



CALIPSO Propulsion Safety Launch Decision

The CALIPSO (Cloud-Aerosol Lidar and Infrared Pathfinder Satellite Observations) spacecraft was designed as a pioneering tool for observing and measuring clouds and aerosols, tiny airborne particles such as smoke and dust. The CALIPSO mission was proposed by Langley Research Center (LaRC) in 1998 for NASA's second series of missions in the Earth System Science Pathfinder (ESSP) program. The mission was under the ESSP program at Goddard Space Flight Center (GSFC) and funded through Goddard's ESSP Program Office.



“For the first time, we will be able to construct three-dimensional structures of the atmosphere to better understand the role of clouds and aerosols in Earth’s climate.” NASA Associate Administrator (AA) for earth science Ghassem Asrar.

Figure 1- CALIPSO observing Earth’s atmosphere.
NASA image

The complex project structure, however, extended well beyond NASA. Langley’s proposal included a partnership with the French space agency Centre National d’Etudes Spatiales (CNES), with a co-principal investigator (co-PI) from the Simon Laplace Institution. Through the NASA–CNES Memorandum of Understanding (MOU), CNES was responsible for providing a number of components and services: the ground stations, mission operations, tracking, and the assembly, integration, and test of the payload onto the spacecraft bus. In addition, the French agency (via Alcatel) was responsible for one of the three science instruments (the imaging infrared radiometer) and for providing the Proteus bus as the spacecraft.

Also on the team was Ball Aerospace & Technologies Corp. (BATC), whose role was to design and build the other two science instruments, the CALIOP lidar—the primary instrument on the satellite—and a wide-field camera. The Ball facility in Boulder, Colorado, was the location for the integration of all three science instruments, and BATC was responsible for delivering all ground equipment to test, calibrate, and install the payload onto the CNES spacecraft bus.

Threaded Hydrazine Fittings

Hydrazine is a highly toxic and dangerously unstable fuel used mostly in maneuvering thrusters on spacecraft. It is dangerous for personnel to handle or work around (symptoms of exposure range from irritation of the eyes to seizures and coma in humans). Hydrazine liquid is also extremely reactive and contact with incompatible materials can spur spontaneous combustion resulting in a fire. It is therefore also a risk to flight instruments if it were to leak. One aspect of risk mitigation for hydrazine involves the exclusive use of welded fittings for any conduits since welded fittings have fewer potential failure modes than traditional threaded fittings. The Proteus spacecraft bus used for CALIPSO being built by Alcatel, called for the use of some threaded (AN) fittings on the hydrazine propulsion lines. While these had been used on other spacecraft built by Alcatel in the past, NASA was relying on an Air Force Range Safety Requirement (in EWR 127-1) for the ELV prelaunch processing.¹

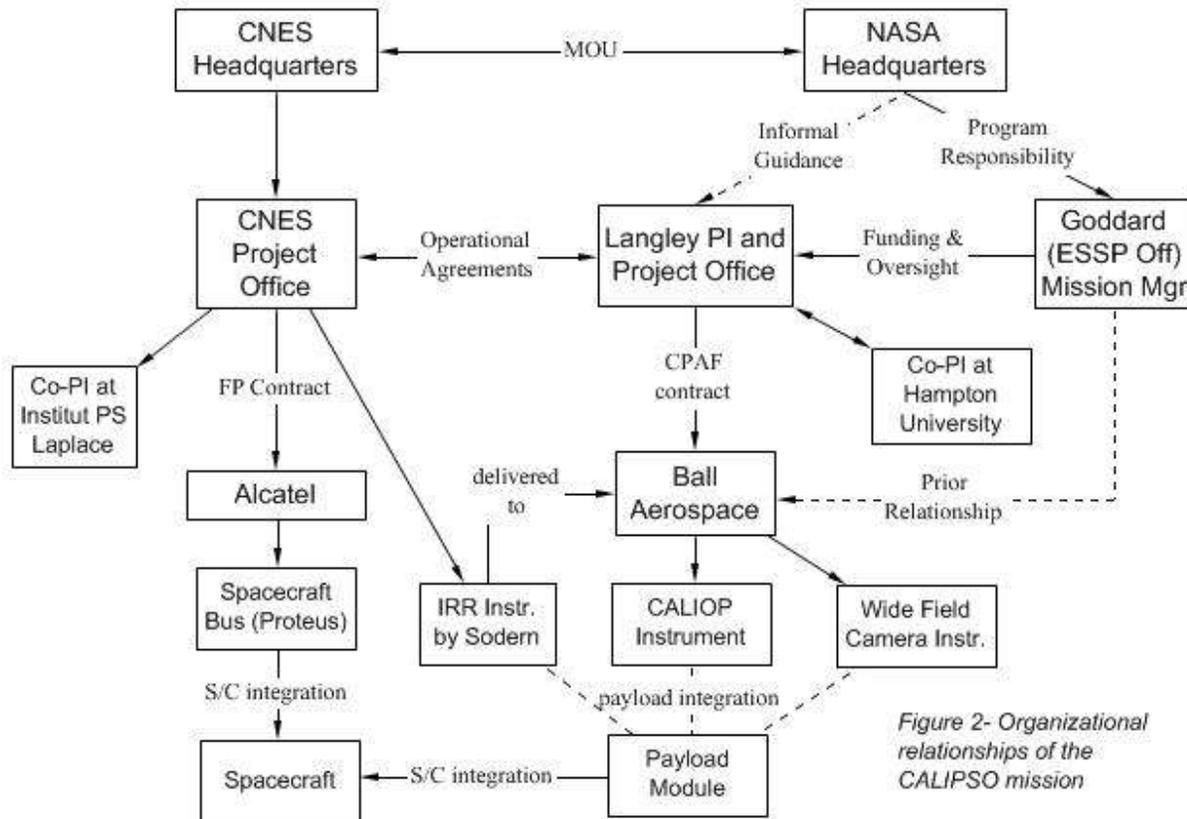


Figure 2- Organizational relationships of the CALIPSO mission

The Goddard Safety Office had raised the issue of the use of threaded fittings not being compliant with the safety requirements as early as 2003 though it was not reported as a risk to the PMC (Goddard Program Management Council) until August 2005 and then carried as a project level risk for months.

¹ Eastern and Western Range (EWR) 127-1 – Range Safety Requirements.

URL: http://www.everyspec.com/USAF/USAF++AFSC/download.php?spec=EWR_127x1_31DEC1999_CHG-1_1997ed.020312.PDF

Goddard Engineering (AETD) also had concerns about the use of threaded fittings as early as 2002 stating in an email:

“The Calipso hydrazine propulsion system is zero-fault tolerant design against leakage of toxic and flammable propellant. The design places personnel at unacceptable risk. The range safety team can provide their assessment of adequacy of this design in protecting their facility.”

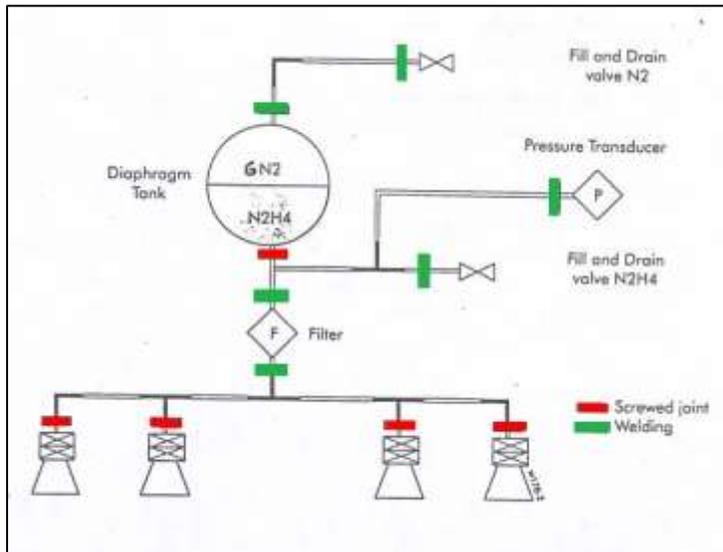


Figure 3- CALIPSO propulsion system simple diagram

The Project Office and CNES had cleared the use of threaded fittings with the Air Force, which had authority over the range for the intended launch of CALIPSO. The project was relying on the precedent of JASON, a previous mission that used the same Alcatel spacecraft bus including the threaded fittings. Though there was some lack of clarity on exactly how JASON had obtained clearance for the threaded fittings, the CALIPSO project pointed to JASON as evidence that it was an acceptable risk. The project

assumed if the range was in concurrence then they could proceed. The Goddard Safety and Mission Assurance Office and the Propulsion Engineering Branch did not feel the issue was closed nor did they feel that the claim of heritage to JASON was valid given the circumstances of how it was handled.

They thought the design should be changed or at least a waiver required especially since the project should not be able to nullify the effect of a range safety requirement by proxy approval from the Air Force without NASA safety concurrence. Given the complicated organization structure and management challenges the project faced, the issue remained unresolved for years. For example, Alcatel indicated they would be willing to make the change but could only change the design if so directed by CNES (and provided additional funds). NASA could not pay CNES or Alcatel to make the change because of the nature of the HQ-CNES partnership which allowed no funds transfers. As the launch date approached this outstanding issue became a flashpoint between the partners.

The Role of the NESCS²

The GSFC Deputy Center Director requested the NASA Engineering and Safety Center (NESC) to independently review the Proteus propulsion bus design for personnel safety to determine what could be done, if anything, to make the existing design as safe as possible. At this point in time the only mitigations left available were level 4—special procedures (see next page for the four levels of hazard reduction). Clearly it is best to use level one and design things as safely as possible. For Calipso it was too late for level 1, 2 or 3 by the time the issue was dealt with.

² More information about the NESC is available from the website at <http://www.nesc.nasa.gov>.

System Safety Principles

- If a system failure may lead to a catastrophic hazard, the system shall have 3 independent verifiable inhibits (dual fault tolerant).
 - A catastrophic hazard is defined as a condition that may cause:
 - death or permanently disabling injury
 - major system or facility destruction on the ground, or
 - mission loss during operations.
- If a system failure may lead to a critical hazard, the system shall have 2 independent, verifiable inhibits (single fault tolerant).
 - A critical hazard is defined as a condition that may cause:
 - severe injury or occupational illness, or
 - major property damage to facilities or systems
- Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called “Design for Minimum Risk” areas of design.
 - Separate, detailed safety requirements
 - Hazard controls related to these areas are extremely critical
 - Warrant careful attention to the details of verification of compliance on the part of the developer.
- INHIBIT – A design feature that provides a physical interruption between and energy source and a function
 - Examples: a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.
- INDEPENDENT INHIBIT – Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

Hazard Reduction Precedence Sequence

1. Design for Minimum Hazard

- Inherent safety through selection of appropriate design features as fail-operational/fail-safe combinations and appropriate safety factors
- Hazards shall be eliminated by design where possible
- Damage control, containment, and isolation of potential hazards shall be included in design considerations

2. Safety Devices

- Hazards that cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment
- Relief devices, interlocks, safe/arm devices, protective barriers, etc.

3. Warning Devices

- Employed for the timely detection of the hazardous condition and the generation of an adequate warning signal
- Alarms, signs, etc.

4. Special Procedures

- Includes personal protective equipment as well as written procedures
- Least effective because dependent on human factors & behavior, which are often unpredictable

The NESC formed a team of propulsion system and mechanical-fastener experts to evaluate the design. The team independently reviewed the design and build of the propulsion bus including a site visit to the manufacturer, Alcatel. In addition, the team performed independent testing of mechanical fasteners, material compatibility reviews, modeling and analysis of hydrazine leak detection capability, and a fire safety analysis.

Flight Readiness Report

In the Redbook (Flight Readiness Report) that Goddard prepared before the launch, the hydrazine leak was carried as a RED risk by the Goddard SMA and Engineering organizations.

F=Flight Hardware and/or Facilities M=Mission Success P=Personnel Residual Risk	Project	SMA	AETD	IIRT
Hydrazine Leakage - Personnel	1,5	2,5	2,5	1,5
Hydrazine Leakage - Flight Hardware	2,5	3,5	3,5	2,5
Hydrazine Leakage – Mission Assurance	2,5	2,5	2,5	2,5
Excessive Battery Charge – Personnel	1,5	2,5	2,5	2,5
Excessive Battery Charge – Flight Hardware	1,5	2,5	2,5	2,5
Excessive Battery Charge – Mission Success	1,5	N/A	N/A	N/A
Use of SADM Without Life Test	2,5	2,5	2,5	2,5
Sample-and-Hold Chips	2,4	2,4	2,4	2,4

Table 1: Residual Risk Chart. Source: CALIPSO Flight Readiness Report, GSFC April 12, 2006 p.13

“The risk to flight hardware/facilities is also due to the possibility of hydrazine leakage from the AN fittings during the launch campaign. This residual risk is mitigated by the customary safeguards in place at the launch site. No additional safeguards are provided by the Project, but the probability of leakage is deemed as low and has been documented in a Propulsion Waiver dated June 10, 2005. Unlike the additional safeguards applied to mitigate the personnel risk, the safeguards described in the waiver do not effectively mitigate the risk to flight hardware or facilities. Hence the risk has been assessed to be a (2, 5) by the Project and the IIRT, and (3, 5) by the SMA and the AETD.” (Source: CALIPSO Flight Readiness Report, GSFC April 12, 2006 p.15)

The NESC report recommended some risk mitigations mostly in handling Hydrazine on the ground to assure safety of personnel. The NESC team concluded that the Proteus propulsion bus design, assembly, and verification along with leak detection and other mitigations put in place at the launch pad were adequate to ensure personnel safety.

"The NESC acknowledges that welded joints are superior to mechanical fittings in preventing leakage but attention to workmanship and proper verification of the joint integrity is required for both. Mechanical fittings do afford a greater degree of flexibility in the assembly and repair of tubing systems. However, a thorough risk assessment must be conducted early in the design process to arrive at a configuration that presents the overall minimum risk to personnel, the mission and the environment. During the course of the review it was noted that the hydrazine system does not have a tank isolation valve. The NESC team acknowledges that the omission of a tank isolation valve in the

propulsion feed system is less safe during ground operations than a system that has the capability to isolate leaks; but while one may be safer, both can be made safe through proper hardware development and launch site processes. Again, a thorough risk assessment must be performed when designing the spacecraft to make these configuration decisions."

Executive Summary of the NESC Final Report on CALIPSO ITA.

Eventually, a waiver was written based upon the NESC report and on implementation of the mitigations that report recommended in order to assure adequate safety of personnel. NESC did not make a final determination of the safety of the design itself. They put forth 11 recommendations for mitigating potential hazards to personnel during handling which the project then adopted. This 'solution' allowed for a waiver and the project to move ahead toward launch.

Reflecting on the unresolved differences of opinion that plagued CALIPSO up until launch, Steve Volz, the HQ Program Executive commented on the different risk charts presented:

"These results hide a more fundamental issue. The disagreements are even wider than the 5x5 matrix shows. The parties could not even agree on the analyses to be used or the criteria for acceptable risk."

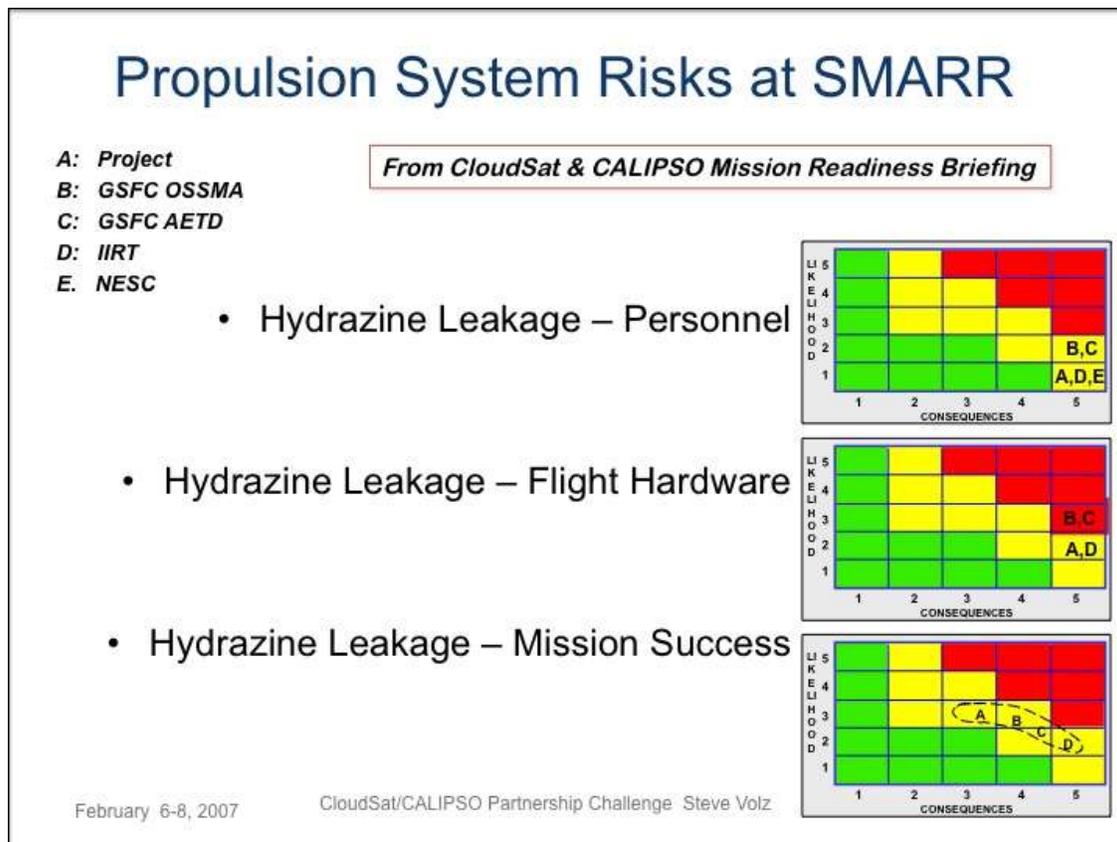


Figure 4- CALIPSO risk charts as presented at the MRR (taken from a HQ Lessons Learned presentation)

Later after the successful launch, the GSFC Deputy Director, Rick Obenschain opined:

"We spent \$10,000,000 to solve a \$100,000 problem because the team wasn't on the same page. We have to take risks but this isn't one we should pay for again."