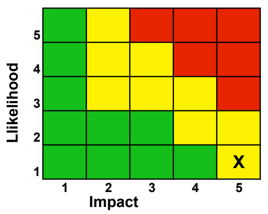
Consequence to sample return	
1	Minimal or no impact to mission
2	Small reduction in mission return
3	Moderate reduction in mission return
4	Significant reduction in mission return (Significant delay in returning samples)
5	Mission failure (Loss/contamination of samples or violation of entry safety criteria)

Example Post-Launch Residual Risk Assessment

Risk #	Risk Rating	Title
1	4x1	Thruster failure causing switch to backup thruster string
2	3x1	Reboot/side swap resulting in unplanned delta V
3	4x1	Spacecraft loss of attitude knowledge
4	5x1	DSN ground station uplink capability lost
5	4x1	DSN ground station downlink capability lost
6	5x1	FPGA in Pyro Initiation Unit (PIU) pyro card fails
7	5x1	Safe mode at end of autonomous sequence recovery window
8	5x1	SRC cable cutters fail
9	5x1	SRC Separation Mechanism (SSM) predicted to be 8 degrees C above flight allowable at release

Example Post-Launch Residual Risk Assessment

- 6. FPGA in PIU Pyro Card
  - Description
    - A failure of the PIU FPGA could cause both the enable and fire outputs of a pyro circuit to fail high resulting in a premature firing of the pyro circuit. The failure occurs if all outputs go high or an enable and fire go high on the same circuit. Waiver XF7045 to PRD Requirement.
  - Mission Risk
    - Impact: 5 During initial power up of the pyro card in the SRC release sequence (SRC separation - 34.5 minutes), the FPGA SPF causes a premature firing of the SRC separation sep nuts, premature cutting of the SRC cables, and/or premature activation of the SRC battery passivation circuits. This could ultimately result in a hard landing.
    - Likelihood: 1 – FPGA failure rate is low per MIL-HDBK 217 especially since the Pyro Card is only operational for ~50 minutes during the entire mission. First flight use of the card was during solar array deployment (~15 minutes). Second and last use is required during the SRC release sequence (~35 minutes).



Example
Risk Trade Study

Risk Balance Trade
Nighttime vs Daytime Entry

- Approach
  - To provide an independent Safety & Mission Assurance assessment of the Stardust daytime vs nighttime entry decision
  - Review the following areas to identify major risk Items:
    - Spacecraft Operations
    - Ground Impact Hazard Assessment
    - STRATCOM Tracking
    - SRC Design Margin
    - Ground recovery Operations
    - Backup Orbit Considerations
  - Recommend an option based on the major risk drivers

Risk Balance Trade
Nighttime vs Daytime Entry

Risk Drivers	Nighttime Human Safety	Nighttime Mission Success	Daytime Human Safety	Daytime Mission Success
Earth Hazard Avoidance	++			
Ground Impact Hazard Assessment	++			
SRC Design Margin		++		
Ground Station Coverage	++	++		
SRC processing time - anomalous				++
SRC processing time - nominal				
Backup Orbit Duration		+		
SRC Release Downlink Data Rate		+		
STRATCOM Tracking		+		

++ = Major Risk Driver **+ = More Robust**

Risk Balance Trade
Nighttime vs Daytime Entry

- Major Risk Drivers
  - The major risk drivers are:
    - Earth avoidance strategy - favors a nighttime entry
    - Ground impact hazard assessment - favors a nighttime entry
    - Redundant ground station coverage - favors a nighttime entry
    - The SRC design margin - favors a nighttime entry
    - The recovery processing time for a breached SRC - favors a daytime entry

- Safety and Mission Assurance Recommendation
  - On risk balance, preserving the SRC design margin by coming in at night and accepting a longer SRC processing time in the event of a breached SRC is recommended.