# GALILEO SPACECRAFT ANOMALY AND SAFING RECOVERY

Ralph R. Basilio and David M. Durham

N94-23864

**Jet Propulsion Laboratory**
**California Institute of Technology**
**Pasadena, California, U. S. A.**


## ABSTRACT

A high-level anomaly recovery plan which identifies the steps necessary to recover from a spacecraft "Safing" incident was developed for the Galileo spacecraft prior to launch. Since launch, a total of four in-flight anomalies have lead to entry into a system fault protection "Safing" routine which has required the Galileo flight team to refine and execute the recovery plan. These failures have allowed the flight team to develop an efficient recovery process when permanent spacecraft capability degradation is minimal and the cause of the anomaly is quickly diagnosed. With this previous recovery experience and the very focused boundary conditions of a specific potential failure, a Gaspra asteroid recovery plan was designed to be implemented in as quickly as forty hours (desired goal).

This paper documents the work performed above, however, the Galileo project remains challenged to develop a generic detailed recovery plan which can be implemented in a relatively short time to configure the spacecraft to a nominal state prior to future high priority mission objectives.


Key Words: Recovery plan, safing, system fault protection, anomaly

## 1. INTRODUCTION

The Galileo Project is an investigative mission undertaken by the National Aeronautics and Space Administration (NASA) to acquire, process, and analyze scientific data obtained from the Jovian system.

### 1.1 The Galileo Spacecraft and Mission

The Galileo spacecraft (Figure 1) was launched on board the Space Shuttle Atlantis and injected into its Venus-Earth-Earth Gravity Assist trajectory by a two-stage Inertial Upper Stage on October 18, 1989. On October 29, 1991 an opportunity of historical significance manifested itself with the first ever flyby of an asteroid (Gaspra) by a man-made spacecraft. Another flyby of a second asteroid (Ida) on August 28, 1993 is currently being planned. Upon approaching Jupiter in 1995, the Orbiter will release a Probe containing six scientific instruments and send it on its way to acquire and relay back scientific data on the Jovian atmosphere. The Orbiter will then be injected into an orbit around Jupiter to perform an intensive twenty-two month scientific investigation of the Jovian system (the planet, its major satellites, and its extensive magneto-sphere). The science investigations will be conducted through the use of four remote sensing and six fields and particles science instruments mounted on the Orbiter.

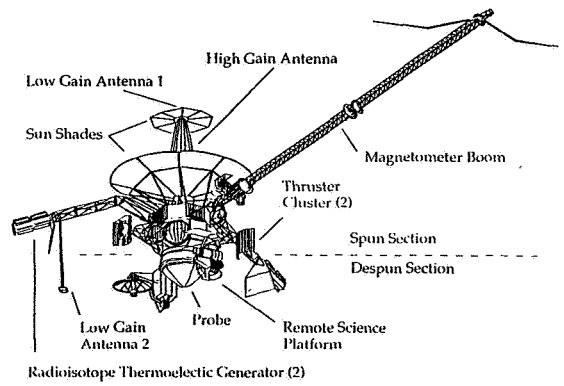


*Figure 1 The Galileo Spacecraft*

### 1.2 Sequence Development and Verification

Normally, the spacecraft is controlled and operated through the execution of Nonpriviledged Memory Sequence Loads (NMSLs). The duration of each of these sequence loads, used to implement mission activities, may last from a few days to many weeks depending upon mission objectives. Development of the NMSL begins with the activities defined in the Galileo Mission Plan which is used to create a detailed timeline of events. This timeline includes all internal and external resources for execution of the sequence load including timing, ground station allocations, and spacecraft monitoring periods. This resulting timeline is called the Cruise Plan (CP), and takes approximately six weeks to develop. Expansion of the CP is accomplished by specifying the detailed parameters and options of the spacecraft blocks, resulting in a detailed time ordered listing of the commands needed to execute the sequenced activities.

This listing is designated the Profile Design (PD) product and its development typically takes four weeks. The PD product is then converted to the actual NMSL via a sequence translation program and a ground command file is created for uplink to the spacecraft. This phase of the development usually takes another four weeks.

To accommodate unplanned activities or respond to anomalies, real time commands are generated and transmitted to the spacecraft. The duration of the real time command development process can vary from minutes or several days depending on command sequence complexity and urgency.

Validation of the NMSLs are accomplished via manual reviews and software constraint checking of activity plans, command sequence files, and sequence of events listings. Final command sequence verification is primarily performed on the Galileo Test Bed, a facility comprised of flight hardware and software. The prime subsystems comprising the test bed are Command Data Subsystem (CDS) and the Attitude and Articulation Control Subsystem (AACS).

Test bed operations provide the detailed command execution and timing verification which is difficult to ensure just by manual inspection by engineering analysts.

### 1.3 System Fault Protection Safing Routine

Under some anomalous conditions, faults may place the Orbiter or Probe in jeopardy. To ensure Orbiter and Probe system health and safety, the Orbiter is equipped with autonomous System Fault Protection (SFP). SFP responds with a pre-determined set of commands to safe the spacecraft. The Safing response specifically established for the interplanetary cruise phase is designed to:

- Terminate the active NMSL to prevent unwanted interference with the Safing response.
- Cycle electrical loads off/on to establish a sufficient power margin and be thermally safe.
- Locate the remote science platform to a safe position to protect light sensitive instruments from the sun and thruster plume contaminants.
- Ensure commandability and telemetry according to mission phase dependent requirements.

The Safing response is accomplished in two parts. Safing-1 halts the NMSL and switch off most non-Safing critical switchable electrical loads. Safing-1 places a message in telemetry to alert the flight team of the safing event. Safing-1 ends with a request to initiate Safing-2. Safing-2 establishes a known, safe quiescent state to enable key functions. Safing-2 first halts all AACS tasks except for periodic benign sun acquisitions. Next the telecommunications state is configured to permit transmission of engineering telemetry. Safing-2 next widens the AACS spin rate and pointing deadbands to more tolerant and robust values. If the safing incident leaves the spacecraft sun pointed, the routine for calling sun acquisitions every 12 hours will continue, thereby causing the spacecraft to track the sun.

Special cruise phase specific instrument safing, propulsion, and thermal safing commands may be issued in real-time to further establish a safe and stable spacecraft state.

### 1.4 Pre-Launch Safing Recovery Plan

A recovery contingency plan was developed pre-launch. Based on the SFP autonomous responses and entry causes, the plan outlines a process guiding a generalized recovery. The flow of this generalized recovery is as follows:

- Recognize that SFP has been invoked and, if in safing, the exact time the NMSL was aborted.
- Identify and immediately correct safety threatening conditions on the spacecraft.
- Determine exact state of the spacecraft at the time of SFP entry, following the spacecraft's autonomous response, and at the projected sequence restart point.
- Establish cause of the anomaly and correct any persistent fault condition or implement work-arounds for any reduction in spacecraft capabilities.
- Implement spacecraft reconfiguration to the selected sequence restart state.
- Restart aborted sequence or next sequence at its designated load boundary.

However, the plan did not try to be specific, recognizing the following uncertainties:

1. What is the nature of the anomaly causing entry into the safing routine and what corrective action or work arounds are necessary?
2. What was the specific state of the spacecraft at the time of the anomaly?
3. What is the desired state of the spacecraft following recovery and resumption of the nominal operations?

Establishing comprehensive reconfiguration command files or stored sequence restart points which provide opportunities to bring the spacecraft back up to specified states was deemed not practical. A large number of contingency files would have to be generated and significant sequencing memory space would have to be reserved for establishing restart points. The latter presented a memory management difficulty for CDS software analysts. In addition, the cause of an anomaly and fix/workarounds cannot be pre-determined and may negate any pre-generated reconfiguration files and/or restart points in the sequence. Therefore, a predetermined and complete

generic safing recovery contingency plan for any anomaly had been determined not feasible. However, assuming a specific failure, the state of the spacecraft at the time of an anomaly and at a specific restart point, a rapid recovery could be realized.

## 2. FIRST SAFING INCIDENT

During the final few weeks of the Earth-Venus leg of the mission, the spacecraft was being commanded via a sequence load designated EV-5. An AACS Star Scanner (SS) calibration, executed during the previous sequence, did not produce all the desired results. Another attempt was then planned for the EV-5 time frame to be executed via real time commands and in parallel with the EV-5 sequence.

### 2.1 System Fault Protection Safing

Early in the morning on Day Of Year (DOY) 90-015, downlinked AACS telemetry data indicated that an attitude estimate-related fault had occurred during the previous evening, and that an autonomous abort had brought the subsystem from inertial (Gyro-based attitude estimate) to cruise mode (celestial-based attitude estimate). After much deliberation, the flight team decided to proceed with the transmission of the SS calibration real-time commands even though the assumed spacecraft initial state had changed. It was believed that data gathered during the calibration may give some insight into the fault occurrence. Shortly after the start of the activity, AACS analysts observed that the clock controller was experiencing difficulty in maintaining control (position and rate) of the Spin Bearing Assembly (SBA). After some time, AACS SBA-related fault monitors began to trip, eventually leading to an AACS Power On Reset (POR). This resulted in SFP canceling the EV-5 sequence and requesting spacecraft safing. With the sequence recovery contingency plan in hand, the flight team embarked on a effort that would test the generalized flow defined pre-launch.

### 2.2 Anomaly Diagnosis

Following verification of all AACS telemetry measurements, AACS analysts set off to recreate the anomaly on the test bed. Using cruise mode as the initial state, the analysts observed similar behavior and trips of the same SBA-related fault monitors as observed in flight. Based on these findings and detailed investigative study, a preliminary theory into the cause of the anomaly was developed within hours of the flight incident. The cause of the problem was attributable to a then unknown idiosyncrasy with the AACS Flight Software (FSW) attempting to maintain a celestial pointing SBA scan type in cruise mode without celestial attitude reference available. Without celestial attitude reference, the AACS FSW calculated stator (despun section) attitude based on a noisy spin rate source (i.e. Solar Acquisition Sensor), resulting in SBA control instability. This theory was eventually verified through further test bed simulations and analysis. The spacecraft had been in a different initial state then what the SS calibration had been designed for. Therefore, it was determined that a sequencing error had caused the anomaly, not a failure of one part of the spacecraft system. No degradation of spacecraft capability was noted.

### 2.3 Recovery and Return to Nominal Operations

To ensure telemetry and thermal safety, real-time commands were sent within hours of the safing incident to reconfigure the telecommunication downlink data rate and propulsion thermal state. Following diagnosis of the anomaly and verifying that no degradation of spacecraft capabilities occurred, the top priority of the flight team was to return the spacecraft to the correct configuration for transmission and execution of the EV-6 sequence, which contained considerably important Venus encounter science activities. The flight team deliberately chose to follow the generalized flow of the recovery plan in a prudent and systematic manner, so as not to jeopardize the Venus science encounter activities.

Although there was a goal to salvage as much of the canceled EV-5 sequence as possible, this was not feasible due to lack of sun-pointed stars needed for reacquiring celestial reference. Since no sun-pointed star sets were available until after the planned final attitude update in EV-5, none of the sequence was salvaged. Consequently, all necessary engineering activities scheduled for execution during the latter portion of the sequence were performed via real-time commands, adding to the flight team's work load. In addition, the first two days of the EV-6 sequence was truncated to allow time for required engineering and science subsystem reconfiguration activities. On DOY 90-037, twenty-three days following the anomaly the shortened EV-6 sequence was successfully transmitted to the spacecraft and executed nominally.

Having taken a prudent and systematic approach, the flight team had an opportunity to verify the generalized recovery process. This gave the flight team confidence in knowing that if future anomalies occur, the flight team would have available a tested contingency plan for reference.

## 3. SUBSEQUENT SAFING INCIDENTS

As noted earlier the Galileo spacecraft has experienced four entries into Safing to date. The

recent three entries have all been caused by the same condition. This condition was caused by one of the two redundant CDS operating strings detecting a despun CDS POR, causing this string to "shut down" after informing the other string and causing this other string to initiate spacecraft safing. Each of the despun CDS POR events have been spurious transients and not a "hard" failure. The CDS POR indications are believed to be caused by momentary debris induced electrical "shorts" in the SBA interface.

The three CDS POR anomalies have occurred as follows:

- 91-085/13:31:18 SCE CDS B String POR
- 91-123/05:26:51 SCE CDS A String POR
- 91-201/02:09:00 SCE CDS A String POR

### 3.1 CDS POR Diagnosis and Recovery Planning

A recovery team comprised of representatives from the flight team was assembled. The recovery approach followed the outline given here:

- Ensure the spacecraft state is known, stable, and per predicts , including telecommunication telemetry link performance.
- Provide a preliminary assessment of the anomaly cause and autonomous actions taken.
- Collect more detailed diagnostic data and an analytical assessment of the anomaly.
- Establish project prioritized goals and guidelines for spacecraft recovery.
- Develop an integrated flight team recovery plan.
- Implement the recovery plan systematically and prudently and using standard Project procedures and reviews of each action.

The recovery process was broken into two major activities, recovery of the CDS from its POR state followed by recovery of the spacecraft from its Safing commanded state. Since the anomaly was transient and the SFP response was pre-dominantly within the CDS, the CDS analysts and FSW engineers lead the activity to diagnose the cause of the POR event and define the process for safety restoring both the CDS strings to their pre-anomaly status.

The other major activity was to identify the target date to resume normal sequence activities, identify activities lost during the recovery time frame and reschedule these as needed. Also to be planned were any required spacecraft maintenance activities and spacecraft reconfiguring events to put the spacecraft in the required state for the targeted sequence restart point.

Detailed project prioritized list of recovery goals and guidelines were established as follows:

- Maintain spacecraft health and safety throughout the recovery period and minimize risk of additional faults and operational errors during the recovery process.
- Confirm anomaly fault analysis and determine state of CDS following the anomaly.
- Restore full spacecraft capability to pre-safing state. Restoration of the CDS shall be accomplish at the earliest, practical time using all relevant and establish project procedure and guidelines.
- Establish a spacecraft state to the correct configuration for loading and executing the nominal NMSL at the targeted sequence restart point.
- Develop at the start of the recovery process an integrated recovery plan which shall obtain project approval and shall be used to direct the recovery process.
- Unique, non-standard, and first time spacecraft activities must be simulated on the test bed prior to uplinking to the spacecraft or project must specifically waive the need to do so.
- Recovery activities shall be real-time commanded using immediate executable commands or accomplished by mini-stored sequence of commands - all standard real-time commands or sequence review checks and procedure shall be used to validate all command files.
- The targeted restart sequence shall be simulated relative to the CDS and spacecraft states.

### 3.2 CDS POR Recovery Activities and Schedules

A full spacecraft recovery plan was devised for the DOY 91-085 anomaly which lasted thirty-one calendar days. The targeted restart point was selected based on the time the project felt was needed to safely implement each of the required recovery activities and to resume the next planned sequence. Stored sequence resumption is important to not burden the flight team with real-time commanding the spacecraft. The plan included the required CDS reconfiguration, spacecraft maintenance activity (normally implemented out of the stored sequence), missed activities from the aborted sequence, and reconfiguration of the spacecraft to the target restart point. The restart point reconfiguration included reconfiguring telecommunications for Engineering High Rate [EHR, 1200 Bits Per Second (BPS)], the High Gain Antenna (HGA) deploy mini-sequence, re-initializing celestial attitude reference, establishing the proper power state of the spacecraft and adjusting the spacecraft attitude for the new sequence. [Unrelated to the CDS anomaly, the HGA deploy sequence failed to deploy the HGA.]

Again, the area of the ecliptic plane in which the spacecraft had been following the sun did not yield many star sets for reacquiring celestial reference, a pre-requisite for returning to nominal spacecraft command sequencing control. This again caused many required spacecraft activities to be performed via real-time commands. Command and control with this method has been found to be taxing to the flight team as a whole.

The CDS POR recovery caused the greatest concern of the recovery process, since it was a never before executed activity on the spacecraft and required cleaning up a number of autonomous actions associated with the CDS software and hardware components. The CDS recovery was broken into four phases:

Phase 1: Error analysis and isolation which provided for detailed telemetry on the CDS state and isolated the down CDS components to allow for reconfiguration.
Phase 2: Reconfiguration and initialization of the down string CDS to establish a state compatible with the processor restart.
Phase 3: Restart the down string processor, synchronize the timing between the two CDS processors and verify proper CDS processing.
Phase 4: Restore and clean-up remaining control flags, telemetry indicators and SFP parameters.

The Project was understandably cautious in implementing each of the phases above, because of the criticality and complexity of the CDS recovery. This part of the recovery alone was spread over thirteen days to allow for complete verification of each phase before committing to the next phase.

The second CDS POR anomaly, DOY 91-123, was similar to the first except that the prime CDS string detected the CDS POR indication. Since normally the engineering telemetry is processed and telemetered through the telecommunications subsystem over the prime string, telemetry was lost as the prime CDS string shut down and the back-up CDS string ran the safing algorithms. This was a previously recognized problem with the SFP in that it does not reconfigure the CDS or the telecommunications interface to allow the back-up CDS telemetry to be downlinked. The initial reaction on the ground following the anomaly was that a ground station problem had prevented proper lock up of the telemetry signal. However, after a review of the SFP and CDS codes it was determined that the anomaly was again a CDS POR but this time on the prime string. Real-time commands were soon processed and transmitted to select the back-up CDS processor for telemetry downlink.

The second CDS POR anomaly recovery followed the same guidelines and approach as the first. The CDS recovery time for this anomaly was reduced from thirteen days to seven days. This was accomplished, because less time was included in the schedule between CDS recovery phases. This was permitted by the Project management once it was determined the anomaly was the same as previously experienced and the recovery process was analogous.

The third and, to date, final CDS POR anomaly occurred on DOY 91-201. Again it was the prime CDS string to detect the POR indication. The one unique aspect of this incident was that telecommunications performance at this phase of the mission could not support the EHR data rate which the previous recoveries were implemented at. Therefore, the recovery command files had to be generated for 40 BPS, the highest supportable telemetry rate at that time. All other events followed closely to the previous recoveries. Again with more confidence in the flight team's recovery action the recovery time was reduced to four working days. This was done by configuring and executing on the same day CDS recovery phases for reconfiguring, restarting and cleaning up of the CDS processors.

It should be noted that during the period of time that the second and third CDS POR anomalies occurred, the Galileo Project was working hard to diagnose and correct the HGA non-deployment anomaly. To maximize flexibility of the flight team and to preclude interruption of a stored sequence during this period, the spacecraft was not executing a NMSL. Therefore the spacecraft recovery following the CDS POR was to essentially reconfigure to a back-ground cruise state.

## 4. AACS Recovery Issues

To significantly reduce the impact caused by the unavailability of star sets for future celestial reference acquisitions following an anomaly, the flight team investigated the possibility of altering the SFP response to a POR. Instead of unconditionally commanding a sun-point from spacecraft safing every 12 hours and possibly losing celestial reference for some considerable time period, a check or conditional would first be performed. If celestial reference were available at the time of the anomaly and AACS indicated an "earth acquired" status, then the spacecraft attitude would remain unchanged (no unconditional sun-point). In a purely technical sense, earth acquired means that the spacecraft HGA is pointed directly towards the earth within some given error tolerance. With the wide range of commanded spacecraft attitudes planned for HGA anomaly resolution purposes (cool turns and warm turns) and the risk of future CDS Despun POR indications, the flight team's challenge was how to convince the spacecraft that is was always earth-pointed, regardless of the actual spacecraft attitude. AACS analysts determined that all that was required for the "earth acquired" status to be set was to have celestial reference available and to have the AACS FSW track an earth vector. Data contained in the earth vector slot did not have to be related to spacecraft-relative earth motion (i.e. could represent the motion of the sun). All that the AACS FSW was concerned about

was that it was directed to follow motion parameters with the label "earth vector". This change in operating strategy has since been implemented.

## 5. CRITICAL ACTIVITY PROTECTION

The previous S/C safing events taught us that a quick recovery can be realized if three things are known or planned before the anomaly occurs:

1. The probable cause and autonomous response of the spacecraft are known.
2. The recovery actions correcting the cause and establishing a normal spacecraft state are known beforehand and command files are pre-generated.
3. A specific planned sequence restart point is targeted and the state of the spacecraft at this point is established beforehand

## 6. GASPRA ENCOUNTER CONTINGENCY

Following the three CDS POR events the Galileo Project had an opportunity to take the events and plan a contingency recovery plan to protect the mission unique Gaspra Encounter. Given the SBA debris theory causing the CDS POR it was considered a real threat to spuriously re-occur prior to the Gaspra encounter scheduled for DOY 91-301. Since the SFP autonomous response had been well characterized it was possible to pre-generate the required command files to correct and restart the CDS state. Looking ahead at the Gaspra sequence designated EE-3', it was possible to determine the exact state the spacecraft had to be in at the start of EE-3'. Thus, a detailed contingency recovery plan could be made such that the duration of the recovery could be minimized. Figure 2 shows a recovery timeline based on the time relative to the occurrence of the POR. Including pad this timeline could be accomplished in as quickly as forty hours for full CDS and S/C recovery, quite a reduction from the twenty-three and thirty-one day recoveries of the first two anomalies. It must be noted without question that the forty hour implementation time was considered only a desired goal (best case). The Galileo project office reserved the right to dictate how fast the flight team should actually implement the spacecraft recovery task. The recovery timeline was to be implemented in the following fashion:

- Identification and confirmation of the anomaly.
- Perform CDS POR recovery and restart.
- Regeneration, if required, of the spacecraft reconfiguration com-mand files based on the actual state of the spacecraft at the time the anomaly occurred.
- Reconfigure the engineering subsystems to the Gaspra sequence initial states.
- Turn on and configure the instruments for the Gaspra science activities.

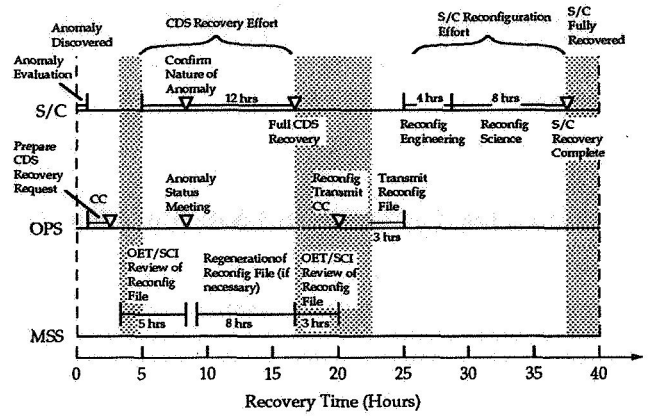


*Figure 2 Gaspra Recovery Timeline*

## 7. LESSONS LEARNED

Obviously recovery time from any anomaly is dependent on the cause of the anomaly and any degradation of the spacecraft capabilities following resolution of the anomaly. From the four cases of safing the Galileo spacecraft has experienced, the duration of fault identification to recovery of the fault was reduced from greater than four weeks to inside a week. Experience has shown that familiarity with the cause of the anomaly and its required recovery plan can significantly reduce recovery time. In addition, establishing a recovery approach following prioritized goals and guidelines lead to expedient, yet safe recovery.

## 8. ACKNOWLEDGMENTS


We would like to thank our colleagues who were previously and are currently involved with Galileo in-flight operations. Also, we would like to acknowledge the encouragement and direction the recovery planning team received from the Galileo Project Office which made it possible to develop and commit to an aggressive and rapid recovery plan to have in place for the Gaspra encounter.

This work was performed at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration.