Prof. Dr. Holger Schlingloff

Institut für Informatik der Humboldt Universität

und

Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik

FIRST

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

- Aufgabe: Landung auf der Marsoberfläche und Übertragung von Messdaten
  - Suche nach Wasser / Klimaänderung/ Lebensspuren
  - Stimuliert von extrem erfolgreichen Vorgängermissionen
- " faster, cheaper, better" - Politik der NASA
  - (z.B. keine Telemetrie während der Landung)
- LAUNCHED: Jan 3, 1999
  LOST: Dec 3, 1999
  - Sonde meldet sich nach der Abtrennung nicht mehr

- December 3, 1999 11 a.m. PST

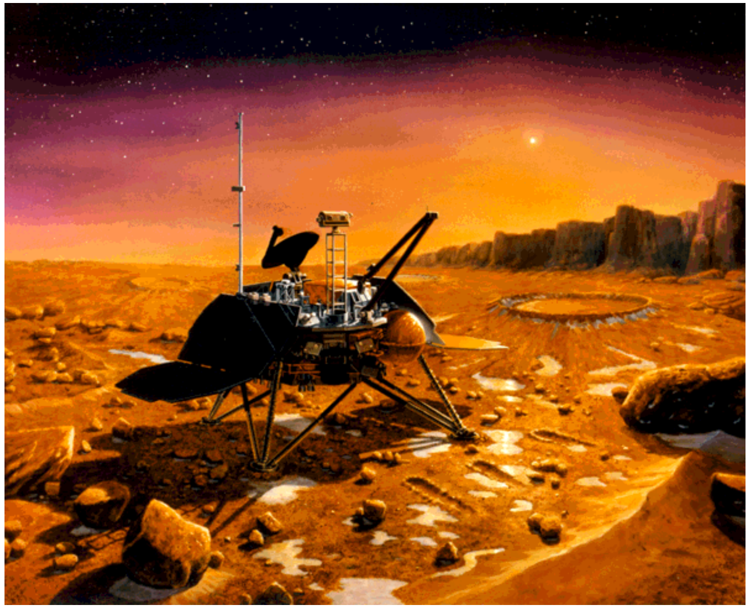
  NASA's Mars Polar Lander is performing flawlessly and poised to land on the layered terrain near the red planet's south polar region shortly after noon Pacific time today.
  "It seems to be coming in pretty much right on the target line," said Michael Watkins, manager of JPL's navigation and mission design section.

- December 3, 1999 5 p.m. PST

  Mission controllers for NASA's Mars Polar Lander mission are awaiting the next opportunity to communicate with the spacecraft, whose transmissions have not yet been received since it landed on Mars today.
  "I'm very confident the lander survived the descent," said Mars Polar Lander Project Manager Richard Cook at JPL. "Everything looked very good. I think we're a long way from getting concerned. It is not unexpected that we would not hear from it during the first opportunity." A variety of hardware problems from which the lander could recover may be responsible for the delay in initial telecommunications.

- December 4, 1999 5:45 p.m. PST

  One scenario that would explain why engineers have not yet heard from the lander is that the spacecraft entered standby, or "safe mode," about 20 minutes after landing shortly after 12 noon PST Friday, Dec. 3. If the lander entered safe mode at that time, it would not be able to receive any communication until it "wakes up" this evening.



?

- December 7, 1999 01:45 AM PST

  Mission controllers for NASA's Mars Polar Lander acknowledge that they hold out very little hope of communicating with the spacecraft, but they vow to learn from the experience and continue exploring the Red Planet.

- December 10, 1999

  Review boards will be set up within JPL and at NASA to study the cause of the apparent loss and explore ways to prevent a recurrence.

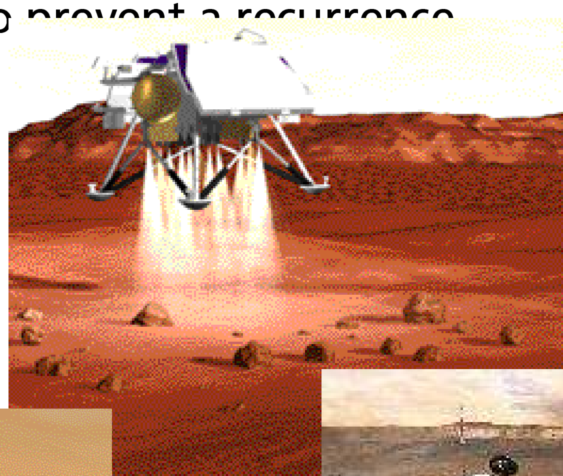
- January 17, 2000

  The Mars Polar Lander flight team has ended all attempts to regain communications with the spacecraft

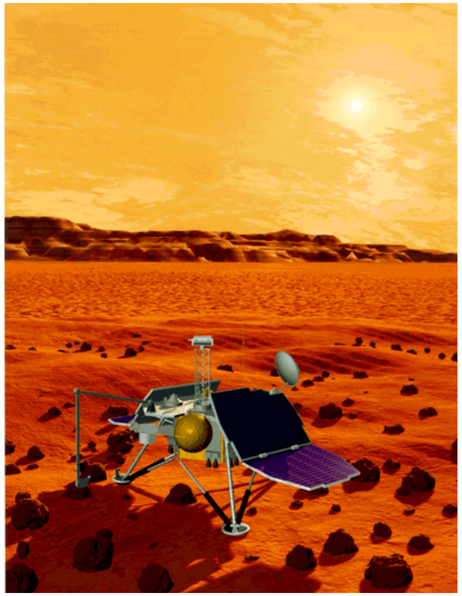
- March 28, 2000

  Mars review reports are now available

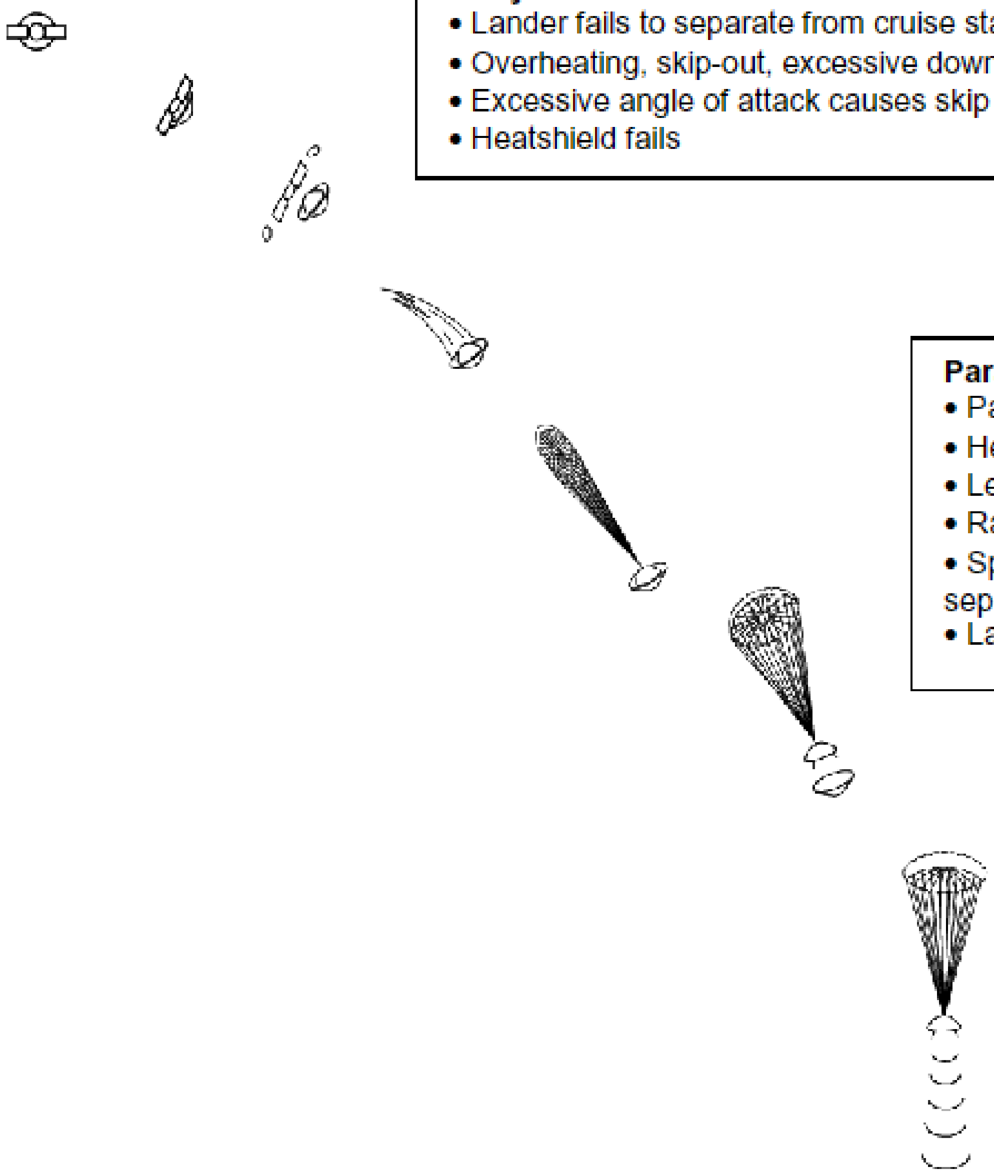
  z.B. http://www.dcs.gla.ac.uk/~johnson/Mars/mpl



- Projektverlust:
  $110 million for spacecraft development, $10 million mission operations; total $120 million (not includding launch vehicle or Deep Space 2 microprobes)
- Schlimmer noch:
  A CDROM with 932.816 names was carried on the lander



- Analyse der möglichen Fehlerursachen
    - Loss of control due to center-of-mass offset
    - Heatshield fails due to micrometeoroid impact
    - Loss of control due to dynamic effects
    - Backshell/parachute contacts lander
    - Premature shutdown of descent engines
    - Landing site not survivable
    - Surface conditions exceed landing design capabilities
- Bewertung durch Simulation und Berechnung der Eintretenswahrscheinlichkeit
- Da keine Flugdaten aufgezeichnet wurden, existiert kein ultimativer Beweis



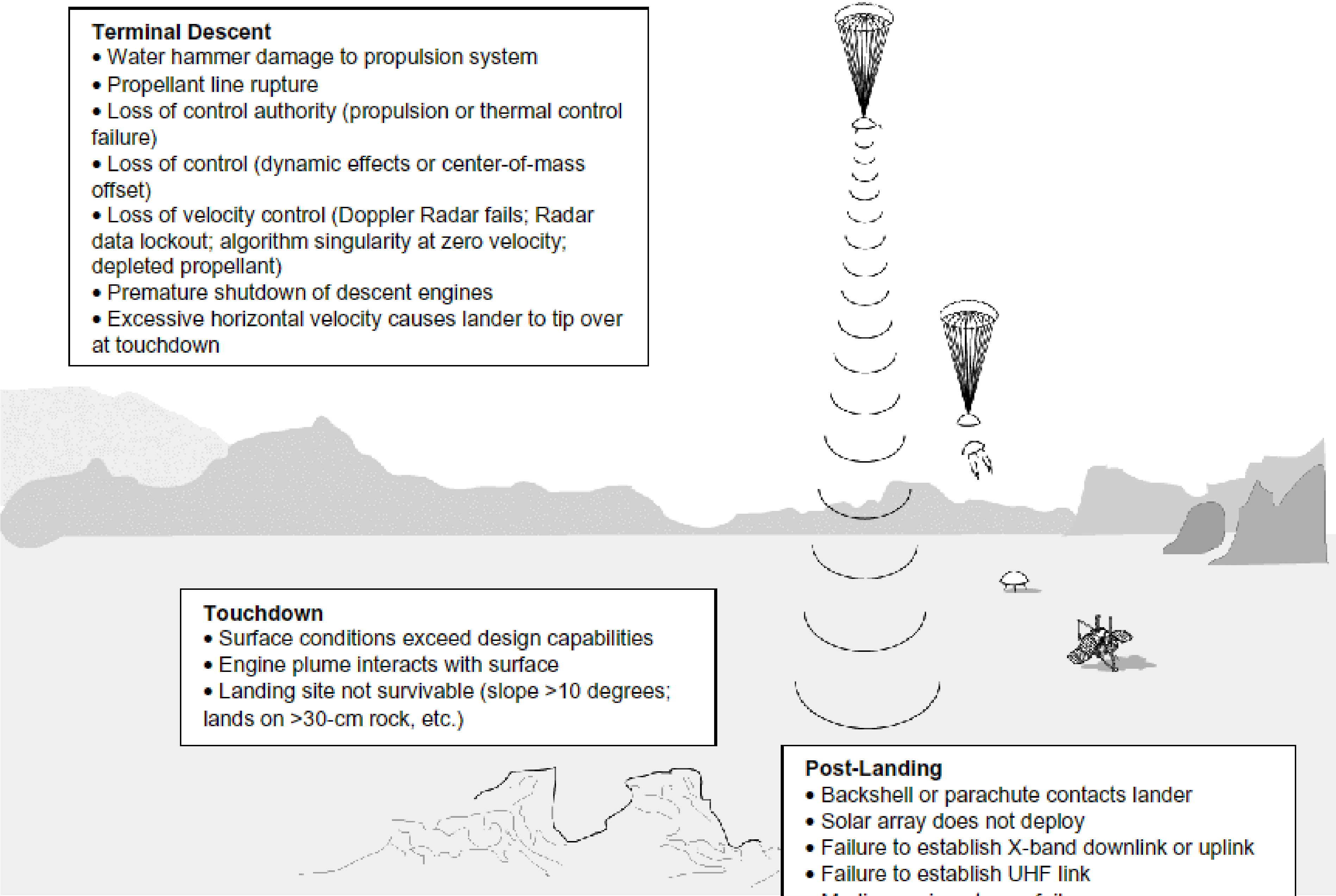
Entry
- Lander fails to separate from cruise stage
- Overheating, skip-out, excessive downtrack entry points
- Excessive angle of attack causes skip out or high-velocity impact
- Heatshield fails

Parachute Phase
- Parachute fails to deploy or fails to open
- Heatshield fails to separate
- Legs fail to deploy
- Radar fails (altimeter)
- Spurious Radar return from heatshield causes lander to separate prematurely
- Lander fails to separate from backshell

Common to EDL Phases
- Flight software fails to execute properly
- Pyrotechnic events fail
- Propulsion component fails
- C&DH subsystem fails
- Freezing temperatures at propellant tank outlet

Terminal Descent

- Water hammer damage to propulsion system
- Propellant line rupture
- Loss of control authority (propulsion or thermal control failure)
- Loss of control (dynamic effects or center-of-mass offset)
- Loss of velocity control (Doppler Radar fails; Radar data lockout; algorithm singularity at zero velocity; depleted propellant)
- Premature shutdown of descent engines
- Excessive horizontal velocity causes lander to tip over at touchdown



Touchdown

- Surface conditions exceed design capabilities
- Engine plume interacts with surface
- Landing site not survivable (slope >10 degrees; lands on >30-cm rock, etc.)

Post-Landing

- Backshell or parachute contacts lander
- Solar array does not deploy
- Failure to establish X-band downlink or uplink
- Failure to establish UHF link
- Medium-gain antenna fails

PARACHUTE PHASE	
Failure Mode	**Assessment**
Parachute fails: —Failure to initiate parachute deployment —Pyro/mortar failure —Chute fails to open	PLAUSIBLE BUT UNSUPPORTED. High reliability, test verification, and Mars Pathfinder similarity of the pyro/mortar deployment system make its failure unlikely. The chute is a pure heritage item from Pathfinder. Although there was not an extensive qualification program as part of the Pathfinder design phase, the Pathfinder chute did, in fact, work, thus providing at least one successful occurrence. The deployment conditions are different from Pathfinder, but are less severe. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.3 and Section 7.6, paragraph 3.f.
Heatshield fails to separate.	PLAUSIBLE BUT UNSUPPORTED. A failure of the heatshield to separate could prevent lander separation. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.4.
Legs fail to deploy.	PLAUSIBLE BUT UNSUPPORTED. A failure of one or more legs to deploy could cause significant damage to the lander at touchdown. Design and test verification of leg deployment was adequate. See Section 7.2.5.

FLAG E Premature shutdown of descent engines. MOST PROBABLE CAUSE OF LOSS OF MISSION	PLAUSIBLE. A magnetic sensor is provided in each of the three landing legs to sense touchdown when the lander contacts the surface, initiating the shutdown of the descent engines. Data from MPL engineering development unit deployment tests, MPL flight unit deployment tests, and Mars 2001 deployment tests showed that a spurious touchdown indication occurs in the Hall Effect touchdown sensor during landing leg deployment (while the lander is connected to the parachute). The software logic accepts this transient signal as a valid touchdown event if it persists for two consecutive readings of the sensor. The tests showed that most of the transient signals at leg deployment are indeed long enough to be accepted as valid events, therefore, it is almost a certainty that at least one of the three would have generated a spurious touchdown indication that the software accepted as valid. The software — intended to ignore touchdown indications prior to the enabling of the touchdown sensing logic — was not properly implemented, and the spurious touchdown indication was retained. The touchdown sensing logic is enabled at 40 meters altitude, and the software would have issued a descent engine thrust termination at this time in response to a (spurious) touchdown indication. At 40 meters altitude, the lander has a velocity of approximately 13 meters per second, which, in the absence of thrust, is accelerated by Mars gravity to a surface impact velocity of approximately 22 meters per second (the nominal touchdown velocity is 2.4 meters per second). At this impact velocity, the lander could not have survived. See Section 7.7.2.

- Wahrscheinlichste Ausfallursache: Absturz
- Magnetsensoren in Landegestell zur Abschaltung der Landetriebwerke bei Bodenkontakt
  - ein Sensor pro Bein, Abschaltung beim ersten Kontakt
  - Beine werden in 1500m Höhe ausgefahren
- Sensoren geben manchmal bereits beim Ausfahren der Beine ein Signal
  - 10 ms sampling Zeit
  - Signal wird um Rauschen korrigiert (nur gültig wenn es mehrere Zyklen andauert)
  - kommt mit hoher Wahrscheinlichkeit vor (5-33 ms im Test)
- Software beachtet dieses Signal als gültiges Anzeichen der Landung
  - schaltet Bremstriebwerke 40 m über dem Boden ab
  - Aufprall mit 22 m/s (80 km/h) auf die Marsoberfläche

1) The touchdown sensors shall be sampled at 100-Hz rate. The sampling process shall be initiated prior to lander entry to keep processor demand constant. However, the use of the touchdown sensor data shall not begin until 12 meters above the surface.

2) Each of the 3 touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic. The test shall consist of two (2) sequential sensor readings showing the expected sensor status. If a sensor appears failed, it shall not be considered in the descent engine termination decision.

3) Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.

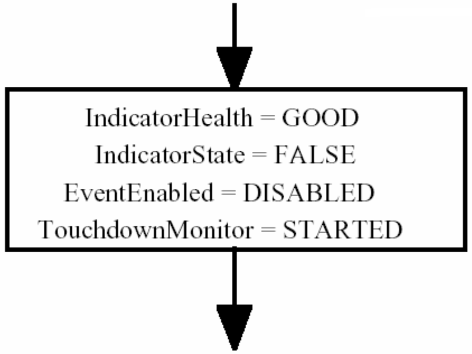
- Touchdown Monitor Start (TDM_Start)
    - Vom BS in 2000 m Höhe einmal aufgerufen
    - Initialisiert Variablen, setzt Flag „started“
- Touchdown Monitor Execute (TDM_Execute)
    - Für jedes Bein eine Inkarnation
    - Vom BS zyklisch aufgerufen (100 Hz Frequenz)
    - Verantwortlich für die Abschaltung der Landetriebwerke
- Touchdown Monitor Enable (TDM_Enable)
    - Vom BS einmal in 400 m Höhe aufgerufen
    - Prüft Sensoren auf Funktionsfähigkeit
    - Schaltet Abschaltüberwachung scharf

Touchdown Monitor Start (TDM_Start)

Called once by command.

Data Variables Used:

- IndicatorHealth = (GOOD, FAILED)
- IndicatorState = (TRUE, FALSE)
- EventEnabled = (ENABLED, DISABLED)
- TouchdownMonitor = (STARTED, NOT-STARTED)

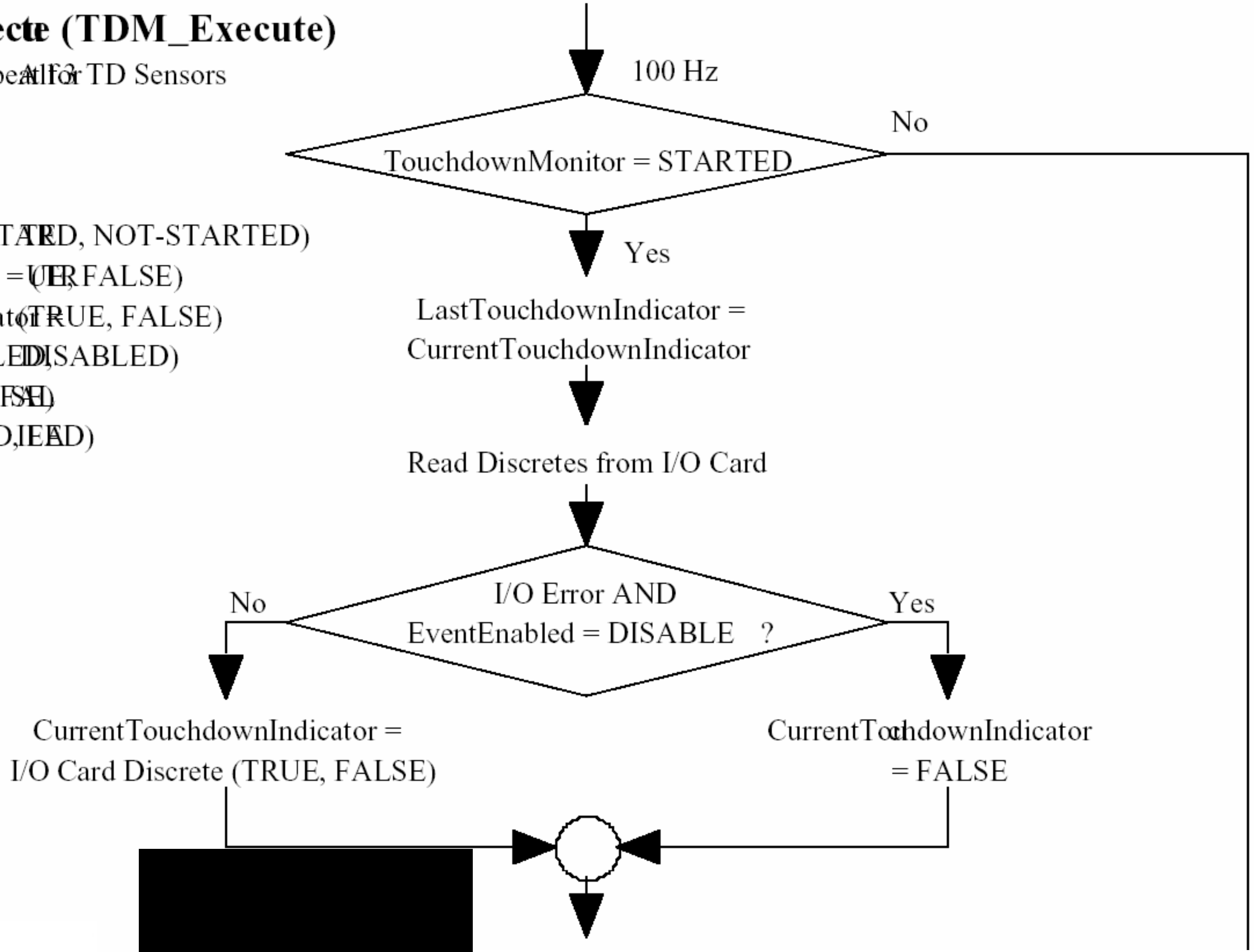


Touchdown Monitor Execute (TDM_Execute)

Chart Shows Single TD Sensor; repeat for All 3 TD Sensors
TDM_Execute is called at 100 Hz.

Data Variables Used:

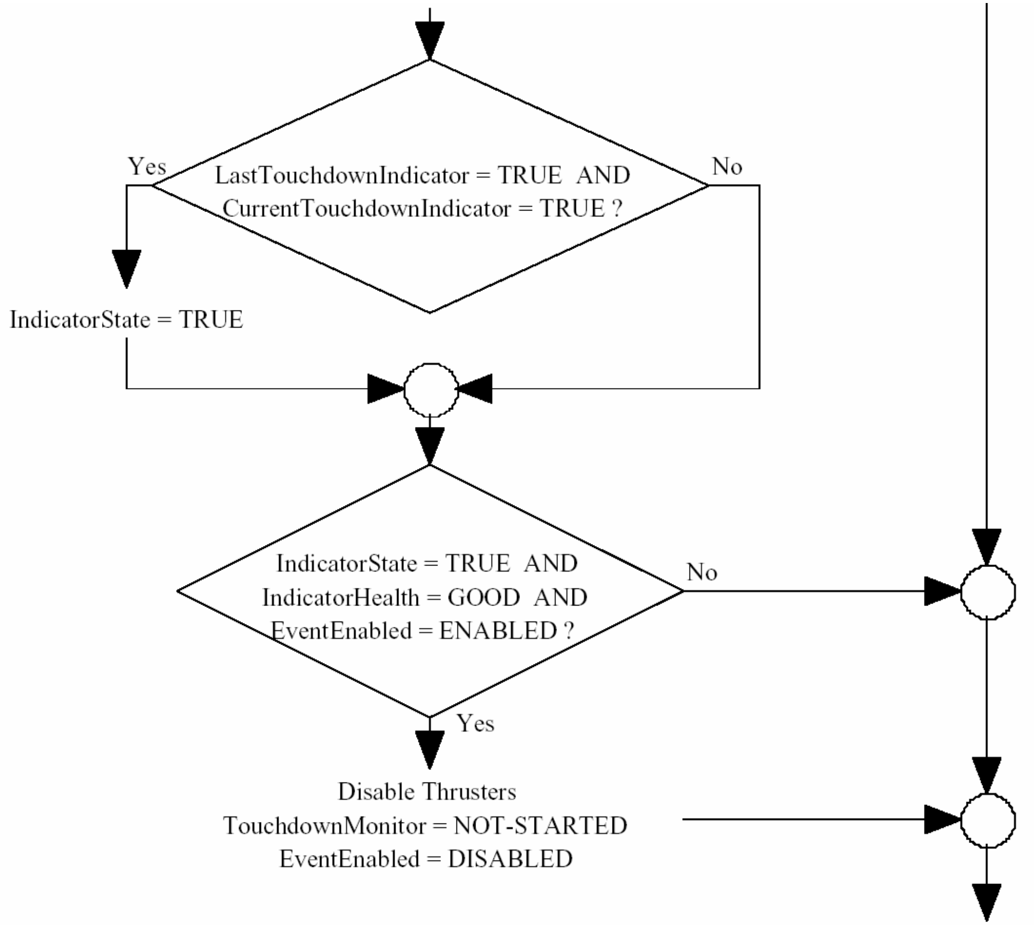
- TouchdownMonitor = (STARTED, NOT-STARTED)
- LastTouchdownIndicator = (TRUE, FALSE)
- CurrentTouchdownIndicator = (TRUE, FALSE)
- EventEnabled = (ENABLED, DISABLED)
- IndicatorState = (TRUE, FALSE)
- IndicatorHealth = (GOOD, FAILED)



[redacted]

[redacted]

[redacted]



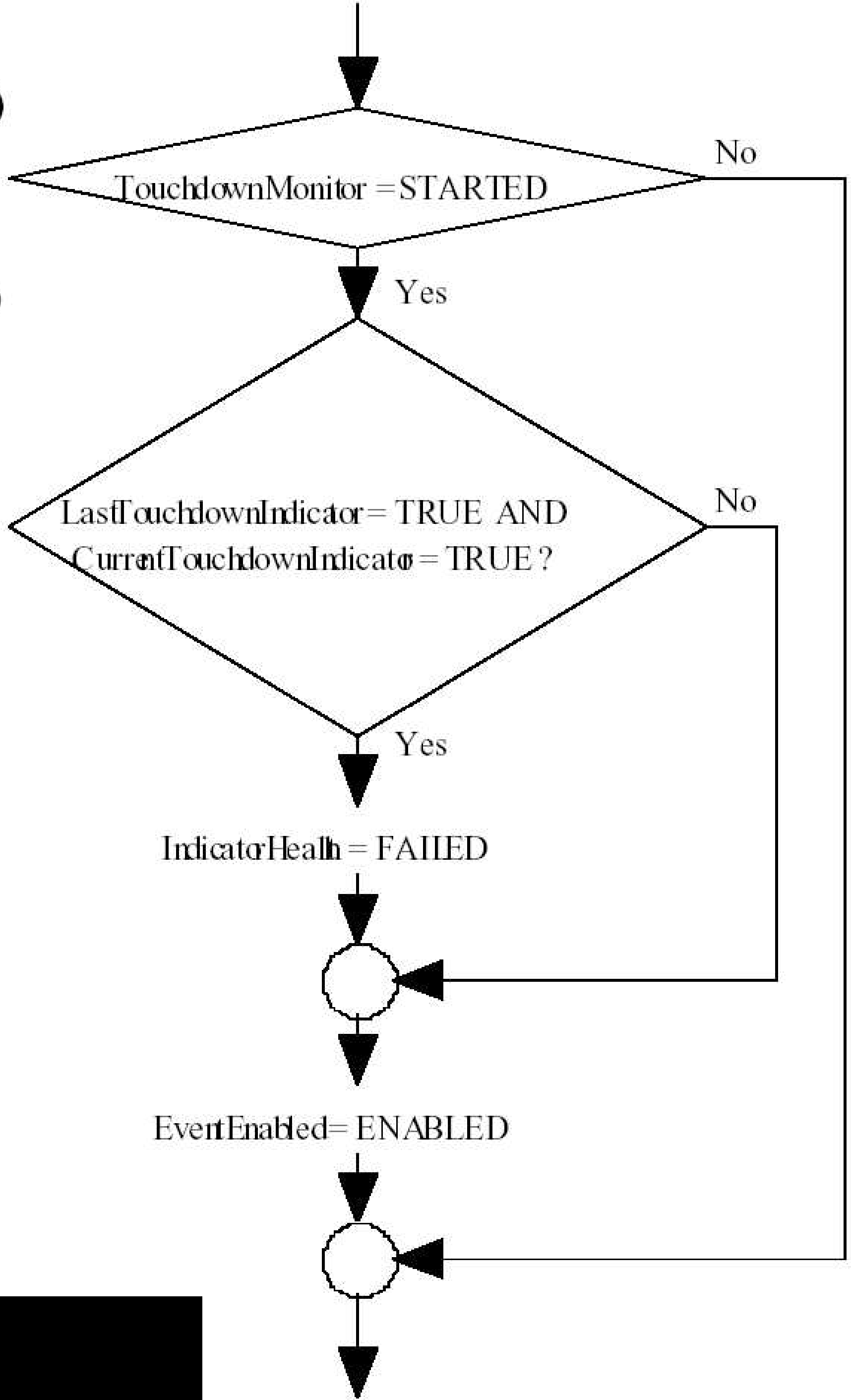
[redacted]

Touchdown Monitor Enable (TDM_Enable)

Called once by command.

Data Variables Used

- TouchdownMonitor = (STARTED, NOT-STARTED)
- LastTouchdownIndicator = (TRUE, FALSE)
- CurrentTouchdownIndicator = (TRUE, FALSE)
- IndicatorHealth = (GOOD, FAILED)
- EventEnabled = (ENABLED, DISABLED)



[redacted]

- Wie hätte der Fehler bei der Entwicklung vermieden oder gefunden werden können? Schreiben Sie 10 Möglichkeiten auf!
- jetzt !

ein Patch

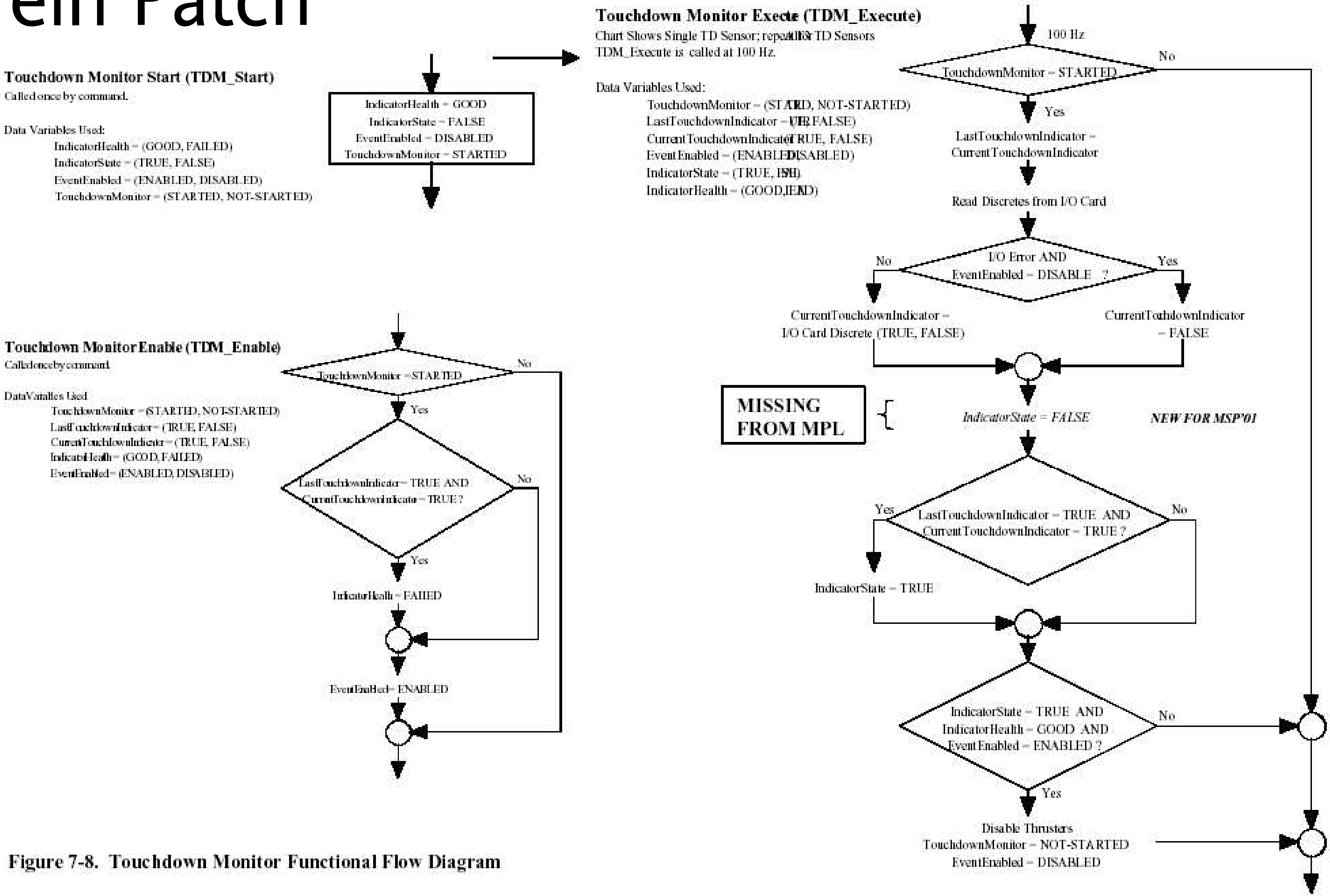


Figure 7-8. Touchdown Monitor Functional Flow Diagram

- zunächst ein reines Programmier-Problem
  - falsche Variablenbelegung
  - Komplizierte Parallelausführung mit gemeinsamem Speicher
- Ursache wurde quasi „zufällig“ beim Test der Software für die nächste Mission gefunden
  - Tester drückt Knopf um Sensorausfall in großer Höhe zu simulieren; wundert sich dass trotz Loslassen des Knopfes die Triebwerke abgeschaltet werden
- Missachtung einer informell spezifizierten Anforderung
  - Probleme mit der Übertragung von Systemanforderungen in Softwareanforderungen

SYSTEM REQUIREMENTS

1) The touchdown sensors shall be sampled at 100-Hz rate.

The sampling process shall be initiated prior to lander entry to keep processor demand constant.

However, the use of the touchdown sensor data shall not begin until 12 meters above the surface.

X

2) Each of the 3 touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic.

The test shall consist of two (2) sequential sensor readings showing the expected sensor status.

If a sensor appears failed, it shall not be considered in the descent engine termination decision.

3) Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.

FLIGHT SOFTWARE REQUIREMENTS

3.7.2.2.4.2 Processing

a. The lander flight software shall cyclically check the state of each of the three touchdown sensors (one per leg) at 100 Hz during EDL.

b. The lander flight software shall be able to cyclically check the touchdown event state with or without touchdown event generation enabled.

c. Upon enabling touchdown event generation, the lander flight software shall attempt to detect failed sensors by marking the sensor as bad when the sensor indicates "touchdown state" on two consecutive reads.

d. The lander flight software shall generate the landing event based on two consecutive reads indicating touchdown from any one of the "good" touchdown sensors.

Figure 7-9. MPL System Requirements Mapping to Flight Software Requirements

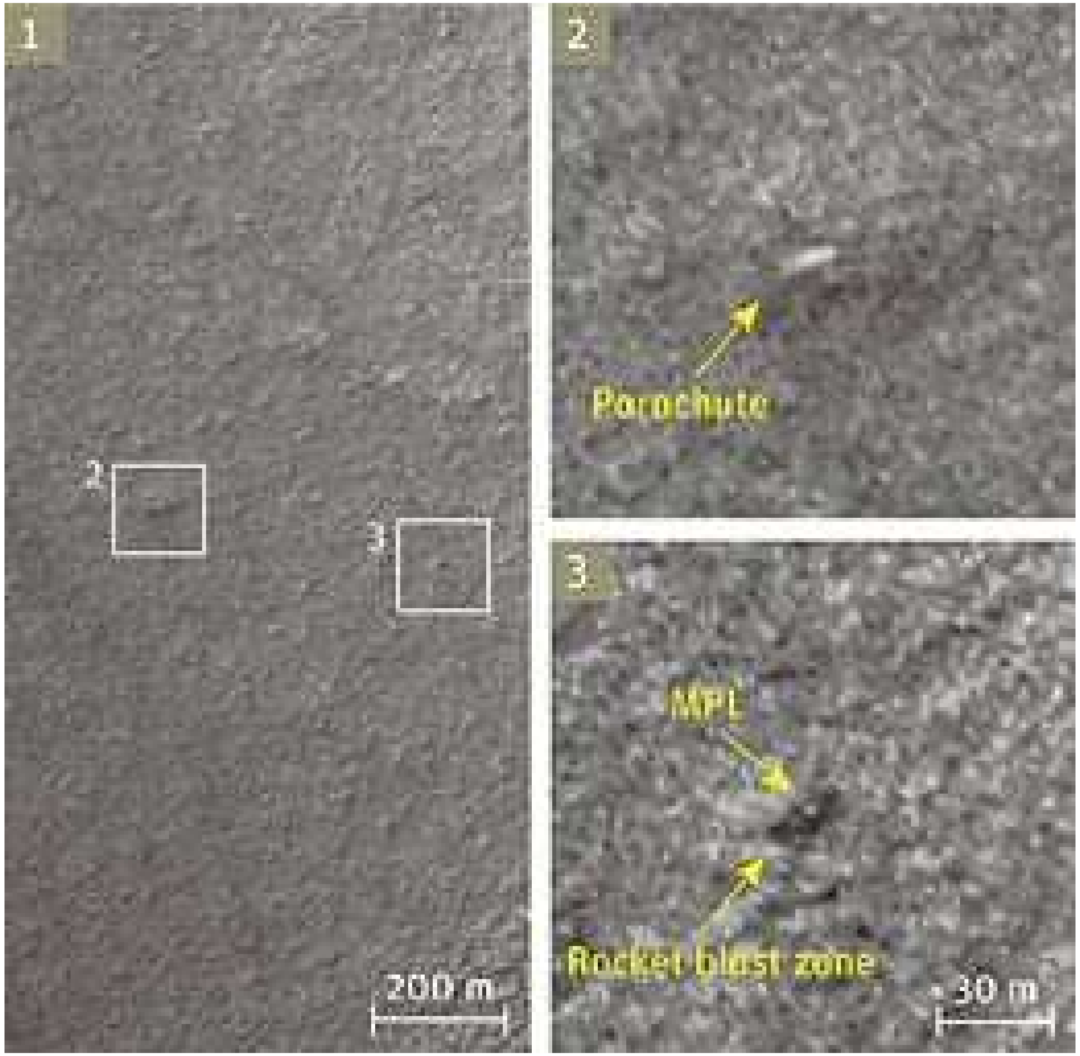
- Test nicht unter realen Bedingungen
  - kein Unit-Test der fatalen Anforderung
  - Systemtest des Landevorganges mit falscher Verkabelung, Wiederholung nur für Aufsetzvorgang
- falsche „Vorsichtsmaßnahmen“
  - vorzeitiger Start der Routine wegen Prozessorauslastung
  - Ausfallbedingung nicht für Rauschen geeignet
- sporadische Fehlmessungen bekannt, aber nicht dokumentiert
  - Beim Code-Walkthrough nicht aufgefallen
  - Messergebnisse des Hardwaretests nicht beachtet
- schlechter Informationsfluss vom Mechanik-Designteam zum Software-Team
  - Ingenieuren war Sensorrauschen klar
  - Verlassen auf unklare Systemanforderung
  - kein Review der Software durch Hardware-Ingenieure und umgekehrt

- From the beginning, the MPL project was under considerable funding and schedule pressure. The project team was asked to deliver a lander to the surface of Mars for approximately one-half the cost of Mars Pathfinder, which had been done for significantly less than earlier planetary missions. In addition, the complexity and technical challenges for MPL were at least as great, if not greater.
  - Use off-the-shelf hardware components and inherited designs to the maximum extent possible.
  - Use analysis and modeling as an acceptable lower-cost approach to system test and validation.
  - Limit changes to those required to correct known problems; resist changes that do not manifestly contribute to mission success.

- The MPIAT report found common characteristics among both successful and unsuccessful missions:
  - Experienced project management or mentoring is essential.
  - Project management must be responsible and accountable for all aspects of mission success.
  - Unique constraints of deep space missions demand adequate margins.
  - Appropriate application of institutional expertise is critical for mission success.
  - A thorough test and verification program is essential for mission success.
  - Effective risk identification and management are critical to assure successful missions.
  - Institutional management must be accountable for policies and procedures that assure a high level of success.
  - Institutional management must assure project implementation consistent with required policies and procedures.
  - Telemetry coverage of critical events is necessary for analysis and ability to incorporate information in follow-on projects.
  - If not ready, do not launch.

- Übrigens: Das Wrack wurde im Mai 2005 gesichtet und identifiziert!

  (Identifikation einzelner Pixel in 150 Megapixel Bild)
- Weitere hochauflösende Aufnahmen (0.5m/Pixel) geplant um den Fall endgültig zu klären



- Beim Entwurf eingebetteter Systeme
  - komplexes Zusammenspiel von Hard- und Software, Realzeit
  - Fehlerursache meist in der Kombination von Ereignissen
  - mangelnde Erprobungsmöglichkeiten, keine Rückrufmöglichkeit
  - Notwendigkeit der Wiederverwendung von Komponenten
  - Termin- und Kostendruck, Konkurrenzdruck
- qualitätsgetriebene Entwicklung
  - Integrierte Verifikation und Validation “IV&V”
  - Spezifikations– und Konfigurationsmanagement, Anforderungsüberwachung und Codeinspektion
  - Statische und dynamische Analyse, automatisiertes Testen
  - Simulation, Formale Verifikation und Modellprüfung
- Technologie-Entwicklung, Qualitätssicherung und Projektmanagement müssen zusammenspielen!