AIAA SPACE 2007 Conference & Exposition
18 - 20 September 2007, Long Beach, California

AIAA 2007-6109

Planning for the Un-plannable: Redundancy, Fault Protection, Contingency Planning and Anomaly Response for the Mars Reconnaissance Orbiter Mission

Todd J. Bayer[1]
NASA Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, 91109

For interplanetary spacecraft the round trip travel time for electromagnetic waves ranges from several tens of minutes to many hours depending on their distance to Earth. The round trip light time for communications with Mars Reconnaissance Orbiter (MRO) can be up to 40 minutes. With this latency, a variety of failures onboard the spacecraft could result in loss of the spacecraft before ground controllers could respond. These spacecraft must therefore be able to autonomously diagnose and fix time-critical failures. For those failures that onboard fault protection cannot diagnose or fix, ground controllers must be prepared to intervene. Using the actual MRO in-flight anomalies experienced to date, the complementary roles of redundancy, on-board fault protection software and ground-based anomaly response are examined to show how they provide a robust and multi-layered safety net for the mission.

I. Introduction

Mars Reconnaissance Orbiter's (MRO) crucial role in the long term strategy for Mars exploration requires a high level of reliability during its 5.4 year mission. This requires an architecture which incorporates extensive redundancy and cross-strapping. The overall MRO architecture is discussed in this context.

Because of the latency due to round trip light time (RTLT), many possible failures could cause spacecraft and hence mission failure before ground controllers could react. Therefore, in order to make use of MRO's hardware redundancy, it must itself be able to respond to these mission-critical failures. The architecture of MRO's semi-autonomous fault protection software, known as the Spacecraft Imbedded Distributed Error Response (SPIDER), is described in the context of each phase of the mission, with emphasis on its key role as 'first responder' in detecting and responding to potentially threatening situations on board the spacecraft. A key aspect of this 'first response' is establishing a stable, power positive, thermally safe and commandable configuration termed "safe mode".

On-board fault protection software is still only semi-autonomous. Assuming it has successfully established safe mode, the ground must then take over to complete the recovery back to nominal operations. The ground would also need to intervene when fault protection is unable to recognize a potentially threatening condition, either due to known limitations or software flaws. In any of these cases it is crucial to have well thought-out plans for how the ground should proceed. Many of the commands the ground might need to send are known beforehand, and these contingency plans incorporate all the commands which might be required, fully tested and ready for uplink. The set of MRO contingency plans is discussed in terms of the relationship of each plan to the on-board fault protection responses.

When anomalies actually happen, all of this redundancy, software and planning is put to the test. MRO has experienced—and survived—several significant anomalies in its mission so far, including command errors, flight software bugs and hardware failures. Each of these significant anomalies is examined in terms of the parts of the overall safety net that came into play, the root cause and lessons learned.

II. MRO Spacecraft Architecture: Redundancy and Cross-Strapping

Reliability of systems can be significantly increased by including redundant elements, so that the system can continue to function after a failure of one or more elements. When a system can be shown to function after any

[1] Chief Engineer, MRO Project, 4800 Oak Grove Drive, Mail Stop 264-535 , AIAA Senior Member.

single failure, the system is referred to as single fault tolerant. MRO's requirements specified that the spacecraft should be fully single fault tolerant. In response, the designers included extensive redundancy and cross strapping.

Redundancy provides protection against random failures. Redundancy is not generally used to address wear-out failures or consumables. Several types of redundancy are commonly employed:

1) Functional Redundancy: Providing more than one means to accomplish the function, possibly with some degradation. An MRO example is thruster backup to reaction wheels[1].
2) Block Redundancy: Providing two or more parallel elements, any one of which can perform the required function. Examples of MRO block redundancy are two identical Command & Data Handling (C&DH) subsystems, two batteries, two star trackers, two inertial measurement units (IMUs), two sets of sun sensors, two Small Deep Space Transponders (SDSTs) and two X-band traveling wave tube amplifiers (TWTAs)[1].
3) Cooperative Redundancy: Splitting the equipment for performing a function into two or more independent portions such that some portion can fail and the function can still be performed, but with some loss of performance. This is also referred to as 'N+1' redundancy. An example of MRO cooperative redundancy is the 4th reaction wheel (RWA), mounted so that it can replace any one of the three primary wheels with reduced control authority[1]. The Compact Reconnaissance Imaging Spectrometer for Mars (CRISM) includes three redundant cryogenic coolers, but this is due to the known wear-out mechanisms of these devices – making the exception to the above rule.
4) Cross Strapping: Cross strapping enables a Single Fault Tolerant system to tolerate more than one failure, as long as no two failures are in the same element. This is illustrated below in Fig. 1[2]. MRO includes extensive cross-strapping, for example allowing either C&DH to access either SDST, and any of the four reaction wheels.

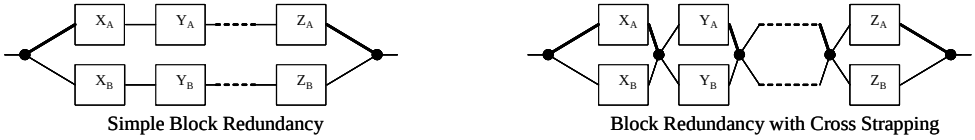

Figure 1. Illustration of cross strapping

III. Autonomous Fault Protection

A. General Role of Autonomous Fault Protection

Interplanetary spacecraft require that, generally, autonomous fault protection provide a fail-safe response. This is in contrast to human spaceflight systems such as the Space Transportation System which generally require a fail-operational response. MRO fault protection responds to major faults by terminating all active onboard command sequences, powering off all components not essential to spacecraft survival (such as science instruments), configuring the vehicle in a stable sun pointed attitude, switching communications to a broad beam, low-rate antenna for maximum coverage, sending critical information regarding the fault and the current vehicle state over this emergency link and then waiting for ground controllers to intervene. It is then the ground's task to diagnose and resolve the fault and return the vehicle to the full operational state required to continue the mission. This autonomous response is termed 'Safe Mode.' MRO's fault protection is analogous to the role of an emergency medical technician: triage and stabilize the patient until a hospital can be reached.

Safe mode, and most—though not all—fault responses are generic to all phases of a mission. The few cases where a unique response is required for a single critical event drove the need to give fault protection reliable knowledge of the mission phase. Mission phase is most often thought of as a ground operations concept, demarking spans of time which correspond to separate and unique activities. MRO's mission phases are: Launch, Cruise, Mars Approach, Mars Orbit Insertion (MOI), Aerobraking, Primary Science Phase (PSP), and Relay. Knowledge of the mission phase is stored onboard in software, which only a ground command can change. Several mission phases contain mission critical events: those events which must succeed in order for the mission to proceed. For these critical events, autonomous fault protection must provide more than a fail-safe response: it must provide enough of a fail-operational response to ensure success of the event. MRO critical events were Launch and MOI. Other events were treated as critical events when they involved significant first time events: The first trajectory correction maneuver (TCM-1) in Cruise and the first several aerobraking drag passes fell in this category. For all these, special fault protection functions were implemented to help ensure success.

B. MRO Mission Phases

Below is a summary of each of MRO's mission phases, and fault protection functions unique to that phase.

Pre-launch (Up through Launch - 45 minutes). The spacecraft defaults to receiving uplink via hard-line ports rather than RF receivers. Many software functions, including fault protection, are disabled for safety of ground personnel. Vehicle defaults to "Pre-launch" phase on power-up, primarily for human safety during integration and test.

Launch. (Launch minus 45 minutes – Launch + 3 days). Launch occurred 12 August 2005 at 2005-224-11:43:00:332 Coordinated Universal Time (UTC). During final countdown and launch, the vehicle was in "Launch" mission phase. Flight Software (FSW) sensed separation from the Atlas Centaur upper stage, and then commands a safe mode entry. Safe Mode configured the vehicle, deployed the appendages, acquired attitude, and slewed to the proper attitude for initial ground acquisition of radio communications. Launch and initial acquisition were successful, and the ground commanded safe mode exit on 13 August 2005. The mission phase was changed by ground command to "Cruise" on 15 August 2005. Unique to this phase: fault protection handles the one time event of appendage deployment. This is also the only time during the mission when safe mode is used to perform a nominal, planned event.

Cruise. (15 Aug 2005 – 07 March 2006). This phase covered the 7 month interplanetary cruise to Mars. The main activities were trajectory correction maneuvers (TCMs) and checkout and calibration of the spacecraft. The first TCM was quasi-critical as a first time event. This was performed on MOI thrusters instead of the TCM thrusters in order to provide in-flight verification of the MOI propulsion system. The MOI-unique fault protection (see MOI section below) was not enabled for this burn. There was no special phase-unique fault protection for Cruise. An additional phase was defined between Cruise and MOI, called Approach. This was between January 2006 and early March 2006, and was primarily for ground operations preparation for MOI and had no special meaning for flight software or fault protection. The onboard mission phase bit remained set to Cruise.

Mars Orbit Insertion. (07 March 2006 - 29 March 2006). MOI burn occurred as planned on 10 March 2006 (2006-69/21:12:33 SpaceCraft Event Time (SCET)). On most past planetary missions fault protection was disabled for critical events such as orbit insertions. This seemingly counterintuitive approach resulted from several factors. First, critical events such as orbit insertions involve large, precisely timed and pointed engine firings. Fault protection response to sensed anomalies usually involves canceling all ongoing activities in order to preserve vehicle safety, but during an insertion burn this response would stop the burn. Unless reliable autonomous means could be developed for restarting the critical event sequence, this would likely mean the end of the mission. Second, fault protection software is still software, and as vulnerable to bugs as any other software. This software may respond unexpectedly or dangerously due to undiscovered bugs and in this way end the mission. Third, fault protection responses are triggered at pre-defined values of engineering telemetry. These trigger points are defined by mission operators, and are vulnerable to incorrect settings. A setting which is too 'tight' and causes an unnecessary fault protection response could endanger the execution of an otherwise nominal critical event. The risk trades in the past have generally considered the risk of a fault protection bug or incorrect trigger to be higher than the risk of actual hardware failure during the short duration of the critical event.

MRO has successfully resolved these issues. We developed new capabilities to enable fault protection to restart and complete the MOI burn after responding to a fault. We ensured through extensive analysis and test that the fault protection software was reliable. We performed in-depth reviews of all trigger points to minimize the possibility of false problem detections during MOI. Finally we disabled any fault protection responses that were not critical to completion of the burn.

Aerobraking. (29 March 2006 – 20 Sep 2006). The first maneuver to place the spacecraft periapsis in the Martian upper atmosphere occurred 29 March 2006, and the final maneuver to lift periapsis back out of the atmosphere occurred 30 Aug 2006. During this time MRO's orbit was reduced from 45,000 km Apoapsis and a 35.5 hour period to a 250 km Apoapsis and a 1.9 hour period. Unique fault protection functions: when in safe mode, fault protection detects and configures the spacecraft for aerobraking drag passes, and based on drag pass deceleration thresholds can infer dangerous heating rates and command an autonomous maneuver to 'pop-up' out of the atmosphere. The pop-up capability was enabled only during the final ten days of aerobraking, when the orbits became short enough that the ground could not guarantee a sufficiently timely pop-up command. See Ref. 3 for more description of the unique fault protection capabilities developed for the Aerobraking phase.

Primary Science Phase. (20 Sep 2006 - 7 Nov 2008). The actual primary science phase (as opposed to the onboard mission phase) did not begin until 7 November 2006, when the spacecraft and payload commissioning activities were completed and the first regular observing programs were initiated. The onboard mission phase was set to PSP earlier in order to complete the period of transition from Aerobraking into Primary Science. There is no fault protection unique to PSP.

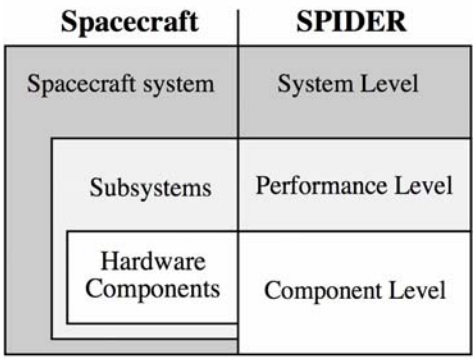

Figure 2. SPIDER architecture compared to spacecraft

Relay. (Nov 2008 – Nov 2010). Nominally defined period where science will continue but where first priority will be on supporting ultra-high frequency (UHF) relay with landed assets. There is no fault protection unique to the Relay phase.

C. MRO Fault Protection Architecture

The following description of MRO's Fault Protection implementation is adapted with permission from a paper by its inventor, Eric Seale[4]. MRO's Fault Protection implementation, known as SPIDER, was invented at Lockheed Martin Space Systems Company (LMSSC) in 1995 to support the Mars Surveyor Program. It has matured and evolved through subsequent application on LMSSC's Stardust, Odyssey, Genesis and now MRO spacecrafts. The system is coded using Object-Oriented Analysis/Design methods, resulting in a system which uses the spacecraft itself as a model, and which can be easily adapted and evolved for subsequent missions. In essence the software objects mirror the spacecraft components, subsystems, and system. SPIDER's architecture is divided into three software layers analogous to the levels in a hierarchical decomposition of a spacecraft design, shown in Fig. 2[5].

Fault detection attempts begin at the interface with hardware; logic within each successive layer then does what it can to resolve and respond to a failure. Parameters are selected to assure that lower levels of SPIDER's logic respond more quickly than upper layers. If logic in a given level can't detect a particular failure, the failure "flows up" for the next highest layer to detect. If logic within a level detects a failure but can't fix it, the logic flags the failure's occurrence; this "indicated failure" flag then becomes fodder for a detection in the next level up. Note that most fault data is passed up the hierarchy only on request (i.e., it is "pulled" by higher layers, not "pushed" by lower layers). This avoids saturating higher layers of the architecture with multiple detections of the same failure from propagated symptoms. Actions of upper levels are then largely based on data from lower levels, although each subsequent level also has new detections based on increasingly abstract health measures.

Upper levels can force lower ones to perform actions (in particular, to reset their logic states), but do not "out prioritize" or overrule them.

Component Level Fault Protection (CLFP) consists of distributed logic, implemented within "virtual component" software objects (each responsible for modeling, and interfacing with, a given hardware component), used perform low-level error detections and responses. At this level, error detections are based on direct measurements from a given component's telemetry. Component level responses are not allowed to affect other objects; accordingly, many objects' component level responses consist of little more than setting a flag to indicate component failure. While a failure is indicated at the component level, the affected object is required to continue outputting "best guess" data, and to continue operations as best it can. This keeps the spacecraft operational while fault protection logic works to resolve the failure.

Performance Level Fault Protection (PLFP) consists of a set of monitors, each responsible for supervising the performance of a subset (domain) of spacecraft behavior. Each domain roughly corresponds to a spacecraft subsystem, although a few subsystems are subdivided into multiple domains, each protected by a separate monitor.

There are 12 performance domains in the MRO implementation of SPIDER:

1. Attitude control
2. Attitude knowledge (i.e., attitude determination)
3. Articulation (High Gain Antenna (HGA) and two Solar Array wings each articulate in two axes)
4. Communications (telecommunications via X-band up/downlink with Deep Space Network)
5. Data bus (intra-spacecraft communications)
6. Guidance Performance (MOI only: collects Delta-V and attitude information to enable restart of burn)
7. Momentum control (monitoring buildup and management of spacecraft angular momentum with reaction wheels and thrusters)
8. Navigation Performance (Aerobraking only: determine onset and end of drag phase of orbit during safe mode in Aerobraking phase)
9. Power control (distribution and consumption of electrical power, bus voltage/current, battery charging)
10. Science (monitoring health of the six science instruments)

11. Sequence (monitoring specific software which controls execution of multiple independent time ordered command sequences)
12. Software (monitoring execution of flight software)

System Level Fault Protection (SLFP) consists of contingency mode executives (Safe Mode, uplink loss, and downlink loss) and various fault protection utilities. System level logic is allowed to manipulate anything on the spacecraft as needed to assure protection from failures. FP knowledge of available redundancy is embodied mainly at the performance and system level.

Historically, SPIDER's system level logic has been fairly unsophisticated (part of a legacy of constrained autonomy), and was an early target for improvements when the mission requirements of MRO were first seen. As would be expected with MRO's increased lifetime and science requirements, programmatic tolerance of risk is dramatically lower than that seen on heritage missions. One particular manifestation of this shift is that MRO must be able to recover from any credible single failure during the critical MOI burn. In contrast, previous missions "waived" the requirement for fault recovery during such short duration mission critical events. From a fault protection perspective, the increase in hardware cross-strapping and the MOI recovery requirement posed the two biggest challenges.

MRO addressed this issue by giving performance level monitors an interface analogous to that of component level objects. Monitors now set indicators corresponding to any need for domain initialization (which generally means that Safe Mode is required), or to indicate a logic dead-end (which generally means that a reboot or string swap must be performed). It is then the responsibility of system level logic to "pull" this information up the hierarchy. A new executive was added (Fault Protection Executive) to handle the new interface with performance level monitors, as well as to coordinate entries to Safe Mode and reboots / string swaps.

IV. Contingency Planning

Contingency Planning for MRO has two main goals: 1) responding to problems which fault protection cannot detect or address; and 2) recovering the spacecraft to full operations after fault protection action.

1) Responding where fault protection cannot. Fault protection should be able to respond autonomously to as many critical real-time faults as possible, given the development resource constraints and current state of the art of software. MRO has achieved high levels of fault protection monitoring and response, but there are still faults which fault protection does not monitor or to which it does not respond.

For example, we chose not to implement a measurement of radiated X-band downlink RF power for cost and complexity reasons. Fault protection can discern the health and status of the transponder and the RF amplifier, but it has no closed-loop check to confirm power is actually leaving the antenna. In this case the ground operations team closes the loop using the Loss of Signal (LOS) Contingency Plan. Other kinds of faults in this category include two-failure scenarios, for example where neither of the redundant star trackers is able determine inertial attitude.

In addition to this very small set of known time-critical anomalies to which the ground must respond, there are contingency plans meant to respond to faults the designers did not or could not anticipate. This type of plan is necessarily general, providing high level guidance on how to proceed. Ultimate resolution of these types of anomalies, if possible at all, requires real-time analysis by operations team experts.

Another area where fault protection is not necessarily designed to respond is the set of faults which do not immediately threaten the spacecraft. Examples include certain temperature measurements provided for information only, long term performance degradation, and failure of elements in an n+1 redundancy scheme such as individual solar array strings. Here again, ground operations monitoring and response are necessary to recognize, evaluate, and mitigate the fault.

2) The second major category of contingency plan involves recovering the spacecraft into nominal operations after a fault protection response. As described above, fault protection responses are designed to act at an architectural level appropriate for the fault. Once the immediate threat posed by the fault is addressed by fault protection, there is usually some amount of 'cleanup' which ground operations must perform. Examples are below.

a) Addressing the loss of a redundant component (Loss of Redundancy Contingency Plan). After fault protection has detected a component failure and autonomously swapped to the redundant unit, the operations team will first examine available data to determine if the component is actually failed. Depending on the outcome, they may re-activate the component or, if it is actually failed, they may need to modify operations to account for the loss of redundancy.

b) Recovery from Safe Mode (Safe Mode Recovery Contingency Plan). Because the Safe Mode response takes the vehicle down to a minimal configuration for survivability, significant work by ground operators is necessary in order to bring the vehicle back into a fully operational state, once the fault is isolated and addressed. This process

has taken anywhere from 7 hours up to 8 days, depending on whether a reboot was involved and how long the ground required to diagnose the cause of safe mode.

Finally, it should be noted that the project has an overarching procedure meant to guide the initial diagnosis and criticality determination of observed faults. This is called the Anomaly Response Procedure. Here the ground operations team is given guidance on the initial steps to take after identification of a possible anomaly. These steps include confirmation of anomalous behavior; determination of whether it is a ground or spacecraft anomaly; determination whether resolution is time-critical; notification of mission management depending on the preceding determinations; and initiation of anomaly report.

All in all, MRO has developed 26 contingency plans.

V. MRO Anomalies

Here we examine the significant anomalies the spacecraft has experienced to date, in terms of the: observables; roles played by autonomous fault protection and by the ground operations team; use of/impact on redundancy; root cause if known; lessons learned.

The six most significant spacecraft-level anomalies since launch are listed below and described in the following paragraphs. Science instrument anomalies not included.

First, a short note regarding the performance of the critical event fault protection functions as described in Section III. Launch fault protection deployed all appendages without incident; in addition there were no faults noted during launch. During MOI, fault protection was enabled but the burn executed flawlessly. Just as importantly, Fault Protection did not raise any false alarms or unnecessary responses during MOI. Aerobraking fault protection by contrast was called into action twice, and performed perfectly in both cases. These are the items C and D, described below in Table 1.

Table 1. MRO significant anomalies

Date	Anomaly	Mission Phase	Root Cause
A. 03-Jan-06	Computer Warm Reset	Cruise	Software bug
B. 26-May-06	Ka-Band Exciter Failure	Aerobraking	Part failure
C. 31-May-06	Safe Mode Entry	Aerobraking	Sequence error
D. 26-Jul-06	Safe Mode Entry	Aerobraking	Command error
E. 16-Aug-06	RF Switch #1 Failure	Aerobraking	Contamination
F. 14-Mar-07	Computer Side Swap	Primary Science	Unknown

A. Computer Warm Reset (Cruise)

On 03 January 2006, during a normal Deep Space Network (DSN) tracking pass, spacecraft downlink was unexpectedly lost. To diagnose and respond to cases such as this, the operations team immediately executes the project's Loss of Signal Contingency Plan. After a DSN anomaly was ruled out, the DSN receivers were configured to search for the safe mode downlink signal from the spacecraft. This downlink mode is a low bit-rate broadcast over the spacecraft's primary low gain antenna. The DSN successfully acquired this signal, confirming that the spacecraft had entered safe mode. Following signal acquisition, examination of the telemetry indicated that fault protection had commanded a warm reset of the flight computer and then configured the vehicle in safe mode.

Ground Response. Executed Safe Mode Recovery Contingency Plan, completed on 6 Jan; determined root cause to be a bug in the downlink buffer management software. A patch was developed and tested, and installed on the spacecraft on 06 February (This was one of several critical patches installed prior to Mars Orbit Insertion on 10 March 2007). After the patch was installed, a downlink buffer re-initialization was performed successfully. To mitigate risk of additional reboots while the patch was in development a Flight Rule was added to prohibit re-initializations of the heap whenever any packets were queued up for retransmit.

Redundancy Considerations. Redundancy was unaffected. MRO's design makes patches usable by both flight computers.

Root Cause. Further analysis of the telemetry implicated a previously undetected bug in the flight software involved in reinitializing the engineering telemetry downlink buffer. When encountered, the bug triggered a software exception. The Software Performance Monitor of fault protection detected this exception, suspended the software task and initiated safe mode followed by a reboot.

Safety nets used. Here the onboard fault protection was critical to vehicle survival, by monitoring flight software execution and responding with task suspension, reboot and safe mode. The ground used existing contingency plans

to find the downlink signal and recover from safe mode back into nominal operations. Anomaly investigation determined root cause was a flight software bug, which the operations team then patched. Redundancy in the design was not necessary here. No significant lesson learned: software bugs can only be minimized not eliminated, and fault protection is designed to ensure vehicle safety as far as possible.

B. Transponder Ka-Band Exciter Failure (Aerobraking)

One of MRO's goals is to demonstrate operational use of Ka-band downlink for science data return. X-band is the primary communication system for MRO, but Ka-band could potentially provide enhanced data return. Because of its narrow beam width compared to X-Band, Ka-band communications represents a challenge for spacecraft pointing. During cruise, the Ka-band exciter and amplifier were powered on, and many of the Ka-band communication demonstration objectives were met. This demonstration confirmed the MRO spacecraft could point the HGA accurately enough to provide a reliable Ka-band downlink, and verified that the new Ka-band receiver equipment installed at stations of the Deep Space Network was operating properly.

MRO incorporates two SDSTs, one primary and one backup. On 26 May 2006, 2022 SCET, after approximately nine months of continuous in-flight operation, the prime SDST exhibited anomalous power consumption, consisting of a large power increase lasting approximately three hours, followed by a slightly larger drop which persisted until, four days later, power consumption decreased again as a result of an unrelated event that caused the spacecraft to enter a "safe" mode (Item C below). Part of the safe mode response is powering off the Ka-band exciter area of the SDST. At this point the SDST power consumption, with only the X-band exciter operating, was as expected. During the anomaly, baseplate temperature sensors on the operating and redundant (Off) SDST tracked the increase and decrease in power consumption.

Safe mode's powering off Ka-band is the action that probably would have been taken had the anomaly been detected in real-time. In that sense, a real-time recovery was not necessary. A real-time recovery was also not possible, because the anomaly was not detected in real time. The power and thermal changes were not quite large enough to trigger red alarms on the ground or fault protection onboard. Alarms and fault protection had been configured to protect the X-band functionality, but this was not degraded during the anomaly. There was also no threat to the spacecraft that required the powering off of non-critical components. Also, because the Ka-band downlink was off (exciter on but amplifier off), there was no sudden disappearance of the Ka-band signal to trigger ground action. The anomaly was noticed several days later during routine trending analysis. The anomaly occurred on a Friday afternoon before a long holiday weekend, which may also have delayed its detection.

Even though the spacecraft was not in danger and the prime X-band communication pathway was unaffected, the failure to notice and respond to this anomaly in real-time was considered an anomaly in its own right. Several mitigations have since been implemented to ensure that any future anomaly is seen in real-time.

Further investigation showed that the anomalous power consumption was related to a failure within the Ka-band portion of the SDST. The X-band functionality of the SDST continued to be nominal. The most probable cause of the anomaly was determined to be failure of a pre-amplifier part used to derive the Ka-band signal within the SDST. It is believed that the pre-amplifier first shorted, then eventually burned open due to excessive heating induced by the short.

For MRO, the mission impacts are:

1) The Ka exciter on the prime SDST is no longer usable
2) Completion of the Ka-band demonstration would require swapping to the backup SDST
3) The backup SDST may have a similar incipient failure, meaning the Ka-band lifetime is unknown

The waveguide transfer switch anomaly (Item E below) creates a possible failure scenario whereby Ka-band would be the only viable communications link for returning the high volume science data. Based upon the demonstrations of this capability during cruise, the use of Ka-band on the backup SDST is considered a feasible option for downlink of science data. In order to preserve this option, the project decided to indefinitely postpone the Ka-Band demonstration.

Safety nets used. In this case the main safety net was actually the modular design of the transponder, which prevented the fault from propagating from the non-critical functions (Ka-band) to the critical functions (X-band). A secondary safety net, if this modularity had not adequately protected X-band, would have been fault protection detecting a problem with the primary transponder and swapping to the backup.

Lesson learned. Alarms and fault protection needed to be refined to catch future occurrences of this anomaly. Additionally, several changes have been made to the SDST design and construction for future builds.

C. Safe Mode Entry (Aerobraking)

On 31 May 2006, during a normal DSN tracking pass, with the spacecraft in the vacuum portion of an aerobraking orbit, spacecraft downlink was unexpectedly lost. As in Anomaly "A" above, the operations team immediately executed the project's LOS Contingency Plan. DSN anomalies were ruled out when the DSN was able to lock onto the spacecraft's safe mode signal. Examination of the telemetry indicated that fault protection had commanded a safe mode entry after detecting the end of valid spacecraft orbital ephemeris information. In order to prevent attitude errors due to inaccurate ephemeris information, fault protection is designed to command a safe mode entry in these cases.

Ground Response. Executed Safe Mode Recovery Contingency Plan. During Aerobraking, one of the first decisions is whether to command a maneuver to raise the spacecraft's orbit out of the sensible atmosphere. This may be necessary in order to prevent entry and burn-up of the vehicle in the atmosphere in cases where the orbit is anomalously low, the atmosphere is anomalously dense (for example due to a global dust storm), or a spacecraft malfunction is preventing the proper functioning of Aerobraking fault protection as described above in Section III. In the early and middle stages of aerobraking (when orbit period is greater than 4 hours), the autonomous pop-up maneuver capability was not yet enabled, so the ground would have to command any such maneuver. In this case, the orbit and atmosphere were nominal, and fault protection was functioning normally. Therefore the project decided no pop-up maneuver was necessary, and allowed fault protection to sense the atmosphere and configure for the upcoming drag portion of the orbit, which it did correctly. Between this drag pass and the next (18 hours at this point) the ground successfully recovered the vehicle into nominal aerobraking operations.

Root Cause. Determined to be a flaw in the design of the command sequences used to configure for drag passes, which led to the breaking of the normally continuous chain of orbital ephemeris files. The operations team quickly developed, tested and uplinked a corrected version of this command block. In addition, the ground operators did not adequately understand engineering telemetry which indicated this condition had occurred, and which would have given several hours warning of the impending safe mode entry. This was treated as a separate anomaly: recognition of the impending safe mode could have allowed its prevention, or at least allowed the operations team to assemble and prepare for the recovery in advance

Safety nets used. As in anomaly "A", the onboard fault protection was critical to vehicle survival. In this case fault protection's monitoring of vehicle operations detected that critical information was no longer available and responded by commanding safe mode. Just as importantly, fault protection performed perfectly in detecting the beginning of the drag passes and configuring the vehicle attitude and state to fly safely through the following drag pass. The ground used existing contingency plans to find the safe mode downlink signal and recover from safe mode back into nominal operations. Anomaly investigation determined root cause was a flaw in command sequence design, which the operations team then fixed. It was not necessary to use available redundancy.

Lessons learned: While fault protection performed exactly as designed by detecting and responding to the lack of critical information, the resulting safe mode was indicated in advance by telemetry, but the signature was not recognized by the ground. A thorough review of these command products was conducted, and the nominal and anomalous telemetry signatures were clarified for future diagnosis.

D. Safe Mode Entry (Aerobraking)

On 26 July 2006, during a normal DSN tracking pass, with the spacecraft again in the vacuum portion of an aerobraking orbit, spacecraft downlink was unexpectedly lost. As in Anomaly "A" and "C" above, the operations team immediately executed the project's Loss of Signal Contingency Plan. DSN anomalies were ruled out when the DSN was able to lock onto the spacecraft's safe mode signal. Examination of the telemetry indicated that fault protection had commanded a safe mode entry after detecting a serious problem with a currently executing command sequence. Special types of command sequences called blocks are stored on-board and can be called by a single parameterized command from the ground. Blocks are non-re-entrant by design, meaning that calling a block which is already executing will result in an error. The proximate cause of this safe mode entry was that a block was called while it was already active. Fault protection detected this problem and commanded safe mode, which halts all executing sequences.

Ground Response. Executed Safe Mode Recovery Contingency Plan, diagnosed root cause and returned to nominal aerobraking operations. As in "C" above, the project considered commanding a "popup" maneuver and again decided this was not necessary. The spacecraft flew nominally through two drag passes in safe mode before the ground could complete the recovery into nominal operations.

Root Cause. Command error: ground operators did not follow written procedures, leaving insufficient time between radiations of consecutive commands. Also, the commands had been inappropriately designated as "Express" commands.

Safety nets used. As in anomaly “A” and “C”, the onboard fault protection was critical to vehicle survival. In this case fault protection’s monitoring of vehicle operations detected a serious problem with command execution and responded by commanding safe mode. As in item C, Fault protection performed perfectly in detecting the beginning of the drag passes and configuring the vehicle attitude and state to fly safely through each drag pass. Ground used existing contingency plans to find downlink signal and recover from safe mode back into nominal operations. It was not necessary to use available redundancy.

Lessons learned: It was determined that some commands had been inappropriately classified as ”Express” commands. MRO designates certain commands as “Express” in order to allow certain routine and safe commands to be sent with a reduced approval process. The commands in question were routine and safe but only when used individually as per the procedures. The project subsequently re-examined and revised the definition of Express commands. Ground operators received re-training on the importance of following procedures.

E. RF Transfer Switch Failure (Aerobraking)

WTS #1 switch was designed to swap downlink between the high-gain antenna (HGA) and the low gain antenna (LGA) without swapping X-band amplifiers. After several hundred trouble-free actuations in flight, WTS #1 failed to actuate. The switch failed to move when commanded, but did move to the proper position when onboard Fault Protection commanded a second actuation. On the next orbit, the switch again failed to move when commanded. After two unsuccessful retries by fault protection, the Fault Protection software declared the switch failed, and instead swapped to the redundant X-band amplifier to achieve downlink over the HGA. Fault Protection performed as designed by recognizing a failed component and utilizing on-board redundancy to achieve an equivalent telecom configuration. There was no Safe Mode entry and aerobraking continued uninterrupted. The immediate observables were telemetry alarms indicating that S1 failed to move when commanded and that the backup amplifier was in use. With the WTS #1 failure, one X-band amplifier is essentially hardwired to the HGA and the other X-band amplifier is hardwired to the LGA. Swapping between the antennas for downlink requires that one X-band amplifier be powered off, and the other powered on. Currently, the mission is successfully operating in this configuration with no impact to nominal science collection and downlink, or to Safe Mode operations.

Ground Response. In real-time, none was necessary. As soon as the command blocks could be revised (about three days), antenna switching during the drag passes was stopped in order to minimize power cycles of the two TWTAs. Steps were taken to prevent any future commanding of this switch. The investigation into root cause commenced, eventually lasting six months.

Analysis of the onboard telemetry and RF downlink characteristics indicates that the switch is stuck in an intermediate position. The RF signal is ~1dB less than nominal, indicating that a mechanical interference is preventing proper positioning of the switch mechanism. Clearances within the switch are small, which means that small amounts of debris could easily cause the switch rotor to bind. An extensive investigation concluded that the most likely root cause was conductive debris (perhaps from flaked plating) floating in the zero g environment, which eventually came into contact with a polyimide tape window at one of the active WTS RF ports. These windows are used as a contamination barrier on the WTS RF ports, but they may have contributed to the severity of the anomaly. Vent holes in the windows can admit contamination, adhesive on the inward-facing side of the tape can entrap it long enough to initiate RF breakdown, and the breakdown can cause the polyimide tape itself to pyrolyze, injecting a large amount of polyimide tape debris into the switch and causing it to bind. Laboratory testing has demonstrated the window destruction mechanism, as shown in Fig. 3. The initiating debris used in testing, a small metal sliver, can be seen in the “before” images. Possible causes other than mechanical interference have also been examined, but do not appear consistent with the observable data. The project does not currently plan any more actuation attempts of the failed wave guide switch; further loss of downlink power would be possible if the switch were to stick in a less favorable position than it is in now.

For MRO, X-band downlink over each antenna is now single string relative to X-band amplifier failure. A subsequent loss of one of the two amplifiers would preclude either low gain or high gain antenna downlink, depending on which amplifier failed. Because Safe Mode was designed to use the low-gain antenna exclusively, failure of the amplifier connected to the LGA would directly impact the functionality of Safe Mode. Steps have being taken to modify Fault Protection’s safe mode configuration to use HGA in this event. Failure of the amplifier connected to the HGA would impact the ability to downlink science data. Here the existence of Ka-band downlink on MRO provides an important potential backup for achieving science mission objectives. Demonstrations performed during cruise have already validated MRO’s ability to use this option. Because of the potentially limited life of the remaining Ka hardware (due to the SDST anomaly discussed above), the MRO project has decided to defer remaining Ka-band demonstration activities in order to keep Ka in reserve as a backup to X-band.

Safety nets used. Onboard Fault Protection was critical to vehicle survival. During the short orbits (~4 hours) of Aerobraking, the ground would have had to diagnose the problem, re-establish communication, and command a maneuver within 48 hours in order to prevent possible loss of the spacecraft in the Martian atmosphere. Because a stuck switch was considered a non-credible failure, the existing Loss of Signal Contingency Plan did not provide detailed diagnosis steps. Because fault protection diagnosed and worked around the problem in real-time, the vehicle was never at risk for entering the atmosphere.

Lessons learned: The primary lessons learned in this anomaly relate to telecom subsystem design and the consequences of contamination. The use of polyimide tape as a contamination barrier at the RF ports of the waveguide switch provides a significant source of additional debris if the polyimide pyrolyzes. The polyimide tape adhesive provides a mechanism to entrap conductive debris which could trigger pyrolysis under the right conditions. When designing high power RF systems, more serious consideration should be given to the role of contamination in causing RF-breakdown.

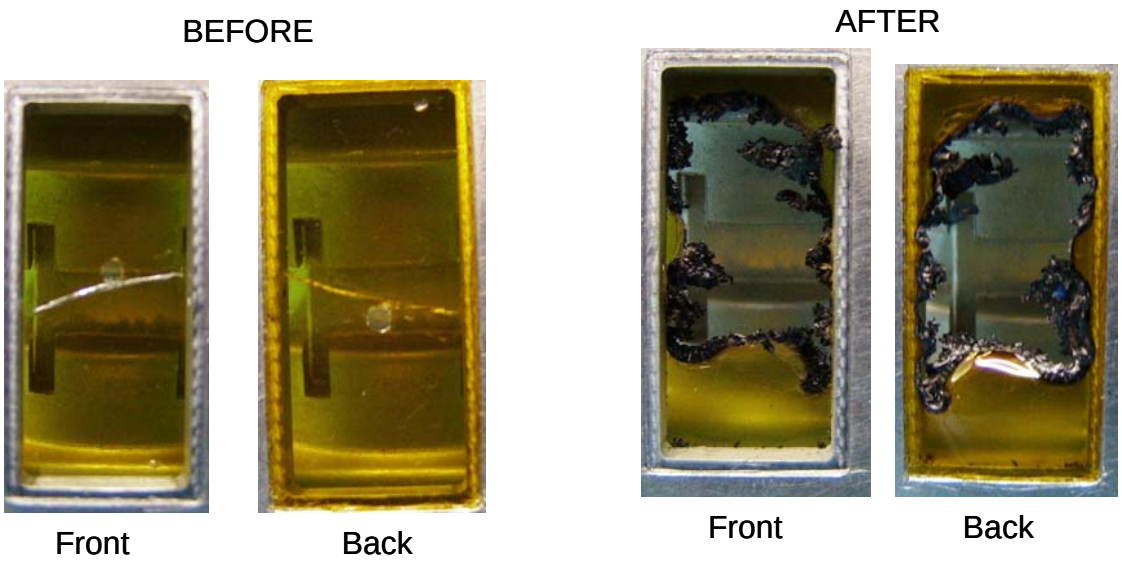

Figure 3. Kapton Pyrolysis From Metal Sliver at 100W RF

F. Computer Side Swap (Primary Science Phase)

On 14 March 2007, planned acquisition of downlink signal following occultation on orbit 2956 was unsuccessful. The operations team executed LOS Contingency Plan. During the entire portion of this orbit with DSN visibility, no downlink signal was detectable. The team was unable to rule out DSN station problems. Nor were they able to rule out catastrophic telecom subsystem failure (due to possible damage from the earlier RF transfer switch failure). Difficulties configuring the DSN resulted in significant delays in the ground's response, but by the second occultation exit the DSN had configured to look for the safe mode downlink, which it found and was able to acquire. Telemetry indicated the spacecraft had experienced two successive timeouts of the heartbeat watchdog timer. The first timeout triggered an autonomous warm reset on side A. The second timeout triggered an autonomous swap to the side B computer, where boot-up proceeded nominally. As part of the nominal B-side configuration, the redundant star tracker and inertial measurement unit (IMU) were activated.. After the boot-up on side B, Fault Protection autonomously configured the vehicle into safe mode.

Fault Protection response. Examination of the telemetry revealed no evidence of fault protection detecting or responding to any problems.

All components appeared to functioning normally in their B-side configuration. The project decided to execute the Safe Mode Recovery Contingency Plan on the B-side. In the meantime the investigation was started to determine the root cause of the side swap. MRO's C&DH redundancy architecture is cold backup (i.e., powered off). When a C&DH is powered off, all of its volatile memory is lost. MRO does record information in nonvolatile memory, but in this case, where the software appears to have stopped executing, this information is limited.

Redundancy Considerations. Before the side swap, the condition of several redundant components was unknown, since they were last powered prior to launch. The condition of all these components is now known to be

good. However the critical unknown is whether the Side A C&DH is usable or not. The investigation has narrowed the possibilities down to eight potential proximate causes, some recoverable and some not. The most likely proximate cause is thought to be an interrupt signal failing active, which would not be recoverable. As of this writing, a root cause has not been isolated.

Safety nets used. In this case it appears that either fault protection software did not detect or respond to any problems, or that hardware faults in C&DH A prevented the recording of that data. In either case, it was the low level firmware-based fault protection which was critical to detection of a failure to boot and forcing a swap to the backup computer. High Level Fault Protection Software was then necessary to configure the vehicle in safe mode. Ground contingency plans for LOS were necessary to find the safe mode signal, and Safe Mode Recovery Contingency Plan was necessary to return the vehicle to nominal operations. The availability of a backup C&DH probably saved the mission.

Lessons learned: future designs should increase the amount of low level information available to diagnose boot-up problems.

VI. Conclusion

Any spacecraft with requirements for high reliability and operating with significant light-time latency needs a multilayered safety net including significant levels of redundancy, sophisticated autonomous fault detection and response, and pre-defined ground response procedures executed by a capable team of experts on the ground. The anomalies MRO has survived so far in its mission illustrate that no one element of this safety net by itself is sufficient. In cases of operational error or software flaw, two of the three elements (autonomous fault protection and ground procedures/teams) were sufficient. In cases of hardware failure, all three elements (the first two plus hardware redundancy) have proven essential.

Acknowledgments

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The author would like to express his appreciation to Eric Seale for permission to use parts of his publication on MRO fault protection design, as well as for his helpful comments on my adaptation.

References

[1] Mars Reconnaissance Orbiter Mission Plan, JPL D-22239 Revision C (General Release), October 2006.

[2] Slonski, J. P., "Cross Strapping Considerations," unpublished briefing materials, 2002.

[3]Kenworthy, J.C., Seale, E.H., Dates, J.A., "Autonomous Fault Protection Orbit Domain Modeling in Aerobraking," IEEEAC paper #1195, 2007.

[4]Seale, E. H., "The Evolution of a SPIDER: Fault Protection, Incremental Development, and the Mars Reconnaissance Orbiter Mission," IEEEAC paper #1098, 2002.

[5] *Ibid.* Seale.