AIAA-2001-3630

PROPULSION LESSONS LEARNED FROM THE LOSS OF MARS OBSERVER

Carl S. Guernsey*
Jet Propulsion Laboratory
Pasadena, CA

ABSTRACT

Contact with the Mars Observer (MO) spacecraft was lost in August 1993, three days before it was to have entered orbit around the planet Mars. The spacecraft's transmitter had been turned off in preparation for pressurization of the propulsion system, and no signal was ever detected from the vehicle again. Due to the lack of telemetry, it was never possible to determine with certainty what caused the loss of the spacecraft, and review boards from JPL, the Naval Research Laboratory (NRL), and the spacecraft contractor were only able to narrow the probable cause of the failure to a handful of credible failure modes. This paper presents an overview of the potential failure modes identified by the JPL review board and presents evidence, discovered after the failure reviews were complete, that the loss was very likely due to the use of an incompatible braze material in the flow restriction orifice of the pressure regulator. Lessons learned and design practices to avoid this and other propulsion failure modes considered candidates for the loss of MO are discussed.

INTRODUCTION

The Mars Observer Spacecraft is pictured in Figure 1 as it was being prepared for launch. MO was envisioned to be the first of a series of spacecraft, known as the Observer series, which were the early 1980's version of the "Faster, Better, Cheaper" mantra that was to be adopted by NASA during the following decade. The cost savings envisioned to be realized by the Observer program were based on: 1) use of a standard spacecraft bus for a large number of missions to minimize non-recurring development costs, 2) use of an existing commercial spacecraft design with the "minimal modifications necessary for the planetary mission", and 3) integration of the instruments onto a separable pallet, such that the spacecraft bus contractor would not have to perform extensive mission-unique integration activities. Finally, since the spacecraft bus was to be an off-the-shelf "assembly line" item, it was procured under a fixed-price contract.

Figure 1 – Mars Observer Spacecraft

Unfortunately, as was pointed out by the NASA failure review board, the MO project deviated significantly from these concepts, eventually building a unique, one-of-a-kind spacecraft with the unique integration challenges of specialized science instruments. From the time the bus contractor was selected, the design became progressively more unique. In spite of this, the project still relied heavily on design heritage that in some cases was not totally relevant to the MO mission. This led to a number of programmatic "lessons learned" which are well

*Principal Engineer, Thermal and Propulsion Engineering Section. Member AIAA.

beyond the scope of this paper. It was be noted that several features of the propulsion subsystem, derived from Earth-orbiting designs, were inappropriate to the planetary mission.

Following launch, the MO spacecraft operated successfully during the cruise to Mars. At the time the transmitters were turned off, there was no indication of anomalous operation of any part of the spacecraft. The transmitters were turned off because the propulsion system pressurization event required pyro valves to be fired and the transmitters had not been qualification tested for pyrotechnic shock in the powered state. The onboard sequence should have turned the transmitters back on following the pressurization events, re-establishing contact after a period of approximately 15 minutes. When no signal was detected, the ground controllers began exhaustive attempts to recover the spacecraft. The primary flight-based evidence the review boards had to work with was that these efforts failed to recover the spacecraft or even detect a signal from it. This "negative information" was used to eliminate a significant number of potential failure modes put forth in the days following the loss of signal.

The JPL Mars Observer "Loss of Signal Special Review Board", of which the author was a member, concluded that there were six credible causes of the loss of the MO spacecraft:

1. Oxidizer and fuel reaction in the pressurization system lines, leading to uncontrolled venting of pressurant and propellant, resulting in loss of spacecraft attitude control and communication capability.
2. Failure of the series-redundant pressure regulator to close during the pressurization event, leading to over pressurization and rupture of the propellant tanks.
3. Expulsion of a NASA Standard Initiator (NSI) from one of the pyro valves fired during the pressurization sequence, leading to impact damage and rupture of the fuel tank.
4. Primary power system failure due to a short to ground within the power system electronics.
5. Loss of computational function on the spacecraft due to electronic part latch-up which could be induced by chassis currents induced by the pyro events during the pressurization sequence.
6. Inability to turn the transmitters on due to electronic part latch-up in the telecommunication subsystem.

The JPL Board chose not to single any of these credible potential causes out as the most probable failure mode. The official NASA review board, chaired by Dr. Timothy Coffee of NRL, identified the first item in the above list as the most probable cause, but acknowledged that there was no "smoking gun" which could bring high confidence that this was indeed the cause of the failure.

The rest of this paper will describe the first three failure modes, each one of which could be directly connected to the pressurization of the propulsion system. Previously unpublished data are presented that, in the author's opinion, make a compelling case that the second cause of failure listed above is the most probable, although not conclusively proven.

PROPULSION SYSTEM DESIGN AND OPERATION

The Mars Observer spacecraft carried both bipropellant and monopropellant propulsion systems. No credible potential causes of the mission loss were found which were related to the monopropellant system, so it will not be discussed in this paper.

A schematic of the bipropellant system is shown in Figure 1. The system used four 490 N main engines and four 22 N thrust vector control thrusters which burn monomethylhydrazine (MMH) fuel and nitrogen tetroxide (NTO oxidizer. [The oxidizer was in fact mixed oxides of nitrogen with a NO content of approximately 3%, but it is commonly referred to as NTO.] This bipropellant system was intended to be used only for large Trajectory Correction Maneuvers (TCMs), Mars Orbit Insertion (MOI), and a few large orbit trim maneuvers after MOI. These maneuvers were to be performed using two of the 490 N main engines at a time, with the other two providing redundant backups. In the event of failure of one or more of the 22 N thrusters, it was possible to off-pulse the 490 N engines to provide pitch and yaw control. Roll control was provided by the monopropellant system. Two small TCMs were performed during the cruise to Mars in the "blow down" mode described below and performance of the bipropellant system was as expected.

The pressurization of the bipropellant tanks in preparation for MOI was to have been accomplished by firing normally closed pyro valve PV-7, which would pressurize the NTO tank, followed approximately 5 minutes later by firing pyro valve PV-5, which would allow the MMH tank to be pressurized. If these pyro valves actuated properly, the ground had the option to cancel a sequenced

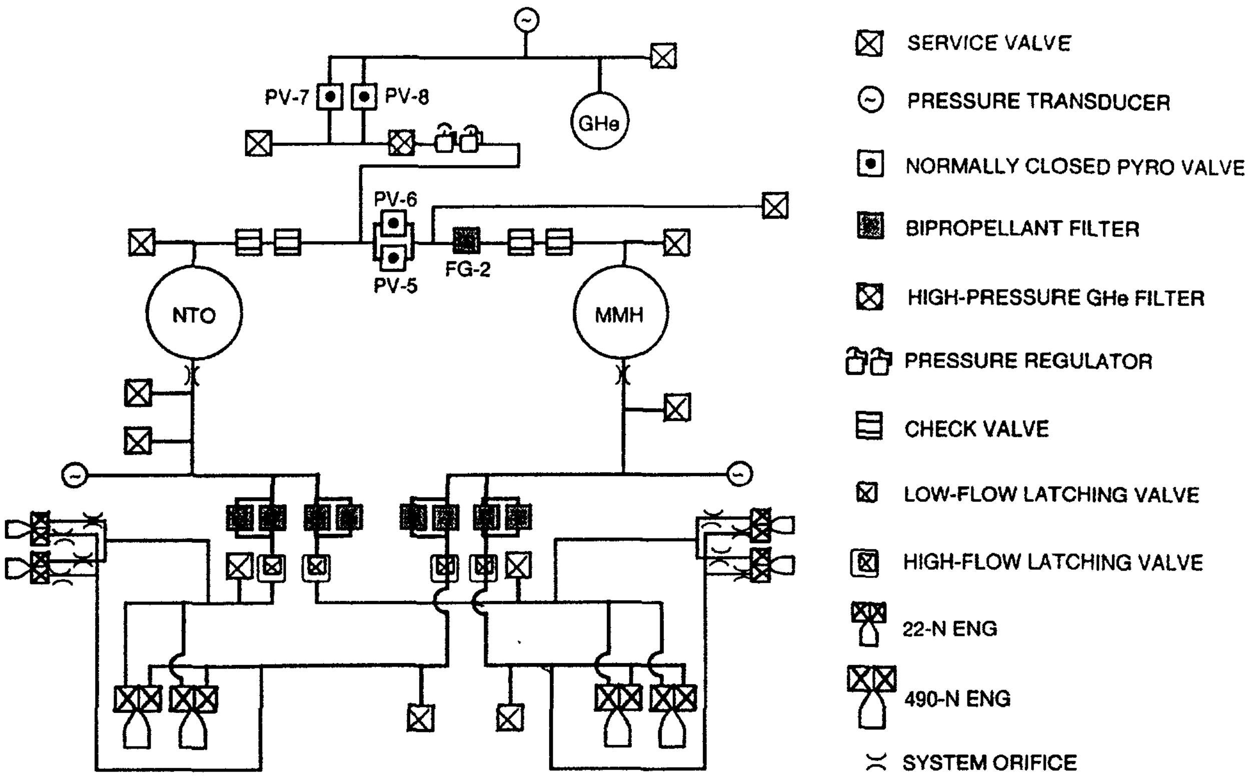

Figure 2 – Mars Observer Bipropellant Propulsion System Schematic

event that would have fired redundant valves PV-8 and PV-6 several hours later. Series-parallel check valves were provided to prevent large-scale propellant transfer between the fuel and oxidizer tanks following pressurization.

The pressurization portion of the MO bipropellant system was very atypical of bipropellant propulsion system designs used on previous planetary missions. Specifically, there was no provision for isolation of the pressure regulator from the high-pressure helium supply during long periods of inactivity, such as the cruise to Mars. This was a holdover from the heritage system design, which was intended to perform a series of apogee boost maneuvers in a very few days following the launch of the spacecraft. In contrast, previous planetary spacecraft (Mariner '71, Viking Orbiter, and Galileo) had provided for isolation of the high-pressure supply during long quiescent periods in order to protect against regulator leakage. In addition, Galileo developed a soft-seat (Teflon) regulator to reduce susceptibility to particulate contamination. The contractor building the Mars Observer system felt that the use of a series-redundant pressure regulator provided adequate protection against such leakage, having seen no evidence of leakage in the heritage system design. Thus the original plan for operation of the spacecraft was to pressurize the system shortly following launch, depending on the regulator to prevent over-pressurization of the propellant tanks during the cruise to Mars.

This plan for operation of the MO bipropellant system came under intense scrutiny by propulsion engineers at JPL in the months leading up to the launch of the spacecraft. The risk of tank over-pressurization was judged to be high, based on the experience of previous planetary spacecraft using hard-seat pressure regulators. Specifically, the first Viking Orbiter had experienced regulator leakage in excess of 7000 scch when brought on line two weeks before MOI, necessitating two unplanned emergency maneuvers to keep the tank pressures within the main engine operating envelope. The second Viking mission sequence was modified to delay pressurization to MOI-12 hours; and while there was some evidence that it's regulator was also leaking, the data were inconclusive. The Problem / Failure Report summarizing the Viking regulator leakage concluded that it could have been caused by a particle of less than 1μ diameter trapped on the valve seat. One potential source of this seat contamination discussed in this report was reaction products of fuel and oxidizer vapors, which would permeate through the check valves and diffuse into the pressurization system during the cruise period.

In evaluating the risk of regulator leakage for MO, it was noted that particles of the size required to cause a Viking-scale leak were abundant throughout the system, and that the filter upstream of the pressure regulator, with a rating of 10μ, would be ineffective in protecting the regulator. Diffusion calculations indicated that the partial pressure of NTO vapor would approach saturation levels during the cruise to Mars, allowing for corrosion of regulator hardware and/or reaction with fuel vapors. It was decided jointly by JPL and the system contractor that the baseline design and operation scenario were unacceptable.

Due to the rapidly approaching launch date and fully assembled state of the spacecraft, options to add additional pyro valves to provide for isolation during cruise were considered to be unacceptably risky. Specifically, they required welding on the fully integrated spacecraft or the use of cryo-fit fittings to plumb the new components into the system. At that time, cryo-fit fittings had never been qualified for application to high-pressure helium systems and it was felt that making such a modification might introduce more risk that the regulator leakage itself. Options for welding the valves into the system carried a high risk due to the proximity of electromagnetically susceptible electronics in the region where the welds would have to be made.

Fortunately, an operational alternative to these hardware changes was found. Rather than launching the propellant tanks at a relatively low pressure, which would require the regulator to be brought on-line prior to the first TCM, it was determined that if the tanks were launched at the high end of the operating pressure range, it would be likely that all of the required TCMs could be performed in "blow-down" mode. The decrease of tank pressures accompanying the consumption of propellants would not exceed the range acceptable for main engine or thruster operation. The nominally equal volumetric flow rates of the propellants during maneuvers helped to avoid undesirable mixture ratio variations. It was necessary to pressurize the propellant tanks above the desired launch pressure to account for helium solubility in the propellants, but this was accomplished using available solubility data and produced almost exactly the desired pressures at launch. It was noted, however, that the process of helium going into solution was very slow until the spacecraft was moved, providing agitation of the propellant.

As noted above, two TCMs were performed during the cruise to Mars and the propulsion system performed adequately. No anomalous behavior of the propulsion system was in evidence when the MO transmitters were turned off for the pressurization event.

PROPULSION-RELATED FAILURE MECHANISMS

As mentioned above, the JPL review board put forward three propulsion-related failure modes that were felt to be credible causes of the loss of MO. Each of these failure modes was also deemed credible by the NASA review board. Each one points to different lessons learned, and these are valid regardless of the actual cause of the failure. While the author will discuss the relative strengths and weaknesses of these failure mechanisms, this does not diminish the validity of the lessons they pose.

A recurring theme in all of these failure modes is an over-reliance on heritage designs. This applies to the heritage design of the propulsion system used for short-term missions, the use of a heritage regulator design not compatible with long-term exposure to NTO vapors, and acceptance of the heritage of a pyro valve design in spite of questionable materials selections and structural margins.

OXIDIZER AND FUEL REACTION

Under this hypothesis, oxidizer condensed in the pressurization system upstream of the oxidizer check valves. Referring to Figure 2, this would be the portion of the system bounded by PV-7 and -8, PV-5 and -6, and the oxidizer check valves. This portion of the system was subject to oxidizer permeation through the check valves from the time the propellant was loaded (approximately 6 weeks prior to launch) until the MOI pressurization event. It was further hypothesized that a portion of this condensed oxidizer was trapped in a dead-end portion of the feed system immediately upstream of pyro valves PV-7 and -8 rather than being swept into the oxidizer tank during the initial phase of the pressurization.

Finally, it was hypothesized that this oxidizer reacted with fuel prior to reaching the fuel tank, causing localized overpressures which caused rupture of the lines. Uncontrolled venting of helium and MMH would then cause the spacecraft to tumble rapidly and eventually damage the spacecraft avionics by corrosion and shorting of electrical connections.

It has long been recognized that propellant vapors will permeate through the soft seal materials used in check valves. Attempts to prevent this by using metallic seals have generally been defeated by leakage problems with hard-seat valves. During the MO failure investigation JPL, in collaboration with the NASA review board, conducted a series of permeation measurements of the check valves used on MO. These data are summarized in Figure 3. For schedule reasons, the MO spacecraft flew two different check valve designs, one build by Vacco and the other by Futurecraft. Data are presented for each valve design at two temperatures for the case where liquid is present immediately

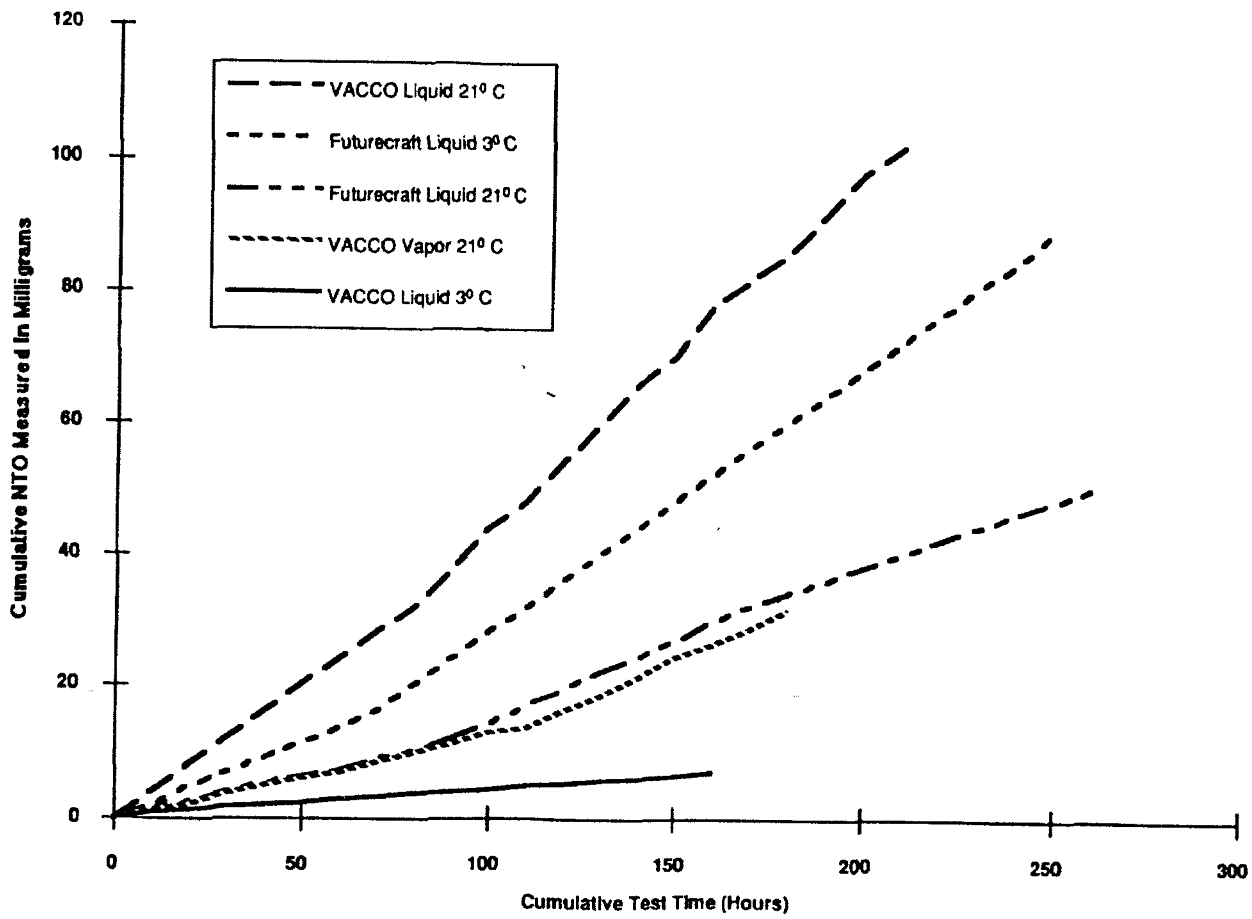

Figure 3 – Check Valve Permeation Data

downstream of the valve seal; it was felt that this was a credible worst case condition since there was no positive means to preclude wetting of the lines downstream of the check valves. A single test with NTO vapor maintained downstream of the valve seal shows a reduced transport, but only by a factor of about three. It can be seen that temperature has a significant impact on NTO transport through each valve. Transport through the Vacco unit increased dramatically at 21°C vs., 3°C, possibly due to the higher vapor pressure of the NTO at the higher temperature. However, the Futurecraft unit exhibited the opposite behavior, possibly due to improved sealing at higher temperatures. The exact causes of this discrepancy could not be determined.

For condensation of liquid NTO to occur in the pressurization system, there needed to be temporal and/or spatial temperature gradients. If the entire system were at one temperature, the pressurization system might become saturated with NTO vapor, but no condensation would be expected to occur. Unfortunately, such gradients did exist; following launch, the pressurization system was consistently running (based on inferences from pre-launch thermal testing) at temperatures from −2°C to +5°C, while the bulk average temperatures of the propellant tanks were significantly warmer, as shown in Figure 4. The oxidizer tank remained above 20°C for more than 4 months following launch.

A detailed permeation and diffusion model of the MO pressurization system was developed at JPL that accounted for transient temperatures in the oxidizer tanks and pressurization system. Conservative assumptions were made wherever possible to obtain an upper bound on the amount of NTO which might have condensed upstream of the

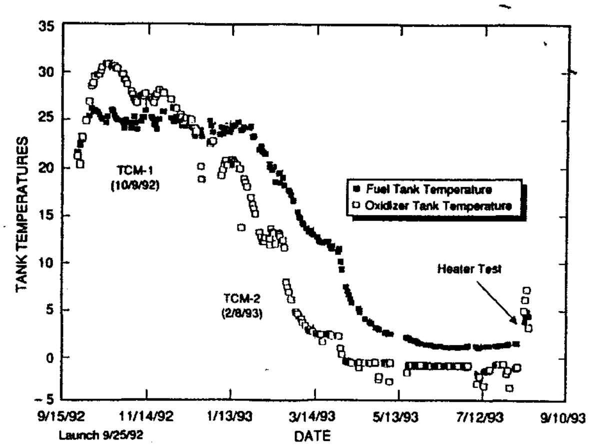

Figure 4 – MO Tank Temperatures

oxidizer check valves. The result was that the maximum quantity of NTO that could have condensed in the feed system was less than 1 g, more probably less than 250 mg.

Once oxidizer condensed in the pressurization system, this hypothesis depends on this oxidizer becoming trapped in dead-end lines just upstream of PV-5 and −6. Any oxidizer that was not in this location would have been swept out of the pressurization system during pressurization of the oxidizer tank. These dead-end lines had a volume capable of holding up to 14 g of oxidizer, which formed an absolute upper bound on the amount of liquid oxidizer which could have been present in the system when pyro valve PV-5 was opened even if the check valves literally failed open, rather than being subject to normal permeation. In point of fact, this quantity of propellant could not have diffused into the pressurization system even in the absence of check valves.

While this work was ongoing at JPL, NRL commissioned the Air Force Phillips Laboratory at Edwards Air Force Base to conduct a series of tests of the effects of oxidizer/fuel reactions in the pressurization system. A mock-up of the portion of the pressurization system downstream of PV-5 and −6 was built and various quantities of oxidizer were injected into the system under pressure. The system downstream of the fuel check valves was filled with MMH to simulate a worst-case condition. This fuel had to be displaced into a fuel supply tank by the incoming helium and NTO. In 13 tests for which data were acquired, only one demonstrated a significant reaction between the MMH and NTO, with peak pressures of approximately 4000 psig. This test occurred with a slug of NTO in excess of 10g, or ten to forty times the amount that might have been present in the MO pressurization system. Attempts to repeat this event were unsuccessful, with overpressures due to reactions being under 200 psig in most cases. By contrast, the burst pressure of the lines in the MO pressurization was in excess of 10,000 psi. It has been suggested that the lines were weakened during the event by heating from the reaction. However, analysis taking into account the film coefficient between the hot gases and the wall of the tube does not support that this was feasible in the short (<1 ms) time period involved.

To this author, this failure mode is credible, but certainly not compelling. A series of events of varying likelihood needs to have occurred:

- Condensation of NTO in the pressurization system (Likely at the 250 mg to 1 g level))
- Capture of condensed NTO in dead ends (Unlikely that most would not be aspirated)
- Reaction violent enough to rupture lines occurs (Unlikely – never reproduced in test)
- Spacecraft never turns on transmitters or signal is never seen due to tumbling (Moderate likelihood)

This failure mode appears to be of low probability. However, it is credible enough to call for adherence to several lessons to be learned:

- Propulsion pressurization system designs for long-life missions must account for

permeation and diffusion of propellant vapors that may occur.
- In order to preclude condensation of liquid propellant in the pressurization system, the portions of the system where condensation might occur should be maintained warmer than the propellant tanks.

It is worth noting that the likelihood of this scenario might have been reduced if the original plan of bringing the regulator on line just after launch had been adhered to. The amount of NTO available for condensation would have been somewhat reduced due to reaction with fuel vapors, although this could have increased the likelihood of other malfunctions, particularly of the fuel check valve. Any helium leakage through the pressure regulator would also have served to reduce the NTO concentration in the pressurization system. Given the relative likelihood of tank over pressurization due to regulator leakage, the author believes the correct decision was made. However, if the risk of condensation had been recognized at the time, it could have been mitigated by adding a few line heaters. This suggests the additional lesson:

- When considering risk mitigation actions for a known risk, care should be taken to ensure that other risks are not being inadvertently increased.

REGULATOR FAILED OPEN

The regulator used in the MO pressurization system was a series-redundant unit with an excellent history of reliability. It is shown schematically in Figure 5.

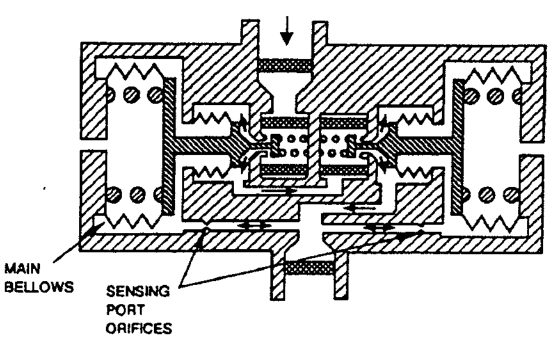

Figure 5 – Regulator Schematic

Due to the blow-down operation during TCMs 1 and 2, both stages of the pressure regulator should have been in their wide-open position at the beginning of the pressurization sequence. If the regulator stayed in that configuration, the oxidizer tank would have reached it's burst pressure about 2 minutes after PV-6 was fired. The JPL board report noted that this could be caused by contamination blocking the regulator sensing ports shown schematically in Figure 5. These sensing ports have restrictors to provide damping which have a minimum flow port diameter of less than 150 μ, making them subject to blockage by minute amounts of contamination. In some cases, blockage of the flow restrictors in similar regulators have been caused by reaction of propellant vapors with incompatible materials, such as the residue of cleaning fluids.

Unfortunately, investigations of this hypothesis during the formal failure review failed to turn up anything resembling a "smoking gun". Review of the regulator materials list failed to turn up evidence of any incompatible material. Review of cleaning practices at the spacecraft manufacturer turned up some suspicious items (components certified as clean, with zero particle counts, when in fact they were well out of specification). However, this did not directly implicate the MO system and the contractor had a good track record of successful spacecraft propulsion system operation, at least on short-lived missions.

New information relevant to this hypothesis was obtained during a hardware heritage review of an essentially identical regulator for another program. One of the heritage review participants recognized that the flow restrictors used in the pressure regulator were commercial items which use AMS 4774 braze to attach filter "screens" (actually drilled sheet metal pieces formed to the desired shape) to the inlet and outlet of the flow restrictor. This braze is used in an oven brazing process which allows a considerable amount of braze material to "wick" along the surface of the inlet and outlet screens. In the opinion of JPL chemists consulted after this review it was extremely unlikely that this silver-copper braze material would be long-term compatible with NTO vapors. The program for which this review was conducted choose to procure the flow restrictors without the inlet and outlet screens and accompanying braze.

It was quickly verified that the MO pressure regulator had indeed used the same flow restrictor. Inexplicably, while the flow restrictor vendor clearly calls out the braze in their catalog, it was omitted from the regulator materials list.

Samples of the flow restrictor were procured and examined visually and by SEM. A significant quantity of braze was indeed found to have "wicked" up the inlet screens during the brazing process, in some cases completely occluding the 100 μ holes in the inlet screen. A sample of AMS-4774 braze wire was placed into NTO vapor and was observed to suffer heavy corrosion in a matter of days.

Finally, a flow restrictor was placed under NTO vapor exposure. Figure 6 is a SEM image of the restrictor after 30 days of exposure. Some evidence of corrosion is evident, indicated by the whitish areas in Figure 6. Some of the 100 μ holes in the inlet screen were seen to be completely occluded by corrosion products; many were ringed by such products. However, the deposits seemed fairly tenacious. The dramatic difference between the test of the raw braze wire and the braze on the flow restrictor is not well understood, but might be caused by an alloying process occurring during the brazing process.

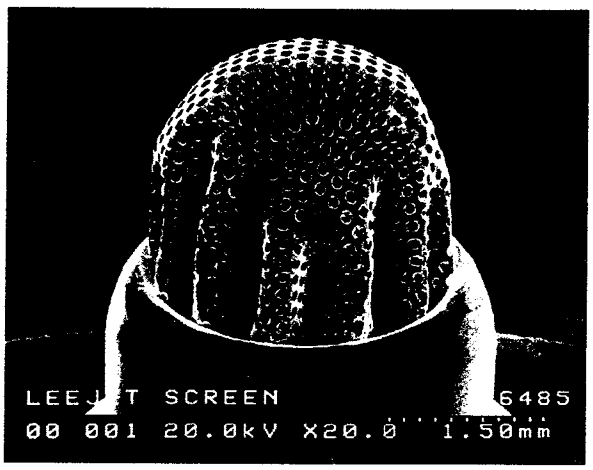

Figure 6 – Restrictor After 30-Day Exposure to NTO Vapor

Figures 7 and 8 show the state of the braze compound after a one year exposure to NTO vapor. It can be seen that the corrosion is extensive, with fragile corrosion products literally hanging off of the inlet screen. Many of the holes in the inlet screen are occluded with corrosion product. A highly qualitative test of the tenacity of the corrosion product was made by dropping the orifice down a 50 cm tube onto a witness tape. It was observed to shed large numbers of particles.

It is important to remember that the critical flow path in the restrictor is only 1.5 times the dimension of the holes in the inlet screen. There would appear to be more than enough corrosion product to produce a nearly complete blockage of this critical orifice.

Figure 7 – Restrictor After 1-Year Exposure to NTO Vapor

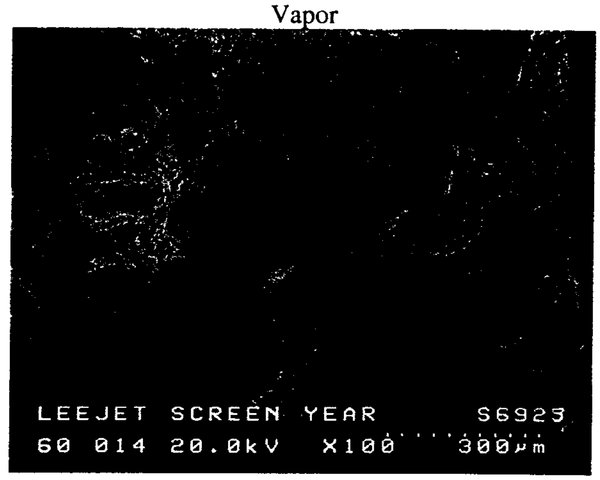

Figure 8 – Close-Up of Flow Restrictor After 1-Year Exposure to NTO Vapor

This hypothesis thus comes down to a remarkably plausible series of events:

- Both stages of the regulator open during cruise when tank pressures drop well below regulator set points,
- Oxidizer vapor permeates check valves and diffuses to flow restrictors, corroding braze material,
- Pyro shock at firing of PV-5 dislodges corrosion products,
- Corrosion products are forced into flow restrictor orifice by helium surge pressure,
- Corrosion products prevent flow through restrictor to main bellows, keeping regulator in near-open state,
- Oxidizer tank reaches burst pressure – end of game.

It is probably obvious to the reader that the author considers this the most credible potential cause of the MO loss. It is directly connected to the pressurization event. There is clear evidence that the incompatible braze was present. Perhaps most importantly, the long time required to see significant corrosion of the braze material by the NTO vapor explains why regulators using the same design have flown on numerous short-duration missions without incident. In addition to lessons previously identified, this failure scenario suggests the following:

- Compatibility of pressurization system components with propellant vapors is essential for long-term missions.
- Short-term tests (days to months) may not always be adequate to show long-term compatibility.
- Vendor material lists may not always be reliable for screening of incompatible materials; long-term testing of component compatibility is preferred.

EXPULSION OF NSI

The final propulsion-related cause of the MO failure proposed by the JPL and NASA boards was expulsion of a NSI from pyro valve PV-5, impacting the fuel tank and leading to tank rupture. The MO propulsion system used pyro valves that were constructed of titanium alloy. On another program, pyro valves of the same design were observed to expel their initiators, exiting the valve at high speeds and damaging nearby equipment.

Figure 9 illustrates the orientation of PV-5 with respect to the MMH tank. The view is looking directly down the axes of the redundant initiators. It can be readily seen that should the initiator facing into the plane of the figure be ejected it would have a high likelihood of striking the tank. For reasons of mass, there was no cabling attached to that NSI (since PV-6 provided the required redundancy), so there would be nothing other than a lock wire to restrain the NSI. Evidence from the other program suggested that this would be ineffective.

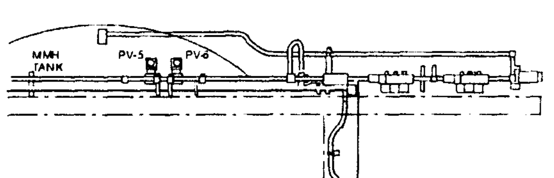

Figure 9 – PV-5 Location

The root causes of the initiator expulsion on the other program were shown to be a combination of damage to the titanium threads holding the initiator in place in the valve body and use of excessive booster charge in the pyro valve, leading to low structural margins for retention of the initiator. The thread damage was caused by combustion of the threads when exposed to the combustion products from the initiators and booster charge. The failures occurred when firing of one initiator caused sympathetic ignition of the other, causing the electrically fired initiator to be expelled.

Significantly, the initiator ejection events occurred only when "NSI equivalent" initiators were used. It is believed this was due to the higher brisance of the equivalents, but the exact cause was not determined. It was also observed that the it was always the electrically fired initiator that was expelled, not the one that ignited sympathetically.

These points argue against the likelihood of this scenario for MO, which used "true" NSIs and in which the electrically fired NSI faced away from the tank. However, examination of the valves used for MO lot acceptance testing showed serious combustion damage on the titanium threads holding the NSIs in place on each valve. Although no NSIs were ejected in this ten-valve test this damage, along with extremely low structural margins based on analysis, suggest that this is a credible, if low-probability, failure mode for MO.

Some lessons derived from this hypothesis are:

- Incipient failures, such as partial combustion of threads in pyro devices, should be carefully evaluated even if they have not lead to failure of the device. They should be eliminated unless their extent can be positively bounded and robust margins can be demonstrated for the degraded hardware.
- Titanium makes an excellent fuel for pyro devices; its use for structural roles in such devices should be carefully considered or avoided.
- Care should be taken with lot-to-lot variations of initiators; "equivalent" initiators may not be so equivalent in actual use.

CONCLUSION

The loss of the Mars Observer was traumatic for all those involved. The fact that there was no telemetry available at the time of the failure means that it can never be proven beyond a shadow of doubt what actually caused the loss; a number of credible causes have been identified. The propulsion-related potential causes lead to the following lessons learned:

- Propulsion pressurization system designs for long-life missions must account for permeation and diffusion of propellant vapors that may occur.
- In order to preclude condensation of liquid propellant in the pressurization system, the portions of the system where condensation might occur should be maintained warmer than the propellant tanks.
- When considering risk mitigation actions for a known risk, care should be taken to ensure that other risks are not being inadvertently increased.
- Compatibility of pressurization system components with propellant vapors is essential for long-term missions.
- Short-term tests (days to months) may not always be adequate to show long-term compatibility.
- Vendor material lists may not always be reliable for screening of incompatible materials; long-term testing of component compatibility is preferred.
- Incipient failures, such as partial combustion of threads in pyro devices, should be carefully evaluated even if they have not lead to failure of the device. They should be eliminated unless their extent can be positively bounded and robust margins demonstrated for the degraded hardware.
- Titanium makes an excellent fuel for pyro devices; its use for structural roles should be carefully considered or avoided.
- Care should be taken with lot-to-lot variations of initiators; "equivalent" initiators may not be so equivalent in actual use.

ACKNOWLEDGEMENT

The work described in this paper was performed by the Jet Propulsion Laboratory, California Institute of Technology, under a contract to the National Aeronautics and Space Administration.

The author would also like to acknowledge the efforts of the many people at JPL, NRL, and Lockheed Martin who worked so hard to try to ascertain the cause of the loss of Mars Observer. In particular, I would especially like to acknowledge the contribution of Mr. Carl Engelbrecht, who recognized the commercial flow restrictor and was aware of the braze compatibility issues. Were it not for this observation, it is possible that two additional planetary spacecraft would have been launched with this flaw.