



JPL

Mars Exploration Rover

The Spirit FLASH Anomaly Story

Glenn E. Reeves

*Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California*

Khaled S. Ali

*Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California*



Root Cause - File System Software Design



Mars Exploration Rover

- **Design**
 - **DOS file system**
 - **The file system software module design uses a RAM resident data structure mechanism to represent the structure of the file system directories and sub-directories**
 - **This mechanism allows optimized management of erase and write operations on the FLASH memory devices**
 - **The complexity of this data structure corresponds to the complexity of the file system structure**
 - **Primarily the number of sub-directories and the number of files in each sub-directory**
 - **The software uses a reserved memory space in which to build and maintain this internal data structure**
 - **The internal data structures are recreated from the file system structure each time the flight software initializes**

- **Design Error**
 - **The design does not compact internal data structures when files are deleted**
 - **This caused continuing growth in the file system data structures (and additional memory allocations) as the number of files grew in the various sub-directories**
 - **The internal data structure use did not change even when the files were deleted**



Root Cause(s)



Mars Exploration Rover

- **Two modules had configuration errors**

- **File system module**
 - **The configuration permitted additional memory to be allocated from the system memory pool once all of the pre-allocated, initial, memory area was in use**
 - **This allowed the system memory pool to be used until no unused space was available**
 - **The correct configuration would have been to not allow additional memory to be used**
 - **This would have been equivalent to a full file system which the design handles correctly**

- **Memory Allocation Module**
 - **The configuration was set to suspend a task when a request for additional memory space could not be satisfied**
 - **The flight software treats suspended tasks as severe errors and initiates a reset**
 - **This was a debug, not a flight, configuration**
 - **No vehicle error telemetry is produced for this action**
 - **The correct configuration would have been to return an error and allow the file system software logic to react**



Repetitive Reset Behavior



Mars Exploration Rover

- **Repetitive reset cycle explained**
 - **The flight software was writing a file in the FLASH file system**
 - **The file system data structures expanded to the point where all memory space was consumed**
 - **This task is suspended in the middle of accessing the file system**
 - **This task suspension was detected and the software reacts with the first reset**
 - **The flight computer resets and the flight software began initialization**
 - **During initialization the FLASH file system is re-mounted; this causes the recreation of the RAM resident file system data structures**
 - **This action consumes all of the available memory**
 - **The cycle repeats**



Ancillary Effects

Mars Exploration Rover

- **The state of the file system software after the error resulted in “deadlock” condition whenever any other part of the flight software attempted to use or access any of the onboard file systems**
 - **The software which performs the vehicle shutdown did not execute successfully because the file system could not be taken off-line**
 - **Debug scripts could not be opened and read**
 - **Debug results could not be written to files**
- **The multitude of resets caused file system corruption**
 - **Some loss of data**
 - **Created concern that FLASH device failures might exist (no failures were detected)**
- **The reset during the Sol 18 HGA communication session resulted in the loss of onboard knowledge needed to point the HGA**
 - **Created concern that there might be an HGA antenna problem**
 - **Forced use of the LGA which dramatically reduced visibility**



Why?

Mars Exploration Rover

- **The problem never occurred during the test program**
- **Later review of the test data did show indications that the memory consumption was occurring**
- **We ***might*** have caused the problem to occur if longer duration tests were conducted AND the activities were more demanding than those done in flight**
 - **This was unrealistic given the development schedule**



Summary



Mars Exploration Rover

- **We were very lucky but we also anticipated the type of problem and built in mechanisms to aid in the recovery**
- **The problem was elusive and debugging software problems in space is very difficult**

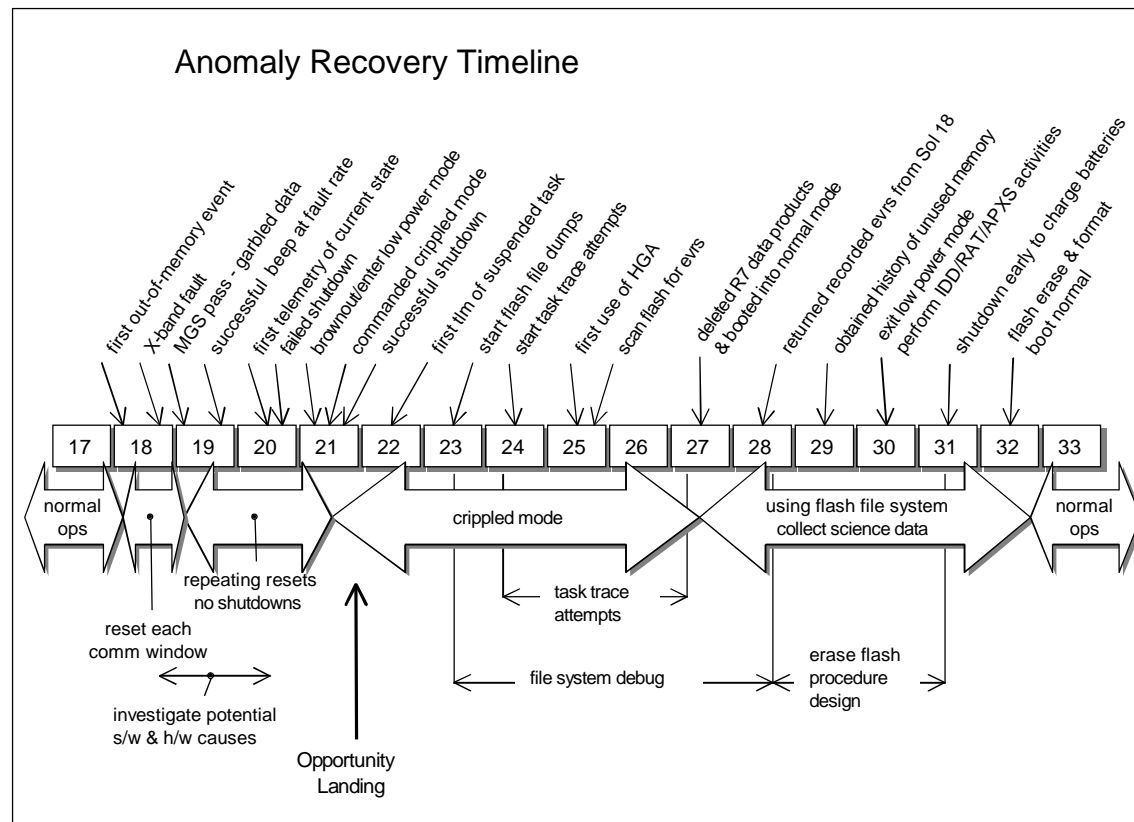


Timeline



Mars Exploration Rover

- **The first indication of trouble was on Sol 18, January 20, 2004**
- **Recovered control of the vehicle on Sol 21**
- **Diagnostic activities continued until Sol 31**
- **Partial science data collection from Sol 27 to Sol 32**
- **Vehicle returned to normal operation on Sol 32**



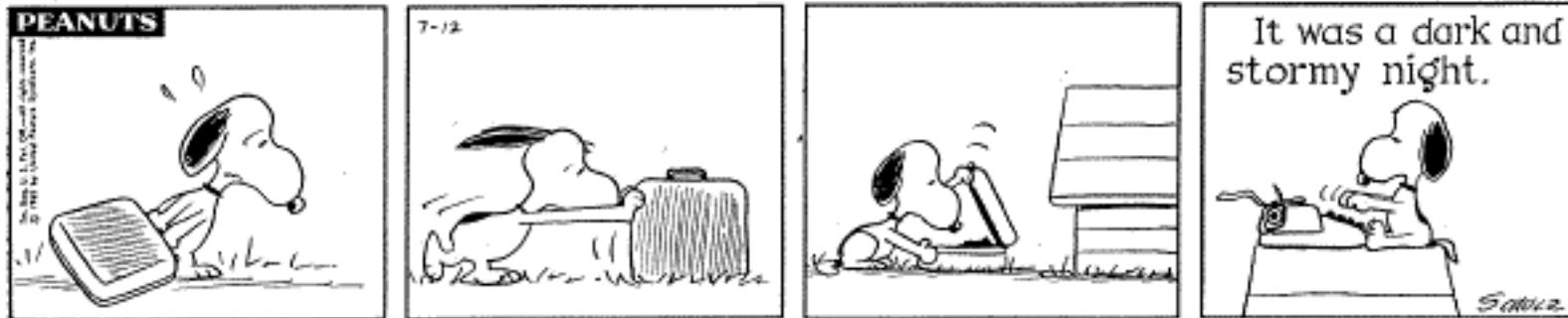


The Tale



Mars Exploration Rover

- **It was a dark and stormy night**



Copyright © United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited.

- **Actually it really was a dark and stormy night at the Deep Space Network facility in Canberra, Australia**
 - Wind, rain, lightning
 - The DSN station had initially reported antenna pointing problems
- **So, a loss-of-signal 14 minutes early, wasn't a cause of concern**



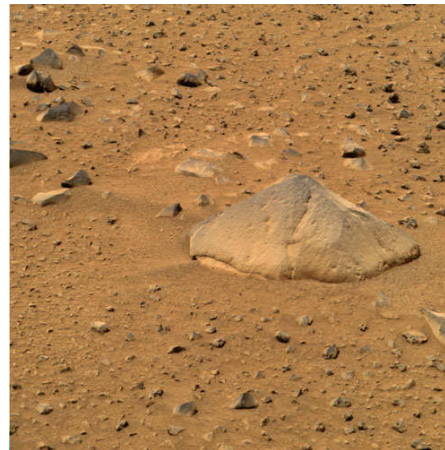


Sol 18



Mars Exploration Rover

- **The Spirit vehicle had been on the surface of Mars for 18 days (i.e. Sol 18)**
- **The vehicle was healthy and all previous activities had occurred as expected**
- **On Sol 18 the early morning activity was a check out of the Mini Thermal Emission Spectrometer (MTES) elevation mirror actuator**
 - **There was concern regarding using the actuator at low temperatures**
- **The remaining activities for the day were to use the MI, APXS, and then the RAT on the target rock Adirondack**



- **The first X-Band communication session began at 9:00 LST right on schedule**



First indications of trouble

Mars Exploration Rover

- **The telemetry from the vehicle indicated that the early morning command sequences were running and that the vehicle was in good health**
 - These command sequences had been loaded the previous day
- **Some transmission errors had occurred during the morning uplink and some of the command sequences for the day had not been successfully received**
 - This was not unexpected due the weather and the DSN station issues
- **When the premature loss-of-signal occurred we attributed it to the weather**
- **The operations team began an effort to salvage as much of the planned activities as possible**
- **We commanded a communication session which would use the onboard high-gain antenna**
 - This would allow us to retransmit the missing command sequences to the vehicle and to receive additional telemetry
- **No signal was seen**





First indications of trouble



Mars Exploration Rover

- **We again attributed the failed communication to either the weather or a DSN station problem**
- **We commanded a “beep” using the low gain antenna**
 - **Worked as expected!**
- **This was good news**
 - **The vehicle was responding to commands and the vehicle had not entered a “fault” mode**
- **We were optimistic that there were no onboard problems**
 - **Commanded the afternoon command sequence to start**
 - **Received confirmation that it did start**
- **But**
 - **No signal was seen at the next HGA communication session**
 - **No signal was seen at the next ODY UHF communication session**
- **Now we really knew something was wrong**





Our Fears



Mars Exploration Rover

- **Hardware failure?**
 - **Telecom hardware?**
 - **Antenna failure?**
 - **Battery failure?**
 - **Electronics failure?**
- **Software problem?**
 - **No way!**
 - **But**
- **What was the state of the system ?**
- **We anxiously awaited the MGS UHF communication session scheduled for Sol 19 at 01:45**



More bad news

Mars Exploration Rover

- **The MGS UHF communication session was very discouraging**
 - **The session only lasted 2 minutes (instead of 10)**
 - **The only data received was a repeating pseudo-noise pattern**
- **This indicated that the UHF radio was being turned on by the software**
 - **Good**
- **But that either the interface to the UHF radio wasn't working**
 - **Very bad!**
- **Or the flight software was not delivering data to the UHF radio**
 - **Also bad!**
- **No signal at all was detected by the ODY spacecraft for the 4:15 AM UHF communications session**



Initial Diagnostic Efforts - Sol 19



Mars Exploration Rover

- **More communication sessions were attempted**
 - **No signal**
- **Several more beeps were attempted at the normal uplink data rate**
 - **All were unsuccessful**
- **Commanded a beep at a lower uplink data rate**
 - **Success!**
- **This indicated that the FSW had entered a “fault” mode**
 - **This narrowed the number of cause/effect possibilities**
 - **We demonstrated we could command the vehicle!**
- **We still did not have enough information!**



First Hope



Mars Exploration Rover

- **Sol 20 did not have a promising beginning . . .**
 - No signal was detected for either of the overnight UHF communication sessions
- **An LGA communication session was commanded that produced brief, repeating, telemetry data**
 - Loss-of-signal occurred earlier than expected
 - The repeating data indicated that the interface to the X-Band radio was working and that the interface between the software and the radio was probably working correctly
 - It appeared that the flight software was not (or could not) get data to the radio
- **The early loss-of-signal could be caused by the flight software turning off the radio as it initialized if a reset had occurred**
- **Hypothesis: The system was resetting each time communication was attempted or perhaps some failure was causing the vehicle to reset repeatedly**



Confirmation and More Bad News



Mars Exploration Rover

- **A subsequent LGA communication session was successful**
 - **Data for the complete session time period was received including a significant amount of engineering data**
- **This new information confirmed our hypothesis**
 - **Multiple resets had occurred**
 - **The first reset had occurred early in the morning of Sol 18**
 - **The resets were repeating and this often caused the communication sessions to terminate early or to never start**
- **The data also indicated that battery state of charge was much lower than expected**
 - **This indicated that the vehicle had been on much longer than expected or planned**



Urgent Commands



Mars Exploration Rover

- **It became a priority to shutdown the vehicle to preserve the battery state**
- **We commanded the vehicle to shut off for the day and wake up the next morning**
- **We then commanded a beep just to verify that the vehicle had actually shut off**
 - We did not expect to see a signal
- **A signal was seen!**
 - This indicated the command to shut off the vehicle was unsuccessful!
- **The flight software did not (or could not) shut the vehicle off**
- **What did this mean?**





Another clue



Mars Exploration Rover

- **The late afternoon, Sol 20, ODY UHF communication session was also successful**
 - 73 Mbits of data was received
 - The first, complete, UHF communication session since Sol 17
- **The telemetry data was not as expected**
 - Only data generated in real-time, during the communication session, was included
 - No recorded data was seen
- **Recorded data is stored as files in the FLASH file system**
- **New Hypothesis :**
 - There is something wrong with the FLASH memory, the file system, or the flight software that reads these data files and creates the telemetry data for downlink. Something related is causing the system to repetitively reset.



Dire Predicament



Mars Exploration Rover

- **The vehicle was in a very precarious state**
 - **The battery was weak and there did not appear to be a way to turn off the computer/electronics**
- **If we could not regain control of the vehicle then eventually the battery voltage would drop too low and the battery would be taken off-line**
 - **Even with the daily solar array energy partially recharging the battery**
- **No heating would occur overnight and eventually the temperature of the vehicle would drop below the design limits**
- **This could result in the complete loss of the vehicle or irreparably damage the battery, electronics, or the science instruments**



Foresight or Luck (or both)

Mars Exploration Rover

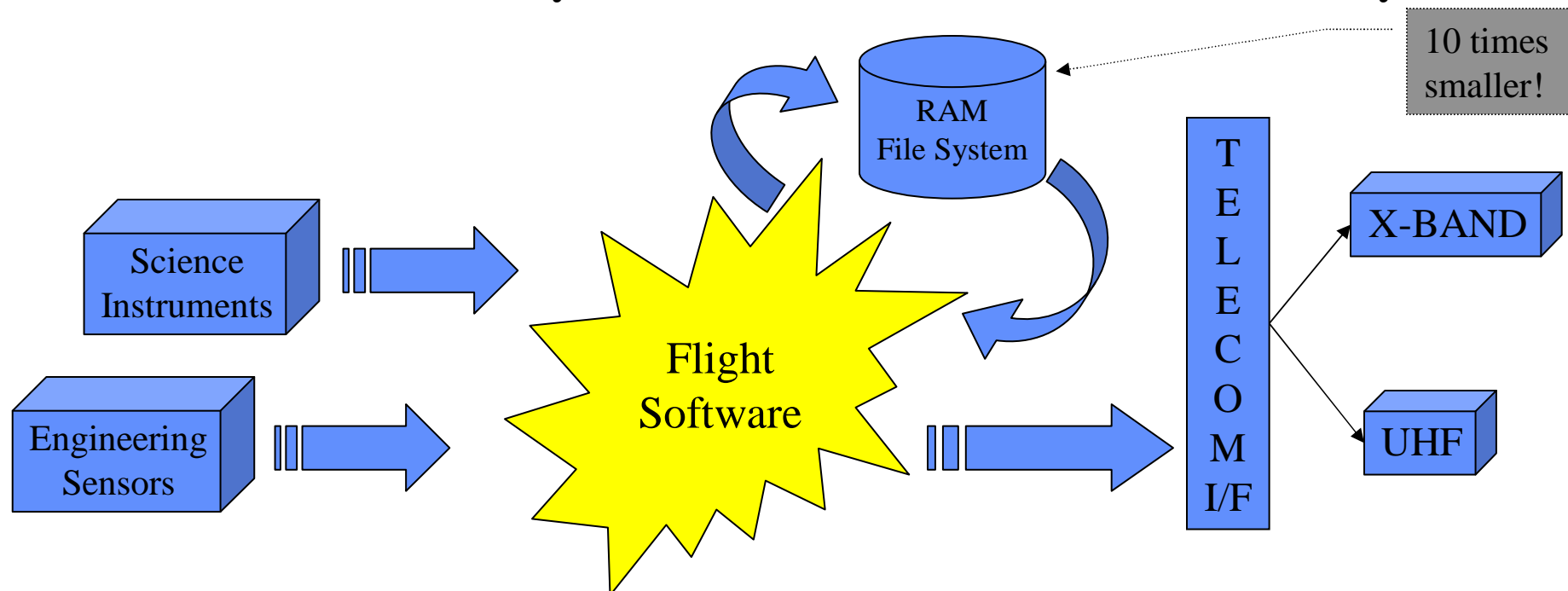
- **The design of the flight software includes a number of contingency commands and modes**
- **One mode, “crippled” mode, would cause the flight software to ignore the FLASH file system and to create a temporary file system in the CPU RAM instead**



System Design - “Crippled” Mode

Mars Exploration Rover

- **Forces the flight software to create and use a file system in RAM memory**
- **This volatile file system is used instead of the FLASH file system**
 - The switch is transparent to the rest of the flight software
- **System is usable and could have done a limited, degraded, mission**
- **Loss of non-volatile storage would have severely reduced mission return**
 - The RAM based file system is 10 times smaller than the FLASH file system





Foresight or Luck (or both)

Mars Exploration Rover

- **The design of the flight software includes a number of contingency commands and modes**
- **One mode, “crippled” mode, would cause the flight software to ignore the FLASH file system and to create a temporary file system in the CPU RAM instead**
- **If there was a problem with the FLASH or the FLASH file system then this mechanism might allow the system to initialize normally and avoid the repeating reset problem**
- **But**
- **The command needed to arrive in between the repeating reset cycles**
 - **It is only acted upon when the flight software is initializing**
 - **It must be commanded each time the vehicle wakes up**



Regaining control

Mars Exploration Rover

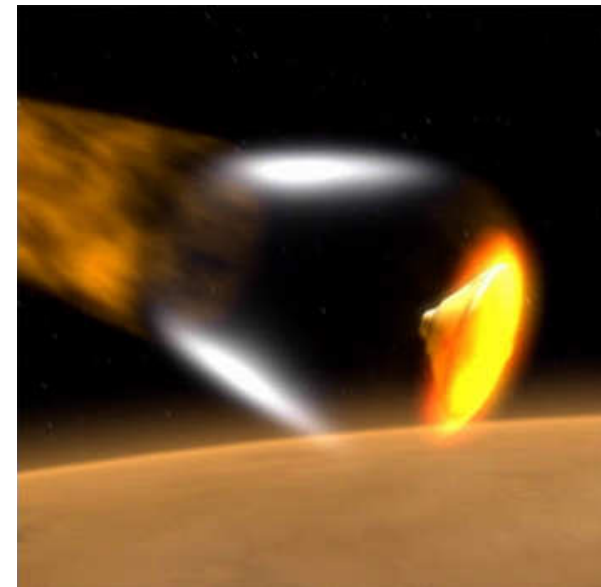
- **The team was able to predict when the repeating resets would occur on the vehicle and was able to send the command so that the flight software would act upon it at the right time**
- **The team demonstrated they had predicted the reset times correctly by identifying when a loss-of-signal would occur during a LGA communication session**
- **Late in the morning of Sol 21 the team commanded a LGA communication session which would either start and complete successfully if “crippled mode” solved the problem or would terminate prematurely if the hypothesis was wrong**
- **Success!**



Regaining control

Mars Exploration Rover

- **A full set of telemetry data was received during the communication session which confirmed the vehicle was in “crippled” mode**
- **The team commanded the vehicle to power off for the night.**
- **Again, a beep was commanded to verify the vehicle was off**
- **No signal was seen!**
- **We had regained control!**
- **And, Opportunity landed tonight (Sol 21)**





What was really wrong?



Mars Exploration Rover

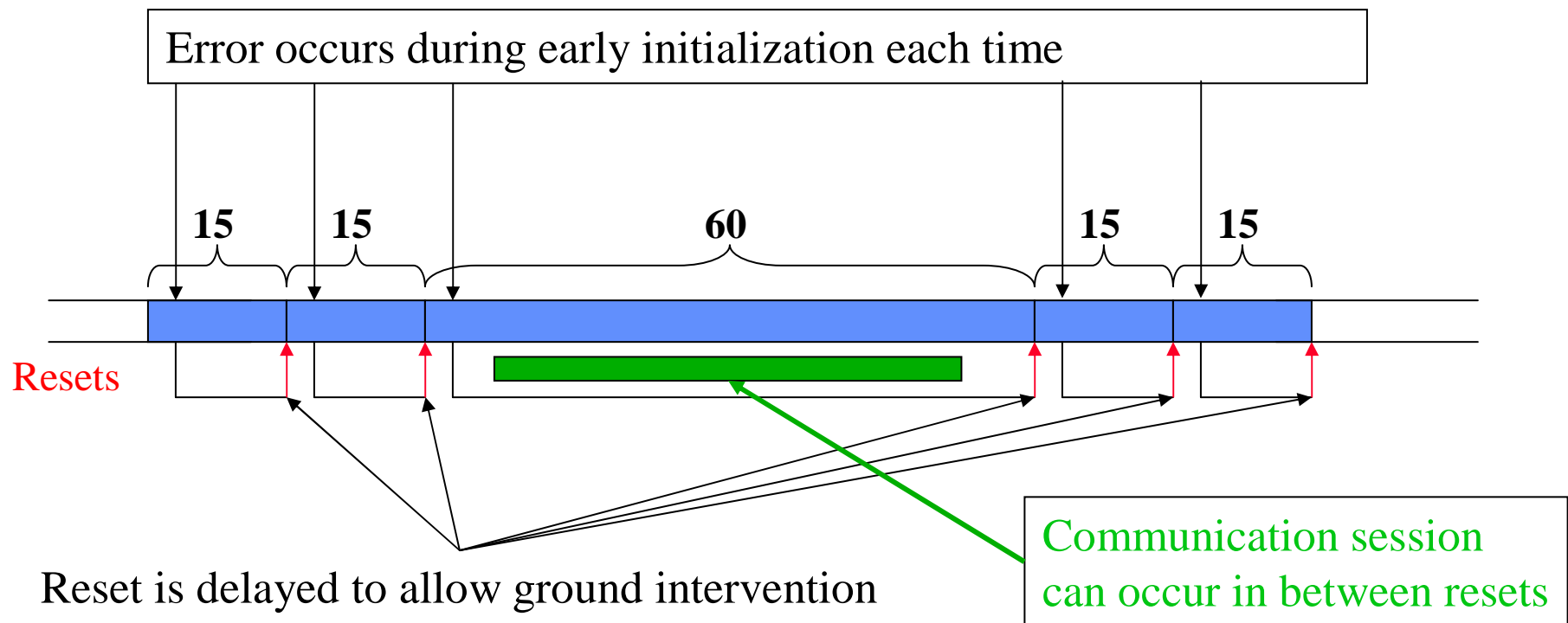
- **We still did not know exactly what was wrong**
- **We knew that :**
 - **The vehicle would repeatedly reset and that this stopped when “crippled” mode was commanded**
 - **We could predict when the resets would occur**
 - **We knew the vehicle would reset during the initialization process but did not know where; we suspected it was when the FLASH file system was mounted**
 - **We knew the vehicle would not shut off unless it was in “crippled” mode**
- **We had found the way to regain control but we still needed more information to diagnose the problem**
- **Unfortunately, most of the information we needed was lost on the next reset or was not retained once we entered crippled mode**
- **We needed a way to interrogate the spacecraft without using “crippled” mode**



Foresight or Luck (Again!)

Mars Exploration Rover

- Normally, if the flight software detects a severe error a reset is invoked
- However, if a severe error is detected during the software initialization period then the reset of the flight computer is delayed for a short period
 - On the surface the delay cycle is 15 minutes, 15 minutes, 60 minutes, and then it repeats
- This delay allows ground controllers a chance to command the vehicle even with a failure that causes repetitive resets





A Software Problem

Mars Exploration Rover

- **This allowed us to issue commands and start communication sessions in the 60 minute period between the second and third reset each morning**
- **Much of the flight software was obviously continuing to function correctly**
- **After several attempts the team was able to command a communication session that transmitted data related to the reset cause**
- **This data indicated a critical flight software task had crashed but did not indicate the precise reason**
- **We spent the next 10 days investigating the precise reason**



The Daily Cycle

Mars Exploration Rover

- **The subsequent diagnostic activities were dictated by the Martian day and the vehicle behavior as it woke up each morning**
- **We recovered sufficient margin in battery capacity quickly that allowed us to command multiple times each day and to command communication sessions multiple times per day**
- **Each day had two distinct activities on the vehicle**
 - **Diagnose the precise cause of the problem**
 - **Complex orchestration of actions prior to “crippled” mode entry**
 - **Determine the state of the FLASH file system**
 - **We wanted to recover data, both (science and engineering, but were concerned the file system was corrupted**
- **In addition many other team activities had to occur in parallel:**
 - **Waiting for telemetry**
 - **Planning for the next day’s ideas**
 - **Exploring theories in the test bed**
 - **Rehearsal of activities in the test bed**
 - **Reporting status**
 - **Coordination among all team members**

-Sleep



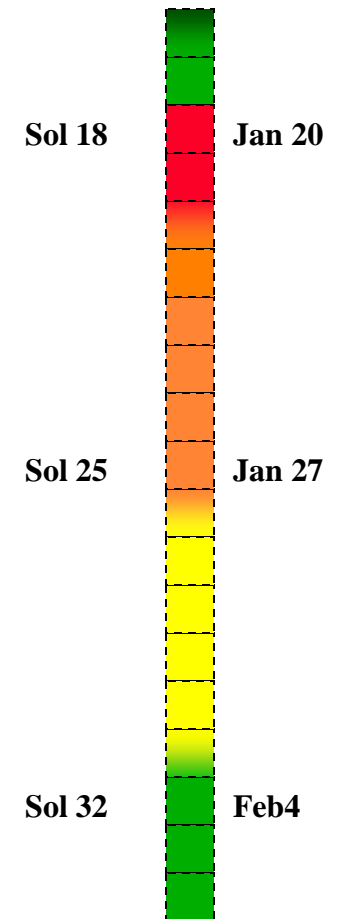


Remote Debugging



Mars Exploration Rover

- **Identifying the precise problem proved to be very challenging**
- **We knew that one of the flight software tasks had crashed**
 - The answer lay in obtaining a trace of the FSW after the error had occurred
- **Techniques**
 - Scripts which used operating system functions to create task data
 - Scripts and commands with primitive functions to dump or examine different areas of the RAM and FLASH memory
 - Designed, implemented, loaded, and executed specialized software to:
 - Scan the FLASH memory areas to identify where engineering and science data was located
 - Perform file system integrity checks on the FLASH file system
 - Scripts to mount and check the FLASH file system while the system was in **CRIPPLED** mode
 - Scripts to manipulate the use of the onboard memory to avoid the root problem during the debug activities
- **Many of our debug techniques failed because of ancillary effects of the problem**
- **We used most of the debug and contingency mechanisms that had been built into the system**



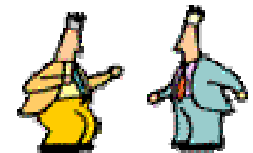


Recovery



Mars Exploration Rover

- **By Sol30**
 - **We knew the root cause of the problem**
 - **We were able to temporarily fix the problem by removing files from the FLASH file system**
 - **We had returned to normal mode and were using the FLASH file system again**
 - **We were able to transmit almost all of the engineering and science data that was stored in the FLASH file system before Sol 18**
 - **We had decided to erase all of the FLASH memory and to reinitialize the FLASH file system**
 - **We understood all of the ancillary effects that the root problem caused**
 - **We had conceived and designed a fix for the root problem**
 - **We would patch the flight software on Sol 98**





Acknowledgments

Mars Exploration Rover

- **The recovery of the vehicle was truly a team effort. Many members of the operations team made valuable contributions to the recovery.**
- **There is a small group of individuals who deserve to be recognized for their thoughtful input and extraordinary effort. This group was the nucleus of the diagnostic team. It was their insight which led to the regaining control of the vehicle. Many of them spent long days and nights in the test bed exploring the problem and testing the recovery actions. Through their efforts the vehicle was recovered and returned to normal operations**

•**Khaled Ali**

•**Jeff Biesiadecki**

•**Mike Deliman**

•**Jim Donaldson**

•**Ed Gamble Jr.**

•**David Hecox**

•**Roger Klemm**

•**Todd Litwin**

•**Tracy Neilson**

•**Cindy Oda**

•**Ed Odell**

•**David Smyth**

•**Joseph Snyder**



JPL

Mars Exploration Rover

Backup Material



Abstract



Mars Exploration Rover

- *The MER vehicle ‘Spirit’ suffered a debilitating anomaly that challenged the team to fix and recover. Only a small amount of science data was lost but several anxious days were spent diagnosing and fixing the anomaly. With the eyes of the world upon us the anomaly team used each scrap of information, their knowledge of the system, and sheer determination to fix the problem and return the vehicle to normal operation. This paper will discuss the Spirit anomaly including the drama of the investigation, the root cause and techniques used to return the vehicle to normal operations.*



System Design - Communication



Mars Exploration Rover

- **Telecom**
 - **X-BAND** direct to earth using either a low-gain or high gain antenna
 - **UHF** to either Mars Global Surveyor (MGS) or Mars Odyssey (ODY)
- **Communication Sessions**
 - **Communication sessions are normally pre-planned and the on board software configures the telecom hardware and begins communication**
 - **Communication sessions can also be commanded to by command**
- **“Beeps”**
 - **A beep is a very short (< 5 minute) communication session without data**
 - **Used to indicate to the ground controllers that an event has occurred**
 - **Usual use was to indicate if the command sequence for the day had started correctly**
 - › **A beep at a slighter later time would indicate that yesterdays main command sequence was still executing**



System Design - On / Off Control



Mars Exploration Rover

- **The overall power and thermal system was designed with the expectation that the vehicle would charge its batteries during the day and be off at night**
 - **Thermostatically controlled heaters operate autonomously when the flight computer is off to keep critical components above their minimum temperatures**
- **The flight computer and electronics are designed to be turned off to conserve energy**
- **Balancing daily activities (communication, driving) with the battery state-of-charge must be done by the operations team**
- **A separate unit, the Battery Charge Board (BCB) monitors the battery voltage and autonomously charges the battery during the day**
 - **Takes the batteries “off-line” if a low voltage condition is detected**
- **The flight software performs the shutdown process upon command**
 - **Idles on board activities**
 - **Saves state information**
 - **Un-mounts file systems to avoid data corruption**
 - **Removes power**
- **Two mechanisms can wake the vehicle**
 - **Alarm clock**
 - **Solar array current detection**



System Design - Resets



Mars Exploration Rover

- **The flight software detects severe errors and reacts by forcing a reset of the flight computer and electronics and a re-initialization of the flight software**
 - **The assumption is that some errors can be cleared by the reset**
- **Examples**
 - **Runaway code execution**
 - **Memory allocation errors**
 - **Errors where parts of the flight software are not responsive**
 - **Logic errors indicating some form of memory or processor or corruption**
 - **Errors indicating illogical software execution**
 - **Errors caused when interface cards or devices do not respond**



System Design - Onboard File Systems



Mars Exploration Rover

- **Multiple file systems are used on board**
 - RAM, EEPROM, and FLASH memory based
- **DOS File system structure**
- **The FLASH file system is used as the non-volatile repository for all data products (files)**

220 MBytes

- **All science data and much of the engineering data is stored in the FLASH file system before transmission**

