

# Mars Pathfinder “Common Sense” Mission Assurance

James F. Clawson  
Jet Propulsion Laboratory  
4800 Oak Grove Drive  
Pasadena, CA 91109  
(818) 354-7021  
james.f.clawson@jpl.nasa.gov

*Abstract* - The Mars Pathfinder Mission Assurance program was the first “tailored” approach at JPL. It featured flexibility, common sense, concurrent engineering, and lower cost. Documentation was cut significantly, MA team members were empowered, a full environmental test program was implemented, selective redundancy was employed, QA was based on processes (not historical points), and the electronic parts program was a mixture of Cassini common buys and Military grades. The MA cost was less than one-third of tradition and the number of Problem/Failure reports was less than one-quarter normal (at one-third the normal closure cost each). There were no significant deviations from the plan created over three years before launch.

## TABLE OF CONTENTS

1. INTRODUCTION
2. ELECTRONIC PARTS PROGRAM
3. RELIABILITY ASSURANCE PROGRAM
4. MISSION ENVIRONMENTS PROGRAM
5. HARDWARE/SOFTWARE QUALITY ASSURANCE PROGRAM
6. SYSTEM SAFETY PROGRAM
7. OTHER WAR STORIES/LESSONS LEARNED
8. CONCLUSIONS
9. BIOGRAPHY

### 1. INTRODUCTION

The Jet Propulsion Laboratory (JPL) has a long history of successful interplanetary missions (Mariners, Viking, Voyager, Galileo, Magellan, etc.) Over the course of 30 or so years, a “culture” of do’s and don’ts in the realm of Mission Assurance evolved and became somewhat “sacred”.

Disciplines in JPL Mission Assurance include Electronic Parts Engineering, Reliability Engineering, Mission Environments Engineering, Hardware/Software Quality Assurance, Systems Safety, and to some extent, configuration management, and Materials and Processes.

At the initiation of the Mars Pathfinder project (early 1992), it was an up-front goal of the project team to change the culture of JPL. The Pathfinder cost-cap of \$ 150M (1992 dollars) was a requirement that many thought impossible. The entire team generated a mind-set that we would meet that goal. As a result, all major elements (Spacecraft Flight System, Science and Instruments, Ground Data System, Mission Operations, Mission Assurance, etc.) committed to

“common sense” approaches rather than rigid traditional approaches.

The Mission Assurance Program was evolved very early and included only what made sense. For example, full redundancy and Class S parts for an 8 month mission (7 months cruise, 1 month minimum on the surface of Mars) did not make sense. The cost, mass, and volume were too high. In 1992, NASA still had mission classes: “A” being lowest risk, through “D” having relatively high risk. In early meetings and discussions, Pathfinder mission assurance details were tailored based on several key mission characteristics, including especially: short duration (8 months), rigid cost cap (\$ 150M), high entry and landing accelerations (design for 100 g’s), and severe Mars surface thermal cycling (-100°C night to 0°C to 20°C during the day). The first 2 led to a generally Class “C” approach but with planetary upgrades as appropriate. The environmental extremes led to a full Class “A” environmental test program.

Similarly the instruments and micro-rover “Sojourner” were tailored towards a then traditional Class “D”, but with planetary upgrades and a good test program.

All tailoring was done jointly between the Mission Assurance Manager and several key project personnel. This is an early Pathfinder example of “concurrent engineering” that became one of the theme success stories of the project.

It is significant that none of these early “conscious engineering decisions” was later changed or waived. Only environmental design and test details (levels, durations, etc.) evolved over the project development.

Documentation of Mission Assurance Plans and Requirements was reduced dramatically. The Cassini Project has about 10 different documents with a total of more than 1500 pages. On the Pathfinder project, these were all combined into a loose-leaf binder with only 250 pages. On more recent projects this total has been reduced to less than 80 pages.

Table I contains a summary of the “meat” of the Mission Assurance program and compares it with more traditional approaches (i.e. Class A). This table is the basis of the rest of the detail of this paper.

Concurrent engineering and collocation were major tenants of the Pathfinder project. The following key members of the Mission Assurance staff were collocated with the main body of project personnel in a somewhat "skunkworks" environment:

- Mission Assurance Manager
- Environmental Requirements Engineer
- Project Reliability Engineer
- Electronic Parts Manager
- Project Quality Assurance Engineer
- One Quality Assurance inspector
- Software Assurance Engineer

Collocation was a major key to the real effectiveness of "concurrent engineering". Many, many decisions could be reached in a matter of hours or even in hallway discussions, rather than the traditional serial paper approach, which takes days, weeks or months.

## 2. ELECTRONIC PARTS PROGRAM

The short mission duration (7 months cruise, 1 month minimum surface operations), allowed the potentially higher risk decision to use Grade 2 (Class B), MIL 883B as the minimum parts quality for the basic spacecraft. Studies performed over the years have shown parts failure rates significantly decreasing as the manufacturers improve their processes with time. In fact, it was felt that Grade 2, Class B parts of 1993 had failure rates equal to or less than the Grade 1, Class S parts of the early 1970s Voyager spacecraft vintage. This trend made the decision to accept the risk easily acceptable.

Another important aspect that reduced this risk even more was the fact that many parts would be obtained from Cassini project spares or three concurrent Cassini/Pathfinder parts purchases. The following statistics are of interest:

### Pathfinder Parts Summary

Its:

- >40% part types are Class S remainder Class B

Actives (Transistors, Diodes, Relays):

- 34% part types are Grade 1 remainder Grade 2

Passives (Resistors, Capacitors):

- Essentially all are Grade 1 (Cassini common buys)

Parts program documentation was simplified and included in the single Mission Assurance loose-leaf binder. In addition, the "formal approved parts list" was simplified to an "informal parts list" which contained all needed information.

A significant element of the electronic parts program was the empowerment of the Parts Manager. Traditionally such a person had teams of specialist reviewing the "formal" parts lists and providing detailed evaluations of any non-standard parts or any other concern. On Pathfinder, the Parts Manager could decide on any parts issue based on his own

experience, or bring in the experts as he saw fit: there were no rigid requirements.

The Parts Manager in conjunction with the Project Procurement Manager developed and implemented a streamlined parts procurement process. Very early in the project, part procurement was being done in a traditional manner with large amounts of paperwork and Laboratory rules slowing the process to the point of failure. The streamlined method reduced the paper flow time to days (or less) versus traditional weeks (or even months). A new raised upper limit on the dollar value of any procurement without high level management signature was also instituted.

Incoming inspections of parts costing less than \$100 were eliminated based on a Quality Assurance survey that found a very small return on such inspections. Only about 20% of incoming lots were inspected, saving several work years of cost.

Destructive Physical Analyses (DPA's) on all lots of parts were eliminated in favor of selected DPA's based on vendor histories. In one case, this "bit" the project later. Another project using the same particular item from a well qualified vendor did the traditional DPA's on all lots, and found a problem in the lot used on Pathfinder. This resulted in a changeout of 7 parts on the Pathfinder electronics.

For Mars Pathfinder, which flew its entire mission during a solar minimum period, the TID was estimated to be only 40 rads. As small as this was, the design requirement was arbitrarily raised to 200 rads (0.2 Krads). Compare this to near earth environments of 1 to 10 Krads/year, and Galileo/Cassini design requirements of 100 to 160 Krads! This integrated dose was so low that no design decisions were affected by it.

The other space radiation aspect of Single Event Effects (SEE) had more of an impact on the design. The environment is what's known as Galactic Cosmic Ray background which is at its highest level when the Sun is not active. Several parts in the main computer system were sensitive to SEE: the processor; the Field Programmable Gate Arrays (FPGA's); and especially, the Dynamic Random Access Memory stacks (DRAM). These DRAM's were of a newer design which had internal correction code for "single" bit upsets; in other words, such errors were undetectable. The parts architecture is quite complex. Radiation testing of these DRAM parts showed that a new phenomena involving error bursts would occur. After a significant analysis and test program, estimates of these error bursts were made as follows: "upper bound" of 120 during the 8 month mission (one every 2 days); and a "best" estimate of 26 (one every 10 days). The later number is not "most likely", but represents a reasonable design value for missions willing to accept some risk. Therefore the Pathfinder fault protection hardware was designed to accommodate at least the "best estimate" error bursts.

As an interesting "war story", several months of cruise went by on Pathfinder without any evidence of "error bursts" or

SEE's of any kind. An in-depth review of all assumptions leading to both "upper bound" and "best estimates" was performed. When all conservatism and uncertainties are removed from the estimating process, the "most likely" error burst rate was about 1 in an 8 month mission. After 2 months on the surface (9 months total), an event occurred which might have been a SEE (but likely not in the DRAM, but in an FPGA!).

Probably the biggest success story of the Pathfinder Parts Program was the fact the parts deliveries (though later than originally desired in many cases) did not significantly affect any hardware deliveries. This is very unusual at JPL.

### 3. RELIABILITY ASSURANCE PROGRAM

The short Pathfinder mission duration (8 months) allowed the possibility of reducing cost and mass significantly by designing an essentially single string spacecraft. Early reliability studies focused on assessing the risk of such a dramatic decision.

JPL historical flight failure records showed the need for redundancy in the following subsystems/assemblies in order of priority:

Gyros (none on Pathfinder)  
Mechanical Tape Recorders (none on Pathfinder)

Telecom

Computer Memory (not CPU)  
Batteries

Another very early reliability activity was the development of a 10000 part single string reliability model. It used typical planetary spacecraft parts types and distributions for the engineering subsystems since no design yet existed. Early results using straight MIL STD-217D parts failure rates were unbelievable. The engineer involved instituted a different statistical method she was developing which accounted for actual flight failure data. This resulted in probability of success predictions that seemed reasonable. Comparative reliability trends for various trades were made at this point.

One interesting result was the prediction that 2 single string spacecraft (even launched on the same Delta II booster) had a slightly higher probability of success than one fully redundant spacecraft. At this point, many of us within the project began pushing such an approach since it was identical to early JPL Mariner projects which had great success (always at least one spacecraft worked). Even though the early estimate of the cost of the second spacecraft was only about 20% that of the first, funding was not available.

Another trade study with this reliability model showed that the biggest single return for a redundant subsystem was a backup transmitter. Note the consistency of this result with the earlier listed JPL failure history. Much later in the project, a small emergency backup transmitter was

implemented on Pathfinder and was successfully demonstrated recently.

The final spacecraft design is anything but truly single-string as shown in Table II. Full redundancy exists within many subsystem elements. Graceful degradation and functional backup existed in much of the design. Of particular concern throughout the design development was the large number (54) of pyrotechnique events during Entry Descent and Landing. From the very beginning, the pyro devices had traditionally redundant firing circuits and NSI's (NASA Standard Initiators). Of interesting note, many claim JPL has never had a pyro device firing failure, but, of course, there is no data on which redundant device actually performed the function!

The main single string elements are the Attitude and information Management (AIM) subsystem elements. This includes the main (and only) computer, and its associated interface and power assemblies. The computer memory has tremendous margin (128 MBytes vs. <300 Kbytes needed for operation). This is, again, consistent with the JPL historical failure data noted above.

The very early tailoring of the reliability assurance program for Pathfinder led to the following analyses requirements based on historical value-added assessments:

- No circuit FMECA'S (Failure Mode Effect Criticality Analysis)
- Do interface FM ECA's between subsystems (2 of 3 major interface analyses led to very simple design modifications to reduce failure propagation across the interface)
- Do Parts Stress Analyses (derating) on all new (therefore most) designs. Relatively few issues found, generally relative to part junction temperatures and one or two power derating issues: all easily resolved.
- Worst Case Analyses (WCA's) not required (based on low radiation dosage and short mission duration). Substitution of a temperature - voltage - frequency margin test was highly recommended and generally implemented. Some designers chose to perform WCA'S as well. One interesting issue occurred with the flight computer at below +5°C. Even a WCA had not shown this noisy circuit, whereas the test identified the problem (replacement of a "noisy" part eliminated the issue).
- A System Failure Modes/Fault Tree Analysis was performed and upgraded periodically. This was one of the major elements of the risk management approach on Pathfinder. Where both the consequences and probability of failure were high, risk mitigation might take this form of a more robust design, more developmental/qualification testing, or as noted previously, some form of redundancy. Use of project reserve dollars was based to a great extent on the results of these analyses.
- Thermal analyses of circuit boards to the piece-part level was not required; however, most designs of the main engineering subsystems were analyzed. These

supplemented the parts-stress (derating) analyses mentioned above. Cost of these analyses were somewhat less than traditional. As design becomes more automated, thermal analyses costs should plummet such that they should always be done.

- Single event analyses were performed on a selected basis and are discussed in the prior Electronic Parts Program section.

Documentation of reliability analyses were informal. No formal independent reviews of such analyses were required (as compared to traditional projects). The single Project Reliability Engineer (who was collocated with Project personnel) worked concurrently with the Design Engineers to assess adequacy of the analyses in support of the designer.

The Pathfinder review program emphasized “informal Peer reviews” for most subsystem and lower levels. In this process, non-project technical peers work around the table with drawings, procedures, requirements, etc. Over 100 of this type of review were used from small I complex mechanical assembly designs up to major subsystems. In general, one peer reviewer would maintain a list of advisories and action items for later disposition. All advisories and action items were resolved with conscious engineering decisions. Formal reviews were intended to be limited to system PDR, CDR, Pre-Ship, and Pre-Launch. External influences resulted in additional Independent Annual Reviews, some of which were combined with formal reviews. The informal peer reviews provided by far the greatest value-added. Preparation for formal reviews did promote order in a programmatic sense. The biggest single value-added recommendation from a formal review was to increase project reserves from \$40M to \$50M very early in the project.

Electronic operating time was established very early as: 200 hrs prior to system integration; 1000 hours at the system level with a goal of 2000 hours. Actual system hours were 2700 hours. This was accomplished by design software and Ground Support Equipment to allow around-the-clock operation, primarily in the cruise mode with automatic shutdown features and one guard. Later “reliability growth” studies implied that perhaps only 500 hours would be a minimum requirement, however the Pathfinder success implies that the higher number of hours adds value. It should be noted that the number of problems encountered with hardware after system integration was quite small (less than 20). This implies that the Pathfinder team may have done something during subsystem development that led to higher reliability.

The Pathfinder project instigated a new electronic Problem/Failure Reporting (P/FR) system that saved a great deal of resources. A “problem log,” electronic format was created. Cognizant engineers found it useful in comparison to paper log-books. All problems were logged, On an almost-daily basis, a concurrent engineering team (generally including the Project Reliability Engineer) would make conscious decisions on which problems should be elevated to a “formal” P/FR. If the source of the problem was well understood and solvable, and its potential impact on the

mission was small, it was not made formal (contrary to JPL traditional approaches). [It was, however, kept in the electronic log database. Making any problem a “formal” P/FR required only one keystroke. Closure of “formal” P/FRs was generally done on a regular basis with a concurrent team involving a member of the Mission Assurance team. Metrics of the Pathfinder P/FR system are impressive: only ~200 total P/FR’s (vs. >1000 normal, with Galileo >4000, and Cassini ~3000); total number of problem logs ~1000 (similar to traditional formal P/FRs, but with much faster and less costly closure); “Formal” P/FR closure cost estimated at \$3K each (versus traditional cost of \$ 10K to \$20 K). Several million dollars appear to have been saved, and this system is now the basis of JPL’s institutional Problem/Failure Reporting System.

The reliability model mentioned early in this section was updated near the end of spacecraft development to include actual flight parts/quality and actual single string/redundant designs. The final predicted electronic subsystem probability of success was about 90%. A correlary reliability study of all the entry, descent and landing (EDL) events had been done earlier with an approach where all design engineers were interviewed as to both the probability of success and uncertainty in that probability for their particular event. Original results were about 78% mean probability of success with about a 20% uncertainty. The final interviews resulted in about 90% probability of success with about a 10% uncertainty. Thus the total probability of success was about 80%. (0.9 electronics x 0.9 EDL) It should always be understood that absolute values of probability of success are dependent on assumptions. Dramatic differences can result from seemingly minor changes in assumptions. JPL does not traditionally publish such results, especially when another project using similar (but not identical) approaches might not be as successful.

#### 4. MISSION ENVIRONMENTS PROGRAM

An instantaneous initial philosophy for the Mars Pathfinder project was -- test - test - test! In order to meet the extremely low cost-cap, the entire early team saw the necessity of testing as a way to mitigate the risks inherently associated with this Mars landing mission. This “mindset” extended to the environmental test program.

Most JPL Class “C” programs (when there were classes), such as Pathfinder, tended to defer all environmental tests to the system level. It was clear from the beginning that there were two major environments that JPL was not used to accommodating: 1) Entry and Landing loads of 10’s of earth g’s; and 2) Severe thermal cycling on the surface of Mars (maybe -100°C to +20°C). Because of these two extreme environments, it was initially proposed to do a traditional assembly subsystem level test program as well as a system test program. These initial test recommendations are shown in Table 1 for both assembly and system level.

Of special note is the fact that none of these tests were deleted as the project evolved. [In fact several significant tests were added, including early thermal-vacuum characterization tests, and a full-up flight lander

electronics/base-plate centrifuge test to simulate landing loads.

The allowable maximum earth "g" level at landing received significant early attention, even before a firm decision to use airbags as the main landing deceleration technique. An industry wide peer review<sup>7</sup> was held in August 1992 to assess electronic packaging and mechanisms technology capability for high "g" loads. The industry consensus was that normal packaging could withstand 10's of g's, but not 100's of g's without expensive ruggedization. This evolved to a general philosophy that the airbag system should limit landing loads to less than 50 g's, but that hardware should be designed for 100 g's wherever practical.

The thermal cyclic environment of Mars (about -100°C to +20°C) presented various challenges. Since there was little or no power available for nighttime heaters, it was obvious that the traditional lower generating qualification temperature of -20°C would have to be extended. Electronic part acceptance test levels are typically -55°C, so this set a lower bound for what our design goals might be. After much evaluation, the general range of thermal control for electronic engineering subsystems was about -40°C to +40°C. Since both the lander and rover Sojourner had well insulated electronic compartments due to the cold nights, internal heating during daytime operations led to the +40°C (vs. 0°C to +20°C external environment). Qualification test levels were generally -50°C (sometimes -55°C) to +70°C, the latter temperature being consistent both with JPL tradition and MIL STD 1540. Our tradition has been that a long hot operating dwell test at  $\geq 70^\circ\text{C}$  provides an excellent reliability demonstration, even if expected flight temperatures are much lower.

Another aspect of this surface environment is the large cyclic nature. Traditional JPL spacecraft have had little or no cycling. Developmental and qualification testing of various assemblies/subsystems and components for Pathfinder ranged from 35 cycles to 100 cycles, or in the case of solder joint issues, generally >200 cycles. The range for interval electronics was on the order of -50°C to +50°C (or more), external elements were generally 6 cycles over similar ranges in conjunction with the long hot operating tests mentioned above. Research completed during Pathfinder development indicated that only 2 cycles were generally sufficient from identification of design and workmanship discrepancies. This latter number was used for a few telecom assemblies to avoid additional costs and a contentious waiver process.

There were development tests far too numerous to list. These included many mechanisms for both the lander and rover, electronic packaging, etc. Emphasis of these tests covered both the high landing loads and the thermal cyclic conditions.

Thermal characterization tests of both a cruise (vacuum) condition, and landed (8 torr GN<sub>2</sub>) condition were performed resulting in some design changes.

Centrifuge tests were performed on both the rover and lander. Minor rover wheel modifications were indicated.

Lack of a system sine test resulted in some extra evaluations to satisfy NASA Headquarters. In essence, the small size of Pathfinder, and its compact no-appendage launch configuration were the bases of this decision.

Real problems found during assembly/subsystem and system environmental testing were relatively few.

System thermal vacuum in the cruise configuration showed propellant line and solar array temperature issues. These had not been analytically foreseen due to thermal modeling of the solar array that was too simplified. Some changes were made and an abbreviated retest of this configuration showed some improvement. However, the propellant line temperature issue was not completely solved. Later changes involving better multi-layer-insulation (MLI) on these lines were accomplished after STV. JPL's traditional philosophy has always been to retest design changes, but this was not possible at the system level. The Mission Assurance Manager (an thermal control engineer by prior experience) was prepared to "spend a silver bullet" with the Project Manager to assure some form of testing for these latter changes. However, in the concurrent engineering teaming spirit of the Pathfinder Project, no "bullet" was needed. The Flight System Manager decided to spend some of the very limited reserve dollars on an additional reasonably high-fidelity thermal test of the propellant lines.

#### 5. HARDWARE/SOFTWARE QUALITY ASSURANCE PROGRAM

From the beginning of the project, traditional hardware formal inspection points were challenged. All inspections performed were based on concurrent engineering design team/QA team decisions evolved throughout development. As noted earlier, incoming electronic parts inspections were eliminated for about 80% of the purchased part lots.

Electronic assemblies (slices) were originally anticipated to be entirely surface mount technology with automated soldering techniques. However, as the design evolved, about 40% of the parts had to be hand soldered. This led to the more traditional inspection of all solder joints (which we had hoped to avoid). No cost increase was noted which leads this author to believe that solder joint inspections are cost-effective.

As noted earlier, both the Project QA Engineer and one key inspector were collocated with the project and its Flight System Testbed. This enabled very rapid response for critical hardware inspections when needed,

In another change from tradition, supplier/vendor Quality Assurance methods were used to the greatest extent practical. JPL QA personnel reviewed their procedures, but only recommended changes when absolutely necessary. An example is one subsystem supplier who traditionally used only 1.75 power magnification for solder joint inspection. JPL studies had shown that 6X to 10X magnification was necessary for fine-pitched part leads.

Another change from tradition was elimination of a JPL QA representative resident at vendors. Roving JPL inspectors were employed instead, and usually only at certain critical points as requested by the vendor. One particular device vendor was having trouble with workmanship and other QA issues. JPL sent small teams a few times to help this company improve their quality and were successful in the final flight unit deliveries.

The JPL Quality Engineering personnel performed several early evaluations for the Pathfinder project. The Lander-Rover modems were commercial units which needed a few changes to meet upscreen testing for the landing shock and, especially, surface thermal cycling. The rover cameras were also commercial in nature and certain material changes were necessary as well as upscreening to about Class B equivalency. As previously noted, a power converter vendor was assisted and materials and processes support was supplied to the computer vendor.

One major lesson learned had to do with handling of highly sensitive devices (Charge Coupled Devices (CCD) in particular). No QA presence was required, and several devices were destroyed inadvertently. Two expensive German Imager for Mars Pathfinder (IMP) camera CCD's were damaged due to mechanical handling where a spacer was left out, Seven rover CCD'S were failed due to Electrostatic Discharge effects in handling fixtures. The "nickel and dimes" cost of a pervasive QA presence could have eliminated both of these incidents.

The Qualification Assurance activities after hardware delivery for system integration were not significantly different than traditional higher cost projects. However, the team was generally only 3 people.

Software Quality Assurance was dramatically different than tradition. One individual was assigned half-time as the QA engineer, and the other half time as part of the software development team. The traditional 25 formal documents were reduced to just a few. Software reviews were reduced from 15 formal reviews/inspection points to the previously mentioned peer reviews where real value was added.

## 6. SYSTEM SAFETY PROGRAM

System Safety (hardware and personnel) was uncompromised compared to traditional JPL projects. Facility reviews prior to use with flight hardware were conducted as normal.

A major product of System Safety is coordination of major formal reviews with KSC/Patrick Air Force Base personnel and their requirements. The traditional (shuttle based) 3 major reviews were reduced to 2 setting a new precedence for Expendable Launch Vehicle (ELV's).

The presence of 3 small Radioisotope Heating Units (RHU's) in the rover, and a small amount of Curium in the rover's Alpha Proton Xray Spectrometer (APXs) required special effort on the part of the System Safety engineer. Similarly the presence of the RAD solid motors required a

tiring circuit interrupt prior to just before launch as well as triple electrical redundancy.

One war story of interest occurred during parachute development testing in the vendor's Northeast locale. A helicopter drop test went awry, and a mass hit a farmer's cucumber truck. JPL bought him a new truck and few other items. This led to a review of safety implications in all subcontracts and some were found sorely lacking. Legal liability implications need to always be addressed in contracts.

## 7. OTHER WAR STORIES/LESSON'S LEARNED

Other incidents of interest include:

1) Parts lids rotated 180° on some Quad Comparator parts causing internal failures after the parts were installed backwards. Incoming QA inspection might have caught these.

2) Relay failures: One set had two relays demagnetized, another type failed and was found to have human contamination on the contacts (probably makeup).

3) Two flight unit DRAM memory stacks had solder joint failures in the upper portion of the stack. A vendor process change (which eliminated the potential for solder reflow), and a better thermal cyclic qualification profile were implemented. The original thermal test was so rapid that internal temperatures were not changing much at all. The bonding process for these stacks to the computer slice board was also changed.

4) Small cable cutters were consistently failing one way, or another, until the entire cutter body was made from steel instead of aluminum.

5) The waveguide transfer switch in the telecom subsystem was inherited from the Cassini project. Their qualification program showed many problems related to materials compatibility. Although the Pathfinder unit needed only a small number of operational cycles, it was changed out with the final redesign.

6) The Rocket Assisted Descent (RAD) motors suffered unexpected pressure oscillations very late in its development testing. A reduction in the amount of aluminum (2% instead of the more common 16%/0) was thought to be the source of acoustically induced oscillation. A return to 16% Aluminum was made for the flight motors.

7) A failed DC-DC converter was returned to the vendor for failure analysis. Delidding of this hybrid device required heating to 300°F. The hot plate used had a °C/°F switch. The switch was set to 300°C! The part was effectively destroyed.

8) An early developmental pyre-shock test of a lander solar array showed 50% of the solar cells had cracked. The extremely conservative test approach was replaced with a higher fidelity test setup, which was successful.

9) A flight power control unit was initiating Power On Resets in the Attitude and Information Management subsystem. A circuit noise fix that had been added to the Engineering Model had not been added to the flight unit!

### 8. CONCLUSIONS

A lower cost “common sense” Mission Assurance (MA) program is very doable in the right kind of concurrent engineering, flexible, teaming project environment. Set the MA requirements only at a high level and leave enough flexibility to avoid later waiver paperwork. Pathfinder had about 15 waivers total, one to wave rigid traditional software development requirements, and the rest were to waive Single Event Effect requirements (we could have stated these more loosely).

Early “tailoring” of the Mission Assurance program was successful as measured by mission success, no budget overruns, and the fact that no significant deviations from the early plans occurred throughout development. A summary of MA approaches versus key mission characteristics are shown in Table 3.

After the successful July 4, 1997 landing, the project Reliability Engineer looked back at the small number of problems which were found at the system level. In his opinion, these were far fewer than normal reliability growth theory. This may mean that the Pathfinder project did something or several things during subsystem development that truly enhanced reliability. We intend to continue to search for any buried positive lesson’s learned.

The original MA budget was about \$5M. When an early formal review board recommended an increase in reserves, the MA team was able to reduce our budget by \$800K. Much of this was elimination of planned failure analysis and parts radiation testing. About \$300K was finally added back in for these two activities.

As noted previously, the electronic parts procurement process is one of the project success stories. Project personnel attitude and empowerment of the parts manager contributed to this success. A full-up “Class A” environmental test program is doable with the right attitude of project personnel from the Flight System Manager on down.

This author observed that the rate of problem resolution equaled or exceeded the rate of problem occurrence. In particular, most problems were resolved in days not the traditional weeks or months.

Finally, this author is of the opinion that management of this Mission Assurance program was easy and fun. By setting a theme of teaming, flexibility and concurrent engineering early and throughout development, there were never any of the contentions issues between MA and the project that were frequent in earlier traditional JPL projects. This author has prior experience in the Apollo and Space Shuttle programs. Pathfinder was a better “team” environment than even the Apollo 11 Mission! It will undoubtedly remain the highlight of his career.

Table 1. Mars Pathfinder Mission Assurance

REQUIREMENT	CLASS A	CLASS C	PATHFINDER SPACECRAFT	CLASS D INSTRUMENT D-8966	PATHFINDER ROVER/ INSTRUMENTS
<u>PLANS</u>	Formal PA Plan	In PA Plans and Requirements	In PA Plans and Requirements	None Required	<b>In PA Plans and Requirements</b>
• RELIABILITY PLANS	Formal Reliability Plan	Formal Reliability Plan	In PA Plans and Requirements	None Required	<b>In PA Plans and Requirements</b>
• SINGLE POINT FAILURE	No Single Failure Points	Single Failure Points Allowed for Critical Assemblies	Single Failure Points Allowed, Selected Redundancy (Baseline)	Not Allowed for Personnel Safety	Not Allowed for Personnel Safety
<u>RELIABILITY ANALYSIS</u>					
• FMECAS	Circuit FMECAS Required	Not Required	None	Project Opinion	None
	Interface FMECAS Required	Assembly Interface	Subsystem/External Interface FMECAS	Interface FMECAS (Level II)	Interface FMECAS

REQUIREMENT	CLASS A	CLASS C	PATHFINDER SPACECRAFT	CLASS D INSTRUMENT D-8966	PATHFINDER ROVER/ INSTRUMENTS
• THERMAL ANALYSIS	Assembly/Pie ce Part Thermal Analysis Required	Not Required	Selected (AIM S/S)	Not Required	None
• PARTS STRESS ANALYSIS	Parts Stress Analysis Required	Required	New Assemblies (and Inherited Assemblies)	For Safety Only	None
• WORST CASE ANALYSIS	Worst Case Analysis Required	Temp/Voltage Margin Test May Be Substituted	Temp/Voltage Margin Test Will Be Substituted	Project Option	<b>Temperature Voltage Margin Test Will Be Substituted (Rover)</b>
• POWER SUPPLY TRANSIENT ANALYSIS	Power Supply Transient Analyses Required	Required	Required	Level II	None
• SINGLE EVENT ANALYSIS	Single Event Analyses Required	Required	Selected Analysis According to Environment	Not Required	<b>Selected</b>
• DOCUMENTATION	All Analysis Formal	Formality Project Option	Cog E's Notebook	Informal except for Personnel and Launch Safety Project Option	Cog E's Notebook
• INDEPENDENT REVIEW	All Analyses Independently Reviewed	Project Option	Reviewed Simultaneously With Cog E	Project Option	Reviewed Simultaneously With Cog E
• PERFORMANCE TREND ANALYSIS	Performance Trend Analysis	Project Option	None	Not Required	None
<u>REVIEWS</u>	Hardware and Software Requirements Review; Subsystem Inheritance; System PDR/CDR; Subsystem PDR/CDR; Pre-Environmental I System Test Review; HRCR; Pre-Ship	Hardware and Software Requirements Review; Subsystem Inheritance; System PDR/CDR; Pre-Environmental System Test Review; HRCR; Pre-Ship	PDR/NAR; Less Formal Subsystem Inheritance; Subsystem Informal Peer Review; System PDR/CDR; Pre-Environmental System Test Informal Peer Review; Pre-Ship (MOS, System); Pre-Launch	Project Option	Informal Reviews and Participation With Spacecraft Reviews
<u>ELECTRONICS OPERATING TIME</u>	Assembly Level 1000 Hours	200 Hours	200 Hours	200 Hours In Assembled Configuration	200 Hours at Instrument Level

REQUIREMENT	CLASS A	CLASS C	PATHFINDER SPACECRAFT	CLASS D INSTRUMENT D-8966	PATHFINDER ROVER/ INSTRUMENTS
	System Level I 500 Hours	300 Hours	1000 Hours	See Above	<b>None Required, But Will Accumulate Hours During System Test</b>
<b><u>PROBLEM FAILURE REPORTING</u></b>					
	Formal PFR Plan	Formal Plan	PA Plan and Requirements	Project Option	PA Plans and Requirements
	Initiated at First Application of Power at Subassembly; PAM Controls	Initiated at First Assembly Test; PAM Controls	Initiated at First Assembly Acceptance Test; PAM Controls	Developmental PFR System Directed By Project; PAM Controls	Developmental at First Application of Power to Flight Boards
	Closure Includes Cog E and Section, Reliability Engineer, PAM (PM if Red)	Same for Red Flag, No Reliability Engineer for Non-Red	Concurrent Closure	Project Option	Cog Section/Tech Manager
<b><u>ELECTRONIC PARTS</u></b>					
• PLAN	Formal Parts Plan	Informal Project Plan	PA Plans and Requirements	Project Option	PA Plans and Requirements
• FORMAL API.	Formal Approved Parts List	Optional	Informal Parts List	<b>Informal Parts List</b>	<b>Informal Parts List</b>
• PARTS SELECTION	Grade 1 Parts Required	Grade 1 or 2 Parts Allowed	Grade 2 Parts <b>Upgrade When Smart</b>	Commercial Parts Acceptable	<b>Grade 2</b> and Commercial Parts
	Formal Nonstandard Parts Approval	Formal Nonstandard Parts Approval	<b>Nonstandard Parts Approval by Parts Manager</b>	Project Option	None
• DESTRUCTIVE, PHYSICAL ANALYSIS	Required - All Lots	Required - All Lots	<b>Selective Based on Vendor History</b>	None Required	None
<b><u>ENVIRONMENTAL PROGRAM</u></b>					
• DOCUMENTS	11 Formal Documents (7 Documents, 4 Forms)	6 Formal Documents (3 Documents, 3 Forms)	<b>Reduce to 1 Formal Document (3 Forms)</b>	Project Option	One Document

REQUIREMENT	CLASS A	CLASS C	PATHFINDER SPACECRAFT	CLASS D INSTRUMENT D-8966	PATHFINDER ROVER/ INSTRUMENTS
• DESIGN	Design Requirements Include Significant Margin	Slightly Less Margin	Full Class C	Only Slightly Less Rigorous Than Full Class C/Per D-9589 (Structural Load Req is Minimum)	Full Class D
• ASSEMBLY TESTS	Required: - Sine - Random Thermal Vacuum Thermal Cycle (As Required) - 'MC Conducted and Radiated - ESD	<b>Usually Deferred to System Level:</b> - Sine (If Resonance <5(1Hz) - Random - Thermal Vacuum - Thermal Cycle (As Required) - EMC As Required - ESD As Required	<b>Required:</b> Landing G Loads - Random - Thermal Vacuum - Thermal Cycle (As Required) - EMC (Selected Hardware Tested Early; Radiated Deferred to System Level) - ESD Not Required	"Level II Requirement" Level	Deferred to Instrument Level
• SYSTEM TESTS	- Sine - Acoustic - Pyro Shock (Selected) Thermal Vacuum >300 Hours - EMC Radiated Tests - ESD Required	- <b>Sine (If Resonance &lt;50 Hz)</b> - Acoustic - Pyro Shock (Selected) - Thermal Vacuum >100" Hours - EMC Radiated - ESD Required	- Acoustic Pyro Shock (Selected) - Thermal Vacuum >400 Hours - EMC Radiated - ESD <b>Not</b> Required	Level I [ Requirements	Instrument: - Random Vibration - Landing Loads - Thermal Vacuum - Thermal Cycle

QUALITY ASSURANCE

• PLAN	Formal QA Plan	Inspection and Audit Plan	<b>PA Plans and Requirements</b>	Level I [ Requirements	<b>PA Plans and Requirements</b>
• QA REP	JPL QA Rep, Resident at Major Suppliers	No Requirement	use of <b>Supplier's QA Procedures, Roving JPL Inspectors</b>	QA Surveillance is Project Option	ICD Verification Only
• WORKMANSHIP	Workmanship Configuration Verification, Test, Etc., 100% Required	Required at Assembly Level and Up	<b>Required at Assembly Level and Up (Lower as Determined By Concurrent Design/QA Team)</b>	Level II Requirement	ICD Verification

REQUIREMENT	CLASS A	CLASS C	PATHFINDER SPACECRAFT	CLASS D INSTRUMENT D-8966	PATHFINDER ROVER/ INSTRUMENTS
-------------	---------	---------	-----------------------	---------------------------	-------------------------------

SOFTWARE PRODUCT ASSURANCE

• DOCUMENTS	25 Formal Documents	20 Formal Documents	3 <b>Formal Documents</b>	Project Option	<b>None (Included in Spacecraft Software Documents)</b>
• REVIEWS	15 Reviews/Formal Inspection Points	10 Reviews/Formal Inspection Points	<b>Software Design and Acceptance Peer Reviews with System Review</b>	Project Option	

**Table 2.** Mars Pathfinder Flight System “Redundancy”

COMPONENT	REDUNDANCY, BACKUP, or GRACEFUL DEGRADATION.
“ELECTROCOMMUNICATIONS: - DST Exciter, SSPA, TMU- 1 - SSPA PCU - HGA	- AXT, TMU-2 Backup. - Redundant, each on own relay. - LGA Backup (Landed Ops.).
<b>POWER &amp; PYRO</b> - Cruise Solar Array - Lander Solar Array - Lander Battery - Lander Thermal Battery - Backshell Thermal Battery - PDU Relays (Critical loads: Petal Acts. 1,2,3; DST+CDU; IMP; CPU; PDE Drive; LPCU; TMU1; DSA; AIM ACCEL; Radar Alt.) - Load Fuses - PSA (Lander& Backshell) - Cruise & Lander Shunt Limiters - Dead face Relays	- Parallel diode isolated cell strings, graceful degrad. - Parallel diode isolated cell strings, graceful degrad. - Daylight operations only, mission degradation - Dual redundant - Dual redundant - Dual redundant, each relay <i>with</i> dual wiper  - Dual redundant - Dual redundant Pyro Relays & NSI’s - Interanlly redundant - Dual redundant
<b>AIM</b> - DRAM Memory - EEPROM Memory - Star Scanner Head & Electronics - Cruise Sun Sensor	- Graceful degradation - Graceful degradation - Dual Redundant, except Optics & Detector - Redundant Heads
<b>Devices</b> - Pyro devices: Cruise Sep; Petal Latch; B/S Cable Cutter; Lander-B/S Sep/Bridle Deploy; HRS Vent; C/S Cable Cutter, HGA Release, Airbag Retainer; RAD Firing; Incremental Bridle Cutter; Parachute Deploy, Heat Shield Rel; Heat Shield Cable Cutter.	- Redundant NSI’s, all
<b>Thermal</b> - Heaters: Lander Battery, Prop Tanks/Lines, Valve/PDM, RAD/Gas Gen, Airbag Retraction Motors, Petal Act. - Thermostats: Prop Tanks/Lines, Valve/PDM, RAD/Gas Gen - HRS Pump Assy, Electronics, & Bypass Valve	- Redundant circuits  - Series redundant  - Dual Redundant

Propulsion - Thrusters - CAT Bed Htrs	- Dual Thruster Branches - Redundant heater elements
Science - IMP Mast Depl., Sci. Mast Rel. (ASI) - Rover RF Modem PCU - Rover Release - Rover Ramps - APXS Deploy	- Redundant NSI's - Redundant - Redundant Pyre's with redundant NSI's - Redundant - Limited use possible, if deployment failure

**Table 3.** Mission Characteristics versus Mission Assurance Approaches

Characteristic	Mission Assurance Approach
<ul style="list-style-type: none"> <li>•Mission Duration (7 month cruise, 1 month surface operations)</li> </ul>	<ul style="list-style-type: none"> <li>•Grade 2 (Class B) electronic parts</li> <li>•Selected (not full) redundancy (also simplifies fault protection software)</li> </ul>
<ul style="list-style-type: none"> <li>•Severe Landing environment and surface thermal cycling environment</li> </ul>	<ul style="list-style-type: none"> <li>•Full-up assembly/subsystem and system environmental test program</li> </ul>
<ul style="list-style-type: none"> <li>•Rigid Cost Cap (\$150 in 1992 dollars, \$17 1M real year dollars)</li> </ul>	<ul style="list-style-type: none"> <li>• Dramatically Reduced Documentation</li> <li>• Reduced "Formal" Quality Assurance inspection</li> <li>• Use of vendor's QA methods</li> <li>• Simpler Software Assurance</li> <li>• Elimination of some expensive reliability analyses</li> <li>• No independent review of reliability analyses</li> <li>• Far less expensive Problem Failure Reporting System</li> </ul>
<ul style="list-style-type: none"> <li>•Very Low Radiation Environment</li> </ul>	<ul style="list-style-type: none"> <li>•Elimination of any concern relative to Total Ionizing Dose radiation design/testing.</li> </ul>